دوفصلنامه مدیریت مهندسی و رایانش نرم/دوره ۸، شماره ۱، بهار و تابستان ۱۴۰۱
(DOI): 10.22091/jemsc.2019.1297 صفحات ۱۵۱- ۱۲۳
JEMSC.QOM
مدیریت مهندسی و رایانش نرم ۱۳۹۴

بهبود حفظ حریم خصوصی داده‌گان در اینترنت اشیاء با در نظر گرفتن محدودیت اینترنت به کمک سیستم ایمنی مصنوعی*

مرضیه فریدی ماسوله [۱]
علی هارون‌آبادی [۲]
عسل صیاد [۳]

چکیده

امروزه حفاظت از حریم خصوصی داده‌گان به عنوان مهم‌ترین چالش در شبکه‌های اینترنت اشیا تلقی می‌شود. این شبکه‌ها حاوی اطلاعات مهمی می‌باشند که در شبکه میان نودها منتقل می‌گردد. به همین دلیل توجه به مسئله حریم خصوصی داده‌گان در اینترنت اشیاء بسیار حائز اهمیت است. تحقیقات نشان می‌دهد که نبود یک مدل کامل، کارا و استاندارد موجب شده تا بسیاری از نقص‌های امنیتی در این شبکه‌ها پدیدار گردد. در این پژوهش با در نظر گرفتن محدودیت اینترنت، چگونگی تشکیل تابع هدف جهت حریم خصوصی داده‌گان در اینترنت اشیاء مطرح شده و هدف از روش پیشنهادی، یافتن یک مسیر بهینه است که از میزان شایستگی خوبی برخوردار باشد. این روش در نرم‌افزار متلب پیاده‌سازی شده است و نتایج حاصل از آزمایشات نشان می‌دهد که الگوریتم سیستم ایمنی مصنوعی برای حل مسائل بهینه‌سازی، هرچند جواب قطعی نمی‌دهد اما جوابی نزدیک به بهینه را پیدا می‌کند. همچنین، زمان پاسخگویی الگوریتم سیستم ایمنی مصنوعی در مقایسه با الگوریتم‌های مورد مقایسه کمتر است و با توجه به نمودارهای همگرایی، مشاهده می‌شود که الگوریتم سیستم ایمنی مصنوعی از همگرایی خوبی برخوردار است.

واژه‌های کلیدی: *اینترنت اشیاء، حریم خصوصی داده گان، محدودیت اینترنت و الگوریتم سیستم ایمنی مصنوعی.*

---

* تاریخ دریافت: ۱۳۹۷/۱۱/۱۰؛ تاریخ پذیرش: ۱۳۹۸/۰۶/۱۴.

۱. استادیار، گروه کامپیوتر، دانشگاه احرار، رشت، ایران **(نویسنده مسئول)** m.faridi@ahrar.ac.ir
۲. استادیار، گروه کامپیوتر، دانشگاه آزاد اسلامی واحد تهران مرکز، تهران، ایران. a.harounabadi@gmail.com
۳. کارشناس ارشد مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی واحد الکترونیکی، تهران، ایران. 90asal@gmail.com

مقدمه

امروزه تغییرات تکنولوژی تأثیر بسـزایی در نحوه انتقال اطلاعات داشـته اسـت. نحوه انتقال اطلاعات در گذشـته تنها میان انسـان‌ها بوده اسـت اما امروزه این نحوه انتقال اطلاعات بین انسان و اشیاء، اشیاء و اشیاء نیز توسعه یافته است. این ارتباط می‌تواند در هر زمان و در هر مکان امکان‌پذیر شود. اینترنت اشیاء در سال ۲۰۰۵ توسط اتحادیه جهانی ارتباطات مخابراتی ارائه شد. این زمینه از آغاز تاکنون در بسیاری از شبکه‌ها مانند شبکه‌های حسگر بی‌سیم مورد استفاده قرار گرفته است. این شبکه‌ها شامل دو مشخصه زیر می‌باشند (اختری، ۱۳۹۴):

اینترنت اشیاء حالت توسعه‌یافته شبکه‌های مبتنی بر اینترنت است؛ و کاربران این نوع شبکه‌ها می‌تواند شی یا انسان باشد.

پژوهش‌های بسـیاری روی اینترنت اشـیاء و چالش‌های آن در حال انجام اسـت. این شـبکه‌ها با سـرعت بالایی در حال توسـعه می‌باشـند و این مسـئله موجب گردیده اسـت که توجه بسـیاری از پژوهشـگران به این زمینه جلب شـود. یکی از این چالش‌ها، حفظ حریم خصوصی داده‌گان است. بسیاری از ارگان‌ها و موسساتی که خواهان بهره‌وری از اینترنت اشـیاء می‌باشـند به این مسـئله توجه بسـیاری دارند. بیشـتر اطلاعات که در این ارگان‌ها و موسـسـات موجود اسـت بسـیار مهم و محرمانه هسـتند. به همین دلیل باید به حفظ حریم خصوصی داده‌گان اینترنت اشیاء توجه ویژه‌ای داشت. تحقیقات پیشین نشان داده است که نبود یک سـیسـتم امن در اینترنت اشـیاء، به دلیل نبود یک معماری و یا الگوریتم کارا می‌باشـد. با مطالعات که انجام شـد (اختری ۱۳۹۴؛ سـرخوش، رضـوانی و تعجبیان، ۱۳۹۴؛ ترکمانی و شاهرخی ۱۳۹۴) سه چالش مهم برای یک معماری یا الگوریتم کارا باید در نظر گرفته شود:

۱) هزینه: هزینه‌ها مربوط به میزان تأمین انرژی، حافظه، سخت‌افزار و غیره می‌شود.

۲) باید روش پیشـنهادی به گونه‌ای تعریف شـود که در تمام شـبکه‌ها اعم از بی‌سـیم حسگر، ادهاک، سیار و غیره امکان استفاده را داشته باشد.

۳) محافظت از حریم خصوصی داده‌ها.

امروزه با گسترش روزافزون اینترنت و در نتیجه، سیستم‌های کامپیوتری مبتنی بر شبکه و نقش مهم آنها در ارتباطات و انتقال اطلاعات، اینترنت اشیا، نقشی اساسی و فزاینده‌ای در جوامع مدرن ایفا می‌کند. از این رو، تأمین امنیت اینترنت اشیا به عنوان یک ضرورت و چالش اساسی برای مدیران امنیتی شبکه‌ها مطرح بوده است. سیستم‌های اینترنت اشیا، یکی از زمینه‌های مهم تحقیقاتی در امنیت شبکه‌های کامپیوتری هستند. هدف سیستم تشخیص نفوذ، کشف و شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا اینترنت اشیا و اعلام آن به مدیران امنیتی می‌باشد (فشارکی و همکاران، ۱۳۹۴).

وقتی که استانداردهای بنیادی اینترنت ایجاد شدند، افرادی کنترل این استانداردها را در دست داشتند که خواسته واقعی‌شان شکل‌گیری استانداردهای جهانی بود. استانداردهایی که به طور برابر در دسترس همه باشد. اما اینترنت امروزه در کنترل شرکت‌هایی است که هر کدام می‌خواهند از این استانداردها بهره بگیرند و با استفاده از آن‌ها رقبا را شکست دهند و سود ببرند. همچنین، اینترنت در دست دولت‌هایی است که در اصل می‌خواهند بر همه چیز نظارت داشته باشند (انگست و اگاروال، ۲۰۰۹).

از موانع و مشکلات موجود در طراحی یک سیستم اینترنت اشیا کارآمد، می‌توان به حجم انبوهی از داده‌های مربوط به ترافیک شبکه، نرخ تشخیص درست پایین و تولید هشدارهای اشتباه اشاره کرد که موجب ایجاد سیستم‌های بسیار بدبین و درنهایت بی‌اعتنایی متخصصان به هشدارهای سیستم خواهد شد (سرخوش و همکاران، ۱۳۹۴). بنابراین، تأمین امنیت یک اولویت کاری بالا برای مدیران ارشد و متخصصین امنیتی اینترنت اشیا می‌باشد. برای تأمین امنیت اینترنت اشیاء بسته به اهمیت و وضعیت سیستم‌ها، تکنیک‌ها و راهکارهای متنوعی توسط متخصصین امنیتی، به کار گرفته می‌شود که می‌توان به رمزنگاری، تأیید هویت کاربران، امضاهای دیجیتالی و غیره اشاره کرد. اما متأسفانه این راهکارها برای تأمین امنیت کامل سیستم‌های کامپیوتری کافی نیست. بنابراین نیاز به یک مکانیزم امنیتی داریم که پیوسته نظارت کافی بر سیستم داشته، موارد مشکوک به نقض امنیت سیستم را تشخیص داده و پاسخ مناسبی صادر کند.

به منظور تحقق مسئله امنیت، IOT[1] با چالش‌های بیشتری مواجه است. دلایل زیر برای این موضوع وجود دارد: ۱) IOT از طریق اینترنت سنتی، شبکه موبایل و شبکه حسگر و ... توسعه داده می‌شود، ۲) بسیاری از اشیاء به این نوع از اینترنت متصل می‌شوند، ۳) این اشیاء با یکدیگر ارتباط برقرار می‌کنند. در نتیجه، یک مشکل امنیتی و حریم خصوصی جدید بروز می‌کند. توجهات بیشتری برای قابلیت اعتماد، تشخیص و تلفیق داده در IOT باید انجام بگیرد. در زیر چالش‌های مشترکی برای امنیت اینترنت اشیاء تحلیل و خلاصه شده است:

الف) ساختار معماری: در مرجع (چین‌لانگ و چوآن‌چانگ، ۲۰۱۶)، IOT در طول کل بازه زمانی، پایدار باقی می‌ماند و مکانیزم امنیت در هر لایه منطقی نمی‌تواند سیستم دفاع کامل را پیاده‌سازی کند. در نتیجه، این موضوع یک چالش بوده و حوزه‌های تحقیقاتی فراوانی جهت ایجاد ساختار امن با ترکیب کنترل و اطلاعات مورد نیاز است.

ب) قوانین و مقررات امنیت: در حال حاضر، قانون و مقررات امنیت، همچنان در مرکز توجهات قرار ندارد و هیچ استاندارد تکنولوژی در مورد IOT وجود ندارد. IOT مربوط به اطلاعات امن ملی، اسرار تجاری و حریم شخصی افراد می‌باشد. در نتیجه، کشور ما نیاز به دیدگاه قانونی جهت توسعه IOT است. مقررات و قوانین به صورت بلا انکاری مورد نیاز است.

ج) نیازمندی‌ها برای کاربردهای نوظهور: با توسعه WSNها، تشخیص فرکانس رادیویی(RFID)، تکنولوژی محاسبات فراگیرنده، تکنولوژی مخابرات شبکه، و تئوری کنترل بلادرنگ توزیع شده، CPS، یک شکل بروز پیدا کرده از IOT است که تبدیل به واقعیت شده است. در این سیستم، امنیت بالا برای تضمین عملکرد سیستم موردنیاز است.

مدیریت اساسی در یک شبکه حسگر مقیاس بزرگ واقعی نیز همواره از مسائل چالشی بوده و مقررات و قوانین این حوزه که مربوط به IOT است نیز جزو موضوعات چالشی می‌باشد. الگوریتم سیستم ایمنی مصنوعی جزء الگوریتم‌های الهام گرفته از

[1] Internet of Things

بیولوژی هستند. این نوع الگوریتم‌ها، الگوریتم‌هایی کامپیوتری هستند که اصول و ویژگی‌های آنها نتیجه بررسی خواص وفقی و مقاومت نمونه‌های بیولوژیکی بدن انسان است. سیستم ایمنی مصنوعی نوعی الگو برای یادگیری ماشین است. یادگیری ماشین، توانایی کامپیوتر برای انجام یک کار با یادگیری داده‌ها یا از روی تجربه است. از دانش موجود در زمینه این روش تاکنون در حل مسائل شناسایی الگو، یادگیری ماشین، بهینه سازی، خوشه‌بندی و غیره استفاده شده است (الودات، کاتینا، چن و الدبی، ۲۰۱۴). در پژوهش حاضر از تکنیک سیستم ایمنی مصنوعی برای یافتن مناسب‌ترین گره بعدی استفاده خواهد شد به طوری که بتواند مصرف انرژی شبکه را کمینه کند.

پیشینه پژوهش

پیش‌بینی تولید انرژی به وسیله اینترنت اشیاء بر اساس یادگیری ماشین پژوهشی است که در سال ۲۰۱۹ انجام شده است. در این پژوهش برای برآورد تولید برق توربین بادی از تکنیک یادگیری ماشین مبتنی بر IoT استفاده شده است. داده‌های واقعی باد و قدرت تولید شده است که برای به دست آوردن منحنی قدرت با استفاده از رگرسیون لجستیک و شبکه عصبی مصنوعی بازگشتی به منظور پیش‌بینی سرعت باد استفاده شده است (ربوماس‌فیلو و همکاران، ۲۰۱۹).

در پژوهشی با عنوان ارائه معماری جدید سه بعدی اینترنت اشیاء با استفاده از الگوریتم یادگیری ماشین برای شناسایی زودهنگام بیماری‌های قلبی که در سال ۲۰۱۸ انجام شد؛ معماری سه‌بعدی قابل مقیاس برای ذخیره و پردازش حجم زیادی از اطلاعات سنسورهای پوشیدنی ارائه شد. در سطح اول این معماری به جمع‌آوری داده‌ها از دستگاه‌های حسگر پوشیدنی IO پرداخته شد.

سطح دوم از Apache HBase برای ذخیره حجم زیادی از داده‌های حسگر IoT پوشیدنی در ابر استفاده می‌کند و سطح سوم از Apache Mahout برای توسعه مدل پیش‌بینی مبتنی بر رگرسیون لجستیک برای بیماری‌های قلب استفاده می‌نماید و در نهایت،

تجزیه و تحلیل ROC برای شناسایی مهمترین پارامترهای بالینی برای بیماری قلبی انجام می‌شود (کومار و گاندهی، ۲۰۱۸).

در سال ۲۰۱۷ در پژوهشی که با عنوان شناسایی سیگنال‌های الکتروکاردیوگرام به کمک اینترنت اشیا بر پایه طبقه‌بندی ترکیبی انجام شد، به شناسایی سیگنال ECG از طریق یک شبکه ساده حسگر بی‌سیم بدن به کمک اینترنت اشیا بر پایه طبقه‌بندی و استخراج ویژگی با برقراری رابطه بین الکتروکاردیوگرام و حسگرهای بدنی پرداخته شد. روش ارائه شده بعد از استخراج بهترین ویژگی‌های سیگنال ECG با استفاده از الگوریتم خفاش، به طبقه‌بندی آن می‌پردازد که از الگوریتم ترکیبی ماشین بردار پشتیبان و شبکه عصبی پرسپترون چند لایه استفاده شده است. تحلیل سیگنال‌های ECG و انتخاب بهترین ویژگی‌های آن به شناسایی و تشخیص زود هنگام بیماری‌های قلبی کمک شایانی نماید (فریدی‌ماسوله و همکاران، ۲۰۱۷).

جین و همکاران در سال ۲۰۱۶ در مورد یک روش کارآمد برای تجمیع داده‌ها و تحویل قابل اطمینان داده‌ها بر اساس روش بی‌سیم اینترنت اشیا مطالعه و ارائه نمودند که یک سناریوی قابل استقرار در نقاط انتهایی شبکه‌های اینترنت اشیاء از قبیل حسگرها است که این نقاط مجبور به ارسال داده‌های خود بر روی پیوندهای پُر اتلاف به سمت دیگر نقاط انتهایی اینترنت اشیاء هستند. به طور خاص، بی‌سیم اینترنت اشیا یک رویکرد توزیع شده است که کاهش سود ترافیک به دست آمده از تجمیع داده‌ها بر اساس محتوا و مسیریابی ترافیک بر روی پیوندهای قابل اعتماد را با ترکیب اطلاعات کیفیت پیوند در نظر می‌گیرد. بر اساس محتوای یک پیام، هر گره یک مسیریابی جدا را برای هر نوع از محتوا با استفاده از اجرای تابع هدف جدید پیشنهادی ایجاد می‌کند؛ ایده اصلی این بود که انواع محتواهای ناهمگن را از طریق پیوندهای قابل اطمینان انتخاب شده مسیریابی شود تا گره‌هایی که قادر به تجمیع و پردازش این نوع از محتواها هستند، آنها را قبل از ارسال به صورت اطلاعات خلاصه شده در بیاورند. این کار تا حد زیادی ترافیک ارتباطی تکراری و ارسال‌های مجدد را کاهش می‌دهد که یک اثر جانبی مثبت است. هم نتایج شبیه‌سازی و هم نتایج پیاده‌سازی

تأیید می‌کنند که بی‌سیم اینترنت اشیا می‌تواند طور عمر شبکه را به طور قابل توجهی افزایش دهد، مدت زمان تأخیر شبکه را کاهش داده و قابلیت اطمینان ارتباط را بهبود دهد (ربوماس‌فیلو و همکاران، ۲۰۱۹).

در سال ۲۰۱۳ پژوهشی انجام شد که پژوهشگران آن بیان کردند که برخی از انواع الگوریتم‌های تشخیص حملات را می‌توان برای حل مسائل بهینه‌سازی استفاده کرد. این الگوریتم‌ها تضمین می‌کنند که یک راه حل بهینه تنها با در نظر گرفتن پیچیدگی زمانی پیدا شود. بنابراین، استفاده از الگوریتم‌های کلاسیک برای حل مسائل، تنها با برخی تغییرات و بهبودها برای کاهش زمان اجرا ممکن است. برای رسیدن به یک گردش کار محکم عملی برای اینترنت با توجه به نیازهای امنیت مصرف کننده، این مشکل معادل یک مشکل در نظر گرفته می‌شود (بندیوپدیای و سن، ۲۰۱۱).

در پژوهشی در سال ۲۰۰۹ روشی بر اساس امنیت و حفظ حریم خصوصی برای محیط‌های ابر و بر اساس نتایج ارزیابی عملکرد، سرویسی ارائه شده است که در آن مکانیسم‌های مختلف امنیتی استفاده می‌شود. این مکانیسم‌ها سربار اضافی در عملکرد سرویس را بررسی کرده و برای مقابله با آن، برای تغییر منابع به طور پویا تلاش می‌کند. بر اساس نتایج، می‌توان نشان داد که تغییر در منابع محاسباتی مجازی در مقدار منابع تأثیر مستقیم دارد (آتزوری، لرا و مورابیتو، ۲۰۱۰).

حلمی در پژوهش خود در سال ۱۳۹۴ به بررسی استخراج قوانین انجمنی با استفاده از سیستم ایمنی مصنوعی پرداخت. در این پروژه به طراحی، پیاده سازی و ارزیابی الگوریتمی بر اساس سیستم ایمنی مصنوعی پرداخته شد که به منظور استخراج اطلاعات از داده‌های دسترسی به وب طراحی شده است. در این الگوریتم از فرآیندهایی از جمله شبکه ایمنی و تئوری خطر برای استخراج مجموعه آیتم‌هایی (URL) استفاده می‌شود که مکرراً با هم در مجموعه داده‌های دسترسی به وب ظاهر می‌شوند. نتایج حاصل از الگوریتم ارائه شده، نشاندهنده درستی پیش‌بینی‌های انجام شده در مورد تناسب نتایج AIS به عنوان الگویی

برای حل مسئله پیدا کردن مجموعه آیتم‌های مکرر در داده‌های دسترسی به وب، است (فاسولو، روسی، ویدمر و زورزی، ۲۰۰۷).

دژکام در سال ۱۳۹۴ با توسعه یک سیستم امنیتی نوین مبتنی بر RFID سعی بر کاهش احتمال دسترسی به داده‌ها داشته است. هدف اصلی این پژوهش استفاده از اینترنت اشیاء در کارخانه‌ها و مراکز صنعتی بود. همچنین در این مقاله یک مطالعه گسترده روی روش‌های پیشین است که برای بهبود حفظ حریم خصوصی دادگان در اینترنت اشیاء ارائه شده است. سیستم پیشنهادی در شبکه‌های حسگر بی‌سیم و شبکه‌های متحرک قابل استفاده است (دژاکام، ۱۳۹۴).

یعقوبی و ذوقی در سال ۱۳۹۴ بر روی مسئله بهره‌گیری از اینترنت اشیاء در سیستم‌های سلامت الکترونیکی یک مطالعه گسترده انجام داده‌اند. چالش‌های بسیاری برای فراهم کردن این یک بستر مناسب وجود دارد اما تمرکز این مقاله بر روی حفظ حریم خصوصی دادگان و نهان‌نگاری در مسئله اینترنت اشیاء مورد استفاده در سلامت الکترونیکی است. استانداردهای متفاوتی در این مقاله مطالعه شده است و در نهایت یک چهارچوب نوین برای مسئله مورد مطالعه پیشنهاد شد (یعقوبی و ذوقی، ۱۳۹۴).

در پژوهشی دیگر که مجدداً در سال ۱۳۹۴ انجام شد، فشارکی و خورسند یک روش بهبود حفظ حریم خصوصی دادگان در سطح فیزیکی در اینترنت اشیاء معرفی کردند. شرایطی که در این پژوهش مدنظر است محدود بودن تعداد منابع است. به همین دلیل باید از توان پردازشی و حافظه به صورت بهینه استفاده شود. روش پیشنهادی مقاله از ویژگی‌هایی چون پیچیدگی پردازشی پایین در رمزنگاری و کمینه هزینه صرف شده در بخش سخت‌افزار بهره می‌برد (فشارکی و خورسند، ۱۳۹۴).

صفری در سال ۱۳۹۴ چالش‌های حفظ حریم خصوصی و نحوه برخورد با آن را در پژوهش خود مورد بررسی قرار داد. او لایه‌های مختلف اینترنت اشیاء (لایه ادراک، انتقال و برنامه) را مورد تحلیل قرار داد و بر حسب هر لایه راهکاری متناسب ارائه کرد. همچنین، بخشی از مقاله به بررسی توسعه سیستم‌های حفظ حریم خصوصی همگون بدون وابستگی

به لایه پرداخته است. این روش اشیائی را تفسیر و مدیریت می‌کند که مشتریان برای استفاده از آنها نیاز به نصب نرم‌افزار خاصی ندارند و از طریق مرورگر وب انجام می‌شود. در این نوع سیستم نیز مشکلات اشیاء مجازی در ارتباط با دیگر نرم‌افزارهای کاربردی یا کاربران خارجی که اشیاء مجازی را اجرا می‌کنند وجود دارد. اخیراً چندین نرم‌افزار کاربردی وب ارائه شده است که می‌توانند یکپارچه‌سازی نرم‌افزار را انجام دهند. اگرچه این جایگزین در بعضی حالت‌ها مؤثر است اما این راه‌حل از حالت ایده‌آل دور است. هنوز مشکلاتی برای شیء مجازی در ارتباط با شیء فیزیکی مشابه آن وجود دارد از قبیل این که چگونه سرویس‌ها اطلاعات محلی خود را نگهداری کنند یا این که اگرچه نرم‌افزارهای تحت وب دسترسی به APIها دارند، اما برای شیء مجازی که در یک نرم‌افزار تحت وب وجود دارد مشکل است که در تماس با دیگر نرم‌افزارها و موجودیت‌ها ابتکار عمل را در دست گیرد (صفری، ۱۳۹۴).

اینترنت اشیا تعداد زیادی از اشیای ناهمگون و فراگیر را با هم یکپارچه می‌کند که پیوسته در حال تولید اطلاعات درباره دنیای فیزیکی هستند (سرخوش، رضوانی و تعجبیان، ۱۳۹۴). اکثر این اطلاعات از طریق مرورگرهای استاندارد قابل دسترسی هستند و چندین بستر نیز رابط‌های برنامه‌نویسی کاربردی برای دسترسی به حسگرها و فعال‌سازها پیشنهاد می‌کنند. مفهوم اینترنت اشیا، در ابتدا از طریق پروژه‌های مؤسسه فناوری ماساچوست و نشریات تحلیلی فراگیر شد؛ اما اصطلاح اینترنت اشیا اولین بار از سوی کوین اشتون در سال ۱۹۹۹ مطرح شد (ترکمانی و شاهرخی، ۱۳۹۴).

تمرکز عمده رویکرد بی‌سیم اینترنت اشیا، تهیه تکنولوژی مسیریابی بهینه به منظور تسهیل جمع‌آوری داده داخل شبکه و کاهش ترافیک مصرفی است. مکانیسم‌های جمع‌آوری داده و مسیریابی، در منابع (دژاکام، ۱۳۹۴ویعقوبی و ذوقی، ۱۳۹۴) در مفهوم شبکه‌های حسگر بی‌سیم، مورد توجه قرار گرفته‌اند. بدنه اصلی کار را می‌توان به دو دسته عمده تقسیم کرد: رویکردهای متمرکز و توزیع. رویکردهای متمرکز معرفی شده در (فشارکی و خورسند، ۱۳۹۴ و صفری، ۱۳۹۴) معمولاً ساختار مسیریابی مناسب بهینه قبل از

شـــروع به کار شـــبکه را محاســـبه و شـــکل می‌دهد. در (اختری، ۱۳۹۴) راه‌حل درخت جمع‌آوری بیشینه زمان عمر شبکه ارائه شده است. تعادل بار در (مشایخی، ۱۳۹۴) در نظر گرفته شده است، و نویسندگان در (صفری، ۱۳۹۴) بیشتر به هزینه محاسبات جمع‌آوری توجه کرده‌اند. در تمامی منابع فوق، داشتن اطلاعات عمومی شبکه لازم است که می‌تواند ســـربار کنترلی قابل توجهی را معرفی کند. به منظور کاهش ســـربار کنترل، رویکردهای خوشـــه‌بندی توزیع شـــده، همچون منابع (چین‌لانگ و چوآن‌چانگ، ۲۰۱۶) و (آلودات و همکاران، ۲۰۱۴) به توپولوژی‌های مســـیریابی ســـلســـله‌مراتبی، از طریق غیبت پیام محلی متوسل می‌شوند. با این وجود، تنها یک توپولوژی درخت کوتاه‌ترین مسیر مورد قبول واقع می‌شـــود (انگســـت و اگاروال، ۲۰۰۹). در (آتزوری، لرا و مورابیتو، ۲۰۱۰) یک رویکرد مبتنی بر خوشـه‌بندی دینامیک معرفی شـده اسـت. با این وجود، پروسـه خوشـه‌بندی در هر رخداد یا کاربرد راه‌اندازی می‌شـود و این باعث هزینه انتقال زیاد در شـکل‌گیری خوشـه می‌شـود. به علاوه، مشـابه با رویکردهای خوشـه‌بندی منابع (اختری، ۱۳۹۴؛ بندیوپدیای و ســـن، ۲۰۱۱ و بندیوپدیای، بالاموراليدهار و پال، ۲۰۱۳) یا DAG نیاز به یک توپولوژی مســـیریابی خاص دارند که بتواند توانایی‌های آن را برای مقابله با شـــرایط دینامیکی شـــبکه راه‌اندازی و محدود کند. این عمل به این خاطر اســـت که هر زمان یک تغییر شـــبکه اتفاق همچون شکستگی لینک و تخلیه انرژی اولیه بعضی از گره‌های مسیریابی بحرانی می‌افتد، اطلاعات توپولوژی شـــبکه نیاز دارند که جهت عکس‌العمل در مقابل این پدیده‌ها به روز شوند.

در منابع (ژو و لی، ۲۰۱۴؛ زیجلدوروف، مورچون و وهرل، ۲۰۱۷ و گولین ونگ، ۲۰۱۷) شرایط کانال کاملی در نظر گرفته شده است که در دنیای واقعی ارتباطات نمی‌تواند تحقق یابد، به این دلیل که کیفیت لینک ارتباطی می‌تواند با زمان تغییر کند. بســـته‌های مســـیریابی مبتنی بر کیفیت لینک و اتصـــالات می‌تواند قابلیت اطمینان ارتباطات را بهبود بخشـــد. علاوه بر بهبود قابلیت اطمینان ارتباطات، حفظ انرژی محدود گره‌های باتری دار،

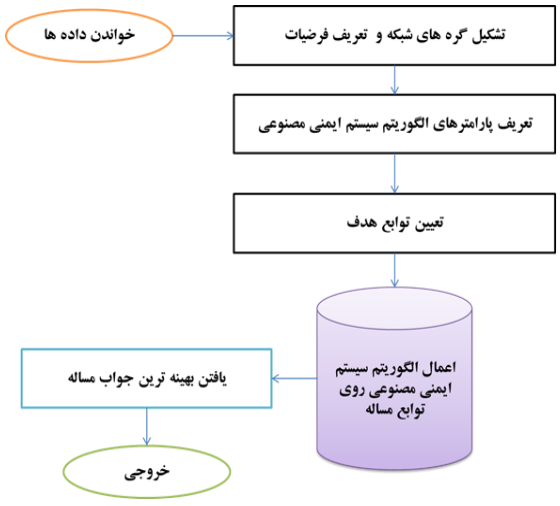
یکی از نیازهای مهم در زنده نگه داشتن گره‌ها و راه‌اندازی آن‌ها در شبکه‌هایی با انرژی محدود است.

روش‌شناسی پژوهش

اخیراً محاسبات توزیع شده در شبکه‌های بی‌سیم، به خصوص با پدیدار شدن اینترنت اشیاء که به دستگاه‌های با پردازش بالا، ارتباطات و قابلیت‌های ذخیره‌سازی مستقل مجهز شده‌اند، توجه زیادی را به خود جلب کرده است. ایده کلیدی این است که به جای ارسال تمام داده‌های خام به طور مستقیم در یک شبکه بی‌سیم گران‌قیمت (چند منظوره) که معمولاً با مصرف انرژی بالا و تأخیر زمانی همراه است، یک روش ارزان‌تر برای اولین بار حجم داده را به صورت محلی با پردازش شبکه کاهش می‌دهد و سپس نتایج پردازش را انتقال می‌دهد. در بسیاری از موارد، داده‌هایی که برای یک برنامه کاربردی جمع‌آوری می‌شوند، به شدت همپوشانی دارند (بناتی و پورنارس، ۲۰۱۸) و به همین دلیل می‌توانند در هنگام انتقال به چاهک، ترکیب شده یا به طور مشترک پردازش شوند. برای مثال، خواندن حسگرهای چندگانه با یک رویداد فیزیکی یکسانی همراه است. چنین پروسه جمع‌آوری داده‌ها می‌تواند کل پیام‌های ارسال شده توسط لینک‌های گران قیمت بی‌سیم را کاهش دهد که تأثیر قابل توجهی بر مصرف انرژی و همچنین بهره‌وری شبکه عمومی دارد. از سوی دیگر، بسته‌های غیرمجاز ممکن است به سادگی از نقطه نظر پردازش جمع نشوند، مثلاً این رویکرد برای محاسبه میانگین دمای و خواندن رطوبت معنی ندارد. بنابراین، یک مسئله مهم در جمع‌آوری داده‌ها، تعیین یک جریان اطلاعات بهینه شده و توپولوژی ارتباطی است تا به طور مؤثر مسیر داده‌های متقابل به گره‌های پردازش در نظر گرفته شده در شبکه فراهم شود.

اینترنت اشیاء نوعی تغییر رویکرد از روش‌های سنتی جمع‌آوری داده‌ها به روش جدید جمع‌آوری داده‌ها و بازیابی محتوا را فراهم می‌کند. این تغییر می‌تواند چندین مزیت همچون بهره‌وری انرژی، پاسخ سریع سیستم، طول عمر طولانی شبکه و غیره را به همراه

داشته باشد و راه‌حلی برای حل مشکل انفجار اطلاعات (بندیوپدیای و سن، ۲۰۱۱) برای شبکه آینده فراهم می‌کند. در (کاسترو، کاسترو و تیمیس، ۲۰۰۲) یک تابع هدف چندگانه پیشنهاد شده است تا تجمیع داده‌های بهینه در شبکه با هدف کاهش تأخیر، تعادل بار و گسترش طول عمر شبکه وجود داشته باشد. بر این اساس، هر گره می‌تواند استراتژی مسیریابی خود را بر اساس الگوهای ترافیکی همسایه و دسترسی انرژی گره‌های همسایه اصلاح کند. علاوه بر این، یک مکانیزم انتخاب نامزد مسیریابی برای جلوگیری از حلقه‌های ارتباطی توسعه داده شد و هزینه انتقال سیگنال‌های پیام محلی برای کنترل گره و منابع محدود می‌شود. بلوک دیاگرام روش پیشنهادی به‌صورت شکل (۱) خواهد بود. ابتدا داده‌ها خوانده می‌شود، سپس گره‌های شبکه تشکیل می‌شوند. پارامترهای الگوریتم سیستم ایمنی مصنوعی مثل آنتی‌بادی - آنتی‌ژن و میزان قرابت را تعریف می‌شود، سپس تابع هدف برای هر محتوای ترافیک از بین گره‌های همسایه اجرا می‌شود تا مناسب‌ترین گره بعدی را پیدا کند و مصرف انرژی شبکه را کمینه کند. در این مرحله، الگوریتم سیستم ایمنی مصنوعی برای به‌روزرسانی مسیر شبکه استفاده می‌شود تا بهترین پاسخ (بهترین مسیر) را برای ارسال اطلاعات بیابد و در نهایت داده‌ها ارسال شود.



شکل ۱. بلوک دیاگرام روش پیشنهادی

برنامه‌های نظارت برای هدف جمع‌آوری اطلاعات در نظر گرفته می‌شود. تمام بسته‌های داده مرتبط با یک پردازش مشابه، به عنوان یک بسته از همان محتوا در نظر گرفته می‌شود که می‌تواند توسط یکی از گره‌ها پردازش شود. به عنوان مثال، یک نوع داده (خواندن درجه حرارت) در یک ساختمان جمع‌آوری می‌شود و محتوای لازم برای یک برنامه را که به دمای متوسط ساختمان نیاز دارد را فراهم می‌کند. برای سادگی، فرض می‌شود که هر برنامه در حال اجرا در شبکه، تنها یک هدف پردازش واحد دارد، اما برنامه‌های متعدد می‌تواند وجود داشته باشد. تعداد کل برنامه‌های کاربردی $K = \{ak \mid k = 1، 2، 3، \ldots\}$ دارای نرخ ورودی پوایسون λ است، اما با طول اجرای مختلف $T = \{tk \mid k = 1، 2، 3، \ldots\}$ و داده‌های ترافیکی ترافیک ناهمگن. تابع تجمعی داده‌های مختلف را می‌توان با توجه به فرایندهای تجمعی از دست رفته یا تلفات اعمال کرد (آلوارادو و همکاران، ۲۰۰۳).

برای هر گره با تابع پردازش یک مدل عمومی جمع‌آوری داده در ادامه تعریف شده است:

رابطه ۱) $$R_i^{out} = \omega_s * R_i^{in}$$

$$0 < \omega_s \leq 1$$

که در آن R_i^{in} و R_i^{out} به ترتیب، نرخ ترافیک ورودی و خروجی را نشان می‌دهند. جمع‌آوری داده یا میزان فشرده‌سازی را نشان می‌دهد که بستگی به تابع پردازش s دارد. اگر $\omega s = 1$، به این معنی است که محتوای کنونی توسط تابع s قابل پردازش نیست. ωs نیز می‌تواند متغیر و وابسته به تابع پردازش باشد. به عنوان مثال، ممکن است همبستگی قابل توجهی از جریان داده‌ها شامل گزارش‌های داده‌ای از میانگین یا ماکسیمم خواندن برای نظارت بر برنامه‌های کاربردی وجود داشته باشد که می‌تواند پیام‌های چندین ورودی را به یک پیام خروجی تنها تبدیل کند. در چنین مواردی، بسته به تعداد کل پیام دریافت شده (فرض M) بر روی گره تجمعی، ωs می‌تواند M1 باشد. با این وجود، ما فرض می‌کنیم که تنها پیام‌هایی از برنامه‌های مشابه می‌توانند جمع شوند. به دلایلی، داده‌ها با نوع مختلف ممکن است به راحتی پردازش نشوند یا فقط در بعضی موارد امکان‌پذیر نباشد.

انتخاب بهینه‌ترین مسیرها با استفاده از الگوریتم ایمنی مصنوعی

CCR یک فرآیند توزیع شده است، زمانی که یک برنامه به دروازه منتقل می‌شود، به طور پیش فرض از ساختار مسیریابی اولیه برای جمع‌آوری داده‌ها استفاده می‌شود. تمرکز فاز بعدی رویکرد معرفی شده بر روی بهینه‌سازی این ساختار مسیریابی است. هر گره دارای یک احتمال pt است تا رله حرارتی بعدی خود را با بهینه‌سازی تابع هدف F پیدا کند. احتمال pt بدون نیاز به اطلاعات کلی از شبکه بصورت مستقل با استفاده از تابع زیر محاسبه می‌شود:

$$p_t = \min\left(\left(\sum_{t_1}^{t}|\Delta_k|+1\right)p_0, 1\right)$$ رابطه ۲)

که در آن Δ_k تغییرات محتوای k است. همچین p_0 پارامتر از پیش تعیین شده برای شبکه مورد نظر است. تابع هدف F بر روی گره هدف i اجرا می‌شود تا برای هر محتوا ترافیک k از میان نامزدهای همسایه، مناسبترین گره hop بعدی j را پیدا کند. از آنجا که ترافیک با نوع محتوای آن تمایز دارد، گره هدف، یک ورودی مسیریابی جداگانه برای هر محتوی K را حفظ می‌کند و آن را با اجرای تابع هدف به روز می‌کند. جریان تابع سیستم برای اجرای F بر اساس p_t نشان داده شده است (صفری، ۱۳۹۴).

$$F(k) = \max_{j\in N}\left(\tilde{g}_j^k - g_j^k + \beta\frac{\tilde{l}_j^k - l_{j^*}}{\tilde{l}_j^k} + \varepsilon_j^k\right)$$ رابطه ۳)

ترم اول در رابطه فوق، $\tilde{g}_j^k - g_j^k$ کاهش داده ارتباطی نرمال شده داده را با فرایند جمع‌آوری محاسبه می‌شود که بهره فرایند حاشیه‌ای نامیده می‌شود. ترم دوم $\frac{\tilde{l}_j^k - l_{j^*}}{\tilde{l}_j^k}$ برآورد هزینه طول عمر شبکه محلی است؛ در حالی که β پارامتر تنظیم برای ارائه وزن بین دو پارامتر می‌باشد. و در نهایت، ε_j^k یک پارامتر پاداش است. پارامتر جمع آوری مربوط به هر محتوا با استفاده از حجم ترافیک خارج شده و داخل شده از گره j با استفاده معادله زیر تعریف می‌شود:

$$g_j^k = \frac{\sum_{k\in K} R_j^{in}(k) - \sum_{k\in K} R_j^{out}(k)}{\sum_{k\in K} R_j^{in}(k)}$$ رابطه ۴)

این معادله جمع‌آوری اطلاعات وارد شده و خارج شده را به هر گره نشان می‌دهد. از طرفی عمر بهره‌وری $\frac{\tilde{l}_j^k - l_{j^*}}{\tilde{l}_j^k}$ مبتنی کمترین عمر بهره‌وری هر گره در میان N همسایگی با استفاده از معادله زیر تعریف می‌شود.

رابطه ۵) $$l = \min\left(\frac{E_i}{e_i}, \min_{j \in N}\left(\frac{E_j}{e_j}\right)\right)$$

که در آن E انرژی باتری هر گره است و e_i شامل انرژی مصرفی شامل پردازش، ارسال و دریافت است. انرژی مصرفی هر گره به مسیری که جهت ارسال انتخاب می‌کند وابسته است که با استفاده از معادله زیر تعریف می‌شود:

رابطه ۶) $$e_j^k = U^k(e_r + e_p) + ETX_j^{nextHop} U_p^k e_t$$

که در آن e_p و e_r انرژی مصرفی دریافت و پردازش هر بیت از محتوای k است. U_p^k کل اطلاعاتی بعد از پردازش از مستر i به j ارسال می‌شود. در نهایت مهمترین پارامتر در بهینه‌سازی انرژی مصرفی هر شبکه مقدار ETX است. بنا به تعریف انرژی انتظاری[1] حسگرهای مصرفی در شبکه است. این مقدار توسط انرژی مصرفی در فضای آزاد امواج الکترومغناطیس تعریف می‌شود:

رابطه ۷) $$ETX_i^j = \begin{cases} E_0 + E_{fs}\left(d_i^j\right)^2 & d \le d_0 \\ E_0 + E_p\left(d_i^j\right)^4 & d_0 \le d \end{cases}$$

که در آن E_0 به عنوان انرژی الکترونیکی شامل کدگذاری دیجیتالی، مدولاسیون، فیلتر کردن و پخش سیگنال و از طرفی E_{fs} و E_p پارامتر تقویت‌کنندگی برای مسیرهای کوتاه و بلند است. همچنین که در آن فاصله قطع با استفاده از $d_0 = E_{fs}/E_p$ تعریف می‌شود(یعقوبی و ذوقی، ۱۳۹۴). همچنین در محدودیت اینترنت در حفظ داده‌های شبکه و دور از گره‌های مخرب کمک می‌کند. این عامل با استفاده از رابطه (۸) تخمین زده می‌شود:

رابطه ۸) $$CV_i = \frac{CC_{Si} - IC_{Si}}{CC_{Si} + IC_{Si}}, -1 \le C_i \le 1$$

[1] Expected Energy count

در این رابطه CV_i مقدار ثبات و پایداری گره iام، CC_{Si} تعداد حسگرهای سازگار با گره iام و IC_{Si} تعداد حسگرهای ناسازگار و متناقض با گره iام هستند و نگهداری اطلاعات مربوط به محدودیت اینترنت به نسبت ارتباطی برای نظم گره است که توسط این عامل نشان داد:

$$SR_i = \frac{SS_i + SF_i}{SS_i - SF_i}$$ رابطه ۹)

در این رابطه SR_i مقدار ارتباطی برای گره iام، SS_i تعداد حسگرهای که موفق به ارتباط با گره iام شدند و SF_i تعداد حسگرهای ناسازگار و متناقض که در ارتباط با گره iام با شکست مواجه شدند (ژو و لی، ۲۰۱۴).

در ادامه از الگوریتم ایمنی مصنوعی برای بهینه‌سازی تابع هدف استفاده می‌شود و به نحوه اعمال این الگوریتم به رابطه ۳ پرداخته خواهد شد.

مقدمه سازی

در این مرحله جمعیت تصادفی از سلول‌های ایمنی تشکیل می‌شوند.

حلقه جست جو

نخست قرابت سلول‌های تدافعی جدید مورد ارزیابی قرار می‌گیرند سپس سلول‌های ایمنی با قرابت بیشتر نسبت به آنتی‌ژن‌ها انتخاب می‌شوند. در ادامه سلول‌های ایمنی تکثیر می‌شوند. تشخیص آنتی‌ژن و قرابت بیشتر با آن یعنی تکثیر بیشتر سلول تدافعی متناظر با آن سلول‌های با قرابت کمتر تحت عملگر جهش تغییر ساختاری پیدا می‌کنند. میزان اعمال عملگر جهش با میزان قرابت نسبت عکس دارد.

بستن حلقه

در نهایت اگر شرط مورد نظر محقق شد حلقه همگرا و بسته می‌شود.

مسیریابی توسط الگوریتم مصنوعی

در قسمت قبل چگونگی و مراحل ایمنی مصنوعی تشریح شد در این قسمت کاربرد ایمنی مصنوعی در مسیریابی تشریح می‌شود. همانگونه در بخش قبل تشریح شد اولین قسمت مرحله شروع فرآیند است.

آنتی‌ژن و آنتی‌بادی

مسیرهای ممکن که هر گره می‌تواند داشته باشد. آنتی‌ژن‌هایی که در این مرحله ارائه شده‌اند مجموعه‌ای از آنتی ژن‌های مرحله قبل از نظر انرژی و مراحل آنتی‌ژن‌های دیگر هستند. آنتی‌بادی مطالعه انرژی و شرط‌های آن هر گره در شبکه بطوری که این ساختار همچنین وضعیت انرژی و مراحل مسیر را بررسی می‌کند. در این الگوریتم، آنتی بادی‌ها مسیرهایی هستند که به مقصد در جدول مسیریابی می‌رسند، در حالی که آنتی ژن مکانیسم است که دو شرایط را از جمله انرژی‌های مسیر و تعداد مسیر را تست می‌کند.

در این الگوریتم، آنتی بادی‌ها مسیرهایی هستند که به مقصد در جدول مسیریابی می‌رسند، در حالی که آنتی ژن مکانیسم است که دو شرایط را از جمله انرژی‌های مسیر و تعداد مسیر را تست می‌کند. هر بار از طریق مرحله جداسازی، یک آنتی بادی (مسیر) با یک آنتی ژن مقایسه می‌شود تا همه آنتی بادی‌ها مقایسه شود. سپس، بدترین مسیرها از لحاظ تعداد انرژی و هُپ، رد می‌شوند. در طی مقایسه آنتی‌ژن با آنتی‌بادی (مسیر) رد یا نگهداری می‌شود، هر آنتی‌بادی (مسیر) با یک آنتی‌ژن مقایسه می‌شود. اگر مقدار انرژی آنتی‌بادی (مسیر) کمتر از انرژی آستانه گره‌های متوسط باشد، رد می‌شود؛ در غیر این صورت، مقادیر وارد یک آرایه می‌شوند که از لحاظ تعداد مخالف‌ها (Opposite) مورد تجزیه و تحلیل قرار می‌گیرد. انرژی آستانه با استفاده از معادله زیر محاسبه می‌شود:

$$E_{thershold} = \frac{e_i}{\max_i e}$$ رابطه ۱۰)

بطوری که معادله (۷) گره‌های متوسط هر مسیر درحفظ حریم خصوصی داده‌گان است. تعداد آرایه‌ها بر مبنای تعداد آنتی‌بادی‌ها (مسیرها) در نظر گرفته می‌شوند. هر مسیری

که از مرحله قبل عبور می‌کند وارد آرایه می‌شود و آرایه بر اساس کل مسیرها تا مقصد شکل می‌گیرد. اگر تعداد مسیرها بیشتر از مسیرهای موجود در آرایه باشد، رد می‌شود، در غیر این صورت ممکن است یک مسیر با حداکثر تعداد جستجو جایگزین شده و آرایه مرتب گردد. این فرآیند پس از آن که همه مسیرها تست شده و در آرایه باقیمانده باقی می‌مانند، وارد مرحله تشخیص می‌شوند. شبه کد شروع فرآیند بصورت شکل ۲ بیان می‌شود.

```
Input: Antigen (Routs)
Procedure: Camparing Antigen with Antibody
If Energy (Node_i) < Threshold then
Delete (Route_i)
Else if
Array== Route_i
Array Sort order by hop count
Output: Array of Routs
```

شکل ۲. شبه کد مربوط شروع فرآیند

با این وجود، آرایه ایجاد شده ممکن است آرایه‌ای از بهترین مسیر نباشد و از این رو اگر لازم باشد جهش فوق انجام می‌شود. سپس بهترین آنتی‌بادی (مسیر مطلوب) انتخاب شده و در حافظه ایمنی نگهداری می‌شود که با استفاده از الگوریتم Clonal G در این کار انجام می‌شود (چین‌لانگ و چوآن‌چانگ، ۲۰۱۶).

قرابت

همانطور که در بخش قبل تشریح شد تابع هدف مورد نظر به منظر یافتن مسیر بهینه انرژی وابسته به فاصله تعریف شده است. از این رو از تابع انرژی تعریف شده در رابطه (۲) به عنوان تابع هدف در الگوریتم ایمنی مصنوعی استفاده می‌شود که بر این اساس حلقه آنتی‌ژن مبتنی بر تابع هدف تشکیل می‌شود به طوری که جمعیت تصادفی مسیرهای انتخاب می‌شود. در مطالعه حاضر مقدار قرابت بر اساس تابع هدف تعریف شده محاسبه می‌شود به طوری که مسیری انتخاب می‌شود که دارای بالاترین مقدار قرابت باشد. زمانی که مسیر با بالاترین مقدار قرابت انتخاب شد.

جهش

مقایسه مسیرها تحت عنوان انرژی توسط عملگر جهش انجام می‌گیرد اگر مسیر مورد نظر بر اساس شرط‌های تعریف شده توسط کاربرسازگار بود، آنگاه مسیریابی بدون جهش باقی می‌ماند. هرچند در این مطالعه شرطی که در مسیربابی باید محقق شود پیوستار بودن شبکه بدون هیچ گره مرده یا خوشه‌ای است از این رو جهش توسط الگوریتم اعمال می‌شود و انتخاب مسیر و قرابت از سرگرفته می‌شود تا با شرط تعریف شده در نهایت سازگار شود. مراحل مربوط به این بهینه‌سازی به صورت شکل ۳ قابل بیان است.

۱. شروع فرآنید با تولید جمعیت
۲. برای هر مسیر (آنتی ژن) حلقه زیر انجام شود
۱.۲ محاسبه مقدار قرابت رابطه ۲
۲.۲ انتخاب جمعیت یا گره مربوط به بالاترین مقدار قرابت
۳.۲ انجام جهش با نرخ انتخاب شده و اضافه به جمعیت
٤.۲ زخیره گرها با بالاترین نرخ قرابت
۵.۲ عوض کردن گره های با کمترین قرابت ممکن در hop بعدی
۳. ادامه حلقه تا زمانی که شرط پیوستار بودن محقق شود

شکل ۳. شبه کد Clonal G

در واقع، در اینجا جهش مسیرها را در شرایط معیار دیگری یعنی معیار انرژی مقایسه می‌کند که تابع فاصله است و این مسیر را با کوتاه‌ترین فاصله بین منبع و مقصد انتخاب می‌کند. سرانجام راه‌حل از مسیرهای باقیمانده در آخرین مرحله انتخاب می‌شود. در الگوریتم تمامی مسیرها موجود این عمل انجام می‌شود به طوری که در نهایت بهترین مسیر در حافظه، به عنوان بهترین مسیر برای انتقال داده معرفی می‌شوند. در نهایت، شبه کد اعمال انتخاب راه جدید یا جهش بصورت شکل ۴ بیان می‌شود.

برای همه مسیرها تا شرط محقق شود:

محاسبه قرابت با استفاده از رابطه ۲

اگر قرابت راه i ام > مقدار بیشه قرابیت

ذخیره مسیر در حافظه

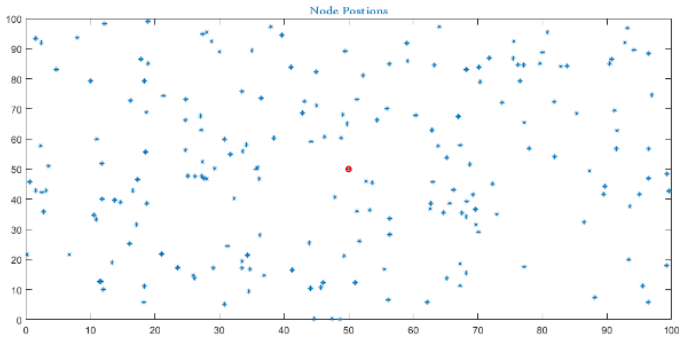
در غیر این صورت جهش:

تا زمانی که گراف یا شبکه به کلی و قرابت انجام گیرد متصل شود

شکل ٤. شبه کد جهش

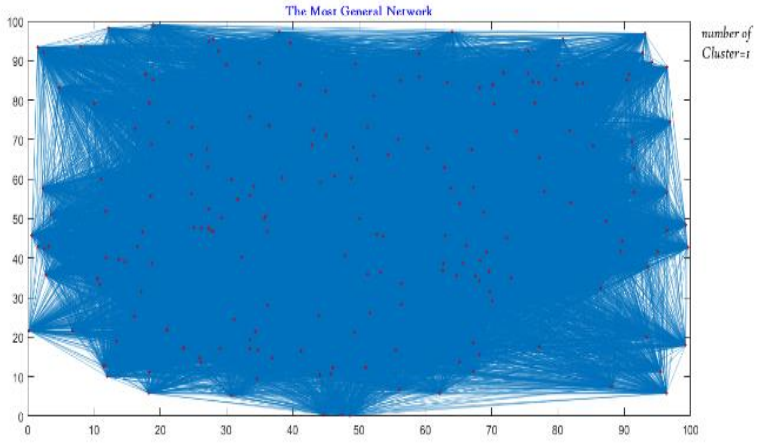
یافته‌های پژوهش

در در این مطالعه ۲۰۱ سنسور در فضای $100 * 100m^2$ بصورت تصادفی قرار داده‌ایم. مرکز شبکه به عنوان سرور دریافت اطلاعات دریافتی توسط حسگرهای اینترنت اشیاء در نقطه (۵۰ ۵۰) در نظر گرفته می‌شود. در ابتدا برای بدست آوردن انرژی مصرفی بهینه فرض می‌شود که هر حسگر بصورت ایده‌آل بدون از دست دادن اطلاعات با منبع انرژی (باتری) نامتناهی عمل می‌کند. مکان سنسورها در هر تکرار از شبیه‌سازی بصورت تصادفی انتخاب می‌شود. شکل (۵) تشکیل گره‌های سنسورها مبتنی بر اطلاعات اینترنت اشیاء را نشان می‌دهد.



شکل۵. مکان سنسورها

در قدم بعدی کلی‌ترین حالت شبکه را تشکیل می‌دهیم که هر گره به n-1 گره متصل می‌شود. شبکه مرکزگرا با نمایشی بسیار متراکم به صورت گرافیکی در نرم افزار متلب رسم شده است.. پر واضح است چنین ساختار شبکه‌ای از ترافیک بسیار در هر گره برخوردار است. این مسئله به خودی خود باعث می‌شود که اطلاعات به سختی پردازش انتقال و دریافت شود و ممکن است در حالت واقعی شبکه به دلیل حجم بالای ترافیک از دست خارج شود. از طرفی هم مصرف انرژی چنین شبکه‌ای بسیار بالاست.



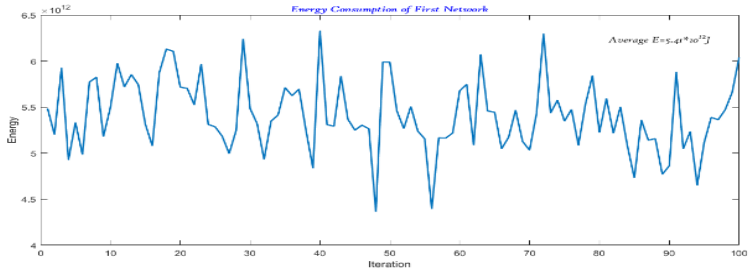
شکل ٦. کلی ترین شبکه برای ۲۰۰ گره

مقادیر مصرف انرژی پردازش انتقال و دریافت هر بیت انرژی در جدول ۱ به صورتی که در معادله (۶) معرفی شده انرژی مصرفی هر نقطه را نشان می‌دهد.

جدول ۱. مقادیر و نوع مصرف انرژی

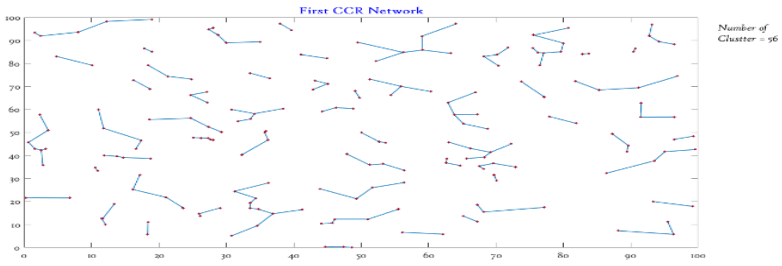
نوع مصرف انرژی	مقدار
انتقال	۹/۷۲
دریافت	۸/۲۲
پردازش	۰/۷٦۰

به دلیل این که مکان گره‌ها تصادفی انتخاب شده است با ۲۰۰ تکرار مصرف میانگین هر گره در هر تکرار در شکل زیر محاسبه شده است. پر واضح است این مقدار مصرف انرژی در شبکه بسیار بالاست. همان طور که قبلاً بیان شد مصرف انرژی به مکان گره سنسورها وابسته است چرا که مقادیر ETX به فاصله گره‌ها از هم وابسته است.



شکل ۷. میانگین مصرف انرژی در هر تکرار مقدار میانگین انرژی برار با μJ ۱۰^۱۲ × ۵.٤۱

در مطالعه انجام شده در مرجع (چین‌لانگ و چوآن‌چانگ، ۲۰۱٦) تابع هدفی را جهت کمینه کردن مصرف انرژی شبکه معرفی کردن به طوری که با استفاده از تابع هدف معرفی شده در معادله (۳) مصرف انرژی کمینه شود. شکل زیر شبکه بهینه شده توسط تابع هدف در معادله (۳) را نشان می‌دهد.

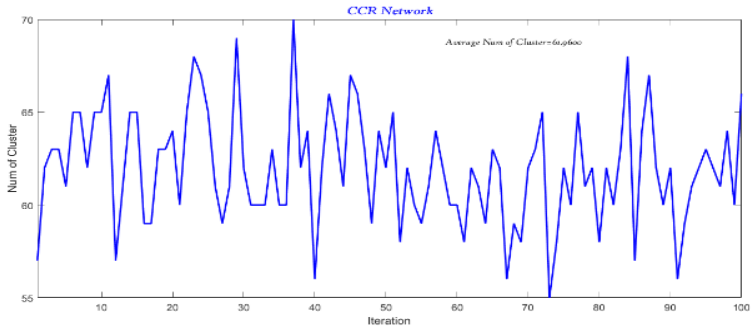


شکل ۸ . نمایش شبکه بی‌سیم اینترنت اشیا

شبکه بی‌سیم اینترنت اشیا با استفاده از تابع معرفی شده با ۵۶ خوشه تشکیل شده است. تابع هدف F بر روی گره هدف i اجرا می‌شود تا برای نامزدهای همسایه، مناسب‌ترین گره hop بعدی j را پیدا کند. اولین ویژگی که در این شبکه به چشم می‌خورد ناپیوستار بودن شبکه است که از انتقال اطلاعات در تمامی گره‌ها جلوگیری می‌کند. این ویژگی به

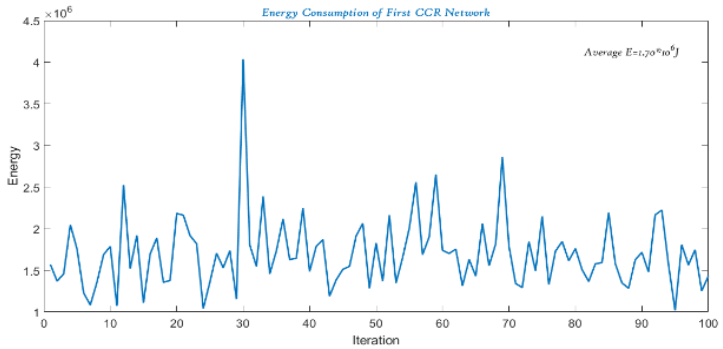
این دلیل است که تابع معرفی شده شامل شرط پیوستار بودن شبکه نیست. به عبارتی در شرط بهینه $\max(F)$ فقط گره‌ای را انتخاب می‌کند که شرط انرژی صدق کند. این ویژگی ارسال و دریافت اطلاعات را در مرکز و کل شبکه با مشکل مواجه می‌کند.

شکل زیر تعداد خوشه‌های تشکیل در ۱۰۰ تکرار را نشان می‌دهد. همان‌طور که شبیه‌سازی نشان می‌دهد، میانگین تعداد خوشه‌ها (که این خود شامل گره‌های مرده نیز می‌شود) در ۱۰۰ تکرار برابر با ۶۱/۹۶ است.



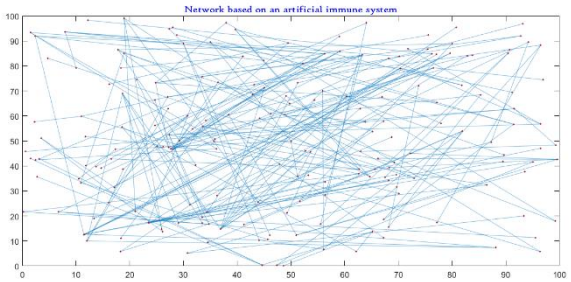
شکل ۹. تعداد خوشه های تشکیل شده در ۱۰۰ تکرار در شبکه بی‌سیم اینترنت اشیا

با این وجود انرژی مصرفی شبکه به شدت کاهش پیدا کرده است. انرژی مصرفی شبکه در ۱۰۰ تکرار در شکل (۱۰) نشان می‌دهد.



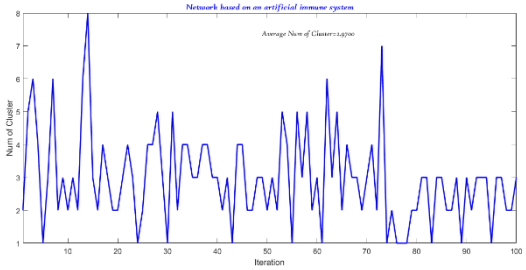
شکل ۱۰: مقادیر مصرف انرژی در شبکه بی‌سیم اینترنت اشیا

همانطور که بیان شـــد، الگوریتم ایمنی مصـــنوعی کاربردهای فراروانی دارد. در این مطالعه از تابع F به عنوان تابع هدف در الگوریتم مصـــنوعی جهت بهینه‌ســـازی اســـتفاده می‌شود. بر این اساس حلقه آنتی‌ژن مبتنی بر تابع هدف تشکیل می‌شود بطوری که جمعیت تصادفی مسیرها انتخاب می‌شود. در مطالعه حاضر مقدار قرابت بر اساس تابع هدف تعریف شده محاسبه می‌شود به طوری که مسیری انتخاب می‌شود که دارای بالاترین مقدار قرابت باشد. زمانی که مسیر با بالاترین مقدار قرابت انتخاب شد که بر اساس این تابع مناسب‌ترین گره را پیدا می‌کند. شکل زیر نمایش گراف شبکه مبتنی بر ایمنی مصنوعی است.



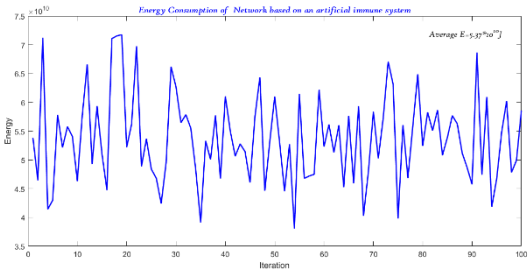
شکل ۱۱. شبکه مبتنی بر ایمنی مصنوعی

در قدم بعدی به بررسی شرط پیوستار بودن شبکه و مسیریابی مبتنی بر ایمنی مصنوعی می‌پردازیم. شکل زیر تعداد خوشه‌های تشکیل شده در ۱۰۰ تکرار را نشان می‌دهد.



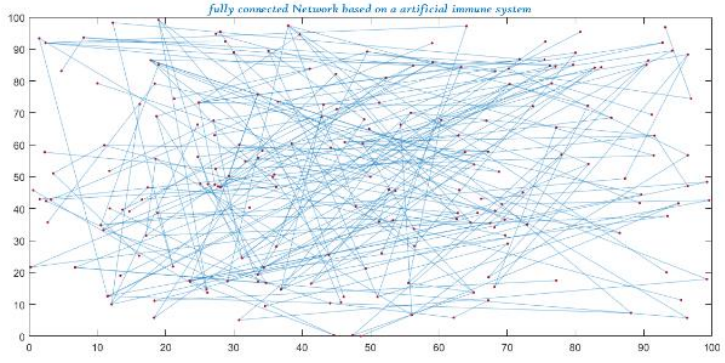
شکل ۱۲. تعداد خوشه‌های تشکیل شده توسط الگوریتم ایمنی مصنوعی در ۱۰۰ تکرار

در شکل ۱۳ مصرف انرژی شبکه در ۱۰۰ تکرار نشان داده شده است.



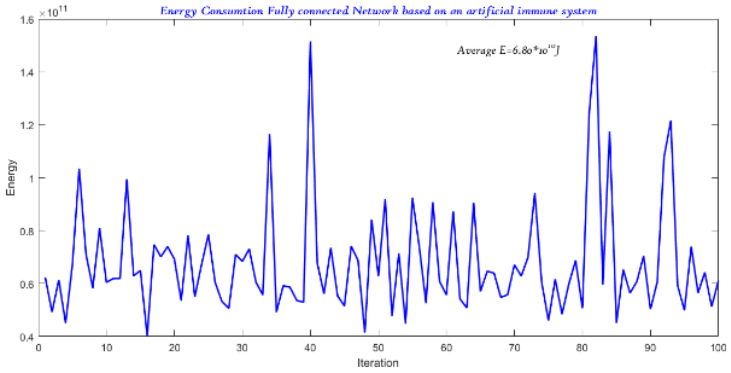
شکل ۱۳. انرژی مصرفی شبکه مبتنی بر ایمنی مصنوعی

از طرفی، الگوریتم ایمنی مصنوعی یک نوع الگوریتم یادگیرنده است به طوری که با استفاده از مسیرهای قبلی مسیر جدیدی را تولید می‌کند. این مزیت بسیار با اهمیتی است چرا که باعث بروزرسانی شبکه در موارد مختلف می‌شود. برای نمونه اگر یکی از سنسورها از مسیر خارج شود یا توسط عوامل خارجی تهدید شود این نوع مسیریابی هوشمند باعث می‌شود که تهدید یا سنسورهای خاموش شده را از کل شبکه خارج کند. در این مطالعه ما تولید مسیرهای مختلف را مبتنی بر تابع هدف مصرف انرژی تا زمانی ادامه می‌دهیم که شرط پیوستار بودن کل شبکه حاکم باشد. شکل (۱۴) شبکه مبتنی بر ایمنی مصنوعی را نشان می‌دهد.



شکل ۱٤. نمایش شبکه مبتنی بر الگوریتم ایمنی مصنوعی

این مسئله باعث افزایش جزئی انرژی شبکه می‌شود. شکل زیر انرژی مصرفی شبکه در مسیریابی مبتنی بر الگوریتم ایمنی مصنوعی را نشان می‌دهد.



شکل ۱۵. مصرف انرژی شبکه پیوستار مبتنی بر مسیر یابی الگوریتم ایمنی مصنوعی

و در نهایت در جدول ۲ میانگین انرژی تمامی پروتکل‌های پیشنهادی به صورت خلاصه نشان داده شده است.

جدول ۲. میانگین انرژی پروتکل‌های پیشنهادی

کلی‌ترین شبکه	$5.64 * 10^6 J$
بی‌سیم اینترنت اشیاء	$1.74\ J$
اولین ایمنی مصنوعی	$5.64 * 10^4 J$
ایمنی مصنوعی	$6.8\ 1 * 10^4 J$

نتیجه‌گیری و پیشنهادها

در این مطالعه از محدودیت اینترنت جهت تشکیل تابع هدف برای یافتن نقاط بهینه و مسیریابی استفاده شد، با این حال مدل برنامه نشان می‌دهد که تعداد گره‌های مرده بسیار زیاد است و شبکه پیوستار نیست. این موضوع باعث می‌شود کل اطلاعات در شبکه منتقل نشوند. از این رو، از الگوریتم ایمنی مصنوعی برای حل این مشکل استفاده شد که باعث بالا رفتن انرژی میانگین شبکه شد. در نهایت، الگوریتم ایمنی مصنوعی نشان داد که شبکه پیوستار تشکیل می‌شود و گره‌های مرده از بین خواهند رفت. با این وجود، انرژی کل شبکه بالا می‌رود. در این پژوهش یک چارچوب جدید برای مسیریابی بهینه در شبکه‌های اینترنت اشیاء با استفاده از الگوریتم سیستم ایمنی مصنوعی ارائه شده است. هدف روش

پیشنهادی یافتن یک مسیر بهینه بود که از میزان شایستگی خوبی برخوردار باشد. الگوریتم پیشنهادی با پارامترهای مختلف پیاده‌سازی شده و نمودارهای مربوط به آن ارائه شد. الگوریتم سیستم ایمنی مصنوعی برای حل مسائل بهینه‌سازی، جواب قطعی نمی‌دهد و جوابی نزدیک به بهینه را پیدا می‌کند. برای نشان دادن عملکرد هر الگوریتم، مقایسه آن با الگوریتم‌های قبلی امری ضروری است؛ بنابراین نتایج حاصل از این پژوهش با الگوریتم‌های بهینه‌سازی ازدحام ذرات، ژنتیک و کرم شب‌تاب و پژوهش‌های لین و همکارانش در سال ۲۰۱۷، باساران و همکارانش در سال ۲۰۱۶ مقایسه گردید. همچنین رویکرد پیشنهادی با دو پروتکل MAODV-with-GA، MAODV-without-GA از نظر توان عملیاتی و تعداد بسته‌ها مقایسه شد و نتایج مناسب‌تری نسبت به سایر روش‌ها از خود نشان داد. زمان پاسخ الگوریتم سیستم ایمنی مصنوعی در مقایسه با الگوریتم‌های مورد مقایسه کمتر است و همچنین الگوریتم سیستم ایمنی مصنوعی از پایداری خوبی برخوردار می‌باشد؛ به طوری که جواب حاصل از روش پیشنهادی نزدیک به جواب بهینه خواهد بود. با توجه به نمودارهای همگرایی، مشاهده شد که الگوریتم سیستم ایمنی مصنوعی از همگرایی خوبی برخوردار است. همچنین با توجه به نمودارهای میزان پایداری، برای الگوریتم سیستم ایمنی مصنوعی با تعداد مسیرهای مختلف، آزمایش جواب واحدی به دست آورده است، بنابراین پایداری الگوریتم سیستم ایمنی مصنوعی بهینه بوده است.

به منظور کارهای آتی پیشنهاد می‌شود روی ارائه روشی جدید برای مکانیسم مسیریابی امن در اینترنت اشیاء با استفاده از ایمنی مصنوعی یا با استفاده از پروتکل بی‌سیم اینترنت اشیاء بهبود یافته یا تعمیم یافته جهت انرژی بهنیه کار شود.

منابع

- Akhtari, M., (1394). Analyzing Security Concerns in IoT. IOT First International Conference on Accounting and Management in the Third Millennium, Rasht, Pioneer of Modern Research.
- Aloudat, A., Katina, M., Chen, X., & Al-Debei, M. M. (2014). Social acceptance of location-based mobile government services for emergency management. Telematics and Informatics, 31, 153e171.
- Alvarado, C., Teevan, J., Ackerman, M. S., & Karger, D. (2003). Surviving the information explosion: How people find their electronic information.
- Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. MIS Quarterly, 33(2), 339e370.
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.
- Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless personal communications, 58(1), 49-69.
- Bandyopadhyay, S., & Sen, J. (2011). Internet of Things: applications and challenges in technology and standardization. Journal of Wireless Personal Communications,58(1), 49e69.
- Bandyopadhyay, S., Balamuralidhar, P., & Pal, A. (2013). Interoperation among IoT standards. Journal of ICT Standardization, 1(2), 253-270.
- Bennati, S., & Pournaras, E. (2018). Privacy-enhancing aggregation of Internet of Things data via sensors grouping. Sustainable cities and society, 39, 387-400.
- Castro, L. N., De Castro, L. N., & Timmis, J. (2002). Artificial immune systems: a new computational intelligence approach. Springer Science & Business Media.
- Chin-Lung Hsu a, Judy Chuan-Chuan Lin, (2016) An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives, Computers in Human Behavior 62 516e527.
- Dzhokam, A., (1394), New Strategies for the Oil and Gas Industry in the Light of the Internet of Things. International Conference on Research in Science and Technology, Tehran, Karine Institute of Excellence.
- E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, In-network aggregation techniques for wireless sensor networks: a survey, IEEE Wirel. Commun. 14 (2) (2007) 70–87, doi: 10.1109/MWC.2007.358967.
- Fesharaki Esfahani, A., and Khorsand Absolute Isfahani, R., et al. (1394). Investigating the challenges, classifying and comparing operating systems for IoT. First National Conference on New Ideas in Computer Engineering, Shahrekord Islamic Azad University, Shahrekord Branch.
- Javier.L, Ruben RiosaFeng Bao Guilin Wang (2017), Evolving privacy: From sensors to the Internet of Things, Future Generation Computer Systems Volume 75, October 2017, Pages 46-57.
- Kumar, P. M., & Gandhi, U. D. (2018). A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. Computers & Electrical Engineering, 65, 222-235.
- Mashayekhi, M., (1394). The future of IoT applications in intelligent transportation system management. National Conference on the Third Millennium and Humanities, Shiraz, Iran Modern Education Development Center (Methana).
- Masouleh, M. F., Kazemi, M. A. A., Alborzi, M., & Eshlaghy, A. T. (2017). Identification of electrocardiogram signals using internet of things based on combinatory classification. International Journal of Modeling, Simulation, and Scientific Computing, 8(03), 1750035.
- Rebouças Filho, P. P., Gomes, S. L., e Nascimento, N. M. M., Medeiros, C. M., Outay, F., & de Albuquerque, V. H. C. (2019). Energy production predication via Internet of Thing based machine learning system. Future Generation Computer Systems.
- Safari, M., (1394). Security and privacy concerns in the Internet of Things. The First National Conference on Computer, Islamic Information and Communication Technology of Iran, Qom, Soroush Hekmat Mortazavi Islamic Studies and Research Center
- Sarkhosh, R., Razvani, M., & Hajjabian, M. (1394). Modern architecture for mobile RFID systems in IoT. International Conference on Applied Research in Information Technology, Computer and Telecommunication, Torbat Heydariyeh, Khorasan Razavi Telecommunication Company.

– Turkmani, S., and Shahrokhi, H. (1394). The Challenges and Threats of the Internet of Things. International Conference on Applied Research in Information Technology, Computer and Telecommunication, Torbat Heydariyeh, Khorasan Razavi Telecommunication Company.
– Yaghoubi, M., and Zoghi, M.S. (1394). Emergency-Based Health Care System Model of IoT. International Conference on Research in Science and Technology, Tehran, Karine Institute of Excellence.
– Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. Computers in Human Behavior.
– Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: threats and challenges. Security and Communication Networks, 7(12), 2728e2742.

استناد به این مقاله: شناسه دیجیتال (DOI): 10.22091/jemsc.2019.1297

فریدی ماسوله، مرضیه؛ هارون‌آبادی، علی؛ صیاد، عسل. (۱۳۹۷). «بهبود حفظ حریم خصوصی داده‌گان در اینترنت اشیاء با در نظر گرفتن محدودیت اینترنت به کمک سیستم ایمنی مصنوعی». *مدیریت مهندسی و رایانش نرم*، ۸ (۱)، ۱۲۳-۱۵۱.