تامین جامعیت داده‌های تولید شده توسط اینترنت اشیا در حوزه سلامت هوشمند

محمد همتی زاده[۱]، فریدون شمس[۲]

۱ - دانشجوی کارشناسی ارشد فناوری اطلاعات - دانشکده مهندسی و علوم کامپیوتر- دانشگاه شهید بهشتی-تهران-ایران

m.hematizadeh@mail.sbu.ac.ir

۲ - دانشیار دانشکده مهندسی و علوم کامپیوتر -دانشگاه شهید بهشتی -تهران-ایران

f_shams@sbu.ac.ir

چکیده: اینترنت اشیاء می‌تواند برای کاربردهای بسیاری در حوزه‌های مختلف مورد استفاده قرار بگیرد. حوزه سلامت بعنوان یکی از اصلی‌ترین زمینه‌های کاربردی اینترنت اشیاء در آینده مطرح خواهد بود. با این حال، در صورت کاربردی شدن کامل اینترنت اشیاء در حوزه سلامت با چالش‌های زیادی مواجه خواهیم شد که یکی از این چالش‌ها جامعیت داده‌ها است. جامعیت داده به ما اطمینان می دهد که هر داده‌ای که توسط فرستنده ارسال می‌شود، همان داده بدون هیچ گونه تغییری توسط گیرنده دریافت می شود. در این مقاله یک پروتکل کنترل جامعیت داده مبتنی بر تئوری آشوب وابسته به فضا و زمان جهت بکارگیری در شبکه سلامت هوشمند ارائه شده است. در پروتکل پیشنهادی، فرآیند کنترل جامعیت در دو فاز اشتراک توالی و تبادل داده صورت می‌پذیرد. در فاز اشتراک توالی، طرفین ارتباط با تبادل امن اطلاعات هویتی و با استفاده از مدل آشوب وابسته به فضا و زمان، یک دنباله توالی مشترک را تولید نموده که براساس این دنباله توالی، زمان ارسال بسته‌های اعتبارسنجی در فاز تبادل داده مشخص خواهد شد. عملکرد روش پیشنهادی از جنبه‌های مختلف مورد ارزیابی قرار گرفته و کارایی آن با پروتکل سنتی کنترل جامعیت داده مقایسه شده است. کاهش پیچیدگی زمانی، کاهش سربار بسته و کاهش انرژی مصرفی نسبت به پروتکل سنتی کنترل جامعیت داده از مزایای روش پیشنهادی محسوب می‌شوند. همچنین نتایج حاصل نشان می‌دهد که روش پیشنهادی در برابر انواع حملات ایمن بوده و می‌تواند بعنوان یک سیستم کنترل جامعیت کارآمد در کاربردهای واقعی مورد استفاده قرار گیرد.

واژه های کلیدی: اینترنت اشیاء، جامعیت داده، شبکه سلامت هوشمند، تئوری آشوب وابسته به فضاوزمان.

تاریخ ارسال مقاله: ۹۹/۰۴/۰۹

تاریخ پذیرش مقاله: ۹۹/۰۶/۲۹

نام نویسنده مسئول: محمد همتی زاده

۱- مقدمه

فناوری اینترنت اشیاء[1] با استفاده از ابزارهای اطلاعاتی، تجهیزات هوشمند ساز نظیر RFID ها[2] شبکه‌های حسگر بی‌سیم و غیره ایجاد می‌شود و با استفاده از میان‌افزارها، بسترهای نرم‌افزاری تحت وب و با تکیه بر رایانش ابری با چالش‌های موجود در کاربردهای مختلف مواجه می‌شود که این امر منتج به تولید حجم بسیار زیادی داده جهت ذخیره، پردازش و ارائه می‌شود. انعطاف پذیری و کارایی بالا در این معماری موجب شده است که اینترنت اشیاء برای استفاده در حوزه سلامت سازگاری مناسبی داشته و در نتیجه شبکه سلامت هوشمند مبتنی بر ساختار اینترنت اشیاء شکل گیرد. یکی از اساسی‌ترین نیازمندی‌ها در شبکه سلامت هوشمند، اطمینان از عدم تغییر ناخواسته و غیرمجاز در حجم عظیم داده‌های تولید شده توسط آن است. این نیازمندی جامعیت داده نامیده می‌شود. جامعیت داده در شبکه سلامت هوشمند از اهمیت بالاتری نسبت به سایر کاربردهای اینترنت اشیاء برخوردار است. چرا که در شبکه سلامت هوشمند، سنسورها و اشیاء موجود در شبکه اغلب علائم حیاتی بیماران و داده‌های اورژانسی (مانند: ضربان قلب، بروز تشنجات صرعی، وقوع یک رویداد اورژانسی در مراکز درمانی و ...) را ردوبدل می‌کنند. در اغلب موارد، بروز کوچکترین تغییرات در این داده ممکن است خسارات جانی و مالی جبران ناپذیری را موجب گردد [۱]. علاوه‌بر این، ماهیت اینترنت اشیاء و حجم بزرگ داده‌های تولید شده در آن موجب شده است که لزوم توجه به جامعیت داده بیش از پیش احساس گردد. زیرا، از طرفی داده‌های مبادله شده توسط اشیاء دارای تنوع زیادی بوده و اشیاء ممکن است طیف وسیعی از داده‌ها را مبادله کنند (تصویر، اسناد متنی، اعداد و ...) و از طرفی دیگر، اغلب داده‌های درحال جریان در اینترنت اشیاء غیرساخت‌یافته[3] می‌باشند. کنترل اصالت این حجم وسیع از داده‌های متنوع و فاقد ساختار به منظور تضمین صحت عملکرد شبکه و قابلیت اعتماد آن از ضروریات خواهد بود. براین اساس، تاکنون تکنیک‌های متعددی به منظور تامین جامعیت داده در اینترنت اشیاء ارائه شده‌اند. بررسی تحقیقات انجام شده اخیر نشان می‌دهد که برای استفاده از این روش‌ها در شبکه‌های هوشمند با حداقل یکی از چالش‌های زیر مواجه خواهیم بود [۲]:

برخی از این تکنیک‌ها به دلیل محدودیت حوزه کاربرد، فقط برای یک نوع داده کاربرد دارند، در حالی که در شبکه سلامت هوشمند انواع داده‌ها از قبیل متن، عدد و تصویر مبادله می‌شود، بنابراین برای استفاده در شبکه‌های سلامت هوشمند کارایی ندارند.

دستگاه‌های استفاده شده در اینترنت اشیاء نسبت به اینترنت سنتی از نظر قدرت پردازنده، حافظه و توان باتری دارای محدودیت هستند، لذا نمی‌توان از روش‌های استفاده کرد که پیچیدگی محاسباتی بالای دارند. پیچیدگی محاسباتی بالا در برخی از این تکنیک‌ها، توانایی بکارگیری آن‌ها در سناریوهای بلادرنگ را با مشکل مواجه می‌کند.

در برخی از این تکنیک‌ها از سیستم حسابرس ثالث به عنوان کنترل کننده جامعیت داده استفاده شده است، که اعتماد به این سیستم‌ها خود یک چالش است، در واقع این روش‌ها به جای حل مسئله اصلی آمده‌اند یک مسئله را با مسئله دیگر جایگزین کرده‌اند.

لذا استفاده از این تکنیک‌ها در برخی سناریوهای عملیاتی شبکه سلامت هوشمند ناکارآمد خواهد بود.

یک حسگر ضربان قلب مانند A در شبکه سلامت هوشمند را درنظر بگیرید که درحال گزارش علائم حیاتی بیمار به رایانه لوحی پزشک معالج B است. این دو شیء، در بازه‌های زمانی منظم و کوتاه به مبادله اطلاعات می‌پردازند. فرض می‌کنیم که شیء A مقدار ۸۹ (مقدار دودویی ۰۱۰۱۱۰۰۱) را بعنوان ضربان قلب بیمار به شیء B ارسال می‌کند. اگر پیش از دریافت داده توسط شیء B بیت ششم این پیام معکوس گردد (به دلایلی مانند نویز محیط یا عملیات خرابکارانه مهاجمین)، مقدار دریافتی توسط شیء B برای ضربان قلب بیمار برابر با ۱۲۱ خواهد بود که دارای اختلاف بسیار زیادی با مقدار واقعی آن است. واضح است که در این شرایط، تکنیک‌های هشینگ داده و فراداده نمی‌توانند این عدم جامعیت را شناسایی کنند؛ زیرا این تکنیک‌ها به کاربرد در حوزه فایل محدود هستند. از طرفی، تکنیک‌های مبتنی بر رمزنگاری از پیچیدگی محاسباتی بالایی برخوردار بوده و برای تجهیزات دارای توان محاسباتی محدود کارایی ندارند. دو تکنیک رایج دیگر برای کنترل جامعیت داده مفروض، امضای دیجیتال و بلوک‌های زنجیره‌ای می‌باشند. تکنیک امضای دیجیتال از طریق یک کنترلگر مرکزی عمل بررسی جامعیت را انجام می‌دهند. در این شرایط، اگر تحریف داده توسط حملات مردمیانی[4] و درست

[1] Internet Of Things (IoT)

[2] Radio Frequency IDentification

[3] Unstructured

[4] Man in the middle

پیش از تحویل داده به شیء B صورت گرفته باشد، تکنیک ذکر شده نیز قادر به شناسایی عدم جامعیت داده نخواهند بود. از طرفی روش‌های مبتنی بر بلوک‌های زنجیره‌ای اگر چه می‌توانند جامعیت داده در این شرایط را کنترل کنند اما بکارگیری آن‌ها مستلزم پذیرش تاخیر و بار محاسباتی بالایی خواهد بود. از طرفی اغلب روش‌های تامین جامعیت، از یک سیستم حسابرس ثالث برای کنترل جامعیت استفاده نموده و فرض می‌کنند که این سیستم کاملا محافظت شده است. در واقع این دسته از راهکارها، مسئله تامین جامعیت را به مسئله تامین امنیت حسابرس ثالث وابسته می‌کنند و این خود یک نارسایی در تامین اطمینان عملکرد سیستم خواهد بود.

این مشکلات و محدودیت‌ها موجب شده است که لزوم ارائه یک روش تامین جامعیت داده در شبکه‌های سلامت هوشمند بیش از پیش احساس گردد. لذا ارائه یک راهکار به منظور رفع مشکلات ذکر شده از اولویت‌های تحقیقاتی در حوزه شبکه سلامت هوشمند خواهد بود. در این مقاله، یک راهکار کارآمد به منظور تامین جامعیت داده در شبکه سلامت هوشمند ارائه شده است. این روش، از یک تابع درهم‌سازی مبتنی بر دنباله آشوبناک برای تامین امنیت تبادل اطلاعات بین اشیاء استفاده می‌کند. عدم وابستگی عملکرد الگوریتم پیشنهادی به نوع داده درحال تبادل، پیچیدگی محاسباتی پایین و قابلیت کنترل جامعیت بصورت نظیربه‌نظیر از مزایای روش پیشنهادی است که در این مقاله مورد بحث قرار خواهند گرفت.

محافظت از جامعیت داده در IoT، به توانایی ایجاد قابلیت اطمینان از داده در زمینه جعل یا تغییر آن اشاره دارد. به معنای وسیع‌تر، از تکنیک‌های جامعیت داده می‌توان برای محافظت و تأیید صحت داده در زمینه‌های زیر استفاده نمود: (۱) داده تولید شده توسط یک دستگاه، (۲) نرم افزار نصب شده بر روی یک دستگاه و (۳) داده های ذخیره شده (به عنوان مثال داده‌های ذخیره شده در فضای ابر). در این بخش، بر روش‌های ارائه شده پیشین در دسته اول یعنی توانایی ایجاد اطمینان از داده‌های تولید شده توسط اشیاء IoT تمرکز خواهیم نمود.

۲- کارهای گذشته

در [۳] یک الگوریتم کنترل جامعیت داده در اینترنت اشیاء مبتنی بر امضای دیجیتال ارائه شده است. این الگوریتم، از امضای دیجیتال با قالب ZSS[5] به منظور کاهش سربار محاسباتی در فرآیند کنترل جامعیت استفاده می‌کند. این فرآیند شامل چهار گام محاسباتی می‌باشد. در گام اول، پارامترهای اولیه سیستم توسط یک سیستم حسابرس ثالث TPA[6] ایجاد می‌شود. سپس کلیدهای خصوصی و عمومی براساس پارامترهای سیستم ایجاد شده و در گام سوم، از کلید خصوصی و محتوای داده برای تولید امضای دیجیتال استفاده می‌شود. در نهایت، عملیات کنترل جامعیت براساس کلید عمومی و پیام مبادله شده صورت خواهد گرفت. این تکنیک با وجود کاهش زمان محاسباتی لازم برای کنترل جامعیت دارای دو ضعف می‌باشد. اولاً، تمامی مراحل کنترل جامعیت باید تحت نظارت سیستم حسابرس ثالث صورت پذیرد و دوماً، زمان تولید امضای دیجیتال در این روش به ازای تعداد بلوک‌های داده بصورت نمایی افزایش می‌یابد. در نتیجه برای شبکه‌های بزرگ و تعداد بلوک‌های زیاد داده کارایی مناسبی نخواهد داشت.

در [۴] به ارائه یک راهکار کنترل جامعیت داده‌های تجمیعی[7] پرداخته شده است. در این روش، حالتی از کنترل جامعیت در نظر گفته شده است که داده از چندین فرستنده به سمت یک گیرنده یکسان ارسال شود. این سناریو در توپولوژی‌های خوشه-بندی شبکه IoT که داده‌های هر خوشه توسط درگاه خوشه تجمیع می‌شود؛ کاربرد دارد. راهکار پیشنهادی در این مقاله از تکنیک امضای دیجیتال مبتنی بر مجموعه‌های همگن[8] استفاده می‌کند. در این روش، اگر امضای دیجیتال مربوط به شیء i برای داده A را بصورت sig(Ai) نشان دهیم؛ آنگاه امضای دیجیتال حاصل از تجمیع دو بلوک داده (مثلا sig(Ai+Bj)) با ترکیب امضاهای دیجیتال تک‌تک این بلوک‌ها (مثلا sig(Ai)+sig(Bj)) متناظر می‌باشد. در این مقاله، تنها صحت عملکرد سیستم کنترل جامعیت بصورت نظری اثبات شده است و کارایی آن در شرایط واقعی یا محیط شبیه‌سازی شده مورد ارزیابی قرار نگرفته است. به همین دلیل در مورد نحوه عملکرد این سیستم در شرایط واقعی اطلاعاتی در دست نمی‌باشد.

در [۵] کاربرد سه تکنیک رمزنگاری به منظور کنترل جامعیت داده در اینترنت اشیاء مورد مطالعه قرار گرفته است. در این مقاله، بر روی سه الگوریتم رمزنگاری AES، RSA و TDES تمرکز شده و کارایی هر کدام از جنبه‌های زمان اجرا، پیچیدگی محاسباتی و میزان حافظه مورد نیاز مورد بررسی شده است.

[5] Zhang's Short Signature

[6] Third-Party Auditor

[7] Aggregated Data

[8] set-homomorphic

مطالعات انجام شده در این تحقیق نشان می‌دهد که استاندارد رمزنگاری AES دارای عملکرد مناسب‌تری از نظر جنبه‌های ذکر شده می‌باشد. بعلاوه این الگوریتم از کلید وسیع‌تری استفاده نموده که نتیجه آن فراهم نمودن سطح بالاتری از امنیت اطلاعات خواهد بود. با این وجود، استفاده از الگوریتم‌های رمزنگاری مانند AES در حوزه کنترل جامعیت داده مشکلاتی را نیز درپی خواهد داشت. یکی از این مشکلات، محدودیت پشتیبانی آن از قالب‌های مختلف داده و همچنین عدم کارایی برای داده‌های غیرساخت‌یافته می‌باشد که کاربرد آن در اینترنت اشیاء را مشکل می‌کند. یکی دیگر از مشکلات موجود، نیاز به توان پردازشی بالا برای گره‌های فرستند و گیرنده می‌باشد که نتیجه آن، غیرقابل اجرا بودن این سیستم در معماری‌های ناهمگن شبکه می‌باشد. بطور کلی، همانطور که در [۳] اشاره شده است، استفاده از تکنیک‌های دیگر مانند امضای دیجیتال برای کاربردهای کنترل جامعیت داده در IoT نتایج بهتری را نسبت به الگوریتم‌های رمزنگاری مانند AES درپی خواهد داشت. در [۶]، یک روش کنترل جامعیت داده با مصرف انرژی پایین برای کاربرد در اینترنت اشیاء ارائه شده است. این تکنیک از نقشه آشوب خطی به منظور جایگشت شبه‌تصادفی داده‌ها و کنترل جامعیت آن‌ها استفاده می‌کند. این تکنیک شامل دو فاز: اشتراک گذاری دنباله و مبادله داده می‌باشد. در فاز اشتراک گذاری دنباله، پارامترهای اولیه مدل بین دو سیستم مبادله شده و براساس آن یک دنباله آشوب خطی تولید می‌گردد. این نقشه آشوب، دارای الگویی شبه‌تصادفی می‌باشد. در فاز مبادله داده، بلوک داده با استفاده از نقشه آشوب خطی و توسط گره فرستنده جایگشت داده می‌شود. پس از دریافت داده توسط گیرنده، از الگوی معکوس نقشه آشوب خطی به منظور بازیابی داده و کنترل صحت آن استفاده می‌شود. کارایی این الگوریتم از جنبه‌های انرژی مصرفی برای محاسبات، میزان حافظه و زمان پردازش مورد بررسی قرار گرفته است. نتایج حاصل، نشان از عملکرد مناسب این سیستم از جنبه‌های انرژی و زمان محاسباتی دارند. اما باید توجه داشت که براساس [۷]، نقشه آشوب خطی –که در این مقاله از آن استفاده شده است- دارای مشکلاتی مانند محدودیت فضای کلید و کارایی پایین در برابر حملات تفاضلی[9] و Brute-Force می‌باشد.

در [۸] یک روش مبتنی بر مدل استنتاج بیزی[1] منظور کنترل جامعیت داده در اینترنت اشیاء ارائه شده است. در این مدل، داده‌های ارسال شده توسط اشیاء مختلف توسط یک سیستم حسابرس ثالث رصد شده و براساس مشاهدات صورت گرفته توسط مدل بیزی، داده در یکی از دسته‌های: «تغییریافته»، «اصیل» یا «غیرقابل تفسیر» قرار می‌گیرد. در نهایت با استفاده از تصمیمات صورت گرفته برای تمامی بلوک‌های داده، اصالت داده تجمیع شده مشخص می‌گردد. این مدل نمی‌تواند بصورت قطعی جامعیت داده‌های مبادله شده در IoT را مشخص کند اما تحلیل‌های صورت گرفته در این تحقیق نشان می‌دهد که روش پیشنهاد شده بصورت کلی دارای عملکردی قابل قبول در مقایسه با مدل‌های قطعی کنترل جامعیت داده می‌باشد. نیاز به یک سیستم حسابرس ثالث برای کنترل تمامی جریان‌های ترافیکی از معایب روش پیشنهاد شده در این تحقیق بوده که موجب عدم کارایی آن در شبکه‌های وسیع خواهد شد. از طرفی، عملکرد مطلوب سیستم، وابسته به تعیین مقادیر بهینه برای پارامترهای متعدد مدل بیزی می‌باشد.

در [۹] یک سیستم تشخیص حملات جامعیت داده برای کاربرد در IoT ارائه شده است. این روش مبتنی بر تکنیک‌های یادگیری ماشین بوده و از مدل مخلوط گاوسی[1] GMM برای یادگیری الگوی مقادیر داده‌ای تولید شده توسط هر شیء استفاده می‌کند. روش پیشنهادی شده در این مقاله، ابتدا با استفاده از داده‌های نمونه‌برداری شده در روزهای متوالی با بازه‌های زمانی مشخص، محدوده مقادیر مجاز برای انواع داده را با استفاده از تکنیک خوشه‌بندی مبتنی بر GMM تعیین نموده و سپس برای بررسی جامعیت داده‌های جدید، آن‌ها را با محدوده‌های بدست آمده از فاز آموزش تطابق می‌دهد. در صورت عدم تطابق داده جدید با محدوده‌های مدل آموزش، یک حمله جامعیت داده شناسایی خواهد شد. این تنها برای شبکه‌هایی با ابعاد کوچک تا متوسط و در شرایطی که حساسیت داده‌ها بالا نباشد کاربرد خواهد داشت. از طرفی، بکارگیر مدل مخلوط گاوسی و نیاز به نگهداری سوابق داده‌ای مختلف موجب می‌شود که عملکرد مناسب این روش وابسته به بکارگیری یک سیستم با توان پردازشی بسیار بالا باشد. مشکل مشترک اغلب روش‌های بررسی شده تاکنون، نیاز به کنترل جامعیت داده تحت نظارت یک سیستم حسابرس ثالث (TPA) می‌باشد. این در شرایطی است که در محیط‌هایی پویا

[1] Bayesian Inference Model

[1] Gaussian Mixture Model

[9] Differential Attacks

مانند اینترنت اشیاء، قابلیت اعتماد TPA خود یک چالش می‌باشد. به همین دلیل، در برخی از تحقیقات صورت گرفته اخیر از تکنیک‌های مبتنی بر بلوک‌های زنجیره‌ای[1][2] برای کنترل جامعیت داده استفاده شده است.

یکی از این تحقیقات، روش ارائه شده در [۱۰] می‌باشد. ویژگی اصلی این روش، کنترل جامعیت داده در اینترنت اشیاء بصورت غیرمتمرکز می‌باشد. براین اساس، در این تحقیق ابتدا سه موجودیت: دارنده داده، مصرف‌کننده داده و سرویس ذخیره ابری معرفی شده و سپس چهار پروتکل مختلف برای کنترل جامعیت در سناریوهای مختلف تبادل داده بین این سه موجودیت معرفی شده است. تمامی این پروتکل‌ها در یک مولفه سرویس کنترل جامعیت قابل اجرا بوده که بصورت یک سرویس در اشیاء IoT اجرا می‌گردد. این روش، اگرچه یک راهکار قابل اطمینان برای کنترل جامعیت داده در اینترنت اشیاء فراهم می‌آورد؛ اما انرژی مصرفی بسیار بالا برای محاسبات و نیاز به سخت‌افزارهای ویژه با توان پردازشی بالا بکارگیری آن در شرایط واقعی را با مشکل مواجه می‌کند.

برای حل این مسئله، در [۱۱] از معماری محاسبات مه[1][3] به منظور کاهش انرژی مصرفی محاسباتی و افزایش کارایی شبکه در کنترل غیرمتمرکز جامعیت داده‌های IoT استفاده شده است. در معماری مه، تجهیزات محاسباتی در واقع واسطه‌ای بین سیستم محاسبات ابری و اشیاء IoT بوده و با انجام پردازش‌ها در نزدیکی اشیاء، هزینه‌های محاسباتی را کاهش خواهند داد. بدین ترتیب، در این روش سرویس کنترل جامعیت مبتنی بر بلوک‌های زنجیره‌ای در سرویس‌دهندگان لایه مه اجرا خواهد شد. این روش، اگرچه می‌تواند تاخیر محاسباتی و کارایی سیستم‌های کنترل جامعیت مبتنی بر بلوک‌های زنجیره‌ای را بهبود بخشد؛ اما با هدایت ترافیک محاسباتی به خارج IoT موجب افزایش تاخیر انتها به انتها و ترافیک داده خوهد شد. بعلاوه این راهکار برای کنترل جامعیت در ارتباطات نظیربه‌نظیر بین اشیاء کارایی ندارد.

در [۱۲] به مشکل اصلی سیستم‌های کنترل جامعیت داده مبتنی بر بلوک‌های زنجیره‌ای اشاره شده است: در پروتکل بلوک‌های زنجیره‌ای، باید تمامی گره‌های شبکه در طی یک مکانیزم توافق عمومی و به منظور کنترل منبع داده با هم همکاری کنند. این خصوصیت، کاربرد تکنیک‌های مبتنی بر بلوک‌های زنجیره‌ای برای کنترل جامعیت داده در شبکه‌هایی با منابع محدود را به چالش می‌کشد.

برای حل این مشکل، در [۱۲] یک راهکار مبتنی بر انتخاب تصادفی اشیاء ارائه شده است. بدین صورت که اشیاء همکاری کننده در فرآیند کنترل منبع بصورت تصادفی انتخاب می‌شوند و تنها این اشیاء عمل حل مسئله هش برای هر بلوک داده را انجام می‌دهند. در نهایت با استفاده از قانون رای‌گیری اکثریت بین اشیاء همکاری کننده، جامعیت داده مشخص می‌گردد. این راهبرد، برای شبکه‌های بسیار بزرگ و دارای تعداد منابع پردازشی قدرتمند کافی مناسب خواهد بود. خلاصه مشخصات مقالات مورد بررسی در این بخش، در جدول (۱) نمایش داده شده است. همانطور که پیش از این اشاره شد، در روش پیشنهادی، تأمین جامعیت داده با استفاده از مفاهیم تئوری آشوب صورت می‌پذیرد.

---

[1] Blockchain [2]

[1] Fog Computing [3]

جدول (۱): خلاصه مشخصات مقالات مورد بررسی در این بخش

منبع	سال	راهکار	مبتنی بر TPA	توزیع‌پذیری	اعمال تبدیل روی داده	افزایش حجم داده	کارایی در شبکه‌های بزرگ	کارایی برای داده‌های بزرگ	مدل تشخیص (قطعی / احتمالاتی)	نیاز به سخت‌افزار ویژه	محدودیت در قالب داده مورد پشتیبانی
[۳]	۲۰۱۹	امضای دیجیتال با قالب ZSS	√						قطعی		
[۴]	۲۰۱۸	امضای دیجیتال مبتنی بر مجموعه‌های همگن	√				NA	NA	قطعی		
[۵]	۲۰۱۷	رمزنگاری AES		√	√	√			قطعی	√	√
[۶]	۲۰۱۸	نقشه آشوب خطی	√	√	√		√	√	قطعی		
[۸]	۲۰۱۷	مدل استنتاج بیزی	√					√	احتمالاتی	√	√
[۹]	۲۰۱۶	مدل مخلوط گاوسی GMM	√						احتمالاتی	√	√
[۱۰]	۲۰۱۷	بلوک‌های زنجیره‌ای		√	√	√		√	قطعی	√	
[۱۱]	۲۰۱۸	بلوک‌های زنجیره‌ای و محاسبات مه		√	√	√		√	قطعی	√	
[۱۲]	۲۰۱۸	انتخاب تصادفی اشیاء همکار در پروتکل بلوک زنجیره‌ای		√	√		√	√	قطعی	√	

به همین دلیل، در ادامه این بخش به مطالعه تئوری آشوب و کاربردهای آن خواهیم پرداخت. تئوری آشوب یا نظریّه بی‌نظمی‌ها به مطالعه سیستم‌های دینامیکی آشوب‌ناک می‌پردازد. سیستم‌های آشوب‌ناک، سیستم‌های دینامیکی‌ای غیرخطی هستند که نسبت به شرایط اولیه‌شان بسیار حساس‌اند. تغییری اندک در شرایط اولیه چنین سیستم‌هایی باعث تغییرات بسیار در آینده خواهد شد. این پدیده در نظریه آشوب به اثر پروانه‌ای مشهور است [۱۳].

رفتار سیستم‌های آشوب‌ناک به ظاهر تصادفی می‌نماید. با این‌حال هیچ لزومی به وجود عنصر تصادف در ایجاد رفتار آشوبی نیست و سیستم‌های دینامیکی معین[1] نیز می‌توانند رفتار آشوب‌ناک از خود نشان دهند. به بیان دیگر، پدیده‌هایی ظاهرا اتفاقی که تاکنون، دلیلی برای آن‌ها نمی‌یافتیم، به کمک مدل-های آشوب، توجیه می‌شوند. یکی از مورد توجه‌ترین کاربردهای تئوری آشوب، امنیت اطلاعات می‌باشد. رمزنگاری، نهان نگاری و واترمارکینگ برخی از کاربردهای تئوری آشوب در حوزه امنیت اطلاعات می‌باشد. ویژگی مهمی که باعث شده تا مدل‌های آشوبناک برای مدل‌های امنیتی بسیار مورد توجه قرار بگیرد تعریف‌پذیری سیستم و در عین رفتار شبه تصادفی آن است که باعث می‌گردد خروجی سیستم از دید مهاجمین تصادفی به نظر برسد؛ در حالی که از دید کاربران مجاز سیستم تعریف‌پذیر بوده و لذا قابل تحلیل است.

ادامه مقاله بصورت زیر سازماندهی شده است: در بخش دوم روش پیشنهادی مطرح خواهد شد، و در بخش سوم نیز، کارایی روش پیشنهادی از جنبه‌های مختلف مورد ارزیابی قرار خواهد گرفت. در نهایت، در بخش چهارم به جمع‌بندی یافته‌ها پرداخته خواهد شد.

۳- مدل پیشنهادی

در این بخش به ارائه پروتکل پیشنهادی جهت تامین جامعیت داده در شبکه سلامت هوشمند مبتنی بر دنباله آشوب وابسته به فضا و زمان خواهیم پرداخت. روش پیشنهادی، براساس مدل تامین جامعیت در [۶] ارائه شده و سعی دارد کاستی‌های این مدل را از دو جنبه بهبود بخشد:

[1] deterministic

بهبود مدل آشوب با استفاده از تئوری آشوب وابسته به فضا و زمان. نقشه آشوب مورد استفاده در [۶] محدودیت فضای کلید مواجه بوده و حساسیت کلید در آن بسیار پایین است. فضای کلید مورد استفاده در [۶] تنها بازه [0,1] را پوشش می‌دهد. این روش امنیت مدل آشوب بکار رفته را مورد بررسی قرار نمی‌دهد. در صورتی که مدلسازی این نقشه آشوبناک از طریق تجزیه و تحلیل الگوی تغییرات آشوب بسیار ساده خواهد بود. همچنین مجموعه عملیات محاسباتی بکار رفته در این روش به منظور تولید دنباله شبه‌تصادفی مبتنی بر آشوب، باز محاسباتی قابل توجهی را بر پردازنده تحمیل می‌کند. به همین دلیل در روش پیشنهادی یک مدل آشوب جدید با فضای کلید گسترده و حساسیت بالاتر نسبت به [۶] استفاده خواهد شد. این تکنیک می‌تواند سطح امنیت پروتکل پیشنهادی را بصورت قابل توجهی بهبود بخشد و در عین حال انرژی مصرفی ناشی از محاسبات را بصورت قابل توجهی کاهش دهد.

قابلیت بکارگیری مدل پیشنهادی برای انواع پیکربندی‌های شبکه. پروتکل پیشنهادی در [۶] برای بکارگیری در یک پیکربندی خاص در IoT قابل استفاده خواهد بود. این پروتکل وجود سرور بعنوان سیستم حسابرس ثالث را از الزامات پیکربندی خود درنظر گرفته است. در روش پیشنهادی این نیازمندی از میان رفته و مدل پیشنهادی می‌تواند برای کنترل جامعیت در انواع الگوهای ارتباطی و پیکربندی‌های شبکه مورد استفاده قرار گیرد. بدین ترتیب، تعمیم حوزه کاربرد از مزایای روش پیشنهادی خواهد بود که آن را برای کاربردهایی مانند: مسیریابی چندگامی، شبکه سلامت هوشمند و ... سازگار می‌کند.

در ادامه، ابتدا مدل سیستم درنظر گرفته شده در مدل پیشنهادی را تشریح نموده و سپس مدل آشوب بکار رفته در روش پیشنهادی را ارائه خواهیم نمود. در نهایت مراحل کنترل جامعیت داده در سیستم مفروض ارائه خواهد شد.

۳-۱- مدل سیستم

مدل شبکه از سه مولفه اصلی تشکیل شده است: ۱- تعدادی حسگر IoT که می‌توانند تجهیزات شبکه سلامت هوشمند باشند، ۲- یک سرور داده که محل ذخیره‌سازی اطلاعات تولید شده توسط حسگرهای شبکه می‌باشد و ۳- اینترنت که بعنوان واسطه ارتباطی بین حسگرهای IoT و سرور داده مورد استفاده قرار می‌گیرد. وجود سرور داده در پیکربندی مدل شبکه الزامی نیست و گره‌های IoT می‌توانند از طریق مسیرهای چندگامی به مبادله داده بپردازند. در صورت بکارگیری چنین سناریویی، طرفین ارتباط چندگامی در حین مبادله داده به کنترل جامعیت خواهند پرداخت.

حسگرهای IoT در یک فضای باز و فاقد حفاظت خاص مستقر شده‌اند و در نتیجه دسترسی به این حسگرها بصورت فیزیکی امکان‌پذیر خواهد بود. درصورتی‌که سرور داده (در صورت حضور در مدل شبکه) ازنظر فیزیکی محافظت شده در نظر گرفته می‌شود و دسترسی افراد به این سرور ممکن نخواهد بود.

منابع انرژی و محاسباتی حسگرهای شبکه سلامت هوشمند محدود می‌باشند؛ درحالی‌که، سرور داده از نظر منابع محاسباتی، ارتباطی و انرژی فاقد محدودیت درنظر گرفته می‌شود.

در این تحقیق، مدل حمله توسط مهاجمین می‌تواند بصورت یکی از حالات زیر باشد:

مهاجم شبکه، یک یا چند مولفه شبکه مانند: حسگرهای IoT، مسیریاب‌ها و یا لینک‌های ارتباطی را مورد تهدید قرار می‌دهد.

مهاجم قادر به شنود تمام ترافیک شبکه بوده و می‌تواند پیام‌های مبادله شده قبلی را بازپخش نموده، هویت یک گره دیگر را جعل کرده و یا داده‌هایی مخرب را در شبکه تزریق کند.

هدف مهاجم، ایجاد اختلال در عملکرد شبکه از طریق تغییر داده‌های مربوط به حسگرهای IoT است.

در ادامه به توضیح مراحل روش پیشنهادی خواهیم پرداخت.

۳-۲- مدل آشوب وابسته به فضا و زمان

در مقایسه با سیستم‌های آشوب خطی، آشوب وابسته به فضا و زمان دارای رفتاری بسیار پیچیده‌تر بوده و خصوصیات بیشتری را ارائه می‌کند. سیستم‌های آشوب‌ناک وابسته به فضا و زمان معمولا از طریق معادلات دیفرانسل جزئی، معادلات دیفرانسیل ترکیبی و یا نقشه‌های ترکیبی شبکه‌ای CML مدلسازی می‌شوند. در الگوریتم پیشنهادی با استفاده از نقشه‌های CML، یک روش جایگشت داده مبتنی بر نظریه آشوب وابسته بر فضا و زمان ارائه شده است. در ادامه به تشریح مدل آشوب پیشنهادی می‌پردازیم.

۳-۲-۱- الگوریتم تولید نقشه آشوب غیرخطی

نقشه آشوب غیرخطی NCA بر اساس نقشه منطقی تولید می‌شود. یک نقشه منطقی را می‌توان براساس رابطه زیر تعریف نمود[۱۴]:

$$x_{n+1} = \mu x_n (1 - x_n), \quad n = 1, 2, 3, \ldots \quad (۱)$$

که در رابطه فوق، $x_n \epsilon (0,1)$, $0 < \mu \leq 4$. در رابطه ۱، در صورتی که $3.57 \leq \mu \leq 4$ باشد نقشه منطقی رفتاری آشوب‌ناک از خود نشان خواهد داد. یکی از معایب استفاده از این مدل، فضای محدود کلید رمزنگاری و در نتیجه امنیت پایین آن می‌باشد. از این رو، در تحقیقات اخیر یک الگوریتم تولید نقشه آشوب غیرخطی بر اساس نقشه منطقی ارائه شده است. این مدل در رابطه ۲ نمایش داده شده است[۱۵]:

$$x_{n+1} = (1-\beta^{-4}).\cot(\frac{\alpha}{1+\beta})(1+\frac{1}{\beta})^{\beta} \\ .\tan(\alpha x_n).(1-x_n)\hat{}\,\beta,\ n=1,2,3,\ldots \qquad (۲)$$

که در رابطه فوق $\alpha \in (1.5,1.57], x_n \epsilon (0.1), \beta \in [3,15]$ محدوده این متغیرها را مشخص می‌کند.

۳-۲-۲- تولید نقشه آشوب وابسته به فضا و زمان

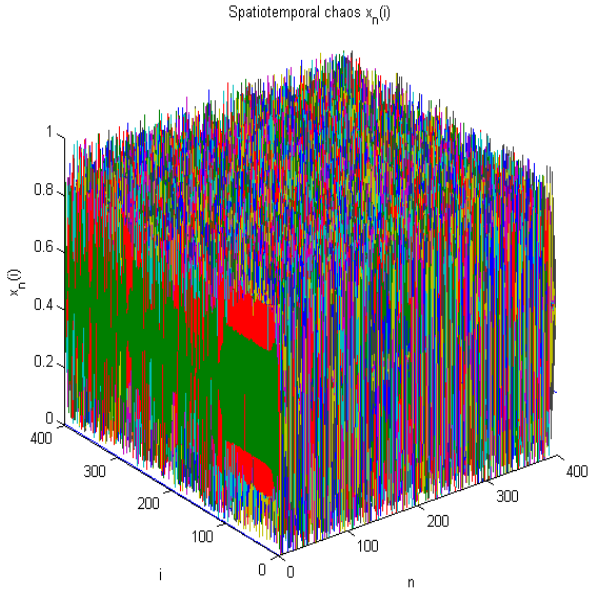
CML مدل کننده یک سیستم پویا با فضا و موقعیت گسسته بوده که دارای حالات متوالی می‌باشد و اغلب به عنوان مدل اولیه برای مطالعه پویایی در سیستم‌های آشوب وابسته به فضا و زمان بکار می‌رود. یک سیستم CML دوطرفه را می‌توان بصورت رابطه ۳ مدلسازی نمود[۱۴]:

$$\begin{cases} x_{n+1} = (1-\varepsilon) f(x_n(i)) \\ +\dfrac{\varepsilon}{2}\ f(x_n(i-1)) + f(x_n(i+1)) \\ f(x) = \mu x(1-x) \end{cases} \qquad (۳)$$

که در رابطه فوق i اندیس موقعیت، n اندیس زمان و ε ثابت ترکیب بوده و در بازه (0,1) قرار دارد. همچنین $0 < f(x) < 1, 3.57 \leq \mu \leq 4, 0 < x < 1$ بازه مقادیر قابل استفاده در رابطه ۳ را مشخص می‌کند. برای بهره گیری از مزیت‌های NCA می‌توان رابطه ۲ را در رابطه ۳ جایگزین نمود. با انجام این عمل، یک مدل آشوب وابسته به فضا و زمان بصورت رابطه ۴ بدست می‌آید:

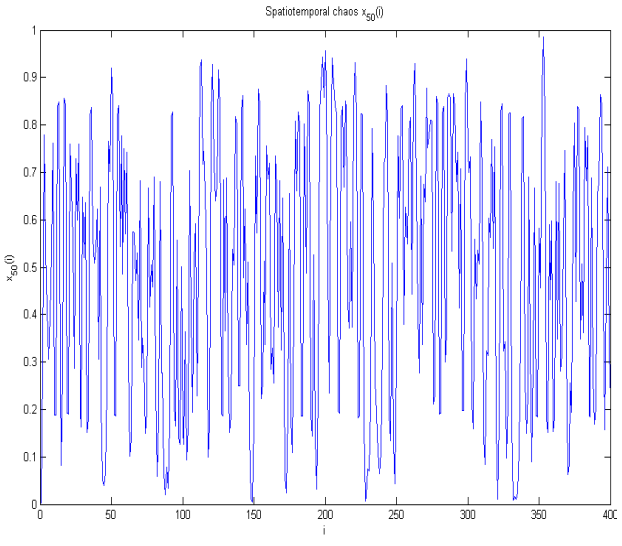
$$\begin{cases} x_{n+1} = (1-\varepsilon) f(x_n(i)) \\ +\dfrac{\varepsilon}{2}\ f(x_n(i-1)) + f(x_n(i+1)) \\ f(x) = (1-\beta^{-4}).\cot(\dfrac{\alpha}{1+\beta})(1+\dfrac{1}{\beta})^{\beta} \\ .\tan(\alpha x_n).(1-x_n)\hat{}\,\beta \end{cases} \qquad (۴)$$

که در رابطه فوق $\varepsilon \in (0,1)$ و $x_n(i) \in (0,1)$ می‌باشد. باقی مقادیر موجود در رابطه فوق مشابه با رابطه ۲ است. شکل (۱) رفتار مدل ارائه شده در رابطه ۴ به ازای $0 < i \leq 400, 0 < n \leq 400, \varepsilon = 0.5, \alpha = 1.51, \beta = 4$ را نمایش می‌دهد.



شکل (۱) آشوب وابسته به فضا و زمان برای xn(i)

همچنین در شکل (۲) این نمودار به ازای n=50 نمایش داده شده است. همانطور که از تصویر مشخص است، این مدل آشوب می‌تواند ویژگی‌هایی مناسب و غیرخطی در بازه صفر تا یک را ارائه کند. در نتیجه برای استفاده بعنوان تابع درهم‌سازی در روش پیشنهادی مناسب خواهد بود.



شکل(۲) آشوب وابسته به فضا و زمان به ازای n=50

۳-۲-۳- درهم‌سازی و تولید جایگشت آشوبگون در روش پیشنهادی

از الگوی شبه تصادفی دنباله آشوب وابسته به فضا و زمان می‌توان برای طراحی یک تابع درهم‌سازی کارامد استفاده نمود. در این بخش، به تشریح این تابع و نحوه تولید جایگشت آشوبگون خواهیم پرداخت. روش پیشنهادی، محتوای بسته‌ها را در سطح بایت درهم‌سازی نموده و شامل مراحل پردازشی زیر می‌باشد:

گام ۱: محتوای داده ورودی جهت درهم‌سازی را به یک آرایه یک بعدی بصورت $M = m_1, m_2, \ldots, m_n$ تبدیل می‌کنیم. که در این آرایه، m_i نشان دهنده بایت iام داده می‌باشد.

گام ۲: در بردار M، تمامی مقادیر دنباله داده را به عدد مبنای ۱۰ تبدیل می‌کنیم. این کار باعث می‌شود که هر بایت داده بصورت یک عدد در بازه [0,255] توصیف گردد. سپس مجموع مقادیر عددی را محاسبه نموده و سپس مجموع را بصورت متوالی بر عدد ۱۰، تقسیم کرده تا نتیجه این تقسیم بصورت یک عدد در بازه [0,1] بدست آید. مثلا اگر مجموع برابر با ۲۵۶۴۴۵۳ باشد؛ نتیجه تقسیم متوالی برابر با ۰/۲۵۶۴۴۵۳ خواهد بود. این عدد نرمالسازی شده به عنوان مقدار اولیه x1 در رابطه ۴ بکار خواهد رفت تا دنباله آشوب‌ناک تولید شود. این دنباله آشوب شبه تصادفی را بصورت $A = \{a_1, a_2, \ldots, a_n\}$ تعریف می‌کنیم.

گام ۳: مقادیر دنباله A را بصورت نزولی مرتب می‌کنیم تا ترتیب مرتب سازی مقادیر این دنباله بصورت دنباله جایگشت IX بدست آید. این دنباله را جایگشت آشوبگون می‌نامیم و در فرآیند نمونه‌برداری از دسته‌های داده بصورت مستقل نیز مورد استفاده قرار خواهد گرفت (بخش ۳-۳-۲). دنباله IX نشان می‌دهد که اعضای دنباله آشوب A به چه ترتیبی جایجا شده‌اند. مثلا، IX(i) نشان می‌دهد که عنصر i-ام در دنباله مرتب شده، با کدام عنصر در A جایگزین شده است. با بکارگیری ترتیب بدست آمده دنباله IX و اعمال همین الگوی جابجایی در دنباله M، دنباله جایگشت یافته M بصورت $M = \{m_{IX(1)}, m_{IX(2)}, \ldots, m_{IX(n)}\}$ بدست خواهد آمد.

گام ۴: براساس دنباله A که از رابطه ۴، بدست آمده بود، توسط رابطه زیر دنباله $Y = \{y_i | i = 1,2,\ldots,n\}$ را محاسبه می‌کنیم:

$$y_i = \left\lfloor (a_i \times 10^{14}) mod 256 \right\rfloor \qquad (۵)$$

رابطه فوق نشان می‌دهد که همواره مقادیر y در بازه [0,255] قرار دارند.

گام ۵: در آخرین گام درهم‌سازی، عمل انتشار روی بردار داده M' را با استفاده از رابطه زیر انجام می‌دهیم:

$$c_i = m_i \oplus y_i \qquad (۶)$$

که در رابطه فوق عملگر $\oplus$ نشانگر عمل بیتی XOR می‌باشد. نتیجه این گام‌ها، داده درهم‌سازی شده c خواهد بود.

۳-۳- تامین جامعیت داده در شبکه سلامت هوشمند مبتنی بر تئوری آشوب

در ادامه‌ی این بخش، پروتکل پیشنهادی به منظور شناسایی داده‌های تحریف شده در شبکه سلامت هوشمند تشریح خواهد شد. بدین منظور، ابتدا به ذکر علائم و نمادهای بکار رفته خواهیم پرداخت. برای نمایش شناسه دستگاه IoT، تابع درهم‌سازی و عملگر الحاق، به ترتیب به ترتیب از نمادهای IX_i، $\phi()$ و \ استفاده خواهیم نمود. همچنین $\oplus$ نشان دهنده عملگر XoR بیتی می‌باشد، و C(M,k) نشان دهنده رمزنگاری پیام M از طریق کلید k می‌باشد. کلید ارتباط بین هر دو جفت شیء مانند A و B بصورت $K_{A,B}$ نمایش داده می‌شود. در مدل پیشنهادی، دستگاه‌های IoT نیازی به ذخیره کلید رمزنگاری در حافظه خود ندارند؛ در عوض، هر دستگاه یک رشته‌ی بیتی متغیر با زمان بصورت CH را در حافظه خود نگهداری می‌کند. یک دستگاه مانند IX_A می‌تواند کلید مخفی ارتباط با دستگاهی مانند IX_B را بصورت $C(CH_A \backslash CH_B, CH_A \backslash CH_B)$ در هر زمان که لازم باشد تولید کند. در اینصورت، یک مهاجم نمی‌تواند با استفاده از این رشته‌ی بیتی، کلید مخفی را بدست آورد. این خصوصیت موجب می‌شود که اشیاء در برابر حملات فیزیکی و جعل هویت ایمن باشند. بعلاوه، هر شیء بجای استفاده از هویت واقعی خود، از یک هویت مستعار برای برقراری ارتباط استفاده می‌کند. این هویت مستعار که بصورت PIX_A برای شیء با شناسه IX_A نمایش داده می‌شود، با استفاده از تابع درهم‌ساز بصورت $\varphi(IX_A \backslash k)$ ساخته خواهد شد. با توجه به اینکه کلید محرمانه ارتباط برای هر دو شیء شبکه یکتا می‌باشد؛ بنابراین هویت مستعار برای برقراری ارتباط بین هر جفت شیء نیز یکتا خواهد بود و این خصوصیت؛ تشخیص هویت اصلی شیء توسط مهاجمین جهت جعل را غیرممکن خواهد نمود.

در طی فرآیند ارسال داده و در مقاطع زمانی شبه تصادفی، هر شیء شبکه بسته‌های اعتبار سنجی را به شیء گیرنده ارسال نموده تا این اطلاعات را بررسی نموده و از صحت تمام داده‌های ارسال شده قبلی توسط فرستنده اطمینان حاصل شود. پروتکل پیشنهادی را می‌توان به دو مرحله اصلی تقسیم‌بندی نمود:

اشتراک توالی
انتقال داده
در ادامه به تشریح هریک از این گام‌ها خواهیم پرداخت.

۳-۳-۱- فاز اشتراک توالی

این فاز مبادله دوطرفه برای ایجاد یک توالی شبه تصادفی بین دو طرف ارتباط استفاده خواهد شد. اگر IX_A و IX_B را به ترتیب، گره‌های فرستند و گیرنده درنظر بگیریم؛ آنگاه فاز به اشتراک گذاری دنباله در پروتکل پیشنهادی از طریق مراحل زیر انجام خواهد شد:

در اولین گام، شیء IX_A براساس روند تشریح شده در قبل، کلید محرمانه $K_{A,B}$ و هویت مستعار PIX_A خود را محاسبه می‌کند و با تولید یک عدد تصادفی مانند R_A، آن را بصورت $C(R_A,K_{A,B})$ رمزنگاری می‌نماید. همچنین با استفاده از تابع درهم‌ساز، حاصل الحاق کلید محرمانه، هویت مستعار و عدد تصادفی را بصورت $\varphi(PIX_A \setminus k_{A,B} \setminus R_A)$ تبدیل نموده و تمامی این اطلاعات را در قالب اولین پیام به IX_B ارسال می‌کند. در این پیام، از تابع درهم‌سازی برای اطمینان از جامعیت داده‌ها و سالم بودن پیام استفاده می‌شود. در نتیجه ساختار پیام بصورت $\langle PIX_A, C(R_A,k_{A,B}), \varphi(PIX_A \setminus k_{A,B} \setminus R_A)\rangle$ خواهد بود.

شیء IX_B با استفاده از کلید محرمانه محاسبه شده خود، عدد تصادفی R_A را بدست می‌آورد. عدد تصادفی محاسبه شده توسط این گره را بصورت R'_A نشان می‌دهیم. سپس به منظور حصول اطمینان از صحت داده‌های دریافتی، با استفاده از عدد تصادفی محاسبه شده توسط خود، مقدار $\varphi(PIX_A \setminus k_{A,B} \setminus R'_A)$ را محاسبه کرده و مقدار آن را با مقدار دریافت شده در پیام مقایسه می‌کند. در صورتی که $\varphi(PIX_A \setminus k_{A,B} \setminus R'_A) \neq \varphi(PIX_A \setminus k_{A,B} \setminus R_A)$ ، آنگاه شیء IX_B درخواست اشتراک دنباله را رد می‌کند. در غیر این صورت، شیء IX_B یک عدد تصادفی مانند R_B را تولید کرده و با ترکیب اعداد تصادفی R_A و R_B مولد دنباله شبه‌تصادفی را بصورت $S = \varphi(R_A \oplus R_B)$ محاسبه خواهد نمود. طرفین ارتباط مقدار S برای تولید یک دنباله شبه تصادفی از اعداد صحیح استفاده می‌کنند. همچنین مقدار مولد دنباله به منظور حصول اطمینان از صحت می‌تواند به صورت دوره‌ای بروزرسانی شود. سپس شیء IX_B پیام دوم فاز اشتراک توالی را به سمت شیء IX_A ارسال می‌کند. این پیام حاوی مقادیر رمزنگاری شده هویت مستعار PIX_A، عدد تصادفی R_B، مولد S و عدد تصادفی R_A در کنار خروجی حاصل از درهم‌سازی الحاق تمامی این مقادیر با کلید محرمانه می‌باشد. بدین ترتیب، این پیام دارای ساختار $\left\langle \begin{matrix} C(\{PIX_A, R_B, S, R_A\}, k_{A,B}) \\ , \varphi(PIX_A \setminus k_{A,B} \setminus R_A \setminus S \setminus R_B) \end{matrix} \right\rangle$ خواهد بود.

شیء IX_A با استفاده از کلید $k_{A,B}$ عدد تصادفی R_B را محاسبه نموده و با مقایسه $\varphi(PIX_A \setminus k_{A,B} \setminus R_A \setminus S \setminus R_B) \neq \varphi(PIX_A \setminus k_{A,B} \setminus R_A \setminus S \setminus R'_B)$ صحت پیام دریافت شده را تأیید می‌کند. اگر تأیید موفقیت آمیز باشد، شیء IX_A مولد توالی S را در حافظه خود ذخیره می‌کند و با کاهش یک واحدی مقدار R_B و ارسال آن در قالب پیامی بصورت $\left\langle \begin{matrix} C(\{PIX_A, R_A, R_B - 1\}, k_{A,B}) \\ , \varphi(PIX_A \setminus k_{A,B} \setminus R_A \setminus R_B - 1) \end{matrix} \right\rangle$ مقدار دریافت شده را تأیید می‌کند.

شیء IX_B با بررسی اعتبار پیام دریافتی از صحت آن اطمینان حاصل نموده و در صورت تأیید، فرآیند اشتراک توالی خاتمه می‌یابد.

پس از اتمام موفقیت آمیز این گام؛ دو شیء یک مولد دنباله توالی محرمانه مانند S را دراختیار داشته و با استفاده از مدل آشوب تشریح شده در بخش قبل؛ یک دنباله توالی را ایجاد می‌کنند. پس از انجام این کار، فاز انتقال داده قابل انجام خواهد بود.

۳-۳-۲- فاز انتقال داده

بعد از مرحله اشتراک توالی، طرفین ارتباط دارای دنباله توالی شبه تصادفی مانند Seq خواهند بود که این دنباله براساس دنباله آشوبگون تولید شده است. در ادامه، دنباله توالی ایجاد شده را بصورت مجموعه‌ای از مقاطع زمانی مانند $Seq = T_1, T_2, \ldots$ درنظر می‌گیریم. این دنباله برای پنهان سازی اطلاعات اعتبار سنجی طرفین تبادل داده استفاده خواهد شد. بدین منظور، اشیاء IX_A و IX_B یک شمارنده برای ترتیب بسته‌های مبادله شده مانند cn را ایجاد نموده و با ارسال هر بسته داده از IX_A به IX_B هر دو شیء شمارنده خود را یک واحد افزایش می‌دهند. هنگامی که شمارنده cn با اولین عضو دنباله Seq یعنی T1 برابر شود، شیء IX_A اطلاعات اعتبارسنجی را به این بسته تزریق می‌کند و در هر دو شی، شمارنده بصورت cn=0 تنظیم می‌شود. انتقال بعدی اطلاعات اعتبارسنجی زمانی است که شمارنده cn به T2 برسد و به همین صورت این روند ادامه خواهد داشت.

در پروتکل پیشنهادی، بخش اعتبار سنجی سایر بسته‌ها (بسته-هایی که حاوی اطلاعات معتبر اعتبار سنجی نیستند) حاوی مقادیر جعلی و ساختگی خواهد بود و گره گیرنده IX_B پس از دریافت این بسته‌ها، بخش اطلاعات اعتبارسنجی را نادیده خواهد گرفت. بدین ترتیب، پیام‌های عادی حاوی اطلاعات اعتبارسنجی ساختگی بوده؛ در حالی‌که پیام‌های اعتبار سنجی، نتیجه درهم-سازی پیام‌های ارسال شده قبلی $\varphi(B)$ خواهد بود. در این حالت، یک مهاجم قادر نخواهد بود تا زمان مبادله بسته‌های حاوی اطلاعات اعتبار سنجی را تشخیص دهد و در نتیجه ایجاد تمایز بین بسته‌های عادی و اعتبار سنجی برای مهاجم ممکن نخواهد بود. در روش پیشنهادی، مقادیر دنباله توالی Seq در بازه [10,20] تعیین می‌شوند. تجهیزات IoT می‌توانند نمونه‌های داده‌های مختلف را در یک حافظه بافر ادغام نموده و سپس کل بافر متشکل از نمونه‌های داده‌های مختلف را در قالب یک بسته واحد ارسال کنند. در ادامه، این بسته را دسته می‌نامیم.

برای ساخت یک بسته اعتبارسنجی، شیء IX_A ابتدا یک جایگشت آشوبناک با طول N (N تعداد بسته‌هایی است که در پیام اعتبارسنجی باهم ادغام می‌شوند) از دسته داده‌های ارسال شده و تایید اصالت نشده قبلی تولید می‌کند. سپس با استفاده از عملگر XoR و تابع درهم‌ساز، بسته‌های انتخاب شده را درهم-سازی می‌کند. بعنوان مثال، اگر مجموعه دسته‌های تایید اصالت نشده قبلی بصورت BT=B1,B2,…,BT1 بوده و جایگشت آشوبگون تولید شده (برای N=3) بصورت I={2,5,1} باشد؛ آنگاه؛ محتوای اعتبارسنجی بصورت $V = \varphi(B_2 \oplus B_5 \oplus B_1)$ خواهد بود. این بسته اعتبار سنجی به گره IX_B ارسال می‌شود. گره IX_B مجددا جایگشت آشوبناک با طول N را تولید نموده و با جستجوی این دسته‌های تایید اصالت نشده در حافظه بافر خود؛ مجددا محتوای اعتبارسنجی را بصورت V' محاسبه می‌کند. در صورتی که $V = V'$ ، آنگاه تمامی دسته پیام‌های تایید اصالت نشده قبلی تایید خواهند شد و در غیر اینصورت کل این مجموعه رد می‌شود.

۴- شبیه سازی و نتایج

در این بخش به ارزیابی عملکرد روش پیشنهادی خواهیم پرداخت. بدین منظور، کارایی روش پیشنهادی در تامین جامعیت داده‌های اشیاء IoT از چهار جنبه مختلف مورد بررسی قرار گرفته است:

مقاومت پروتکل پیشنهادی در برابر حملات: در این آزمون عملکرد روش پیشنهادی در مواجهه با انواع مختلف حملات شبکه مورد بررسی قرار خواهد گرفت. بدین منظور باید بتوان سناریوهای مختلفی را در شرایط حضور مهاجمین و براساس الگوی حملات شبیه‌سازی نموده و مقاومت پروتکل پیشنهادی را در هر سناریوی حمله بررسی نمود. به منظور ارزیابی مقاومت پروتکل پیشنهادی در برابر حملات مختلف از نرم‌افزار ProVerif (PV) استفاده شده است. چرا که این ابزار شبیه‌سازی می‌تواند با استفاده از فرآیندهای جبری طیف وسیعی از سناریوهای حملات مختلف را پیاده سازی نموده و پروتکل پیشنهادی را از جنبه‌های مختلف امنیتی مورد بررسی قرار دهد.

ارزیابی کارایی محاسباتی: یک پروتکل امنیتی باید از پیچیدگی محاسباتی پایینی برخوردار بوده و در صورتی قابل استفاده خواهد بود که بار محاسباتی ناشی از آن کمتر از پروتکل‌های مورد استفاده فعلی باشد. بدین ترتیب، در این آزمون بار محاسباتی که از کنترل جامعیت داده توسط پروتکل پیشنهادی بر پردازنده گره‌های شبکه تحمیل می‌شود بررسی خواهد شد.

آنالیز سربار ارتباطی: در این آزمایش، میزان افزایش حجم بسته-های مبادله شده توسط پروتکل پیشنهادی مورد مطالعه قرار خواهد گرفت. اغلب پروتکل‌های کنترل جامعیت داده به منظور حفظ سطح قابل قبولی از امنیت، به ناچار سربار زیادی را در بسته‌های داده ایجاد می‌کنند. این امر می‌تواند کارایی شبکه را تحت تاثیر قرار دهد. به همین دلیل، در این آزمایش، سربار ارتباطی ناشی از پروتکل پیشنهادی مورد تجزیه و تحلیل قرار گرفته و با روش‌های پیشین مقایسه می‌شود.

ارزیابی کارایی انرژی: انرژی مصرفی گره‌های شبکه، ناشی از دو مولفه اصلی است: انرژی مصرفی حاصل از اجرای عملیات محاسباتی و انرژی مصرفی حاصل از تبادل داده. در یک پروتکل کنترل جامعیت داده با پیچیدگی محاسباتی پایین، تعداد عملیات محاسباتی پردازنده کاهش یافته و در نتیجه انرژی مصرفی محاسباتی کاهش خواهد یافت. از طرفی، کاهش سربار ارتباطی در یک پروتکل نیز موجب کاهش اندازه بسته خواهد شد که نتیجه آن، کاهش انرژی مصرفی برای تبادلات داده می‌باشد. در این آزمایش، دو مولفه انرژی مصرفی ذکر شده به ازای پارامترهای مختلف مورد ارزیابی قرار خواهد گرفت. به منظور ارزیابی دقیق این مقادیر، از ابزار شبیه‌ساز MATLAB که یک نرم‌افزار محاسبات عددی با کارایی بالاست استفاده خواهد شد.

در ادامه این بخش، به ارائه نتایج حاصل از آزمایشات و تحلیل‌ها خواهیم پرداخت.

۴-۱- شبیه سازی پروتکل

به منظور شبیه‌سازی پروتکل پیشنهادی از نرم‌افزار تأیید امنیت PV استفاده شده است. PV از فرآیند جبری برای تعریف پروتکل‌ها و شبیه‌سازی مبادلات جهت اثبات برخی از خصوصیات امنیتی استفاده می‌کند. حالت خاتمه شبیه‌سازی عملکرد یک پروتکل توسط PV عبارتند از: «اثبات موفق یک خصوصیت» یا «کشف بروز یک حمله». اثبات موفق یک خصوصیت بدین معناست که پروتکل امنیتی توانسته است فرآیند شبیه سازی را با موفقیت پشت سر گذاشته و در اثبات ابعاد امنیتی ادعا شده موفق عمل کرده است. به منظور شبیه‌سازی عملکرد روش پیشنهادی در این نرم‌افزار؛ دستگاه IoT و سرور به صورت فرآیندهای جداگانه‌ای مدلسازی شده و نمونه‌های نامحدودی از این فرایندها تولید می‌شود. سپس نشست‌های فراوان و دلخواهی بین دو طرف ارتباط شبیه‌سازی خواهد شد. برای اثبات احراز هویت متقابل و موفق بین دو طرف ارتباط، اظهارات طرفین ارتباط با هم تطابق داده شده و محرمانه بودن کلید با استفاده از دستورات پرس‌وجو مورد ارزیابی قرار گرفته است. شبیه‌ساز PV می‌تواند هرگونه حمله احتمالی یا قطعی را در پروتکل‌های امنیتی شناسایی کند. با توجه به اینکه، نتیجه تحلیل پروتکل پیشنهادی توسط PV، عدم کشف حمله بود؛ لذا می‌توان نتیجه گرفت که پروتکل پیشنهادی در برابر انواع حملات ایمن می‌باشد.

۴-۲- کارایی محاسباتی

با فرض رمزگذاری بلوک‌های ثابت، پیچیدگی عملیات رمزنگاری و درهم‌سازی را می‌توان برابر با $O(N)$ فرض کرد که در آن، N نشان دهنده اندازه یک پیام می‌باشد. با این وجود، پیچیدگی محاسباتی برای تولید دنباله جایگشت برابر با $O(n\log(n))$ خواهد بود، که در آن n نشان دهنده تعداد دسته‌های داده در هر پیام اعتبارسنجی می‌باشد. با استفاده از این مقادیر پیچیدگی، می توانیم نتیجه گرفت که در روش پیشنهادی، پیچیدگی مرحله اشتراک کلید برابر با $O(N)$ و پیچیدگی محاسباتی مرحله تبادل داده برای بسته‌های اعتبار سنجی برابر با $O(N+n\log(n))$ و برای بسته‌های عادی برابر با $O(1)$ می‌باشد. همانطور که پیش از این اشاره شد، مقدار مناسب برای تعداد دسته‌های داده در هر پیام اعتبارسنجی بصورت $10 \le n \le 20$ تعیین می‌شود؛ در نتیجه پیچیدگی محاسباتی روش پیشنهادی بسیار کم خواهد بود. در طرف مقابل؛ اگر از راهکار سنتی ارسال MAC به همراه هر بسته استفاده کنیم، پیچیدگی مرحله تبادل داده برای تمامی بسته‌ها برابر با $O(N)$ خواهد بود. از طرفی می‌دانیم که $n \ll N$ و در نتیجه روش پیشنهادی از پیچیدگی محاسباتی کمتری برخوردار می‌باشد.

۴-۳- کارایی انرژی

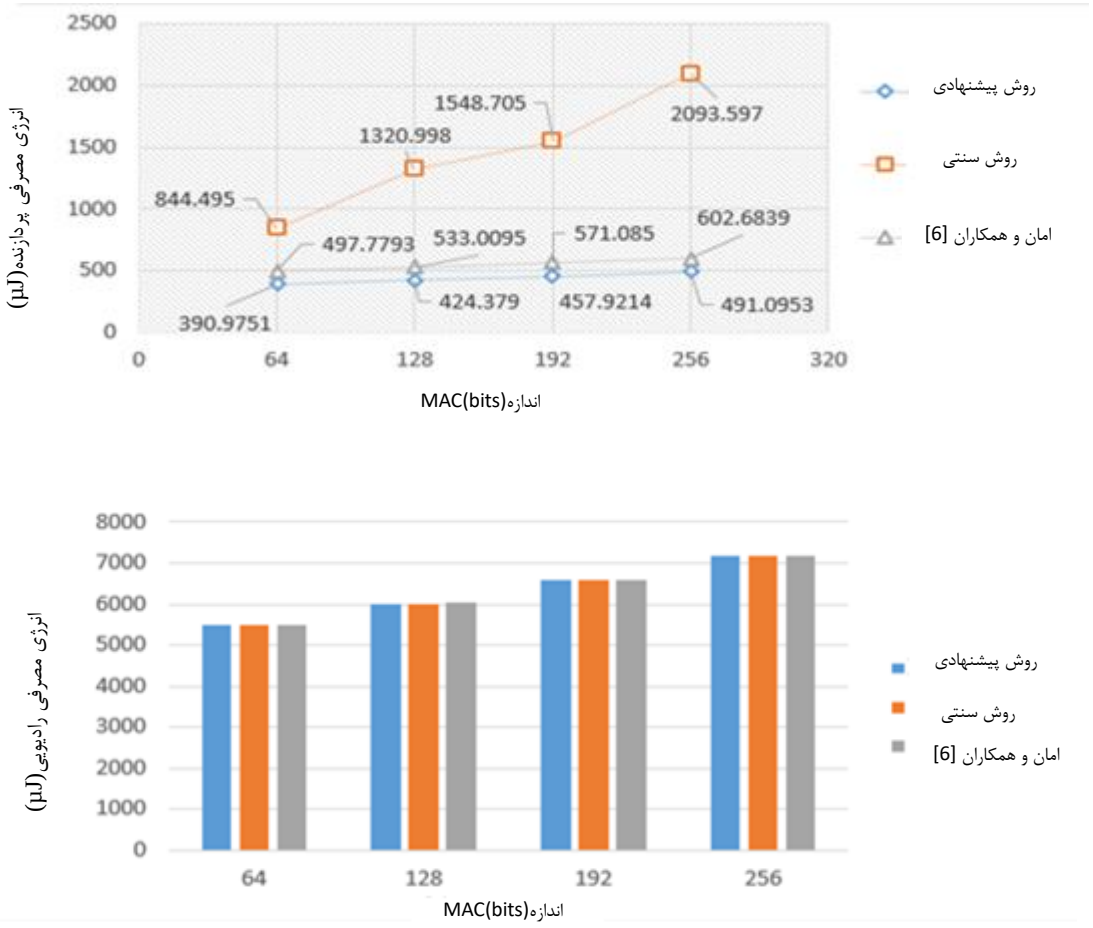
به منظور شبیه‌سازی عملکرد پروتکل پیشنهادی از جنبه انرژی مصرفی، از نرم‌افزار MATLAB استفاده شده است. بدین منظور، یک شبکه متشکل از ۱۰۰ حسگر بدن که خصوصیات گره MICA 2 را منعکس می‌کنند در یک محیط محدود با ابعاد ۱۰۰×۱۰۰ متر درنظر گرفته شده است. در طی فرآیند شبیه‌سازی، هریک از این ۱۰۰ حسگر، تعداد ۱۰۰ بسته داده را با نرخ ارسال ۱۹,۲ کیلوبیت بر ثانیه معادل ۲,۴ کیلوبایت در ثانیه ارسال نموده و میزان انرژی مصرفی حاصل از این مبادلات براساس روش پیشنهادی محاسبه خواهد شد. در نتیجه، مقادیر گزارش شده در این بخش، نتیجه تبادل ۱۰۰۰۰ بسته (۱۰۰ بسته ارسال شده توسط هریک از ۱۰۰ گره) خواهد بود. همچنین در این آزمایشات، کارایی پروتکل پیشنهادی با روش ارائه شده در [۶] و رویکرد سنتی موجود برای تامین جامعیت داده‌ها مقایسه خواهد شد. در رویکرد سنتی، برای کنترل جامعیت و عدم تحریف داده به همراه هر بسته یک MAC ارسال خواهد شد. این رویکرد، به عنوان معیار مقایسه در اغلب تحقیقات پیشین مورد استفاده قرار گرفته است و به همین جهت، در روش پیشنهادی نیز از این پروتکل برای مقایسه کارایی انرژی استفاده خواهد شد. به منظور ارزیابی عملکرد پروتکل پیشنهادی، دو سناریوی مختلف درنظر گرفته شده است. در سناریوی اول، اندازه MAC در پروتکل کنترل جامعیت سنتی و اندازه دنباله جایگشت در روش پیشنهادی و [۶] را یکسان درنظر خواهیم گرفت. در این حالت، انرژی مصرفی حاصل از تبادل داده برای روش پیشنهادی و پروتکل کنترل جامعیت سنتی تقریبا یکسان خواهد بود. زیرا اندازه بسته‌های مبادله شده در هردو پروتکل یکسان می‌باشد. با این وجود، در روش پیشنهادی دنباله جایگشت فقط برای بسته‌های اعتبار سنجی محاسبه می‌شود؛ در صورتی که در پروتکل کنترل جامعیت سنتی ساخت MAC برای تمامی بسته‌ها صورت می‌پذیرد. در نتیجه طبیعی است که در حالت استفاده از پروتکل پیشنهادی، پردازنده انرژی مصرفی کمتری را نسبت به پروتکل کنترل جامعیت سنتی مصرف کند. از طرفی روش پیشنهادی، عمل جامعیت داده را از طریق عملیات محاسباتی کمتری نسبت به [۶] انجام داده که نتیجه آن، کاهش انرژی مصرفی پردازنده خواهد بود. این نتایج را می‌توان در جدول (۲) مشاهده نمود.

براساس جدول (۲)، با افزایش اندازه MAC/دنباله جایگشت، اختلاف انرژی مصرفی پردازنده در روش پیشنهادی و دو روش مورد مقایسه نیز افزایش می‌یابد. بصورتی که در برای MAC/دنباله جایگشت با طول ۶۴ بیت روش پیشنهادی موجب صرفه‌جویی ۵۳,۷ درصدی انرژی پردازنده شده و برای طول ۲۵۶ بیت، این میزان صرفه‌جویی به بیش از ۷۶,۵۴ درصد می‌رسد. مقادیر انرژی مصرفی ناشی از تبادل داده و پردازنده برای این آزمایش بصورت نمودار در شکل (۳) نمایش داده شده است. همانطور که در بخش قبل تشریح گردید، امنیت پروتکل پیشنهادی از پیچیدگی الگوی شبه‌تصادفی جایگشت مبتنی بر مدل آشوب ناشی می‌شود. بصورتی که با کوتاه کردن طول دنباله آشوب، کشف الگوی جایگشت دشوارتر خواهد شد. بنابراین، می‌توان یک تابع درهم‌سازی ۶۴ بیتی را برای پروتکل پیشنهادی کافی دانست [۶]. با این وجود، اغلب پروتکل‌های مبتنی بر MAC برای دستیابی به همان سطح از امنیت به MACهایی با طول بیشتر از ۱۲۸ بیت نیاز دارند. با این توضیحات در سناریوی دوم، اندازه دنباله جایگشت در پروتکل پیشنهادی را برابر با ۶۴ بیت درنظر گرفته و اندازه MAC در پروتکل سنتی را از ۶۴ بیت تا ۱۲۸ بیت تغییر خواهیم داد. در این حالت، با افزایش طول MAC، اندازه بسته‌های مبادله شده در پروتکل پیشنهادی کمتر از پروتکل سنتی خواهد بود. در نتیجه طبیعی است که در این حالت، روش پیشنهادی بتواند در تبادل داده نیز موجب کاهش انرژی مصرفی گردد. این نتایج در جدول (۳) نمایش داده شده است. براساس نتایج نمایش داده شده در جدول (۳)، پروتکل پیشنهادی می‌تواند در این حالت، علاوه بر صرفه‌جویی در مصرف انرژی پردازنده؛ در تبادل داده نیز میزان انرژی مصرفی را تا بیش از ۲۳ درصد کاهش دهد. این نتایج بصورت نمودار در شکل (۴) نمایش داده شده است.

این نتایج نشان می‌دهد که پروتکل پیشنهادی برای شناسایی داده‌های تحریف شده و تأمین جامعیت داده‌ها در شبکه سلامت هوشمند منجر به کاهش چشمگیر انرژی مورد نیاز نسبت به روش‌های پیشین می‌شود.

جدول (۲): مقایسه انرژی مصرفی پروتکل پیشنهادی با روش‌های پیشین در سناریوی ۱

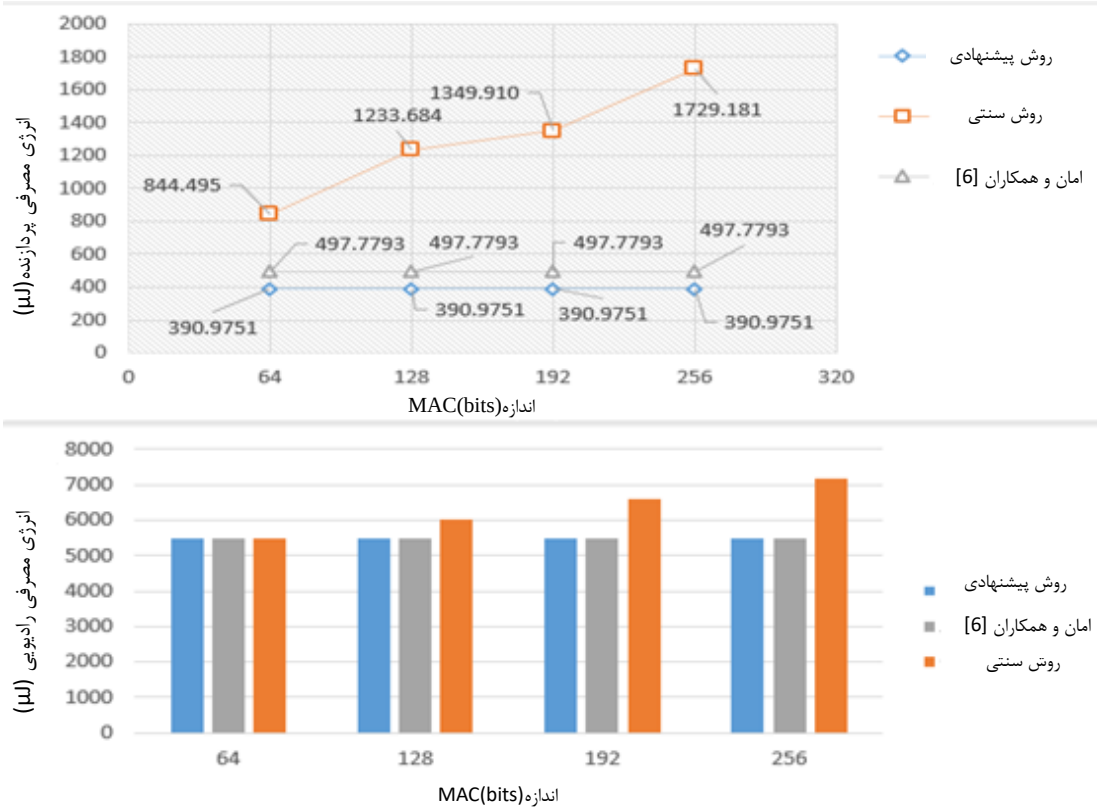
	اندازه MAC (bits)	روش پیشنهادی(µJ)	امان و همکاران [6] (µJ)	روش سنتی(µJ)	بهبود نسبت به مرجع (%) [6]	بهبود نسبت به روش سنتی(%)
انرژی مصرفی پردازنده	۶۴	۳۹۰.۹۷۵۱	۴۹۷.۷۷۹۳	۸۴۴.۴۹۵	۲۱.۴۶	۵۳,۷۰
	۱۲۸	۴۲۴.۳۷۹۰	۵۳۳.۰۰۹۵	۱۳۲۰.۹۹۸	۲۰.۳۸	۶۷.۸۷
	۱۹۲	۴۵۷.۹۲۱۴	۵۷۱.۰۸۵۰	۱۵۴۸.۷۰۵	۱۹.۸۲	۷۰.۴۳
	۲۵۶	۴۹۱.۰۹۵۳	۶۰۲.۶۸۳۹	۲۰۹۳.۵۹۷	۱۸.۵۲	۷۶.۵۴
انرژی مصرفی رادیویی	۶۴	۵۴۷۹.۴۶۵	۵۴۸۱.۶۹۲	۵۴۸۳.۴۵۲	≈ ۰,۰۰	≈ ۰,۰۰
	۱۲۸	۶۰۱۹.۵۲۸	۶۰۲۲.۱۹۳	۶۰۱۹.۱۲۸	≈ ۰,۰۰	≈ ۰,۰۰
	۱۹۲	۶۵۸۶.۵۰۶	۶۵۸۸.۲۳۷	۶۵۹۰.۹۱۵	≈ ۰,۰۰	≈ ۰,۰۰
	۲۵۶	۷۱۶۴.۹۱۶	۷۱۶۵.۹۰۹	۷۱۶۸.۲۷۵	≈ ۰,۰۰	≈ ۰,۰۰



شکل (۳): مقادیر انرژی مصرفی در سناریوی ۱

جدول (۳): مقایسه انرژی مصرفی پروتکل پیشنهادی با روش‌های پیشین در سناریوی ۲

	اندازه MAC (bits)	روش پیشنهادی (µJ)	امان و همکاران [6] (µJ)	روش سنتی(µJ)	بهبود نسبت به مرجع (%) [6]	بهبود نسبت به روش سنتی(%)
انرژی مصرفی پردازنده	۶۴	۳۹۰.۹۷۵۱	۴۹۷.۷۷۹۳	۸۴۴.۴۹۵	۲۱.۴۶	۵۳.۷۰
	۱۲۸	۳۹۰.۹۷۵۱	۴۹۷.۷۷۹۳	۱۳۲۰.۹۹۸	۲۱.۴۶	۶۸.۳۱
	۱۹۲	۳۹۰.۹۷۵۱	۴۹۷.۷۷۹۳	۱۵۴۸.۷۰۵	۲۱.۴۶	۷۱.۰۴
	۲۵۶	۳۹۰.۹۷۵۱	۴۹۷.۷۷۹۳	۲۰۹۳.۵۹۷	۲۱.۴۶	۷۷.۳۹
انرژی مصرفی رادیویی	۶۴	۵۴۷۹.۴۵۶	۵۴۸۱.۶۹۲	۵۴۸۳.۴۵۲	≈ ۰.۰۰	≈ ۰.۰۰
	۱۲۸	۵۴۷۹.۴۵۶	۵۴۸۱.۶۹۲	۶۰۱۹.۱۲۸	≈ ۰.۰۰	۸.۹۷
	۱۹۲	۵۴۷۹.۴۵۶	۵۴۸۱.۶۹۲	۶۵۹۰.۹۱۵	≈ ۰.۰۰	۱۶.۸۶
	۲۵۶	۵۴۷۹.۴۵۶	۵۴۸۱.۶۹۲	۷۱۶۸.۲۷۵	≈ ۰.۰۰	۲۳.۵۶



شکل (۴): مقادیر انرژی مصرفی در سناریوی ۲

۴-۴- سربار ارتباطی

سربار ارتباطی برای بیشتر روش‌های مبتنی بر رمزنگاری مانند RSA معمولاً در محدوده ۱۲۸ تا ۲۵۶ بایت است. با توجه به تابع درهم‌سازی ۶۴ بیتی، پروتکل پیشنهادی فقط ۸ بایت سربار در هر بسته تولید خواهد نمود. اگر ارسال MAC همراه هر بسته را نیز در نظر بگیریم، باز هم حداقل ۸ بایت سربار در هر بسته تولید خواهد شد. با این حال، بسیاری از روش‌های مبتنی بر MAC به یک MAC با اندازه ۱۲۸ بیت احتیاج دارند، که نتیجه آن افزایش سربار ارتباطاتی هر بسته به ۱۶ بایت خواهد بود. در نتیجه، پروتکل پیشنهادی دارای سربار ارتباطی کمتری نسبت به این روش‌ها می‌باشد.

۵- نتیجه گیری

در این مقاله یک روش جدید و کارآمد به منظور تأمین جامعیت داده در شبکه سلامت هوشمند ارائه گردید. روش پیشنهادی از یک تابع درهم‌سازی و جایگشت آشوبگون مبتنی بر تئوری آشوب وابسته به فضا و زمان جهت کنترل جامعیت داده استفاده می‌کند. مطالعه عملکرد پروتکل پیشنهادی در فرآیند شبیه‌سازی نشان داد که روش پیشنهادی در برابر انواع حملات مانند تحریف و تزریق داده غیرمجاز ایمن بوده و بعلاوه می‌تواند سربار داده درحال تبادل در شبکه را کاهش دهد. از طرفی پیچیدگی محاسباتی پایین روش پیشنهادی موجب می‌شود تا این پروتکل از اتلاف منابع محاسباتی جلوگیری نموده و انرژی مصرفی پردازنده بصورت قابل توجهی کاهش یابد. تمامی این ویژگی‌ها موجب می‌شود تا روش پیشنهادی یک راهکار مناسب و قابل اعتماد جهت کنترل جامعیت داده در کاربردهای بلادرنگ باشد.

در کارهای آینده تلاش می‌شود تا با ترکیب مدل پیشنهادی با یک پروتکل مسیریابی، یک پروتکل مسیریابی ایمن و انرژی کارآمد جهت بکارگیری در شبکه سلامت هوشمند ارائه شود. همچنین مطالعه کاربرد روش پیشنهادی در سایر انواع شبکه‌های بی‌سیم می‌تواند موضوع تحقیقات آینده باشد.

منابع

[1] Masood, I., Wang, Y., Daud, A., Aljohani, N. R., & Dawood, H., *Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure.* Wireless Communications and Mobile Computing, 2018.

[2] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G., *Security and privacy in the medical internet of things: a review*. Security and Communication Networks, 2018.

[3] Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y., *A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature*. IEEE Access, 7, 90036-90044. 2019.

[4] Kaâniche, N., Jung, E., & Gehani, *A. Efficiently Validating Aggregated IoT Data Integrity.* IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService) (pp. 260-265). IEEE. 2018.

[5] Matsemela, G., Rimer, S., Ouahada, K., Ndjiongue, R., & Mngomezulu, Z. *Internet of things data integrity*. In IST-Africa week conference (IST-Africa) (pp. 1-9). IEEE. 2017.

[6] Aman, M. N., Sikdar, B., Chua, K. C., & Ali, A., *Low Power Data Integrity in IoT Systems*. IEEE Internet of Things Journal, 5(4), 3102-3113. 2018.

[7] Zhang, Y. Q., He, Y., & Wang, X. Y., *Spatiotemporal chaos in mixed linear–nonlinear two-dimensional coupled logistic map lattice*. Physica A: Statistical Mechanics and its Applications, 490, 148-160. 2018.

[8] Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K., & Kamhoua, C. *Preserving data integrity in iot networks under opportunistic data manipulation.* IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 446-453). IEEE. 2017.

[9] Yang, X., Zhao, P., Zhang, X., Lin, J., & Yu, W. ,*Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid*. IEEE Internet of Things Journal, 4(1), 147-161. 2016

[10] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L., *Blockchain based data integrity service framework for IoT data*. IEEE International Conference on Web Services (ICWS) (pp. 468-475). IEEE. 2017.

[11] Machado, C., & Fröhlich, A. A. M. *Iot data integrity verification for cyber-physical systems using blockchain*. IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC) (pp. 83-90). IEEE. 2018.

[12] Chen, Y. J., Wang, L. C., & Wang, S. *Stochastic Blockchain for IoT Data Integrity*. IEEE Transactions on Network Science and Engineering. 2018.

[13] Zeraoulia, E., "Models and applications of chaos theory in modern sciences" . CRC Press. 2011.

[14] Xu, G., Miao, X., & Zheng, Y. *A Novel Diffusion-Permutation Image Encryption Scheme Based on Spatiotemporal Chaos.* Sensors & Transducers, 160(12), 348, 2013.

[15] Gao, H., Zhang, Y., Liang, S., & Li, D. *A new chaotic algorithm for image encryption*. Chaos, Solitons & Fractals, 29(2), 393-399, 2006.