ششمین همایش بین‌المللی افق های نویـن در
مهندسی برق، کامپیوتـر و مکانیک
6th International Conference on the New Horizons in
Electrical Engineering, Computer and Mechanical
www.mhconf.ir

A Survey on IoT Security and Attack

مرجان محمودی*[۱]، هلدا شاکری[۲] ، بهرنگ برکتین [۳]

[۱] دانشکده مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران. Marjan.Mahmoudi208@sco.iaun.ac.ir

[۲] گروه مدیریت، دانشگاه آزاد اسلامی واحد علوم تحقیقات، تهران، ایران. Heldashakeri@gmail.com

[۳] دانشکده مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران Behrang_Barekatain@iaun.ac.ir

چکیده

امنیت و پشتیبانی از آن در اینترنت اشیاء (IoT)، با توجه به ماهیت توزیع‌شدگی، خصوصیات منحصر به فرد و محدودیت‌های فراوان این شبکه‌ها، از مباحث چالش‌برانگیز و مهمی محسوب شده که در صحت عملکرد و بهبود کارایی شبکه نقش حیاتی ایفا می‌نماید. این در حالی است که به دلیل وجود ویژگی‌هایی اعم از همبندی پویا، معماری توزیع‌شدگی، مقیاس‌پذیری شبکه و تبادلات چندگامی، پشتیبانی از امنیت در IoT متفاوت از سایر شبکه‌های موجود می‌باشد. وجود این شرایط در کنار سایر مسائل حاکم بر اینترنت اشیا، بحث امنیت را به یکی از مهم‌ترین چالش‌های IoT مبدل نموده است. این اهمیت بالا باعث شده تا پژوهش‌های گسترده‌ای در راستای بهبود این حوزه حیاتی معرفی گردند. اما همچنان برخی چالش‌های مهم نیز به قوت خود باقی بوده که بر ضرورت انجام تحقیقات بیشتر و مؤثرتر در این حوزه دلالت دارد. در این مقاله یک بررسی جامعی از حوزه امنیت IoT، انواع حملات و تکنیک‌های مقابله گردآوری و بررسی شده است. بدین منظور در ابتدا مفهوم امنیت و اعتماد در IoT و به ویژه در ارتباط با بحث مسیریابی و تبادلات داده‌ها بررسی گردیده است. در ادامه انواع حملات و روش‌های مقابله تحلیل و تشریح شده است. سپس یک دسته‌بندی جدید از مدل‌های امنیتی معرفی شده و این مدل‌ها از نظر اهداف، محدودیت‌ها و قابلیت‌ها بحث و بررسی گردیده‌اند. در پایان مقاله نتیجه‌گیری شده و در ارتباط با اساسی‌ترین چالش‌های طراحی مدل‌های امنیت و بهینه‌سازی این مدل‌ها به منظور کاربرد در IoT جزئیات ارائه گردیده است.

واژه‌های کلیدی

اینترنت اشیاء، حملات، امنیت، اعتماد.

۱. مقدمه

شبکه‌های اینترنت اشیاء (IoT)[1] از تعداد زیادی گره و یک یا چند گره ریشه[2] تشکیل شده‌اند. اعضای شبکه می‌توانند هر عامل شامل انسان، حیوانات، اشیاء و حتی پدیده‌های مختلف باشند. این اعضا وابسته به اهداف شبکه، اطلاعات مورد نیاز را حس و گردآوری نموده و به واسطه ارتباطی که یا یکدیگر دارند، اطلاعات گردآوری شده را برای گره‌های ریشه ارسال می‌کنند [۱]. گره‌های ریشه دروازه‌های شبکه با محیط بیرون بوده که تمامی اطلاعات گردآوری شده شبکه برای آن‌ها ارسال می‌شود [۲]. پس از گردآوری داده‌ها توسط گره‌های ریشه، این اطلاعات یا توسط خود گره‌های ریشه پردازش شده و پس از آن فرامینی صادر می‌شود. یا آن‌ها برای کاربران، جایگاه مرکزی[3] یا سایر سازمان‌های مربوطه ارسال می‌شوند. به منظور حفظ همپوشانی و تضمین پایداری این شبکه خاص و پیچیده، از ارتباطات گره‌ها با یکدیگر استفاده می‌شود. گره‌ها از طریق ارتباطات بی‌سیمی که با یکدیگر دارند، ارتباطات اعضا با ریشه را تضمین نموده، و به واسطه این ارتباطات اطلاعات گردآوری شده خود (اعم از حرارات، ویدئو، صوت، تصویر، رطوبت و غیره) را برای گره‌های ریشه ارسال می‌نمایند [۳]. اطلاعات دریافت شده توسط گره‌های ریشه برای اهداف متعددی اعم از کنترل، نظارت و پایش، ارزیابی سلامت، پیش‌بینی، کنترل تغییرات، مدیریت حمل و نقل و غیره، استفاده می‌شوند [۳و۴].

IoT در ازاء ویژگی‌های منحصر به‌فرد خود و مزایای بی‌نظیری که فراهم می‌سازد، امروزه در زمینه‌های گسترده‌ای از قبیل حمل و نقل هوشند، عرصه‌های نظامی، کاربردهای پزشکی، شهر هوشمند و غیره، مورد استفاده قرار گرفته و روزبه‌روز به کاربردها و اهمیت این فناوری ارتباطی افزوده می‌شود [۳-۵]. از بارزترین خصوصیات این شبکه‌های توزیع شده می‌توان به عدم نبود زیرساخت ثابت و کنترل-کننده مرکزی، ماهیت توزیع شده، همبندی پویا، محدودیت‌های شدید مرتبط با گره‌ها و ارتباطات آن‌ها، خودسازماندهی اعضای شبکه و مبادله چندپرشی داده‌ها را اشاره کرد [۶و۷]. این ویژگی‌های خاص و منحصر به‌فرد باعث شده تا مسائل مختلف مطرح در سایر شبکه‌ها، به خصوص بحث امنیت و پشتیبانی از آن در این شبکه‌ها متفاوت از سایر شبکه‌های سیمی و بی‌سیم مطرح باشد. این تفاوت در کنار سایر خصوصیات و چالش‌های درگیر با IoT منجر به آن شده تا این شبکه‌ها در مقابله با حملات عوامل مخرب آسیب‌پذیرتر از هر شبکه‌ای باشند [۸]. این در حالی است که اغلب کاربردهای IoT (مانند کاربردهای نظامی، پزشکی، صنعتی و غیره) کاربردهایی حساس و مهم هستند. اهمیت بالای این کاربردها باعث شده تا شبکه‌های IoT به شدت در معرض اعمال حملات مختلف قرار داشته باشند. بنابراین از یک سو شبکه به دلیل محدودیت‌ها و خصوصیات خاص به شدت در مقابله با حملات آسیب‌پذیر بوده و از سوی دیگر به علت کاربردهای مهم در معرض اعمال انواع حملات مختلف قرار دارد [۹]. این مباحث بر ضرورت وجود تدابیری برای تأمین و تضمین امنیت IoT دلالت داشته تا در قبال آن شبکه به عملکرد صحیح و پایدار خود به صورت پیوسته ادامه دهد. حال آن‌که این تدابیر باید به نحوی اتخاذ و منظور شوند که علاوه بر پشتیبانی مؤثر از امنیت، سازگار و متناسب با خصوصیات IoT و ماهیت خاص این شبکه‌ها باشند [۹].

وجود این مباحث در کنار اهمیت انکارناپذیر مفهوم امنیت برای IoT، باعث شده تا تکنیک‌ها و روش‌های متعددی در ارتباط با این حوزه و به منظور بهبود جوانب حائز اهمیت آن معرفی شوند. در این مقاله مروری جامع بر بحث امنیت، حملات وارده بر IoT و انواع روش‌های مقابله، به ویژه در حوزه مسیریابی و تبادلات گردآوری و ارائه خواهد شد. در پایان نیز با استناد به مطالعات انجام شده مهم‌ترین چالش‌های پیش‌روی این حوزه را معرفی و تشریح خواهند شد.

ادامه ساختار مقاله بدین شرح خواهد بود. در بخش دوم به بررسی حوزه امنیت و اعتماد IoT پرداخته شده و مباحث مورد نیاز در این باره ارائه و تشریح خواهند گردید. در ادامه مهم‌ترین حملات وارده بر IoT معرفی خواهند شد و در ارتباط با هر حمله و چگونگی آن‌ها جزئیاتی ارائه خواهد شد. سپس انواع تکنیک‌های مقابله با این حملات معرفی شده و در ارتباط با هر تکنیک و مزایای و معایب آن مفاهیم

---

[1] Internet of things
[2] Root
[3] Base Station

ارائه و تشریح خواهد شد. در بخش پنجم یک دسته‌بندی جدیدی از مدل‌های امنیت پیشنهادی برای IoT ارائه شده و مباحث مربوط به این دسته نقد و بررسی خواهد گردید. در ادامه برخی پیشنهادات به منظور بهبود عملکرد و کارایی تکنیک‌های امنیتی معرفی و تشریح شده و سرانجام در بخش پایانی مقاله نتیجه‌گیری خواهد شد.

۲. امنیت و اعتماد در IoT

امنیت و اعتماد در IoT، مفهومی شبیه به اعتماد در شبکه‌های اجتماعی دارد. بر همین اساس دیدگاه‌ها متفاوتی برای این حوزه مطرح است. بعضی اعتماد را یک باور ذهنی از یک امانت‌دار در ارتباط با رفتار و صداقت او در یک زمینه خاص معرفی می‌کنند [۱۰]. در [۱۱] پیشنهاد شده که برای پشتیبانی از اعتماد IoT، بهترین ایده بهره‌وری از مفاهیم مرتبط با مدل‌های اعتماد مرتبط با نظام اجتماعی است. در این پژوهش محققین اعتماد را به‌عنوان یک کمیت ذهنی در ارتباط با انجام یک رفتار مشخص تعریف کرده‌اند. در [۱۲] اعتماد، انجام یک رفتار توسط یک عامل با درجه اطمینان بالا بوده و بر این اساس تعریف می‌شود. در [۱۳] اعتماد مجموعه‌ای است از روابط میان عواملی که در یک فرایند شرکت می‌کنند. این روابط بر مبنای شواهد ایجاد و به‌روزرسانی می‌شوند. در مجموع اعتماد در شبکه‌های اجتماعی همچون پل ارتباطی بوده که برای ایجاد رابطه‌های معتمد میان افراد مختلف تعریف می‌شود. در مجموع می‌توان این‌گونه استدلال نمود که بحث اعتماد از نقطه نظر جامعه شناسی به علم IoT مشتق شده است.

با توجه به آن‌چه پیش‌تر در ارتباط با ویژگی‌ها و خصوصیات IoT ارائه و تشریح شد؛ بحث امنیت و پشتیبانی از آن بنا بر ماهیت کاملاً توزیع شده و همچنین سایر ویژگی‌های مرتبط با این فناوری ارتباطی، متفاوت از سایر شبکه‌ها بوده و بسیار پر مخاطره‌تر است. بیشترین تمایز مرتبط با بحث ارتباطات و مبادلات داده‌ها بوده که به عنوان مهم‌ترین بحث IoT محسوب می‌شود [۱۳]. با توجه به اهمیت بالای بحث مسیریابی و تعاملات داده‌ها، اغلب حملات وارده بر اینترنت اشیاء نیز به این حوزه اعمال شده و در سوی مقابل سازوکارهای امنیتی و روش‌های مقابله نیز به همین حوزه (با هدف پیش‌گیری از حملات و برقراری اعتماد) متمرکز هستند. در ادامه به طور دقیق‌تر به بحث در ارتباط با امنیت و اعتماد حوزه مسیریابی و مبادلات پرداخته شده است.

- امنیت و اعتماد در حوزه مسیریابی و تعاملات

در IoT هر گره عضو شبکه دارای یک شناسه دیجیتالی یکتا و منحصر به فرد بوده که از طریق آن قابل شناسایی، کنترل و مدیریت است. گره‌ها به واسطه همین شناسه با یکدیگر ارتباط برقرار نموده و اقدام به مبادلات داده‌ها می‌نمایند. این امر در کنار سایر خصوصیات و مسائل مرتبط با IoT، باعث شده تا تمامی مفاهیم رایج در سایر شبکه‌های موجود برای این شبکه‌ها از جوانب و زوایای دیگر مطرح باشند [۱۶]. یکی از اساسی‌ترین این مسائل، در ارتباط با بحث امنیت و اعتماد به ویژه در ارتباط با حوزه مسیریابی و مبادلات داده‌ها مطرح بوده که در ادامه جزئیات حائز اهمیت در این باره ارائه شده است [۱۷].

همان‌گونه که پیش‌تر نیز اشاره شد، IoT عملاً شبکه‌ای بدون زیرساخت[1] بوده که از تعداد زیادی گره خودسازمان‌ده، مجهز به فرستنده-گیرنده‌های رادیویی تشکیل شده‌اند. این گره‌ها هر عاملی شامل اشیاء فیزیکی و غیرفیزیکی بوده که وابسته به اهداف شبکه اقدام به بررسی، جمع‌آوری و مخابره داده‌ها نموده تا در ازاء این گزارشات، اهداف متصور از شبکه محقق گردد. قابل توجه است که در IoT مبادلات داده‌ها از طریق مسیریابی و به واسطه خود اعضای شبکه انجام می‌شود [۱۸]. در این شبکه‌ها در غیاب کنترل‌کننده مرکزی، گره‌ها می‌توانند نه فقط به عنوان یک میزبان (مولد داده)، بلکه به عنوان یک مسیریاب نیز ایفای نقش نمایند. ازاین‌رو هر گره علاوه بر مبادلات داده‌ها به عنوان مبدأ یا مقصد تعاملات، قادر بوده تا به عنوان یک گره میانی در نقش مسیریاب عمل نماید. ازاین‌رو به

[1] Non-Inferstructrual Networks

شبکه‌های IoT، شبکه‌ای خود سازمان‌ده نیز گفته می‌شود. در مجموع با توجه به ویژگی‌های ذاتی IoT و نبود زیرساخت ثابت فعالیت این فناوری ارتباطی به شدت وابسته به همکاری و مشارکت گره‌ها با یکدیگر است [۱و۱۹].

بنابر آن‌چه در رابطه با IoT ارائه شد به وضوح مشاهده می‌شود که مبحث مسیریابی و ارتباطات کلیدی‌ترین بحث این شبکه‌ها محسوب شده و جایگاه بسیار ارزشمندی در این شبکه‌ها دارد. ازاین‌رو اغلب حملات (به جهت اختلال در روند فعالیت شبکه) و در سوی مقابل راه‌کارهای مقابله به این حوزه متمرکز شده و سعی بر پیش‌گیری از حملات را دارند. در واقع بخش عمده‌ای از اعتماد و امنیت در IoT متوجه بحث مسیریابی و مبادلات داده‌ها است..

۳. انواع گره‌های مخرب و حملات وارده بر حوزه مسیریابی IoT

همان‌گونه که پیش‌تر نیز اشاره شد، حملات مختلفی بر حوزه مسیریابی و مبادلات IoT اعمال می‌شود. گره‌های مخرب که عامل این حملات هستند را در یک بخش‌بندی کلی می‌توان به دو دسته گره‌های خودخواه[۱] و بدخواه[۲] بخش‌بندی نمود [۱۳و۲۰]. گره‌های خودخواه گره‌هایی هستند که عملاً قصد تخریب و آسیب به فعالیت شبکه را ندارند. این گره‌ها با هدف صرفه‌جویی و حفظ منابع خود از همکاری و مشارکت در فعالیت شبکه خودداری نموده و بر این اساس سعی دارند تا انرژی و منابع خود را ذخیره نمایند. از آن‌جایی که این عمل به صورت معتمدانه رخ داده و باعث آسیب به فعالیت شبکه می‌شود، در زمینه رفتارهای مخرب قرار می‌گیرد. دسته دوم گره‌های بدخواه هستند. هدف این گره‌ها تخرب عملکرد شبکه است. برای این منظور گره‌ها بدخواه با اهداف از پیش تعریف شده و مشخصی قصد به انجام حمله زده که نتیجه آن اختلال در مسیریابی و سرویس‌دهی بوده که باعث افت شدید کارایی شبکه خواهد شد.

در مجموع تنوع حملات وارده بر IoT از سوی گره‌های خودخواه و بدوخواه را از منظر شبکه می‌توان به دو دسته داخلی[۳] و خارجی[۴] بخش‌بندی نمود [۲۱]. حملات داخلی، حملاتی بوده که گره‌های داخلی شبکه انجام داده و رفتارهای مخربی بوده که توسط یکی از اعضای شبکه رخ می‌دهند. در سوی مقابل حملات خارجی توسط گره‌هایی خارجی شبکه (گره‌هایی که عضوی از شبکه نیستند) انجام می‌شوند. اغلب حملات وارده بر حوزه مسیریابی و مبادلات، شامل حملات داخلی بوده که توسط اعضای شبکه انجام می‌شوند. از دیدگاه دیگر و از لحاظ نوع عملکرد حملات به دو نوع فعال[۵] و غیرفعال[۶] تقسیم می‌شوند [۲۱و۲۲]. حملات فعال، حملاتی بوده که به صورت فعالانه توسط گره‌های مخرب انجام شده و اغلب با نشانه‌ای از آثار حمله همراه هستند. از جمله رایج‌ترین این حملات می‌توان به حمله سیاه‌چاله[۷]، حمله حفره خاکستری[۸]، حملات تغییر بسته[۹]، حملات رتبه[۱۰] و حمله‌ی شماره ورژن[۱۱] را اشاره نمود. این حملات از آن‌جایی که با نشانه همراه بوده، تشخیص ساده‌تری داشته ولی اغلب تأثیرات مخرب شدیدتری بر شبکه دارند. در سوی مقابل حملات غیرفعال، بدون هیچ‌گونه نشانه‌ای بوده و به صورت غیرفعالانه اعمال می‌شوند. در این نوع حملات گره قصد تخریب فعال شبکه را نداشته و تنها هدف آن شنود و دسترسی غیرمجاز به اطلاعات ارسالی در شبکه است. در واقع در این نوع حمله گره با شنود و بررسی ارتباطات، سعی بر دسترسی به اطلاعات ارسالی در شبکه را دارد. بیشتر برای مقابله با حملات فعال، روش‌هایی همچون مدل‌های اعتماد، سیستم تشخیص

---

[1] Selfish
[2] Malicious
[3] Internal Attacks
[4] External Attacks
[5] Active Attacks
[6] Passive Attacks
[7] Black Hole Attack
[8] Grey Hole Attack
[9] Packet modification
[10] Rank attack
[11] Version Number

نفوذ و روش‌های کنترل مسیریابی مطرح هستند. در سوی دیگر برای مقابله با حملات غیرفعال اغلب روش‌هایی رمزنگاری، حفظ محرمانگی و احراز هویت مطرح و مورد استفاده هستند.

حملات را از نظر لایه‌بندی TCP-IP و لایه‌ای که حمله در آن رخ می‌دهد را نیز می‌توان به پنج دسته حملات مرتبط با لایه فیزیکی[1]، حملات مرتبط با لایه پیوند داده[2]، حملات مرتبط با لایه شبکه[3]، حملات مرتبط با لایه انتقال[4] و حملات مرتبط با لایه کاربرد[5] بخش‌بندی نمود [۲۳و۲۴]. در میان انواع حملات مرتبط با لایه‌بندی TCP-IP، حملات مرتبط با لایه شبکه، رایج‌ترین و مهم‌ترین حملات وارده بر شبکه‌های IoT می‌باشند. این حملات علاوه بر تنوع و اهمیت بالا، تأثیرات مخرب به نسبت شدیدتری در مقایسه با حملات مرتبط با سایر لایه‌ها دارند [۲۵]. در ادامه به طور تخصصی‌تر به این حملات و جزئیات مربوط به آن‌ها پرداخته‌ایم.

- حملات لایه شبکه

بنابر آن‌چه ارائه شد، اغلب حملات مهم مرتبط با IoT حملات لایه شبکه هستند. تقریباً تمامی این حملات در ارتباط با حوزه مسیریابی و مبادلات داده‌ها مطرح بوده و سعی بر تخریب و اختلال در این فرایند حیاتی شبکه را دارند. در ادامه تعدادی از مهم‌ترین این حملات معرفی شده و مباحثی در ارتباط با چگونگی عملکرد و تأثیرات آن‌ها بر شبکه ارائه گردیده است.

حمله سیاه‌چاله: در این نوع حمله گره سیاه چاله در ابتدا با فریب فرایند مسیریابی را به سمت خود جلب نموده و در ادامه در طی ارسال داده‌ها به جای ارسال صحیح داده‌ها، اقدام به حذف داده‌های ارسالی می‌نماید. این حمله به سه صورت تکی، همکارانه و انتخابی انجام می‌شود. در حمله تکی گره سیاه‌چاله به صورت مستقل عمل نموده که پس از جذب مسیریابی اقدام به حذف داده‌ها می‌نماید. در حملات همکارانه دو یا چند گره مخرب به جهت انجام حمله با یکدیگر مشارکت می‌نمایند. در حمله انتخابی گره سیاه‌چاله پس از جذب فرایند مسیریابی اقدام به حذف همه‌ی بسته‌های داده ننموده و تنها به صورت انتخابی بخشی از داده‌ها را حرف می‌نماید. دو نوع حمله همکارانه و انتخابی به نسبت حمله سیاه‌چاله معمول شناسایی به نسبت مشکل‌تری دارند [۲۶و۲۷].

حمله حفره خاکستری[6]: در این نوع حمله گره مخرب به طور نرمال در مسیر مبادلات قرار گرفته و در طی مبادله و ارسال داده‌ها، اقدام به حذف بخشی از بسته‌ها به صورت هوشمندانه می‌نماید. در واقع در این گره مخرب برخی از داده‌ها را حذف و در قبال سایر داده‌ها رفتار صحیحی دارد. این عملکرد هوشمندانه تشخیص این نوع حمله را به نسبت سیاه چاله دشوارتر می‌نماید [۲۸].

حمله سوراخ کرم[7]: در این حمله دو گره مخرب به واسطه یک اتصال فیزیکی به یکدیگر متصل هستند. این اتصال باعث شده تا مسیر عبوری از طریق این دو گره، در اکثر مواقع به عنوان مسیر بهینه باشد. در ادامه گره‌های مخرب به واسطه مسیر ایجاد شده، اقدام به تخریب یا حذف داده‌های ارسالی می‌نمایند [۲۹].

حملات تغییر بسته[8]: در این حمله عامل مخرب به جاری ارسال صحیح داده، با اهداف از پیش تعیین شده بخشی یا تمام داده را تغییر می‌دهد [۳۰].

---

[1] Physical layer Attacks
[2] Data link layer Attacks
[3] Network layer Attacks
[4] Transport layer Attacks
[5] Apllication layer Attacks
[6] Grey Hole Attack
[7] Worm Hole Attack
[8] Packet modification

حملات رتبه: این حمله در ارتباط با پروتکل RPL (به عنوان استاندارد مسیریابی اینترنت اشیا) مطرح می‌باشد. در این حمله عامل مخرب با تغییر در رتبه خود سعی نموده تا خود را به عنوان گره با مسیر بهینه جلوه داده و فرایند مسیریابی را به سمت خود جلب نماید. در ادامه‌ی جذب فرایند مسیریابی، در طی مخابره داده‌ها اقدام به انجام رفتارهای نادرست به جای ارسال صحیح داده‌ها می‌نماید [۳۱].

حمله روشن و خاموش[1]: در این حمله عامل مخرب در یک پریود زمانی رفتارهای خود و در یک بازه زمانی، رفتار نادرست دارد. ازاین-رو این حمله در مجموعه حملات فریبنده‌ای دسته‌بندی می‌شود. هدف از این عملکرد دشوار نمودن تشخیص است [۳۲].

حمله جعل[2]: در این حمله عامل مخرب با تغییر در بخش سرآیند[3] بسته‌های داده یا پیام‌های مسیریابی (مانند تغییر در آدرس گره فرستنده، مقصد و غیره)، تلاش بر اختلال در پروسه مسیریابی و تبادلات را دارد [۲۳].

حمله‌ی شماره ورژن[4]: این حمله نیز در ارتباط با پروتکل RPL ممطرحح بوده که در آن گره مهاجم با تغییر ورژن گراف DODAG قصد بر تخریب و فریب پروسه مسیریابی را دارد [۳۳].

حمله ارسال انتخابی[5]: در این حمله، عامل مخرب بخشی از بسته‌های داده را به صورت انتخابی حذف و در قبال سایر بسته‌ها رفتار صحیحی دارد. این عمل با هدف جولگیری از شناسایی به عنوان مخرب انجام شده و از این نظر در قیاس با سایر حملات خطرناک‌تر بوده و تشخیص مشکل‌تری دارد [۳۴].

حمله همسایگی[6]: در این حمله عامل مخرب قصدش فریب فرایند مسیریابی است. توجه شود که طی پروسههای مسیریابی گره‌های میانی پس از دریافت پیام‌های کنترلی، مشخصات خود را در پیام درج نموده و سپس آن را به سایر گره‌ها ارسال می‌کنند. در حمله همسایگی، عامل مخرب بدون آن‌که مشخصات خود را به پیام اضافه نموده یا اطلاعات غلطی را به جای مشخات خود به پیام افزوده، و آن را برای سایر گره‌ها ارسال می‌نماید. این امر باعث فریب مسیریابی می‌شود [۳۵].

حمله حذف بسته: در این نوع حمله عامل مخرب، با حذف داده‌های ارسالی تلاش بر اختلال در روند فعالیت شبکه را دارد [۳۶].

حمله محرومیت از خدمات (DoS)[7]: در این حمله سعی بر آن بوده تا با انجام رفتارهای مخرب روند سرویس‌دهی شبکه را مختل نمود [۳۷].

حمله سایبل[8]: احمله سایبل یکی از حملات هوشمندانه بوه که گره در قالب حذف بسته انجام می‌دهد، اما به نحوی در قبال تغییرات رفتار بین رفتارهای منفی و مثبت، حمله انجام شده که قابلیت شناسایی دشواری دارد [۳۸].

آن‌چه در این زیر بخش ارائه شد، بررسی انواع حملات وارده بر IoT به ویزه حملات متمرکز بر حوزه مسیریابی و مبادلات داده‌ها را شامل می‌شود. در بخش بعدی به نقد و بررسی انواع تکنیک‌ها و روش‌های مقابله با این حملات خواهیم پرداخت.

۴. روش‌های مقابله با حملات وارده بر حوزه مسیریابی و تبادلات IoT

---

[1] On-off Attack
[2] Fabrication
[3] Header
[4] Version Number
[5] Selective-Forwarding
[6] Neighbour Attack
[7] Denial of Service
[8] Sibyl Attack

همان‌گونه که مشاهده شد، حملات متنوعی برای اختلال در عملکرد شبکه‌های IoT مطرح بوده که بخش عمده‌ای از این حملات مرتبط با لایه شبکه و به طور خاص متمرکز بر بحث مسیریابی و تبادلات داده‌ها هستند. در سوی مقابل مکانیزم‌ها و روش‌های مختلفی نیز به منظور شناسایی و مقابله با این حملات ارائه شده‌اند. در یک بررسی سطح بالا، انواع حملات وارده بر حوزه مسیریابی و تبادلات IoT به دو دسته حملات فعال و غیرفعال تقسیم می‌شوند. تکنیک‌های مقابله با این حملات را به طور کلی به دو دسته تکنیک‌های حفظ محرمانگی و تکنیک‌های نظارتی به شرح زیر بخش‌بندی نمود.

- تکنیک‌های حفظ محرمانگی

هدف این تکنیک‌ها فراهم‌سازی قابلیتی به منظور حفظ محرمانگی داده‌های ارسالی به جهت پیش‌گیری از دسترسی‌های غیرمجاز است. در این تکنیک‌ها با استفاده از روش‌های مختلفی اعم از رمزنگاری، درهم‌سازی، توزیع چندپخشی و غیره، به گونه‌ای داده‌ها از مبدأ برای مقصد ارسال شده که حتی در صورت دسترسی گره‌های مخرب، محرمانگی اطلاعات تضمین می‌شود. در واقع این تکنیک‌ها با استفاده از تدابیری که برای رمزنگاری و درهم‌سازی اطلاعات فراهم می‌سازند، در صورت دسترسی عامل‌های مخرب اطلاعات ارسالی بر آن‌ها قابل فهم و بازیابی نمی‌باشد. مهم‌ترین هدف این تکنیک‌ها مقابله با حملات غیرفعال است [۳۹و۴۰]. روش‌های مختلفی به منظور پشتیبانی از این حوزه معرفی شده که آن‌ها را وابسته به عملکردشان می‌توان به دو دسته کلی به قرار زیر بخش‌بندی نمود.

حفظ محرمانگی مبتنی بر رمزنگاری (محرمانگی مبتنی بر کلید): روش‌های رمزنگاری از مزایا و کاربردهای الگوریتم‌های رمزنگاری برای حفظ محرمانگی اطلاعات، جلوگیری از دسترسی غیرمجاز به اطلاعات شبکه و در مجموع ایجاد خصوصیت گمنامی اطلاعات پشتیبانی می‌کنند. عملکرد تمامی الگوریتم‌های رمزنگاری بر پایه کلید رمزنگاری است. در این روش‌ها داده‌های ارسالی به واسطه کلید، رمزنگاری شده و پس از رمزنگاری برای مقصد مورد نظر ارسال می‌شوند. مقصد در با دریافت اطلاعات عملیات رمزگشائی را انجام داده و اطلاعات را دریافت می‌کند. بزرگ‌ترین محدودیت‌های روش‌های رمزنگاری نبود تدابیر امنیتی در برابر حملات فعال می‌باشد. در واقع روش‌های رمزنگاری تنها بر پیش‌گیری از دسترسی به اطلاعات غیرمجاز شبکه یا حملات نفوذی‌ها متمرکز شده و در برابر حملات فعالت هیچ‌گونه مکانیزم امنیتی ندارند. همچنین از دیگر محدودیت‌های این سیستم در برقراری امنیت، مسئله تبادل امن کلید است که عدم توانایی در تبادل امن کلید برابر با از بین رفتن امنیت خواهد بود [۴۱].

حفظ محرمانگی مبتنی بر درهم‌سازی (محرمانگی بدون داده کلید): این روش‌ها نیز همچون روش‌های رمزنگاری هدف‌شان حفظ محرمانگی بوده با این تفاوت که چنین قابلیتی را بدون نیاز به کلید فراهم می‌سازند. این روش‌ها مبتنی بر تکنیک‌های همچون درهم-سازی و توریع چندپخشی، به گونه‌ای در قبال مبادلات داده‌ها عمل نموده که بدون نیاز به کلید محرمانگی داده‌ها پشتیبانی خواهد شد. بارزترین مزیت این روش را می‌توان پشتیبانی از محرمانگی بدون کلید عنوان کرد. اما این روش‌ها در پاره‌ای از شرایط مانند حضور گره-های کلیدی (گره‌ای که دو بخش شبکه را به یکدیگر متصل می‌نماید) ناکارآمد بوده و محرمانگی آن‌ها خدشه‌دار می‌شود [۴۲].

مکانیزم‌های اعتماد: هدف این مکانیزم‌ها فراهم‌سازی تدابیری به جهت نظارت بر عملکرد و رفتار گره‌ها و پس از آن تشخیص و شناسایی گره‌های مخرب است. در این روش‌ها به گره‌های شبکه بر حسب عملکردشان یک مقدار اعتماد اختصاص داده شده که این معیار شاخص تشخیص عوامل مخرب است. این اعتماد در قبال رفتارهای مثبت و منفی گره‌ها افزایش و کاهش یافته که در صورت کاهش اعتماد به زیر مقدار آستانه تشخیص، گره مورد نظر به عنوان عامل مخرب در نظر گرفته خواهد شد. این روش‌ها علاوه بر تشخیص مؤثر عوامل مخرب، در ازاء فراهم‌سازی مسیریابی و مبادلات معتمد داده‌ها نیز بسیار مؤثر می‌باشند. ازاین‌رو بخش عمده‌ای از تحقیقات گذشته بر اساس این مکانیزم و مزایای آن طراحی و توسعه یافته‌اند [۱۱و۱۲].

مکانیزم‌های تشخیص نفوذ: هدف و تمرکز این مکانیزم‌ها بر تشخیص و شناسایی عوامل مخرب است. این مکانیزم‌ها بر پایه ارزیابی ناهنجاری‌ها عمل نموده و بر اساس نتیجه این ارزیابی‌ها تلاش بر تشخیص نفوذ را دارند که از آن‌ها با عنوان سیستم‌های تشخیص نفوذ (IDS) یاد می‌شود [۴۳]. منظور از ناهنجاری‌ها تفکیک رفتارهای غیرنرمال از رفتارهای نرمال است. این مکانیزم‌ها اغلب بر مبنای تحلیل فرایندهای مسیریابی، نحوه عملکرد گره‌ها و ارزیابی تاریخچه رفتاری آن‌ها عمل نموده و بر این اساس تلاش بر تشخیص مخرب‌ها را دارند. الگوریتم‌های یادگیری از جمله روش‌هایی بوده که به افزایش دقت و کارایی این مکانیزم‌ها کمک شایان توجهی می‌نماید [۴۴]. زیرا این الگوریتم‌ها بر مبنای قابلیت‌هایی که بر اساس یادگیری فراهم می‌سازند، دقت تحلیل و ارزیابی‌ها را به‌طور قابل توجهی افزایش می‌دهند. اما در سوی دیگر تنها هدف این روش‌ها تشخیص نفوذ و شناسایی مخرب‌ها بوده و اگرچه در این حوزه موفق می‌باشند، ولی تدابیری را برای پشتیبانی از اعتماد مسیریابی و مبادلات فراهم نمی‌سازند.

مکانیزم‌های ترکیبی: روش‌های ترکیبی، تکنیک‌هایی بوده که بر اساس تلفیقی از مزایای مکانیزم‌های اعتماد و تشخیص نفوذ طراحی و توسعه یافته‌اند. از آن‌جایی که این روش‌ها از مزایای هر دوی بحث مکانیزم‌های اعتماد و تشخیص نفوذ بهره می‌برند، روش‌های مؤثرتری به لحاظ شناسایی مخرب‌ها و پوشش سایر جوانب حائز اهمیت اعتماد هستند. اما در سوی مقابل پیچیدگی و هزینه‌های جانبی بسیار بیشتری را نیز در پی داشته که ممکن است منجر به ناکارآمدی روش شود [۴۵و۵۰].

همان‌گونه که پیش‌تر نیز اشاره شد، بخش عمده‌ای از حملات وارده بر IoT حملات فعال بوده که اهمیت و تأثیرات مخرب بسیار بیشتری بر شبکه دارند. این حملات بنابر آن‌چه بحث شد، به حوزه مسیریابی و تبادلات داده‌ها اعمال شده و هدف‌شان تخریب این فرایند حیاتی شبکه است. برای مقابله با این حملات سه روش کلی معرفی شده که در این میان مکانیزم‌های اعتماد به نسبت سایر روش‌ها قابلیت‌ها و مزایای بیشتر و محدودیت‌های کمتری دارند. بر همین اساس اغلب روش‌ها بر مبنای این مکانیزم طراحی و توسعه یافته‌اند. در بخش بعد به طور تخصصی‌تر مکانیزم‌های اعتماد و جزئیات عملکرد آن‌ها نقد و بررسی شده است.

۵. مکانیزم‌های اعتماد در IoT

بنابر آن‌چه ارائه گردید، شبکه‌های IoT علاوه بر آسیب‌پذیری بالا به شدت در معرض هجوم انواع حملات قرار دارند. به‌طوری که بیشتر این حملات بنابر اهمیت بالای مبحث مسیریابی و تبادل اطلاعات، بر این مقوله متمرکز شده‌اند. ازاین‌رو بیشتر پژوهش‌ها و روش‌های پیشنهادی در حوزه امنیت نیز متمرکز بر مسیریابی و مقابله با تهدیدهای امنیتی مرتبط با این حوزه طراحی و معرفی شده‌اند [۲و۱۷و۱۹]. روش‌های پیشنهادی به جهت پیاده‌سازی امنیت و برقراری اعتماد را می‌توان در دسته‌های مختلفی تقسیم و طبقه‌بندی نمود. در این میان، تکنیکی مرسوم به مکانیزم‌های اعتماد[1] در قیاس با سایر تکنیک‌ها عملکرد موفق‌تری داشته و سازگارتر با خصوصیات توزیع شده و نیازهای شبکه‌های IoT است. روش‌های طراحی شده بر پایه این تکنیک تنها روش‌هایی بوده که علاوه بر تشخیص مخرب‌ها، مسیریابی و مبادلات معتمد را نیز پشتیبانی می‌نمایند. همچنین این روش‌ها قابلیت تشخیص و مقابله با هر دو نوع گره‌های مخرب (حملات گره‌های بدخواه و سوءرفتارهای خودخواهانه) را فراهم می‌سازند. این مزایا باعث شده تا اکثریت مقالات حوزه امنیت و اعتماد، بر پایه این تکنیک طراحی و توسعه یابند. منشاء و ایده این تکنیک، از امنیت و اعتماد جامعه انسانی حاصل شده و منطبق با این سیستم می‌باشد. در مکانیزم‌های اعتماد، همانند جامعه انسانی، گره‌ها در قبال رفتارهای صحیح و خیرخواهانه با افزایش اعتماد و اعتبار تشویق شده، و در قبال رفتارهای منفی و مخرب با کاهش اعتماد جریمه و تنبیه می‌شوند [۱۱و۱۲]. در این حالت اگر اعتماد عاملی بنابر توالی رفتارهای منفی و مخربش به زیر مقدار آستانه مشخصی با عنوان آستانه اعتماد آید، گره خاطی به عنوان عاملی مخرب و مهاجم در نظر گرفته شده و در شبکه قرنطینه خواهد شد. زمانی که گره‌ای قرنطینه می‌شود هیچ از یک از گره‌های شبکه تا بازه زمانی مشخصی هیچ

[1] Trust Model

تعاملی با عامل مخرب نخواهند داشت و در اصطلاح گره به لیست سیاه افزوده می‌شود. در نهایت مکانیزم‌های اعتماد مبتنی بر این افزایش و کاهش اعتماد گره‌ها، تلاش بر تمایز عامل‌های مخرب از سایر گره‌ها و پشتیبانی از مبادلات معتمد را دارند [۱۰]. در اغلب روش‌هایی که بر پایه مکانیزم‌های اعتماد طراحی می‌شوند، اعتماد گره‌ها بر پایه دو عامل اعتماد مستقیم و اعتماد غیرمستقیم (توصیه‌های ارسالی) محاسبه و ارزیابی می‌شود. اعتماد مستقیم نتیجه‌ای از نظارت بر تبادلات مستقیم بین گره‌ها بوده و اعتماد غیرمستقیم برآیندی از توصیه-های ارسالی سایر گره‌ها می‌باشد [۱۰و۱۲].

در ادامه روش‌های که بر پایه مکانیزم‌های اعتماد از دیدگاه مختلف دسته‌بندی و طبقه‌بندی شده‌اند.

۶. دسته‌بندی مدل‌های اعتماد

در این بخش روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد را بر حسب تکنیک‌های کاربردی برای محاسبه اعتماد تفکیک و ارزیابی کرده و از این حیث نقد و بررسی نموده‌ایم.

از دیدگام محاسبات اعتماد، روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد را به طور کلی می‌توان به پنج بخش کلی تقسیم‌بندی نمود. شرح جزئیات این بخش‌بندی در ادامه نقد و بررسی شده است.

۱- مؤلفه‌های ارزیابی اعتماد

از دیدگاه مؤلفه‌های ارزیابی اعتماد روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد را می‌توان به دو دسته تکنیک‌های ارزیابی مبتنی بر معیارهای کیفی اعتماد و تکنیک‌های ارزیابی مبتنی بر اعتماد اجتماعی تقسیم‌بندی نمود. در دسته نخست محاسبات اعتماد بر پایه معیارهای کیفی اعتماد شامل اعتماد به انرژی، اعتماد به اتصال، اعتماد به عملکرد و غیره ارزیابی شده [۴۶و۵۰] و در دسته دوم محاسبات اعتماد بر پایه روابط بین اجتماعی بین گره‌ها شامل صداقت، صمیمت، خودخواهی و سایر مفاهیم مرتبط با اعتماد اجتماعی محاسبه می‌شود [۴۷]. از این میان روش‌های مبتنی بر معیارهای کیفی اعتماد در برقراری اعتماد موفق‌تر بوده و همچنین دریافت‌های موفق، تأخیر تعاملات و قابلیت اطمینان بهتری ارائه می‌نمایند

۲- اشتراک‌گذاری اعتماد (تبلیغ اعتماد)

منظور از تبلیغ اعتماد، نحوه انتشار و اشتراک‌گذاری شواهد اعتماد با سایر گره‌های شبکه است. از این دیدگاه روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد به دو دسته توزیع شده و متمرکز تقسیم می‌شوند. در نوع توزیع شده انتشار اعتماد توسط خود گره‌های شبکه، بدون نظارت نهاد مرکزی انجام می‌شود [۴۷]. این روش‌ها اغلب از تکنیک‌های پیشنهادی برای شبکه‌های حسگر بی‌سیم و موردی پیروی می‌نمایند. دسته دوم روش‌های متمرکز هستند. در این روش‌ها اشتراک‌گذاری اعتماد تحت نهاد مرکزی انجام می‌شود [۴۸]. این نهاد می‌تواند گره ریشه، ابر یا هر موجودیت دیگری باشد. در این میان روش‌های توزیع شده به نسبت روش‌های متمرکز، سازگاری بیشتری با شبکه‌های IoT داشته و به جهت برقراری اعتماد در کاربردهای مختلف موفق‌تر هستند.

۳- گردآوری اعتماد

منظور از گردآوری اعتماد، جمع‌آوری اطلاعات مربوطه به اعتماد (شامل مشاهدات خود گره و نظرات سایرین) است. از این دیدگاه روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد به پنج دسته شامل تجمیع مبتنی بر وزن‌دهی، تجمیع مبتنی بر فازی، تجمیع مبتنی بر نظریه باور، تجمیع مبتنی بر استنباط بیزی و تجمیع مبتنی بر رگرسیون تقسیم می‌شوند [۵۱-۵۴]. هدف این روش‌ها تجمیع اطلاعات و

داده‌های مربوط به اعتماد بوده تا در نهایت بر اساس آن تصمیم‌گیری نهایی اتخاذ شود. از این میان منطق فازی در ازاء تصمیم‌گیری چند پارامتری مؤثرتر بوده، این در حالی است که نظریه باور و استنباط بیزی دقت بالاتری را برای تشخیص مخرب‌ها فراهم می‌سازند.

۴- به‌روزرسانی اعتماد

از دیدگاه به‌روزرسانی اعتماد روش‌های پیشنهادی بر پایه مکانیزم‌های اعتماد به دو دسته تکنیک‌های رویداد محور و تکنیک‌های زمان‌محور تقسیم‌بندی می‌شوند. در نوع نخست اطلاعات اعتماد در یک گره با رخداد رویدادی به‌روزرسانی می‌شوند. این رویداد اغلب تعامل و تبادل داده بین دو گره می‌باشد [۴۹]. در نوع دوم اطلاعات اعتماد به صورت دوره‌ای و در پریودهای زمانی مشخص به‌روزرسانی می‌شوند [۵۰]. اغلب تحقیقات گذشته برای به‌روزرسانی اعتماد، عملکردی رویداد محور دارند. زیرا که روش‌های زمان‌محور از مسئله کهنگی اعتماد رنج برده و پاسخ‌گوی ویژگی وفق‌پذیری اعتماد نیستند.

۵- تشکیل اعتماد

منظور از تشکیل اعتماد، ویژگی‌های تأثیرگذار بر ارزیابی اعتماد است. از این دیدگاه روش‌های ارزیابی اعتماد به دو دسته اعتماد تک-بعدی و چند بعدی تقسیم می‌شوند. در نوع نخست اعتماد تنها بر مبنای یک ویژگی ارزیابی و محاسبه می‌شود [۳۶]. برای مثال نرخ تعاملات موفق به مجموع تراکنش‌ها. در این روش‌ها اعتماد تنها بر مبنای این شاخص و برآیندی از آن در طی تعاملات دو گره ارزیابی و حاصل می‌شود. در مدل‌های اعتماد چندبعدی، ویژگی‌های مختلفی بر ارزیابی اعتماد تأثیر دارند. برای مثال اعتماد نهایی، بر پایه برآیندی از صداقت، خودخواهی و تعاملات موفق گره‌ها ارزیابی و حاصل می‌شود [۴۸]. در این میان روش‌های ارزیابی چندبعدی اعتماد به نسبت روش تک‌بعدی کارایی و دقت بالاتری برای پیاده‌سازی اعتماد فراهم می‌سازند.

۷. نتیجه‌گیری

در این مقاله، یک بررسی جامع از حملات و در سوی مقابل مدل‌ها امنیت و اعتماد کاربردی در IoT، به ویژه در ارتباط با بحث مسیریابی و تبادلات داده‌ها انجام و ارائه شد. برای این منظور، در ابتدا به بحث امنیتو اعتماد در اینترنت اشیاء و سپس انواع حملات وارده بر این شبکه‌ها نقد و بررسی گردیدند. سپس انواع روش‌های مقابله معرفی شده و در ارتباط با این روش‌ها و عملکرد هر یک مباحثی به تفصیل بحث و بررسی گردید. در مجموع بررسی‌ها نشان می‌دهد که با توجه به جدید بودن این شبکه‌ها و تفاوت‌ها و خصوصیات منحصر به فرد آن، هم‌چنان باید کارهای پوهشی زیادی انجام شود تا بتواند جوانب حائز اهمیت بحث امنیت و اعتماد را به شکلی مؤثر بهبود و پوشش داد.

منابع

[1] Marietta, J., and B. Chandra Mohan. "A review on routing in internet of things." *Wireless Personal Communications* 111.1 (2020): 209-233.
[2] Almusaylim, Zahrah A., Abdulaziz Alhumam, and N. Z. Jhanjhi. "Proposing a secure RPL based internet of things routing protocol: a review." *Ad Hoc Networks* 101 (2020): 102096.
[3] Sharma, Meera, et al. "An Application of IoT to Develop Concept of Smart Remote Monitoring System." *Business Intelligence for Enterprise Internet of Things*. Springer, Cham, 2020. 233-239.
[4] Hornillo-Mellado, Susana, Rubén Martín-Clemente, and Vicente Baena-Lecuyer. "Prediction of Satellite Shadowing in Smart Cities with Application to IoT." *Sensors* 20.2 (2020): 475.

[5] Garg, Lalit, et al. "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model." *Ieee Access* 8 (2020): 159402-159414.
[6] Ahn, Sang-Jin. "Three characteristics of technology competition by IoT-driven digitization." *Technological Forecasting and Social Change* 157 (2020): 120062.
[7] Pekar, Adrian, et al. "Application domain-based overview of IoT network traffic characteristics." *ACM Computing Surveys (CSUR)* 53.4 (2020): 1-33.
[8] Nebbione, Giuseppe, and Maria Carla Calzarossa. "Security of IoT application layer protocols: Challenges and findings." *Future Internet* 12.3 (2020): 55.
[9] Liao, Bin, et al. "Security analysis of IoT devices by using mobile computing: a systematic literature review." *IEEE Access* 8 (2020): 120331-120350.
[10] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "A survey on trust management for mobile ad hoc networks." *IEEE communications surveys & tutorials* 13.4 (2010): 562-583.
[11] Chahal, Rajanpreet Kaur, Neeraj Kumar, and Shalini Batra. "Trust management in social Internet of Things: A taxonomy, open issues, and challenges." *Computer Communications* 150 (2020): 13-46.
[12] Boudagdigue, Chaimaa, et al. "Trust management in industrial internet of things." *IEEE Transactions on Information Forensics and Security* 15 (2020): 3667-3682.
[13] Qureshi, Kashif Naseer, et al. "Trust management and evaluation for edge intelligence in the Internet of Things." *Engineering Applications of Artificial Intelligence* 94 (2020): 103756.
[15] Qureshi, Kashif Naseer, et al. "A novel and secure attacks detection framework for smart cities industrial internet of things." *Sustainable Cities and Society* 61 (2020): 102343.
[16] Sobral, José VV, et al. "Routing protocols for low power and lossy networks in internet of things applications." *Sensors* 19.9 (2019): 2144.
[17] Kamble, Arvind, Virendra S. Malemath, and Deepika Patil. "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey." *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*. IEEE, 2017.
[18] Dian, F. John, Reza Vahidnia, and Alireza Rahmati. "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey." *IEEE Access* 8 (2020): 69200-69211.
[19] Dhumane, Amol, Rajesh Prasad, and Jayashree Prasad. "Routing issues in internet of things: a survey." *Proceedings of the international multiconference of engineers and computer scientists*. Vol. 1. 2016.
[20] Kiran, Vidhu, Shaveta Rani, and Paramjeet Singh. "Towards a light weight routing security in iot using non-cooperative game models and dempster–shaffer theory." *Wireless Personal Communications* 110.4 (2020): 1729-1749.
[21] Nawir, Mukrimah, et al. "Internet of Things (IoT): Taxonomy of security attacks." *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, 2016.
[21] Kumar, Upendra, et al. "Isolation of ddos attack in iot: A new perspective." *Wireless Personal Communications* 114 (2020): 2493-2510.
[22] Safkhani, Masoumeh, and Nasour Bagheri. "Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things." *The Journal of Supercomputing* 73.8 (2017): 3579-3585.
[23] El Mouaatamid, Otmane, Mohammed Lahmer, and Mostafa Belkasmi. "Internet of Things Security: Layered classification of attacks and possible Countermeasures." *electronic journal of information technology* 9 (2016).
[24] Nguyen, Van-Linh, Po-Ching Lin, and Ren-Hung Hwang. "Energy depletion attacks in low power wireless networks." *IEEE Access* 7 (2019): 51915-51932.
[25] Pongle, Pavan, and Gurunath Chavan. "A survey: Attacks on RPL and 6LoWPAN in IoT." *2015 International conference on pervasive computing (ICPC)*. IEEE, 2015.

[26] Patel, Himanshu B., and Devesh C. Jinwala. "Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach." *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019.
[27] Babu, M. Rajesh, et al. "Proactive alleviation procedure to handle black hole attack and its version." *The Scientific World Journal* 2015 (2015).
[28] Butun, Ismail, Patrik Österberg, and Houbing Song. "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures." *IEEE Communications Surveys & Tutorials* 22.1 (2019): 616-644.
[29] Bhosale, Snehal Ajit, and S. S. Sonavane. "Wormhole Attack Detection System for IoT Network: A Hybrid Approach." (2021).
[30] Coman, Florian Laurentiu, et al. "Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT." *2019 Global IoT Summit (GIoTS)*. IEEE, 2019.
[31] Yavuz, Furkan Yusuf, Devrim Ünal, and Ensar Gül. "Deep learning for detection of routing attacks in the internet of things." *International Journal of Computational Intelligence Systems* 12.1 (2018): 39-58.
[32] Caminha, Jean, Angelo Perkusich, and Mirko Perkusich. "A smart trust management method to detect on-off attacks in the internet of things." *Security and Communication Networks* 2018 (2018).
[33] Almusaylim, Zahrah A., et al. "Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things." (2020).
[34] Neerugatti, Vikram, and A. Rama Mohan Reddy. "Artificial intelligence-based technique for detection of selective forwarding attack in rpl-based internet of things networks." *Emerging Research in Data Engineering Systems and Computer Communications*. Springer, Singapore, 2020. 67-77.
[35] Thomas, Arun, T. Gireesh Kumar, and Ashok Kumar Mohan. "Neighbor attack detection in internet of things." *Advanced Computational and Communication Paradigms*. Springer, Singapore, 2018. 187-196.
[36] Shin, Sooyeon, Kyounghoon Kim, and Taekyoung Kwon. "Detection of malicious packet dropping attacks in RPL-based internet of things." *International Journal of Ad Hoc and Ubiquitous Computing* 31.2 (2019): 133-141.
[37] Chen, Qifeng, et al. "Denial of service attack on IoT system." *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*. IEEE, 2018.
[38] Pu, Cong. "Sybil attack in RPL-based internet of things: analysis and defenses." *IEEE Internet of Things Journal* 7.6 (2020): 4937-4949.
[39] Zhang, Yushu, et al. "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT." *IEEE Transactions on Industrial Informatics* 16.12 (2019): 7566-7578.
[40] Ahmed, Abdul Wahab, et al. "A comprehensive analysis on the security threats and their countermeasures of IoT." *Int J Adv Comput Sci Appl* 8.7 (2017): 489-501.
[41] Mousavi, Seyyed Keyvan, et al. "Security of internet of things based on cryptographic algorithms: a survey." *Wireless Networks* 27.2 (2021): 1515-1555.
[42] Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: A solution to secure IoT." *Wireless Personal Communications* 112.3 (2020): 1947-1980.
[43] Sicato, Jose Costa Sapalo, et al. "A comprehensive analyses of intrusion detection system for IoT environment." *Journal of Information Processing Systems* 16.4 (2020): 975-990.
[44] Thakkar, Ankit, and Ritika Lohiya. "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." *Archives of Computational Methods in Engineering* 28.4 (2021): 3211-3243.

[45] Soni, Gaurav, and R. Sudhakar. "A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT." *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2020.
[46] Nitti, Michele, et al. "A subjective model for trustworthiness evaluation in the social internet of things." *2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC)*. IEEE, 2012.
[47] Chen, Ray, Jia Guo, and Fenye Bao. "Trust management for SOA-based IoT and its application to service composition." *IEEE Transactions on Services Computing* 9.3 (2014): 482-495.
[48] Nitti, Michele, Roberto Girau, and Luigi Atzori. "Trustworthiness management in the social internet of things." *IEEE Transactions on knowledge and data engineering* 26.5 (2013): 1253-1266.
[49] Chen, Ray, et al. "Trust management for encounter-based routing in delay tolerant networks." *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, 2010.
[50] Djedjig, Nabil, et al. "Trust-aware and cooperative routing protocol for IoT security." *Journal of Information Security and Applications* 52 (2020): 102467.
[51] Prathapchandran, K., and T. Janani. "A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression." *Journal of Physics: Conference Series*. Vol. 1850. No. 1. IOP Publishing, 2021.
[52] Ali, Bader A., Hanady M. Abdulsalam, and Aseel AlGhemlas. "Trust based scheme for IoT enabled wireless sensor networks." *Wireless Personal Communications* 99.2 (2018): 1061-1080.
[53] Wu, Hao, and Wei Wang. "A game theory based collaborative security detection method for Internet of Things systems." *IEEE Transactions on Information Forensics and Security* 13.6 (2018): 1432-1445.
[54] Mehmood, Amjad, et al. "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks." *The Journal of Supercomputing* 74.10 (2018): 5156-5170.