فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Fall 2021, 2 (3), 37-51
DOR: 20.1001.1.27832570.1400.2.4.8.5

Received: 09 June 2021
Accepted: 24 July 2021

A Two-Layered Trust Management Approach in Software Defined Wireless Sensor Networks

Navid Mohammad Ebadati Esfahani[1], Mehrdad Ashtiani[2*], Nasrin Hamzelou[3]

1. PhD. Student, Faculty of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.
2. Assistant Professor, Faculty of Computer Engineering, Iran University of Science and Technology, Tehran, Iran.
(*Corresponding Author*) m_ashtiani@iust.ac.ir
3. PhD. Student, Faculty of Electrical Engineering, IT & Computer Sciences, Qazvin Branch Islamic Azad University, Qazvin, Iran.

Abstract

Background and Purpose: The main purpose of software-defined networks is to separate data from the control. That is, the elements are obtained through centralized remote controllers, rather than through distributed control protocols. Identifying a trusted node from an unsafe node is also one of the challenges in this area. By finding and removing malicious nodes from secure nodes, packets are re-sent and energy is prevented, and network life is increased. On the other hand, the existence of hostile nodes to collect information or destroy sensitive data, as well as disabling the network and disrupting it in various ways, has made this area of great importance. In cases where the workspace and environment are secured, the sensor node may become a selfish node for the rest of its life, refusing to send or receive information. In this way, the data that exists in the previous path to the destination node will never be collected and without trust management, the validity of the received information will remain unclear. Therefore, the failure of a sensor node or its death due to lack of energy should not cause failure or disruption of the entire network, and the existence of various routes to send data using the calculated trust can be considered as a way to do this. Even so, they are often controlled in a distributed way. However, their potential challenges are more complex and can theoretically be solved with better network knowledge. In software-defined wireless sensor networks, security and energy are two critical issues. However, few studies have provided these two aspects simultaneously. With the widespread deployment and use of sensor networks, security and trust management issues are becoming a major concern. So far, the main focus of different research has been on building practical and useful sensor networks, with less emphasis on security.

Methods: This research examines the security challenges in software-defined wireless sensor networks and summarizes the key issues that need to be addressed to achieve security. In this study, sensors were studied that, to conserve their energy, became selfish nodes and refused to receive or send data. Trust in such nodes will be discussed through the four criteria of honesty, intimacy, energy, and humility. In this regard and as the first step, the clustering is taking place by a software-defined network, to cluster the number of distributed sensors. For this purpose, the combination of two algorithms, which are *k*-means and *k*NN, is done based on the number of sensors used by the software-defined network, and then the optimal routing, which is based on energy consumption and trust priority is considered.

Results: The proposed model is deployed for three different scenarios, with 50, 100, and 200 sensors with random distribution. Furthermore, some safe methods for achieving security in wireless sensor networks are described, and finally, a proposed integrated approach based on trust to ensure the security of sensor networks is presented.

Discussion and Conclusion: The results of this study show that the proposed model has been able to have optimal energy consumption due to building trust.

Keywords: Wireless sensor networks, software-defined networks, trust, security.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران

ارائه یک رویکرد مدیریت اعتماد دولایه در شبکه‌های حسگر بی‌سیم تعریف‌شده برمبنای نرم‌افزار

تاریخ دریافت: ۱۴۰۰/۰۳/۱۹ سال دوم، پاییز ۱۴۰۰
تاریخ پذیرش: ۱۴۰۰/۰۵/۰۲ شمارهٔ سوم، صص: ۳۷ - ۵۱

نویدمحمد عبادتی‌اصفهانی[1] ، مهرداد آشتیانی[2*]، نسرین حمزه‌لو[3]

۱. دانشجوی دکتری، دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر، تهران، ایران. n_ebadati@iust.ac.ir
۲ .استادیار، دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر، تهران، ایران. (نویسندهٔ مسئول) m_ashtiani@iust.ac.ir
۳ .دانشجوی دکتری، دانشگاه آزاد اسلامی واحد قزوین، دانشکده مهندسی برق، آی‌تی و کامپیوتر، قزوین، ایران.nasrinhamzelou@qiau.ac.ir

چکیده: امنیت و انرژی دو مسئله حیاتی در شبکه‌های حسگر بی‌سیم نرم‌افزارمحور، هستند. ولی، پژوهش‌های کمی این دو جنبه را همزمان ارائه‌کرده‌اند. با استقرار گسترده شبکه‌های حسگر و کاربرد این شبکه، مسائل امنیتی و مدیریت اعتماد، تبدیل به یک نگرانی اساسی می‌شود. در این تحقیق به بررسی چالش‌های امنیتی در شبکه‌های حسگر بی‌سیم مبتنی‌بر نرم‌افزار تعریف‌شده پرداخته‌شده‌است. در این پژوهش به حسگرهایی پرداخته‌شده که برای حفظ انرژی خود، به گره خودخواه تبدیل‌شده و از دریافت و یا ارسال داده‌ها خودداری‌می‌کنند. اعتماد به این‌گونه گره‌ها از طریق چهار معیار صداقت، صمیمیت، انرژی و تواضع بحث و بررسی‌شده‌است. در این راستا، از ترکیب دو الگوریتم k-means و k-NN، خوشه‌بندی بر اساس تعداد حسگرهای به‌کاررفته توسط شبکه تعریف‌شده نرم‌افزاری، انجام و سپس مسیریابی بهینه بر اساس مصرف انرژی و با اولویت اعتماد صورت‌می‌پذیرد. سپس شبیه‌سازی در سه سناریو تعریف‌شده ۵۰، ۱۰۰ و ۲۰۰ حسگر توزیع‌شده به‌صورت اتفاقی پیاده‌سازی‌شده‌است. همچنین برخی از روش‌های ایمن برای دستیابی به امنیت در شبکه‌های حسگر بی‌سیم توضیح‌داده‌شده و در آخر رویکرد یکپارچه پیشنهادی مبتنی بر اعتماد برای تأمین امنیت شبکه‌های حسگر ارائه‌شده‌است. نتایج تحقیق نشان‌می‌دهد که مدل پیشنهادی با توجه به ایجاد اعتماد، توانسته مصرف انرژی بهینه‌ای نیز داشته‌باشد.

واژه‌های کلیدی: شبکه‌های حسگر بی‌سیم، شبکه‌های نرم‌افزار محور، اعتماد، امنیت.

۱. مقدمه

توسعه حسگرهای هوشمند در سال‌های اخیر باعث پیشرفت شبکه‌های حسگر بی‌سیم شده‌است. شبکه‌های حسگر بی‌سیم[1] شامل میکروحسگرهایی هستند که قادر به کنترل عوامل فیزیکی و محیطی مانند دما، رطوبت، ارتعاشات، حرکات، وقایع لرزه‌ای و غیره هستند. گره‌های حسگر کوچک، ارزان و هوشمند هستند [۱]. با بهبود سیستم های مکانیکی میکروالکترونیکی ظهور پارادایم اینترنت اشیاء[2] دامنه تقاضای شبکه‌های حسگر بی‌سیم را افزوده است. یک شبکه حسگر بی‌سیم شامل گره‌های حسگر با ارتباطات، محاسبات و قابلیت‌های سنجش است. گره‌های حسگر عمدتاً باتری دارند که عمر آن‌ها را محدود-می‌کند. آن‌ها اغلب به‌طور تصادفی در یک منطقه بزرگتر برای اهداف نظارتی مستقرمی‌شوند. بنابراین، ارتباطات و محدوده‌های سنجش برای کنترل ارتباط با دیگر گره‌ها و پوشش کل منطقه با درخواست موردنظر کنترل‌می‌شود. در گذشته، مدیریت خودمحور با کنترل توزیع‌شده، رویکرد بصری برای اجرای این شبکه‌ها بوده‌است. به‌این‌ترتیب، صرفه‌جویی در انرژی همیشه یک هدف مهم برای گسترش عمر شبکه است [۲]. شبکه تعریف‌شده نرم‌افزار[3]، یک معماری شبکه در حال ظهور است که این امکان را برای غلبه بر محدودیت‌های فعلی زیرساخت شبکه فراهم‌کرده و کنترل شبکه و داده را از هم جدامی‌کند. به این معنا که کنترل‌کننده هوشمند عناصر ارسال را با قوانین ارسال برای بسته‌های داده‌ای از جریان‌های مختلف تنظیم‌می‌کند. کنترل‌کننده، اطلاعات کافی برای انجام این کار را دارد به طوری که پروتکل‌های کنترل توزیع در عناصر ارسال، دیگر موردنیاز نیست. علاوه‌براین، کنترل‌کننده ممکن است برای بهینه‌سازی شبکه با برنامه‌ها ارتباط برقرارکند [۳, ۴].

شبکه‌های حسگر بی‌سیم مبتنی‌بر نرم‌افزار تعریف‌شده اخیراً با این هدف ارائه‌شده‌است که حسگرها بتوانند از نرم‌افزار تعریف‌شده سودببرند. عملیات گره‌های حسگر باید ساده‌تر شود تا صرفه‌جویی در انرژی و مدیریت از طریق یک کنترلر قدرتمند که دارای دید کلی از شبکه است، اتفاق‌بیفتد نه از طریق پروتکل‌های کنترل توزیع. کنترل‌کننده قادر به مدیریت شبکه و برنامه‌های کاربردی است و باعث صرفه‌جویی در انرژی می‌شود، به‌طورقطع ایجاد تعادل انرژی باقیمانده در شبکه باعث به-حداکثررساندن طول‌عمر شبکه خواهدشد. تفاوت اصلی وجود نرم‌افزار تعریف‌شده در مرکز داده‌ای، این است که کنترل‌کننده در یک شبکه حسگر بی‌سیم برای ارتباط و ارسال اطلاعات با گره‌های حسگر که در فاصلهٔ دورتری هستند احتمالاً به جای استفاده از یک شبکه کنترل اختصاصی بیش از چندین معامله خواهندداشت [۵]. در این مطالعه تحقیقاتی هدف، بررسی راه‌حل‌های ایجاد اعتماد است. یکی از مهمترین مسائل پس از پیدایش نرم‌افزار تعریف‌شده در شبکه‌های حسگر بی‌سیم و اینترنت اشیاء، نقش اعتماد به داده‌های واقعی دریافتی و ارسال آن به کنترلر مرکزی است که بیشترین انرژی نیز در این راستا مصرف‌می‌شود.

بنابراین در بررسی حاضر، مقدمه‌ای برای نرم‌افزار تعریف‌شده در شبکه‌های سیمی و شبکه‌های حسگر بی‌سیم فاقد نرم‌افزار تعریف‌شده ارائه‌می‌گردد. در بخش دوم کارهای انجام‌شده برای حل مسئله اعتماد و امنیت در شبکه‌های حسگر بی‌سیم مبتنی‌بر نرم‌افزار تعریف‌شده بررسی و در بخش سوم به ارائه مدل پیشنهادی و مدل اعتماد و الگوریتم‌های مربوطه پرداخته‌شده‌است. بخش چهارم به ارزیابی و پیاده‌سازی مدل پیشنهادی، شبیه‌سازی مربوطه و بررسی مصرف انرژی، خطا و میزان ارسال بسته‌های شبکه در مسیریابی اعتماد پرداخته و در بخش پنجم، نتیجه‌گیری نهایی، محدودیت‌ها و پیشنهادهای آتی برای محققان بیان-شده‌است.

۲.پیشینهٔ پژوهش

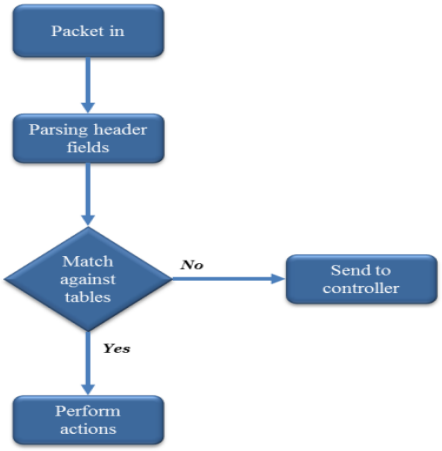
این تحقیق بر روی ابزارهای منبع باز که آزادانه در دسترس و قابل-استفاده‌اند متمرکزشده‌است و مروری کلی از ابزارهای نرم‌افزاری برای نرم‌افزار تعریف‌شده شبکه‌های حسگر بی‌سیم ارائه‌شده و رویکردهای مبتنی‌بر نرم‌افزار تعریف‌شده برای شبکه‌های حسگر بی‌سیم بررسی‌شده و ادبیات تحقیق در چند دسته طبقه‌بندی‌می‌شود:

۱. جریان آزاد، ۲. بهره‌وری انرژی، ۳. مسیریابی، ۴. پویایی
۵. خوشه‌بندی، ۶. قابلیت اطمینان، ۷. کیفیت خدمات
۸. مدیریت، ۹. بومی‌سازی، ۱۰ مدیریت اعتماد، ۱۱. انتقال قدرت بی‌سیم.

جریان آزاد، معماری رابط جنوبی برای نرم‌افزار تعریف‌شده شبکه است که در دانشگاه استنفورد توسعه‌داده‌شده‌است [6]. هر سوئیچ جریان آزاد، دارای جداول جریان است که عمدتاً تعداد کمی از قوانین جریان را به‌عنوان جریان ورودی حفظ‌می‌کند و شامل زمینه‌های تطابق، شمارنده‌ها و اقدامات می‌باشند. قوانین ارسال و انتقال داده‌ها را می‌توان به دو روش پیشگیرانه و واکنشی تعریف‌کرد [7].

جریان حسگر تلاش‌می‌کند ویژگی‌های جریان آزاد را در شبکه‌های حسگر بی‌سیم استفاده‌کند [8]. این موضوع باعث جدایی سطح کنترل و سطح داده در شبکه حسگر بی‌سیم می‌شود. در جریان حسگر، ارتباط بین کنترل‌کننده و ایستگاه پایه بر اساس جریان آزاد است. جریان حسگر، قواعد TCP/IP[4] بر پایه آی‌پی را برای ارتباطات ایستگاه پایه و گره‌های حسگر در سطح داده استفاده‌می‌کند. شکل (۱) جریان اصلی در ارسال یک بسته را به صورت جریان آزاد، نمایش می‌دهد. جریان آزاد شامل سه بخش ارتباطی است: کنترل‌کننده تغییر[5]، ناهمزمان[6] و متقارن[7] [9] . کنترل‌کننده تغییر برای تنظیم، برنامه‌نویسی و بازیابی اطلاعات استفاده-می‌شود. ارتباط ناهمزمان توسط سوئیچ به کنترلر آغازمی‌شود و در مورد ورود بسته‌ها، تغییرات، خطاها و غیره است. ارتباط متقارن بدون ارسال درخواست از کنترل‌کننده یا سوئیچ ارسال‌می‌شود. حسگر جریان آزاد[8] به عنوان پروتکل ارتباطی بین سطح داده و سطح کنترل معرفی‌شده‌است. در این معماری، هر گره حسگر قسمتی از ارسال بسته مبتنی‌بر جریان و کنترل‌کننده بخش هوشمند برای تصمیم‌گیری است. هر گره می‌تواند با کنترل‌کننده از طریق حسگر جریان آزاد ارتباط برقرارکند و کنترل‌کننده نیز از طریق واسط‌های برنامه کاربردی قابل برنامه‌ریزی است. این حسگر

از هر دو ارتباط مبتنی‌بر آی‌پی و نامبتنی‌بر آی‌پی، بین کنترل‌کننده و شود و شبکه، دیگر قابل‌اعتماد نیست. استفاده از یک کنترل اضافی برای گره پشتیبانی‌می‌کند [10].

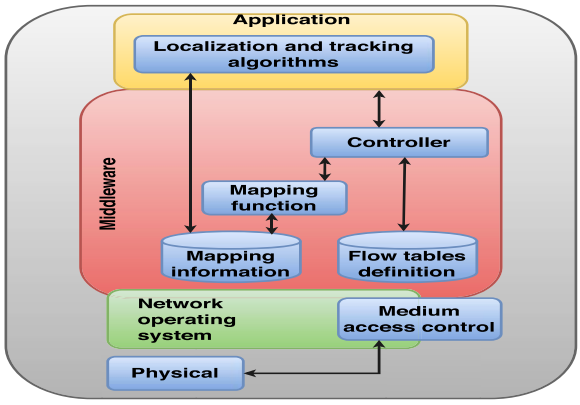


شکل۱: جریان آزاد ارسال بسته‌ها [11]

یک پیشنهاد این است که ارتباطات با محاسبه قبلی انجام شود، یعنی کاهش هزینه‌های ارتباطی با انجام محاسبات بیشتر. بنابراین راه‌حل‌های مختلف برای پردازش هوشمندانه داده‌های محلی برای به‌حداقل‌رساندن استفاده از انرژی پیشنهادشده‌است [12]. در اینجا، ایجاد انرژی کارآمد را به سه بخش تقسیم‌می‌کنیم: طول‌عمر، کنترل پوشش و خوشه‌بندی [13, 14]. در معماری پیشنهادی برای برنامه‌ریزی خواب، تمام گره‌ها از طریق اتصالات مناسب به سوئیچ و سوئیچ به کنترل‌کننده نرم‌افزار تعریف‌شده، متصل‌می‌شوند. درنتیجه، هر گره در شبکه می‌تواند دو نوع اتصال داشته باشد: ارتباط با دیگر گره‌ها و ارتباط با کنترل‌کننده. در این مورد، وظایف محاسبات فقط از گره‌ها به کنترلر منتقل‌می شود. پس از تصمیم‌گیری توسط کنترل‌کننده برای هر گره، قواعد می‌تواند بر روی گره‌ها نصب‌شود [15, 16]. چندین پروتکل مسیریابی برای نرم‌افزار تعریف‌شده شبکه‌های حسگر بی‌سیم گزارش‌شده‌است [۴, 17, 15, 18].

راه‌حل پویایی مبتنی‌بر نرم‌افزار تعریف‌شده برای گره‌های موبایل پیشنهادشده‌است. در این کار، پوشش مانع، برای یک منطقه پویا درنظرگرفته‌شده‌است و گره‌ها می‌توانند در کل شبکه حرکت‌کنند. یک کنترل استراتژی حرکت وجوددارد که حرکت گره را کنترل‌می‌کند. برای رفع نیاز پوشش مانع، کنترل‌کننده مکان‌های جدید را برای گره‌ها تعیین‌می‌کند، به‌گونه‌ای که گره‌های فعال می‌توانند هر گونه نفوذ به شبکه را تشخیص‌دهند [19]. یک روش خوشه‌بندی مبتنی‌بر نرم‌افزار تعریف‌شده برای به‌حداقل‌رساندن انرژی مصرف گره‌ها پیشنهادشده‌است [20]. کنترل‌کننده نرم‌افزار تعریف‌شده گره‌ها را به چند دسته بر اساس انرژی باقیمانده و تعداد گره‌های همسایه تقسیم‌می‌کند. در راستای تعادل هزینه‌های ارتباطات، یک درخت مسیریابی در میان خوشه‌ها برای هدایت ترافیک شبکه ایجادمی‌کند.

در این بخش، گره‌ها را با استفاده از زنجیره مارکوف پیوسته[9] بررسی‌می‌کنیم. هر کنترل‌کننده یا گره می‌تواند خراب‌شود، مثلاً اگر شبکه از یک کنترل‌کننده واحد استفاده‌کند، می‌تواند نقطه شکست[10] بهبود قابلیت اطمینان کل شبکه پیشنهاد می‌شود. در این حالت، اگر یک کنترل‌کننده نتواند به‌درستی عمل‌کند، کنترل‌کننده یدکی را می‌توان جایگزین کرد تا قابلیت اطمینان موردنظر را در لایه کنترل، حفظ‌کند. هر گره حسگر در این الگوریتم احتمال شکست خاصی دارد. [21]. معماری پیشنهادی برای افزایش بهره‌وری کلی شبکه درنظرگرفته‌می‌شود و چندین جنبه از جمله ناهمگونی، پوشش، شکست و اعتبار را لحاظ‌می‌کند. کنترل‌کننده نرم‌افزار تعریف‌شده با انتخاب گره‌های مناسب، مصرف انرژی را متعادل‌می‌کند[22]. در الگوریتم مبتنی‌بر نرم‌افزار تعریف‌شده، تأمین کیفیت خدمات در تکرار و ازدحام تراکم داده بررسی‌شده‌است. ازاین‌رو، تعداد ترافیک و اطلاعات ترافیکی محلی در کنترل‌کننده شبکه برای توزیع ترافیک استفاده‌شده‌است. با کنترل تراکم به‌وسیله کنترل‌کننده نرم‌افزار تعریف‌شده در شبکه حسگر بی‌سیم، ۴۶٪ ازدست‌رفتن بسته‌ها کاهش‌یافته‌است [23]. شکل (۲) معماری ایستگاه پایه هوشمند را نشان‌می‌دهد. این هوشمندی دارای پنج لایه در ستون پروتکل است: کنترل دسترسی فیزیکی، سیستم‌عامل شبکه[11]، میان‌افزار[12] و لایه کاربردی. در این معماری که در ایستگاه پایه مستقر است، مسئولیت تعریف جداول جریان از برنامه‌های شبکه، مانند مسیریابی است.

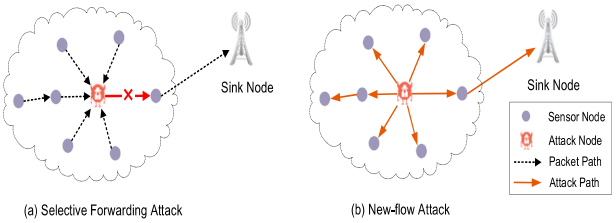


شکل ۲: معماری ایستگاه پایه هوشمند [23]

در پژوهش‌هایی اقدامات اعتماد و امنیت در نرم‌افزار تعریف‌شده، شبکه حسگر بی‌سیم و شبکه‌های سنتی به‌خوبی بررسی‌شده‌اند مثل: تشخیص نفوذ، مسیریابی امن و داده‌های امن. به‌عنوان یک مکمل ضروری برای مکانیزم‌های امنیتی مبتنی بر رمزنگاری، مدیریت اعتماد و طرح‌های اعتماد مسیریابی شبکه حسگر بی‌سیم سنتی می‌توانند به‌طور مؤثر در برابر مهاجمین داخلی دفاع‌کرده و امنیت، اطمینان و بی‌طرفی سیستم را افزایش‌دهند [24]. با طراحی سنترا[13]، یک پروتکل مسیریابی کارآمد مبتنی‌بر اعتماد متمرکز با یک طرح احراز هویت مناسب برای شبکه‌های حسگر بی‌سیم ارائه‌شده که هر گره در این سیستم به‌صورت دوره‌ای، لیستی از همسایگان و تجربه‌های ارسال بسته خود را به ایستگاه پایه ارسال‌می‌کند [25]. همان‌طور که در شکل (۳) قسمت a نشان‌داده‌شده‌است، در یک شبکه بی‌سیم چندمنظوره، حمله ارسالی منتخب[14]، تهدیدی است که توسط گره آسیب‌دیده اتفاق‌می‌افتد و در آن بسته

ارسالی را برای پایین‌آوردن نسبیت تحویل بسته در شبکه، انتقال-نمی‌دهد. این حمله، حمله حفره خاکستری[15] نامیده‌می‌شود. اگر مهاجم نوع خاصی از بسته‌ها را ازبین‌ببرد، یا حمله حفره سیاه[16] اگر مهاجم تمام بسته‌ها را ازبین‌ببرد. در مقایسه با شبکه حسگر بی‌سیم، گره آسیب‌دیده برای عملکرد عادی نرم‌افزار تعریف‌شده شبکه حسگر بی‌سیم، مضر است.

مطابق شکل (۳) قسمت b، از زمانی که بسته‌ها به کنترلر ارسال-می‌شود، مهاجم می‌تواند حمله جدید را با تزریق بسته‌های جدید[17] به گره‌های همسایه خود راه‌اندازی‌کند. گره‌های همسایه نمی‌توانند ترافیک قانونی و غیرقانونی را تشخیص‌دهند و بسته‌های جدید را در قالب درخواست قانونی[18] به کنترل‌کننده ارسال‌می‌کنند. به‌این‌ترتیب، این حمله به‌راحتی می‌تواند ترافیک مخرب را به شبکه وارد و پهنای باند و انرژی زیادی را از شبکه مصرف‌کند.



شکل ۳:حمله‌های مخرب ارسال به نرم‌افزار تعریف‌شده شبکه حسگر بی‌سیم [25]

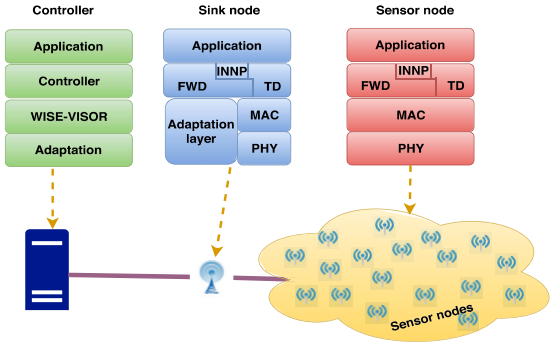
بنابراین، بر اساس اطلاعات اعتماد جمع‌آوری‌شده از گره‌های حسگر، یک طرح مدیریت اعتماد متمرکز در سطح کنترل‌کننده برای شناسایی و جداکردن گره‌های مخرب نیاز است تا بتوان مشکلات امنیتی شبکه را حل‌کرد. در پژوهش دیگری مکانیزم مسیریابی اعتماد، مدیریت انرژی و مؤثربودن مکانیزم مسیریابی برای نرم‌افزار تعریف‌شده شبکه حسگر بی‌سیم را پیشنهادمی‌کند که برای اداره حملات مخرب، مانند انتقال و ارسال انتخابی و حمله جدید است. در ابتدا جداول جریان حسگر[19] را برای تحقق یک طرح نظارت و ارزیابی اعتماد در سطح گره گسترش‌داده و یک کنترل مدیریت اعتماد متمرکز در سطح کنترل‌کننده برای شناسایی و جداکردن گره‌های مخرب بر اساس اطلاعات جمع‌آوری‌شده از گره‌های حسگر را پیشنهادمی‌کنند[26].

۱/۲. نرم‌افزار تعریف‌شده وایز[20]

نرم‌افزار تعریف‌شده وایز، یک چارچوب نرم‌افزاری برای نرم‌افزار تعریف‌شده شبکه‌های حسگر بی‌سیم و یک سخت‌افزار اولیه برای نرم‌افزار تعریف‌شده شبکه‌های حسگر بی‌سیم ارائه‌می‌دهد. این نرم‌افزار تعریف‌شده دارای دو هدف اصلی است: (۱) کاهش میزان اطلاعات مبادله بین گره‌ها نسبت به شبکه‌های حسگر بی‌سیم فاقد نرم‌افزار تعریف‌شده (۲) ایجاد گره‌های حسگر قابل برنامه‌ریزی [27]. معماری این مدل دارای سه جزء مختلف است: گره حسگر، گره سینک و کنترل‌کننده. شکل (۴) معماری کلی و ستون پروتکل هر مؤلفه را نشان‌می‌دهد. هر گره حسگر، در ستون پروتکل خود این لایه‌ها را شامل‌می‌شود: (۱) برنامه (۲) پردازش بسته‌بندی درون شبکه[21] ارسال و کشف پیکربندی (۳) کنترل دسترسی رسانه (۴) فیزیکی.

یک گره سینک دقیقاً مشابه گره حسگر عمل‌می‌کند. لایه‌های دیگر، مانند کشف توپولوژی، ارسال، برنامه کاربردی و غیره. کنترل‌کننده مطابق شکل فوق دارای لایه‌های زیر در ستون پروتکل است. (۱) برنامه (۲) کنترل‌کننده (۳) وایزر (۴) انطباق [28]. لایه انطباق کنترلر، دارای عملکرد مشابه همان لایه در گره سینک است [۲۹].

وایز شامل یک لایه پیکربندی مدیریت است که انتزاع منابع شبکه را فراهم‌می‌کند [30]. لایه کنترل‌کننده، خط مشی‌های شبکه را که توسط گره‌های حسگر اجرامی‌شود، تعریف‌می‌کند.



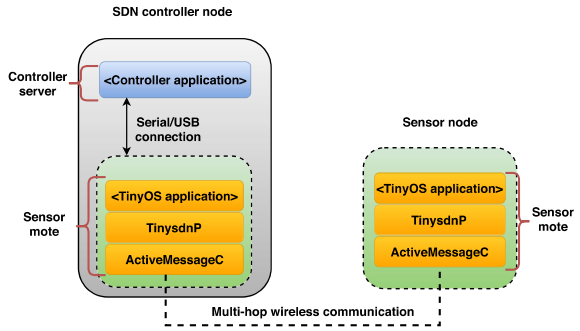
شکل ۴: معماری نرم‌افزار تعریف‌شده وایز و پروتکل پشته [28]

۲/۲. نرم‌افزار تعریف‌شده تاینی[22]

این مدل، یک چارچوب نرم‌افزار تعریف‌شده مبتنی‌بر سیستم‌عامل تاینی برای شبکه‌های حسگر بی‌سیم است [31]. معماری آن دارای دو جزء مختلف است: (۱) گره حسگر فعال که دارای قابلیت‌های یک گره حسگر و سوئیچ نرم‌افزار تعریف‌شده‌است (۲) کنترلر که مسئول کنترل عملیات‌هایی مانند تصمیم‌گیری مسیریابی است. ساختار آن‌ها در شکل (۵) نمایش‌داده‌شده‌است.

۳. روش پیشنهادی

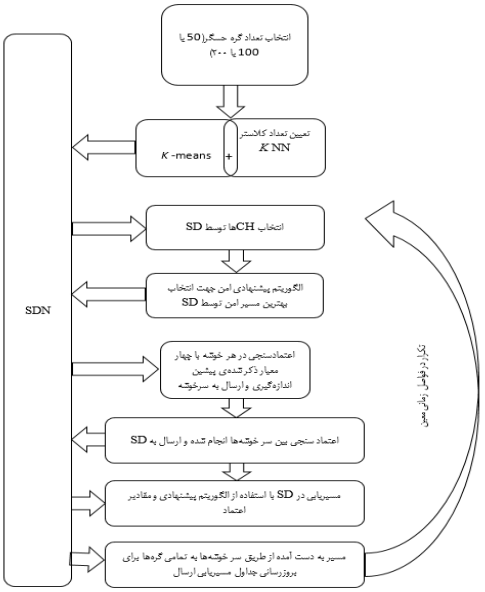
مدل کلی تحقیق در شکل (۶)، در سه سناریو ۵۰ و ۱۰۰ و ۲۰۰ حسگر طراحی‌شده‌است. در ابتدا برای خوشه‌بندی از ترکیب دو الگوریتم k-mean و k-NN استفاده‌شده‌است. پس از آن، سرخوشه‌ها بر اساس انتخاب شبکه نرم‌افزارمحور انتخاب و مسیریابی شروع‌می‌شود. اعتمادسنجی در هر خوشه براساس چهار معیار تعریف‌شده صورت‌گرفته و بر اساس ایجاد اعتماد بین سرخوشه‌ها و سپس بین حسگرها مسیریابی انتخاب‌می‌شود. بعد از آن الگوریتم پیشنهادی پیاده‌سازی‌شده و بر آن اساس، پس از بررسی اعتمادسنجی بر اساس معیارهای ذکرشده، مسیریابی و ارسال اطلاعات صورت‌می‌پذیرد. کنترل کلی مدل توسط شبکه تعریف‌شده نرم‌افزاری صورت می‌پذیرد که خود باعث رفع بسیاری از مشکلات اساسی در شبکه‌های حسگر بی‌سیم است.



شکل۵:لایه‌های اجزای نرم‌افزار تعریف‌شده ریز [31]

۱/۳. الگوریتم خوشه‌بندی

یکی از روش‌های جلوگیری از ازدحام و کاهش مصرف انرژی، خوشه‌بندی است. در این تحقیق از *k*-mean که یکی از پرکاربردترین الگوریتم‌ها در تعیین تعداد خوشه‌های لازم برای خوشه‌بندی است، استفاده‌شده‌است. زمانی که تعداد خوشه‌ها معین‌شد، با به کارگیری الگوریتم *k*NN، نزدیک‌ترین گره همسایه به گره سینک را در هر خوشه مشخص‌می‌کنیم. اصولاً در جایی که گره‌ها همگن و یک‌دست هستند نیاز است تا گره‌ای از گره‌های همان خوشه که معمولاً به گره سینک نزدیک‌تر است را به عنوان سرخوشه معین‌کنیم. به لت تراکنش بالا، به مرور زمان انرژی گره منتخب کم‌می‌شود که برای جلوگیری از مردن گره، مجدد نزدیکترین گره که فاصله اقلیدسی و انرژی بالاتری داشته‌باشد به‌عنوان سرخوشه جدید انتخاب و معرفی‌می‌شود [32]. از ترکیب الگوریتم *k*-mean و *k*NN، جهت خوشه‌بندی به‌شرح زیر استفادشده‌است: این الگوریتم همواره k خوشه با حداقل یک گره در آن‌ها را به‌وجودآورده و تنها مرکز خوشه‌ها را بهینه‌می‌کند، ولی حدود و مرز آن‌ها را بهینه‌نمی‌کند. این الگوریتم تعداد خوشه‌ها را بهینه و مناسب‌ترین سرخوشه را برای هر خوشه تعیین‌می‌کند. خوشه‌بندی با استفاده از الگوریتم (۱) انجام‌می‌شود.



شکل۶: شمای کلی تحقیق

۲/۳. مدل و الگوریتم اعتماد پیشنهادی

بادرنظرگرفتن نقاط قوت و ضعف و همچنین راه‌حل‌های مطرح‌شده، می‌توان ایده‌گرفت تا با ارائه راه‌حلی مناسب برخی از این نقاط ضعف پوشش‌داده‌شود و برخلاف بسیاری از راه‌کارهای ارائه‌شده دیگر، قابل به‌کارگیری در دنیای واقعی باشد. به‌طورکلی، موضوع امنیت در پژوهش‌ها جداگانه و با تأکید کمتر بر ایجاد چارچوب‌های امنیتی قوی برای پشتیبانی از مدل مبتنی‌بر نرم‌افزار تعریف‌شده، بررسی‌شده‌است. درنتیجه، ادغام هر دو مکانیسم امنیتی موجود در شبکه‌های حسگر بی‌سیم و شبکه‌های مبتنی‌بر نرم‌افزار تعریف‌شده برای استفاده در شبکه‌های حسگر بی‌سیم مبتنی‌بر نرم‌افزار تعریف‌شده موردنظر است.

در بیشتر تحقیقات، ماژول اعتماد در کنترل‌کننده است و میزان اعتماد درخواست‌کننده، بر اساس نظرات دریافت‌شده از گره‌های همسایه محاسبه‌می‌شود. این طرح، امکان نظری محاسبه اعتماد متمرکز را نشان‌می‌دهد؛ با این حال، روند جمع‌آوری اعتماد که ممکن است توسط مهاجمین اصلی نیز آسیب‌دیده‌باشد، درنظرگرفته‌نشده‌باشد. همچنین ارزیابی عملکرد این پیشنهادات نیز باید تکمیل شود. با توجه به مشکلاتی که در تحقیقات پیشین به آن اشاره‌شد، نبود کنترل‌کننده و اعتماد به برنامه، یک تهدید جدی است. مکانیسم‌های غیرقابل‌دسترسی اعتماد بین کنترل‌کننده و برنامه نرم‌افزار تعریف‌شده می‌تواند آسیب‌پذیری آن را افزایش‌دهد. حملات می‌توانند کل شبکه را به‌مخاطره‌بیاندازند. درنتیجه به مکانیسم مدیریت اعتماد برای ایجاد امنیت سیستم نیازمندیم. در این تحقیق، چندین خوشه که هر خوشه شامل یک سرخوشه و چندین گره حسگر هستند، بررسی‌می‌شود که همگی در یک ناحیه جغرافیایی با هم همکاری‌می‌کنند. سرخوشه‌ها توسط الگوریتم‌های *k*-mean و *k*NN انتخاب‌می‌شوند. یک گره داده‌های حس‌شده خود را به سرخوشه هدایت و ارسال‌می‌کند و سرخوشه این اطلاعات را به پایگاه اصلی می‌فرستد. اگر سرخوشه به پایگاه اصلی نزدیک نباشد، اطلاعات را به سرخوشه‌های دیگر ارسال و به این ترتیب اطلاعات به پایگاه اصلی می‌رسد.

با ترکیب معیارهای دو نوع اعتماد، کیفیت سرویس و اعتماد اجتماعی به یک اعتماد جامع‌تر دست‌یافته و در مدل از آن استفاده‌خواهدشد. اعتماد اجتماعی و کیفیت سرویس دارای معیارهای گوناگونی در ارزیابی اعتماد هستند و از میان آن‌ها، صمیمیت برای به‌دست‌آوردن نزدیکی تجربه ارتباطات و صداقت برای ارزیابی عادی/غیرعادی درنظرگرفته‌می‌شود. همچنین معیار انرژی برای اندازه‌گیری میزان صلاحیت و شایستگی و تواضع برای اندازه‌گیری میزان همکاری در اعتماد کیفیت سرویس استفاده‌خواهدشد. صمیمیت در اعتماد به میزان نسبی درجه تجربه تبادلات بین دو گره حسگر اشاره‌دارد. هرچه تجربه مثبت گره a به گره b بیشتر باشد، اعتماد و اطمینان بالاتر است. صداقت در اعتماد تعیین‌کننده بدخواهی یک گره است. فرض بر این است که یک گره ذاتاً بدخواه است و صداقت ندارد. انرژی از دیگر پارامترهای مهم کیفیت سرویس برای اندازه‌گیری میزان صلاحیت یک گره حسگر است.

تواضع نیز برای ارزیابی میزان همکاری در اجرای یک گره استفاده‌می‌شود. در شبکه‌های حسگر بی‌سیم ممکن است یک گره، در شرایط محیطی و وضعیت عملیاتی مختلف تغییر رفتار دهد، لذا از مدیریت اعتماد استفاده‌می‌شود. بسیار محتمل است که یک گره در شرایطی که انرژی کافی یا همسایه متواضع نداشته‌باشد به خودخواه مبدل‌شود و به‌علاوه، یک گره به دلیل اینکه در اطرافش گره‌های موردمصالحه قراردارند، مصالحه‌شده فرض‌شود. طبیعی است که یک سرخوشه، انرژی بیشتری نسبت به گره حسگر مصرف‌می‌کند. زمانی که یک مصالحه بین گره‌های حسگر یا سرخوشه‌ها برقرارمی‌شود، ممکن است انرژی بیشتری صرف اجرای حملات شود. از طرف دیگر گره خودخواه به‌دلیل توقف عملیات حس‌کردن و امتناع از دریافت بسته‌ها، انرژی کمتری از گره تواضع مصرف‌می‌کند.

در این پژوهش، دو سطح از مدیریت اعتماد مدنظر قرار داده شده است:

۱. سطح گره حسگر.
۲. سطح سرخوشه.

هر گره حسگر، گره‌های هم‌خوشه خود را مورد ارزیابی قرار می‌دهد در حالی که یک سرخوشه گره‌های درون خوشه خودش و دیگر سرخوشه‌ها را ارزیابی‌می‌کند.

به‌روزرسانی اعتماد به‌صورت دوره‌ای و مشاهده مستقیم یا غیرمستقیم انجام‌می‌شود. دو گره به‌صورت نظیربه‌نظیر و از راه مستقیم یا غیرمستقیم می‌توانند به یکدیگر متصل‌شوند. دو گره در یک محدوده ی رادیویی، همسایه مستقیم هم هستند و از طریق تجسس[۲۳] و استراق سمع[۲۴] نتایج ارزیابی اعتماد را برای هم می‌فرستند. نتایج این ارزیابی به سرخوشه و از آنجا به پایگاه اصلی ارسال‌می‌شود. مشابه گره حسگر، ارزیابی و نتایج ارزیابی سرخوشه‌ها نیز به فرمانده سرخوشه‌ها[۲۵] که معمولاً در پایگاه اصلی مستقر است، ارسال و درصورتی‌که پایگاه اصلی وجودنداشته‌باشد به سرخوشهٔ منتخب ارسال‌می‌شود. اگر گره‌ای همسایه مستقیم نداشته‌باشد، یتیم[۲۶] نامیده‌می‌شود و در ارتباط نظیربه‌نظیر قادر به همکاری نیست. پارامتر Δt به‌صورت دوره‌ای به‌روزرسانی اعتماد را برعهده‌دارد. هر گره حسگر مسئول ارسال گزارش نتایج ارزیابی اعتماد خود از دیگر گره‌های همان خوشه به سرخوشه است. به همین ترتیب یک سرخوشه ارزیابی خود از دیگر سرخوشه‌ها را به گره سینک یا پایگاه اصلی ارسال‌می‌کند.

```
//k-means Initiated
For k-meansFunction (cluster: list) do
        AK ← AK + cluster.A
        Bk ← Bk + cluster.B
End for
AK ← AK /long (cluster)
BK ← BK /long (cluster)
N ← N − 1
Return (AK, BK)
//Cluster_Head_Selection
For (j from 1 to long (Cluster))
        Do A ← Cluster.A
        B ← Cluster.B
        Distance = sqrt ((AK − A) * (AK − A) + (Bk − B) * (Bk − B))
        If (distance < distance_minimum)
                Then
                        Distance minimum=distance
        End if
End for
Return (distance_minimum)
//Cluster Selection
        Nodes number for CH (k)
                Do Network clusters
                Random choice of k nodes based on number of total_nodes
                Repeat Apply the k-means method until cover_all
        Clusters_Created
// Clusters creation with their members
For each Cluster Head
        Calculate the centroid of N nodes
                A = (1/N) Σ_{i=1}^{N} A_i
                B = (1/N) Σ_{i=1}^{N} B_i
        Choose the node closest to centroid with sufficient energy
        //Check for Nearest Neighbor
        For z← 1 to n do visit all the nodes in a cluster
                Initialize the list path nodes
                Visit node ← True
                Check for Current node
        For i←2 to n
        Find the minimum Distance between each node in each row
                d(nodeA, nodeB) = sqrt((nodeA_1^2 − nodeB_1^2) + (nodeA_2^2 − nodeB_2^2))
                Visit all nodes
                Preserve the K observations from the localized nodes close to A using the
                Distance calculation function d accordingly
                Add each new closest to a k cluster
        Return path
        If the node was a Cluster Head in the the last propagation,
        Then
                Choose based on Trust & Energy
        Select the adequate Cluster Head
End
```

الگوریتم ۱: محاسبه تعداد خوشه موردنیاز و یافتن نزدیک‌ترین گره به گره سینک برای تعیین سرخوشه

چهار جزء اعتماد بین گره‌های حسگر بررسی و همین اجزا نیز برای سرخوشه‌ها استفاده‌شده‌است: صمیمیت[۲۷]، صداقت[۲۸]، انرژی[۲۹]، تواضع[۳۰]. مقدار اعتماد گره اعتمادکننده[۳۱] a به گره اعتمادشونده[۳۲] b در واحد زمانی t یک عدد حقیقی است بین صفر و یک که به‌صورت $T_{ab}(t)$ نمایش‌داده‌می‌شود. مقدار حاصل از ارزیابی اعتماد اگر یک باشد، نشانگر اعتماد کامل، مقدار صفر، نشانه بی‌اعتمادی و ۰٫۵ ، بیانگر جهل است. با استفاده از وزن هر جزء اعتماد به‌عنوان ضریب در همان لحظه زمانی، فرمول (1) که مجموع آن‌ها برابر یک است، حاصل‌می‌شود:

$$T_{ab}(t) = w_1 T^i_{ab}(t) + w_2 T^h_{ab}(t) + w_3 T^e_{ab}(t) + w_4 T^u_{ab}(t) \quad (1)$$

اعتماد اجتماعی در شبکه‌های حسگر بی‌سیم ممکن است شامل صمیمیت، صداقت، حریم خصوصی، مرکزیت و اتصال باشد. اعتماد کیفیت سرویس ممکن است شامل شایستگی، همکاری، قابلیت اطمینان، قابلیت اتمام کار و غیره باشد. لذا پروتکل اعتماد طوری تنظیم‌شده که عمومی باشد، همچنین می‌تواند ترکیبی از معیارهای اعتماد اجتماعی و اعتماد کیفیت سرویس را تشکیل‌دهد تا معیار اعتماد کلی شکل‌گیرد. بدون ازدست‌دادن کلیت در این کار، صمیمیت برای اندازه‌گیری نزدیکی بر اساس تجارب متقابل؛ صداقت برای اندازه‌گیری نظم یا ناهنجاری، انرژی برای اندازه‌گیری صلاحیت و ازخودگذشتگی(تواضع) برای اندازه‌گیری میزان همکاری به‌کاررفته‌است:

$$T_{ab}(t) = 0.5w_1\left[T^i_{ab}(t) + T^h_{ab}(t)\right] + 0.5w_2[T^e_{ab}(t) + T^u_{ab}(t)] \quad (2)$$

۱. **صمیمیت**: بر پایه مدل سطح تجربه تبادل[۳۳] و بر اساس تعداد

تبادلات صورت‌گرفته بین یک گره و همسایگان مستقیم آن در بازه زمانی [0,t] محاسبه‌می‌شود.

۲. **صداقت**: گره تخمین‌می‌زند که مقدار T چقدر ا ست، به‌این صورت که تعداد تجارب بی صداقتی و بدگمانی با ا ستفاده از مجموعه‌ای از قوانین غیرمتعارف[۳۴]را در بازه زمانی [0,t] نگه‌می‌دارد. اگر این تعداد از حد آ ستانه تعریفی سیستم فراتر رفت به‌عنوان عدم صداقت و با مقدار صفر درنظرگرفته‌می شود. درغیراین صورت، تعداد نسبت به حدّ آ ستانه از عدد ۱ کسر و محا سبه‌می شود. پیشنهاد این تحقیق استفاده از قواعد ارسال مجدد، بازگویی و تأخیرات است.

۳. **انرژی**: م قدار کافی انرژی برای اجرای توابع که ممکن اســـت به صورت در صد محا سبه شود ، برای تخمین آن از ا ستراق سمع تبادلات بسته‌ها در بازه زمانی [0,t] استفاده‌می‌شود.

۴. **تواضع**: یک گره می‌تواند با تکنیک استراق سمع و تجسس، برخی رفتارهای خودخواهانه مانند حس بی‌وفایی، توابع ارســـال و توابع گزارش‌گیری را نسبت به گره مستقیم دیگر محاسبه‌کند. همچنین ممکن اســـت تجربه تبادلات اخیر را با اولویت بالاتری نســـبت به تجربیات گذشته اولویت‌دهی کند.

$$T_{ab}^{X}(t) = \begin{cases} (1-\propto)T_{ab}^{X}(t-\Delta t)+ \propto T_{ab}^{X_a}(t), \\ if\ a,b = 1-hop\ neighbors \\ avg\left[(1-\gamma)T_{ab}^{X_a}(t-\Delta t) + \gamma T_{kb}^{X_{recom}}(t)\right], otherwise \end{cases} \quad (3)$$

در فرمول (۳)، X به اجزای اعتماد برای به‌روزرسانی دوره‌ای اشاره‌می کند و مقدار آن بر پایه مشاهدات مستقیم انباشته‌شده در طول زمان است:

در تغییرات زمان به‌روزرسانی دوره‌ای، آلفا به‌عنوان ضریبی برای وزن‌دهی دو مقدار اعتماد قدیم و اعتماد جدید استفاده‌شده که مقدار آن همواره عددی بین صفر و یک است و بر مشاهدات مستقیم تمرکزدارد.

γ برای وزن‌دهی پیشنهادات نسبت به آخرین تجربیات، ارزیابی و رسیدگی به اعتمادهای منقرض‌شده در واحد زمان است و مقدار آن از فرمول (4) محاسبه‌می‌شود:

$$\gamma = \frac{\beta T_{ak}(t)}{1+\beta T_{ak}(t)} \quad (4)$$

که در آن $\beta \geq 0$ برای تعیین پیشنهادهای غیرمستقیم استفاده و در موارد خاص مقدار یک به آن داده‌می‌شود. تغییرات این ضریب می‌تواند مانع حملات بددهان و خوش‌دهان در حملات نوع تهمت‌زدن شود. برای محاسبه اعتماد سرخوشه به مقادیر اعتماد اعلامی یک گره حسگر از فرمول (۵) استفاده‌شده‌است:

$$i \in Mc \wedge T_{ca}(t) \geq T^{th} \quad (5)$$

گره حسگر مقادیر اعتماد خودش را به دیگر گره‌های موجود در همان خوشه، اطلاع‌می‌دهد. سرخوشه از روش آماری آنالیز عمومی فوق، برای تشخیص نفوذ حملات استفاده‌می‌کند. نماد c نشانگر سرخوشه و Mc مجموعه‌ای از گره‌های حسگر در یک خوشه است. اگر مقدار حاصل کمتر از مقدار اعتماد حدّ آستانه باشد، توافق برقرارمی‌شود وگرنه توافقی صورت‌نمی‌گیرد. جهت محاسبه اعتماد پایگاه به سرخوشه نیز به‌ترتیب زیر عمل‌خواهدشد:

در مدل‌های ناهمزمان، قدرت انتقال و ظرفیت سرخوشه از دیگر گره‌ها بالاتر است و درنتیجه محدوده رادیویی بیشتری را حمایت‌می‌کند. در مدل پیشنهادی، به‌این‌منظور گره نوع همگن به‌کاررفته‌است و از همان روش گره‌های حسگر برای ارزیابی اعتماد دو سرخوشه نیز استفاده-می‌شود. سرخوشه با به‌کارگیری همان روش آماری توضیح‌داده‌شده به بررسی اعتماد خود نسبت به دیگر سرخوشه‌ها می‌پردازد و بعد از جمع‌آوری اطلاعات، آن‌ها را هاپ به هاپ و از طریق سرخوشه‌های دیگر به پایگاه اصلی گزارش‌می‌کند. سپس ایستگاه اصلی تصمیم‌می‌گیرد که سرخوشه باید نسبت به کدام گره یا سرخوشه، بی‌اعتماد باشد و از وظایف ارزیابی و ارسال خود مستثنی‌شود. نرخ مصرف انرژی تحت‌تأثیر وضعیت گره است. زمانی که گره خودخواه باشد میزان آن پایین‌تر است؛ چراکه برای اجرای حملات، انرژی لازم است. یک گره خودخواه ممکن است خواندن داده را متوقف و دریافت بسته‌ها را رهاکند. یک گره تواضع ممکن است در هر ارزیابی اعتماد و با توجه به میزان انرژی باقیمانده و تعداد گره‌های تواضع اطرافش به گره خودخواه تبدیل‌شود.

۳/۳. الگوریتم مسیریابی پیشنهادی

در روش پیشنهادی برای طراحی یک پروتکل مسیریابی ایمن و مناسب برای شبکه‌های حسگر بی‌سیم تعریف‌شده نرم‌افزارمحور، برای مطابقت با روندهای کنونی، یک پروتکل مسیریابی مبتنی‌بر مکان انتخاب‌شده-است. در این مسیریابی جغرافیایی هر گره بسته اطلاعاتی خود را برای باز ارسال بعدی به نزدیک‌ترین همسایه مقصد می‌فرستد. مسیریابی مبتنی‌بر مکان بر این فرض متکی است که هر گره مکان خود را در اصطلاح پیام[۳۵] اعلام‌می‌کند. این امر مستلزم اجرای تکنیک‌های بومی‌سازی است. تکنیک‌های محلی‌سازی برای شبکه‌های حسگر بی‌سیم را می‌توان به‌طورکلی به دو دسته اصلی طبقه‌بندی‌کرد: ۱) مبتنی‌بر دامنه و ۲) بدون دامنه.

رویکردهای مبتنی‌بر دامنه، در دسترس بودن اندازه‌گیری‌های دقیق را مستقیماً مربوط به فواصل و یا زاویه‌های نسبی بین جفت گره‌های شبکه فرض‌می‌کنند. از طرف دیگر، روش‌های بدون دامنه فقط از پارامترهایی که به‌راحتی در سطح لایه فیزیکی در دسترس هستند استفاده‌می‌کنند که فقط با موقعیت گره ارتباط آزاد دارند. پروتکل مدیریت اعتماد پیشنهادی به‌عنوان یک برنامه کاربردی، در مسیریابی جغرافیایی مبتنی‌بر اعتماد اعمال‌می‌شود. در مسیریابی جغرافیایی مبتنی‌بر اعتماد، گره i، پیامی را به حداکثر همسایگان L نه‌تنها نزدیک به گره مقصد بلکه با بیشترین ارزش اعتماد T_{ab} (t) نیز ارسال‌می‌کند. ترکیبی از یک طرح مدیریت اعتماد توزیع‌شده با یک روش مسیریابی جغرافیایی، راه‌حل پیشنهادی را برای شبکه‌های نرم‌افزارمحور مقیاس بزرگ مناسب می‌کند، زیرا مقیاس‌پذیری یک ویژگی غالب در تمام پروتکل‌های مبتنی‌بر مکان است. خلاصه کارکرد اعتماد و نحوه انتخاب

مسیر و همچنین بررسی انرژی در بخش اصلی الگوریتم (۲) آورده‌شده-است.

۴. شبیه‌سازی و ارزیابی نتایج

در این بخش از مقاله، به شبیه‌سازی مدل پیشنهادی با استفاده از شبیه‌ساز شبکه حسگر بی‌سیم[۳۶] [33] پرداخته‌شده‌است. همچنین در ادامه بخش به تجزیه و تحلیل مدل پیشنهادی و مقایسه آن با الگوریتم-های مختلف و ایجاد اعتماد در مسیریابی حسگرها پرداخته‌شده‌است.

۱/۴. ساختار شبیه‌ساز

ابزار شبیه‌سازی از دو لایه اصلی نرم‌افزار تشکیل‌شده‌است، یک لایه هسته شبیه‌ساز و لایه دوم محلی‌سازی است. لایه هسته شبیه‌ساز، شامل چندین کلاس است. کلاس شبکه که شامل کلاس‌هایی مانند کلاس حسگر، کلاس سرخوشه، کلاس بسته و غیره است و کلاس رابط توسعه‌دهنده که شامل تمام روش‌های کنترل مثل اجرا / توقف، مکث / از سرگیری شبیه‌سازی و غیره. است. لایه دوم این شبیه‌ساز، لایه محلی‌سازی است. بنابراین توسعه‌دهنده توانایی نوشتن الگوریتم خود در آن را دارد. گره حسگر بی‌سیم معمولاً از چند ماژول تشکیل‌شده‌است مثل CPU، تایمر، رادیو، لایه‌های شبکه.

ابزار شبیه‌سازی، کلاس‌های مربوط به هر ماژول را تعریف‌می‌کند، مثل: کاربرد، مسیریابی و لایه فیزیکی. هر ماژول به عنوان یک کلاس *C#* پیاده‌سازی‌می‌شود که از یک کلاس لایه شبیه‌ساز هسته گرفته‌شده-است. همچنین، *Tasks* به‌عنوان متدهای درون کلاس ماژول پیاده‌سازی-می‌شوند. شبیه‌سازی‌ها، بر روی یک ماشین با مشخصات زیر انجام‌شده-است:

- CPU Intel Core i5 (6th Generation)
- RAM 8 GB
- Operating System, Windows 10
- Simulation Duration in each level: 150s

```
Public class Secure_Trusted_Algo
{
   Public int counter, slot_duration, delimiter = 0; public DateTime timeStart;
   Public String path, pathl;
   Public float locatorRadius = 0, sensorRadius = 0;

   Public Secure_Trusted_Algo (ArrayList asensor, int counter, int slot_duration, String path, String pathl,
float locatorRadius, float sensorRadius, int delimiter, int SensorModel, double initialenergy)
   {
    set_parameters (locatorRadius, sensorRadius, counter, slot_duration); localize (asensor,
    locatorRadius, path, pathl, delimiter, SensorModel, initialenergy);
    }

   Public void set_parameters (float locatorRadius, float sensorRadius, int counter, and int slot_duration)

   {
    this.locatorRadius = locatorRadius;
    This sensorRadius = sensorRadius:
    This counter = counter;
    This slot_duration = slot_duration;
    }

//Residual Energy Consumption

 If (sensorResidualEnergy > 0)

 {
       If (counter = 0)
       {
        String sector = "", sect = '';
        Sector = path + %slot" + (counter / slot_duration) + "_sectors_of_sensor" + s +'." + extV/tile to store
max point in each of eight sector
        String location =write_location = "", samples = '', sample = '", sample! = "", pos

        Location = path + \\sensor + s + "." + ext; //file to store estimated position only write  location =
        path + \\slot_" + (counter / slot_duration) + "_sensor" + s + ".* +
Ext;
        Int xg = 0, yg = 0, score, scorel, ns = 0, nsl = 0;
        Float sx = 0, sy = 0, sxl = 0, syl = 0;
        Ax = 0; ay = 0;
        Int min_x = 1000, mint' = 1000, max_x = 0, max_y = 0; double k = 0://number of
        samples
        Double ERth = 4 * locatorRadius * locatorRadius, ER = 0;
        }
}
```

الگوریتم (۲) : کارکرد اعتماد و نحوه انتخاب مسیر و همچنین بررسی انرژی

۲/۴. ویژگی‌های شبیه‌ساز

برخی از ویژگی‌های این شبیه‌ساز عبارتند از:

۱. از مدل‌های پویای بسیاری مانند: Random Waypoint ، Random Direction ،Modified Random Waypoint ، Manhattan ،Modified Boundless و RPGM پشتیبانی‌می‌کند.
۲. پشتیبانی از دو مدل Ray ground و Shadowing
۳. تمام وقایع انجام‌شده در زمان شبیه‌سازی در یک فایل ردیابی خارجی نوشته‌می‌شود.
۴. قابلیت ایجاد فضای ناامن با حملات کرم‌چاله، سیبیل، کلاه‌برداری و اجرای‌مجدد را دارد و اجازه ایجاد الگوریتم‌های دفاعی آن‌ها را نیز پشتیبانی‌می‌کند.
۵. از دو مدل حسگر پشتیبانی‌می‌کند: MICA2 وTelosB
۶. به کاربران اجازه‌می‌دهد تا سناریوهای مختلفی را ایجاد و دوباره از پرونده‌های تولیدشده بخوانند.

۳/۴. شبیه‌ساز

شبیه‌ساز شبکه حسگر بی‌سیم که بر اساس زبان برنامه‌نویسی C# طراحی‌شده، شامل تعیین موقعیت گره‌های حسگر است. در این شبیه‌ساز، تعیین و تخمین موقعیت حسگرها در شرایط مختلف

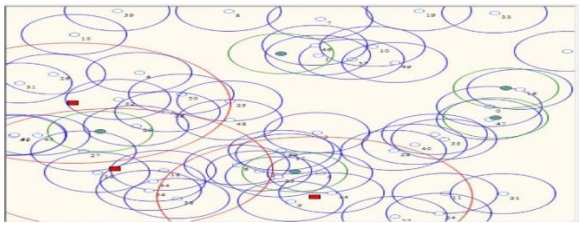
درنظرگرفته‌نمی‌شود. الگوریتم‌های محلی‌سازی بسیاری وجوددارند که سعی‌می‌کنند در تعیین موقعیت گره‌های حسگر دقیق‌تر عمل‌کنند و این به معنای خطای محلی‌سازی کمتر است. لذا برای طراحی و توسعه مؤثر الگوریتم‌های محلی‌سازی جدید، باید از یک محیط شبیه‌سازی مؤثر و قابل‌اعتماد استفاده‌کرد.

۴/۴. شبیه‌سازی روش پیشنهادی

شبیه‌ساز امکان ایجاد رویدادهای متفاوت را دارد و پیاده‌سازی مدل پیشنهادی به زبان برنامه‌نویسی C# امکان‌پذیر است. همچنین براساس رویدادهای متوالی زمانی برای تغییر وضعیت سیستم، قابل‌تنظیم است. هسته شبیه‌سازی که بخش نرم‌افزارمحور تلقی‌می‌شود این وقایع را پردازش‌می‌کند. ترکیب گره و طرح شبکه، همراه با پارامترهای محیطی و تنظیمات، از طریق رابط کاربری انجام‌می‌شوند. پس از آن ماژول‌ها با هسته شبیه‌سازی تفسیر و پیوند داده‌می‌شوند و منجر به بهره‌گیری از هسته شبیه‌ساز می‌شود. بر همین اساس در این فصل، سناریوهای مختلفی برای بررسی کارایی روش پیشنهادی بررسی و در لایه دوم کدهای آن‌ها پیاده‌سازی‌شده‌است. سه سناریو با تعداد ۵۰، ۱۰۰ و ۲۰۰ گره حسگر، جداگانه بررسی‌شده‌اند. بر اساس روش پیشنهادی، خوشه‌بندی گره‌ها با روش ترکیبی دو الگوریتم k NN و k-means انجام‌شده‌است. در هر سناریو تعداد سرخوشه‌ها متفاوت خواهدبود. اجرای الگوریتم و خوشه‌بندی توسط بخش نرم‌افزارمحور انجام‌می‌شود. در قسمت مسیریابی، با مقایسه روش پیشنهادی و تشخیص گره‌های غیرقابل اطمینان با الگوریتم‌های دیگر از جمله الگوریتم MCL، الگوریتم IMCL، الگوریتم KFL و الگوریتم MPL، کارایی روش پیشنهادی بررسی‌شده‌است. این مقایسه بر اساس پارامترهایی مانند انرژی مصرفی، انرژی باقیمانده، درصد خطا در تشخیص گره‌های غیرقابل اطمینان و هزینه الگوریتم‌ها صورت‌گرفته‌است.

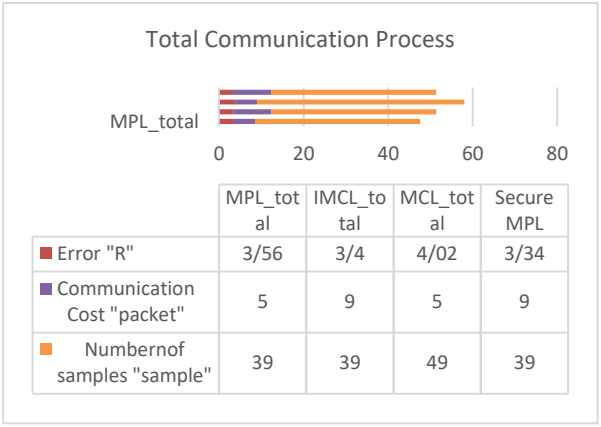
۱،۴،۴. سناریوی اول: شبیه‌سازی با ۵۰ گره حسگر

در این سناریو تعداد گره‌های حسگر که به‌صورت استاتیک و از نوع Mica2 در نظر گرفته‌شده‌اند ۵۰ عدد است. تعداد k برای مشخص‌نمودن تعداد سرشاخه ۵ عدد انتخاب‌شده‌است. تعداد گره‌های غیرقابل‌اعتماد ۳ عدد است که به‌صورت کلاه‌برداری[۳۷] به شبکه حمله خواهندکرد. استقرار و مدل انتشار همه گره‌ها به‌صورت تصادفی تنظیم‌شده است و هر بار اجرای سناریو مکان گره‌ها و مسیریابی تغییرمی‌یابد. انرژی اولیه همه گره‌ها به‌صورت مساوی ۱۰۰۰ ژول درنظرگرفته‌شده‌است که در هر مرحله مسیریابی نسبت به فعالیت گره تغییرمی‌کند. اندازه بسته‌های ارسالی شامل اطلاعات، ۵۱۲ بایت است، اندازه بسته‌هایی که جهت ایجاد خوشه و شناسایی گره‌ها ارسال می‌شوند۲۱۰ بایت و اندازه بسته تصدیق[۳۸] ۴۰ بایت است. در شکل (۷) انتشار گره‌های حسگر در سناریو اول نشان‌داده‌شده‌است. سرخوشه‌ها توسط بخش نرم‌افزارمحور با استفاده از الگوریتم k-means جهت خوشه‌بندی اولیه و از ترکیب آن با الگوریتم kNN جهت مشخص‌کردن نزدیک‌ترین همسایه هر حسگر در هر خوشه ایجادمی‌شود. در این شکل، سرخوشه‌ها با دایره‌های سبز و گره‌های غیرقابل‌اعتماد با مربع‌های قرمز نشان‌داده‌شده‌است. برای بررسی کارآیی، الگوریتم پیشنهادی با الگوریتم‌های MPL، الگوریتم MCL، الگوریتم IMCLو الگوریتم KFL که الگوریتم‌هایی نزدیک به الگویتم پیشنهادی هستند، مقایسه‌شده‌است. در شکل (۸)، نرخ خطاها جهت تشخیص گره غیرقابل‌اعتماد، هزینه ارسال و دریافت بسته‌ها برای داشتن شبکه‌ای امن و تعداد نمونه‌ها برای ایجاد شبکه مورداعتماد آورده‌شده‌است.



شکل۷: انتشار گره‌های حسگر و اجرای مسیریابی، ارسال و دریافت بسته در سناریوی اول

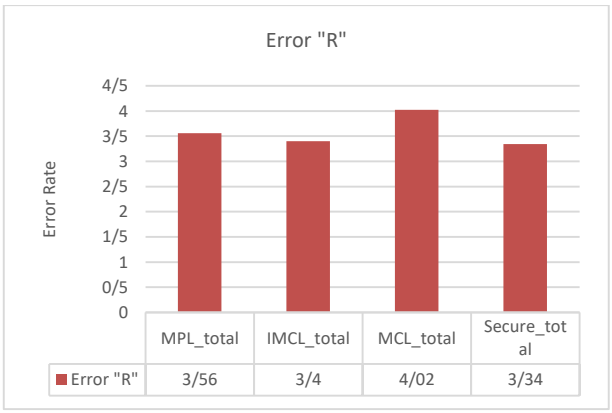
این مقدار برای آخرین مرحله اجراشده‌است. چون الگوریتم KFL در این تعداد گره برای هر سه بخش عدد صفر را نشان‌داده، قابلیت ایجاد شبکه امن را نداشته و نیاز به تعداد نمونه‌های بیشتری دارد، در گراف، این شکل حذف‌شده‌است.



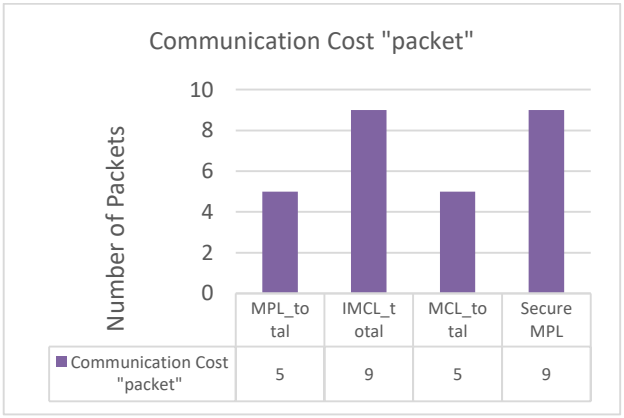
	MPL_total	IMCL_total	MCL_total	Secure MPL
Error "R"	3/56	3/4	4/02	3/34
Communication Cost "packet"	5	9	5	9
Numbernof samples "sample"	39	39	49	39

شکل۸: نرخ خطا، هزینه مسیریابی و ارسال اطلاعات و تعداد نمونه‌هابرای ایجاد شبکه مورداعتماد

مطابق شکل (۹) برای بهتر نشان‌دادن و مشخص‌نمودن کارایی الگوریتم امن پیشنهادی، مجموع نرخ خطا در تشخیص مکان گره‌های غیرقابل‌اعتماد با الگوریتم‌های MPL، MCL، IMCL مقایسه‌شده است. الگوریتم پیشنهادی با نرخ خطای پایین‌تر نتیجه بهتری جهت شناسایی گره‌های غیرقابل‌اعتماد دارد و نتیجه آن داشتن شبکه‌ای امن‌تر است. مقایسه هزینه ارتباطات در شبکه با الگوریتم‌های مختلف تعریف‌شده در شکل (۱۰) نشان‌داده‌شده‌است. با توجه به نتیجه حاصل از پیاده‌سازی این الگوریتم‌ها و مقایسه صورت‌گرفته، الگوریتم بهبودیافته IMCL و الگوریتم پیشنهادی دارای ۹ بسته هزینه هستند و دو الگوریتم محلی‌سازی MCL و پیش‌بینی تحرک هزینه کمتری برابر ۵ بسته داشته‌اند. در مجموع و بر اساس خروجی‌های شکل شماره ۳ و ۴ و مقایسه آن با تشخیص گره‌های غیرقابل‌اعتماد، الگوریتم امن پیشنهادی با استفاده از ۳۹ نمونه و نرخ خطا ۳،۳۴ در مجموع دارای مقدار هزینه قابل‌قبول است.



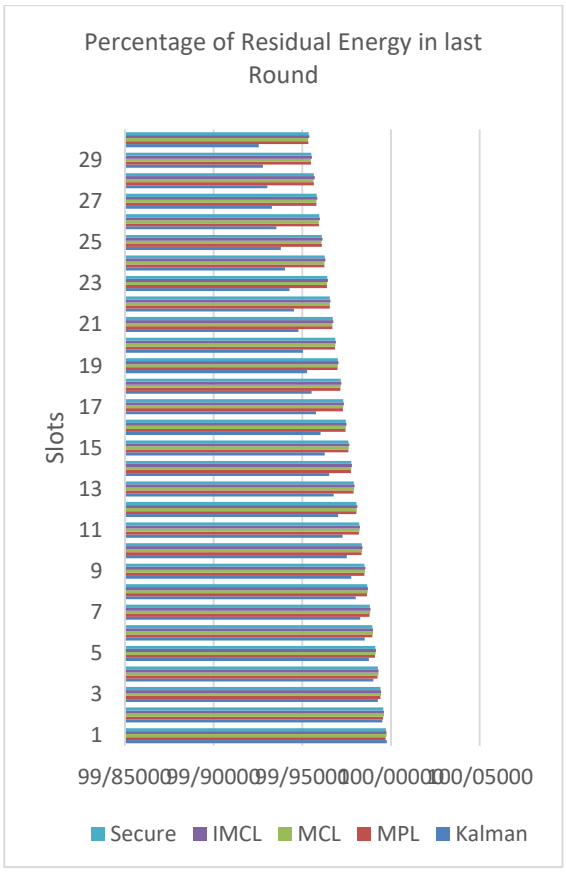
شکل۹: درصد نرخ خطا در تشخیص گره‌های غیرقابل‌اعتماد – سناریوی اول



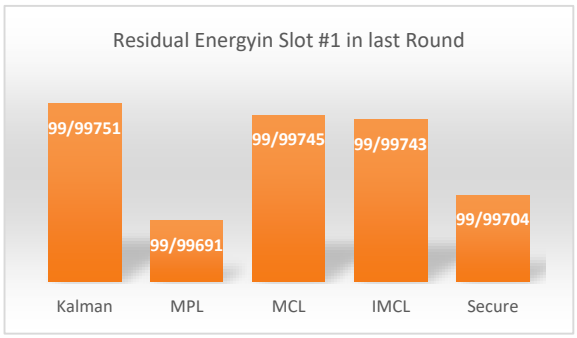
شکل۱۰: مجموع هزینه ارتباط (تعداد بسته) در شبکه – سناریو اول

در شکل (۱۱) درصد انرژی باقیمانده گره‌ها در مرحله آخر ارسال اطلاعات مشاهده‌می‌شود. در هر مرحله، ۳۰ شکاف[۳۹] تعریف شده و برای مشخص‌نمودن دقیق انرژی باقیمانده، در شکل (۱۲) و شکل (۱۳) انرژی باقیمانده گره‌های شبکه در شکاف اول و آخر به‌ترتیب آمده‌است. همان‌طورکه در خروجی‌های شبیه‌سازی مشاهده‌می‌شود، در شروع هر مرحله، الگوریتم امن پیشنهادی مقدار انرژی بیشتری برای شناسایی گره‌های غیرقابل‌اعتماد و ارسال اطلاعات مابین گره‌ها مصرف‌می‌کند. ولی درمجموع و در پایان فعالیت شبکه، درصد انرژی باقیمانده الگوریتم پیشنهادی بیشتر است و درنتیجه طول‌عمر شبکه با روش پیشنهادی، کارایی بهتر و مصرف انرژی مناسب‌تر دارد.

در سناریوی دوم، تنظیمات اولیه مانند انرژی گره‌های حسگر و اندازه بسته‌های ارسال‌شده همانند سناریوی اول است. تفاوت این سناریو در تعداد بیشتر گره‌های حسگر و درنتیجه تعداد بیشتر مراحل برای اجرای شبکه است. در این سناریو نیز الگوریتم امن پیشنهادی با الگوریتم‌های محلی‌سازی مقایسه‌شده‌است تا کارآیی آن مشخص‌شود.



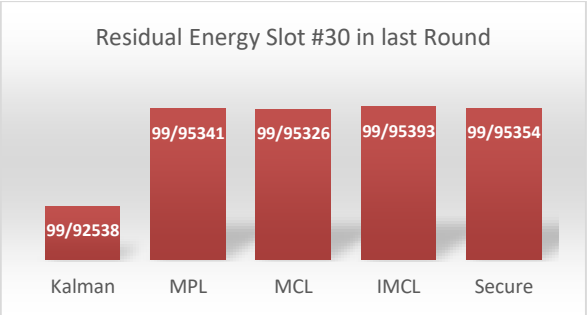
شکل۱۱: درصد انرژی باقیمانده شبکه در مرحله آخر در ۳۰ شکاف مرحله و مجزا – سناریوی اول



شکل۱۲: درصد باقیمانده انرژی شبکه در شکاف اول – سناریو اول

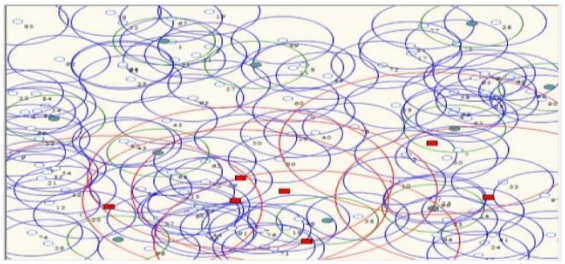
۲،۴،۴. سناریوی دوم: شبیه‌سازی با ۱۰۰ گره حسگر

در این سناریو تعداد سرخوشه‌ها به ۱۰ و تعداد گره‌های غیرقابل‌اعتماد نیز به ۷ عدد افزایش یافته‌است. در شکل(۱۴) زمان اجرای ارسال اطلاعات در شبکه شبیه‌سازی‌شده بعد از مشخص‌شدن سرخوشه‌ها توسط نرم‌افزار تعریف‌شده و با دایره‌های سبز مشخص‌شده‌اند. گره‌های غیرقابل‌اعتماد نیز به‌صورت اتفاقی انتخاب و با مربع قرمز مشخص‌شده‌اند.



شکل ۱۳: درصد باقیمانده انرژی شبکه در شکاف۳۰ (آخر) – سناریو اول

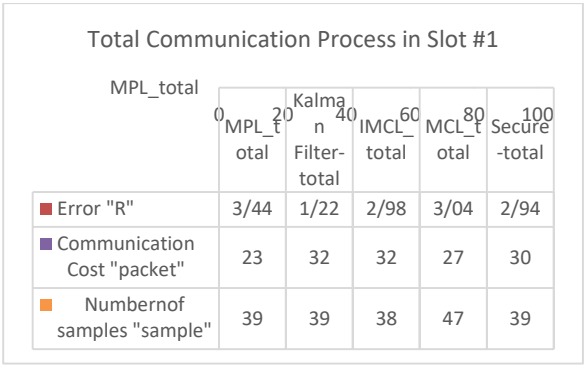
در این سناریو به‌علت تفاوت مقدار نرخ خطا، هزینه و نمونه در شکاف اول و آخر در مرحله پایانی هر دو نتیجه آمده‌است. فرآیند کامل ارتباط در شکاف اول، آخرین مرحله شکل (۱۵) آمده‌است. تعداد نمونه‌ها به‌ترتیب برای الگوریتم‌های MPL، KFL، MCL و IMCL و الگوریتم پیشنهادی امن، ۳۹، ۳۹، ۴۷، ۳۸ و ۳۹ است. در میان الگوریتم‌ها، MCL در هر سناریو تعداد بیشتری نمونه برای اجرا نیازدارد. ولی مدل پیشنهادی امن همانند الگوریتم‌های MPL و Kalman Filter با ۳۹ نمونه اجرامی‌شود.



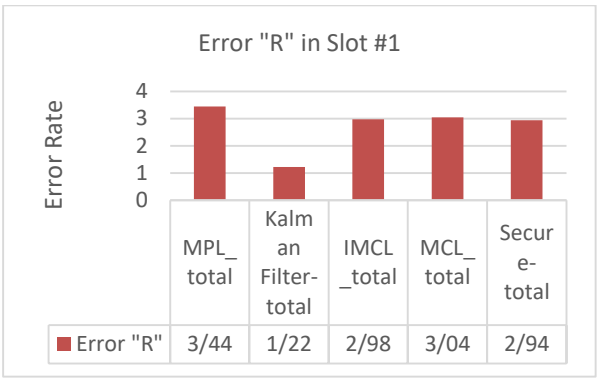
شکل۱۴: انتشار گره‌های حسگر و اجرای مسیریابی، ارسال و دریافت بسته در سناریوی دوم

در سناریوی مورداستفاده در الگوریتم KFL و در مرحله آخر از شکاف اول، کمترین مقدار نرخ خطا وجوددارد و بعد از آن الگوریتم پیشنهادی با داشتن ۲,۹۴ درصد نرخ خطا است. بیشترین نرخ خطا متعلق به مدل MPL با ۳,۴۴ درصد است. درصد نرخ خطا به‌صورت مجزا در شکل (۱۶) آمده‌است. لذا مدل پیشنهادی نسبت‌به الگوریتم‌های IMCL، MCL و MPL دارای خطای کمتری است.

شکل (۱۷) شامل هزینه ارتباط در شبکه است که مقدار هزینه الگوریتم پیشنهادی ۳۰ بسته است. دو الگوریتم MPL با ۲۳ و MCL با ۲۷ بسته از مدل پیشنهادی هزینه کمتری دارند، ولی الگوریتم KFL که در شکاف اول نرخ خطای کمتری را داراست، هزینه بیشتری صرف‌می‌کند.

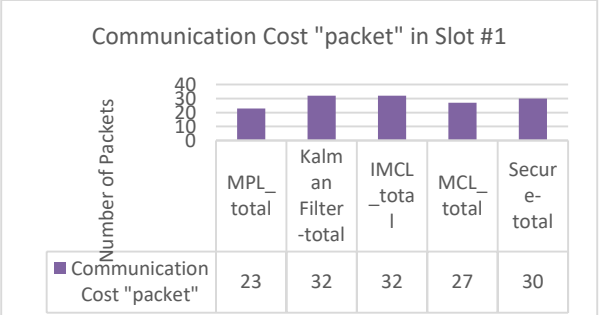


شکل۱۵:مجموع روند ارتباط در شبکه در شکاف اول – سناریو دوم

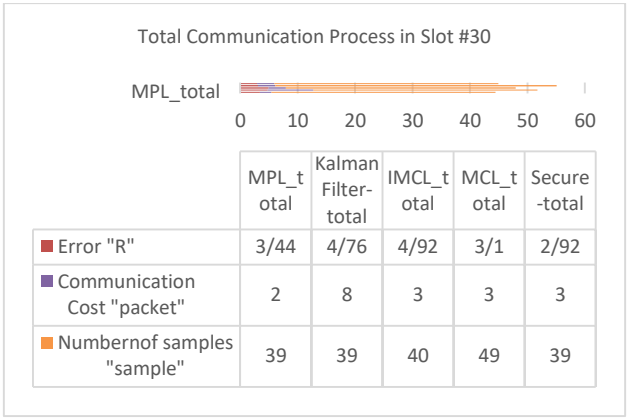


شکل ۱۶: درصد نرخ خطا در تشخیص گره‌های غیرقابل‌اعتماد در شکاف اول مرحله آخر –سناریو دوم

البته در این سناریو نیاز است تا به شکاف آخر هر مرحله نیز توجه‌شود و علت آن مقدار نرخ خطا و هزینه متفاوت است. در شکل (۱۸)، مجموع روند ارتباط در شبکه در شکاف آخر نشان‌داده‌شده‌است. همان‌طورکه در این گراف نشانداده شده، مقدار نرخ خطا در روش KFL از ۱,۲۲ به ۴,۷۶ درصد رسیده که نشان‌می‌دهد این روش متناسب با گره‌های غیرقابل‌اعتماد رفتارنمی‌کند و در طول یک مرحله در مسیریابی و ارسال اطلاعات نرخ خطای بالایی دارد. در شکل (۱۹) صرفاً به مقدار نرخ خطا در شناسایی گره‌های غیرقابل‌اعتماد اشاره‌شده که الگوریتم پیشنهادی با درصد ۲,۹۲ دارای کمترین نرخ است. درحالی‌که در مقایسه با شروع مرحله، فقط ۰,۰۲ درصد تفاوت‌دارد که نشان‌دهنده الگوی مناسب تشخیص گره است و در رده دوم و پس از این الگوریتم، MCL با نرخ خطای کمتری نسبت به روش بهبود خود عمل‌کرده‌است.



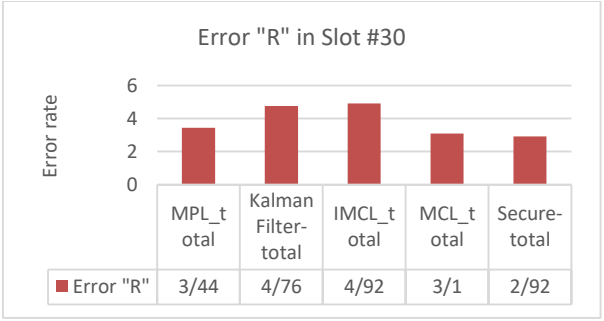
شکل ۱۷: مجموع هزینه ارتباط (تعداد بسته) در شبکه در شکاف اول مرحله آخر- سناریو دوم



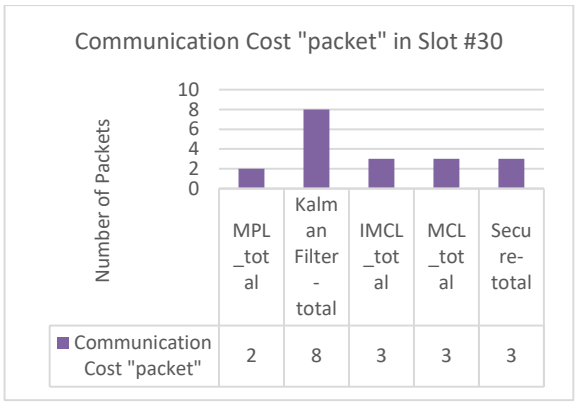
شکل۱۸: مجموع فرآیند ارتباط در شبکه شکاف آخر مرحله آخر – سناریو دوم

در شکل (۲۰) هزینه ارتباط کل در سناریو دوم آورده‌شده‌است. الگوریتم MPL هزینه کمتری در مقایسه با روش امن پیشنهادی دارد، ولی با توجه به نرخ خطا و تفاوت بسیار کم مقدار هزینه، می‌توان‌گفت روش پیشنهادی در این سناریو نیز دارای کارایی بالاتری نسبت به سایر الگوریتم‌ها است. در این سناریو نیز مقدار انرژی باقیمانده پس از مرحله آخر ارسال اطلاعات، بررسی‌شده که مقدار درصد انرژی شکاف‌ها در مرحله آخر، جداگانه در شکل (۲۱) آمده‌است. برای مشخص شدن بهتر مقدار درصد انرژی مصرفی در شبکه، مقدار اولین و آخرین شکاف در مرحله آخر، جداگانه در شکل‌های (۲۲) و (۲۳) نشان‌داده‌شده‌است.

همانند سناریوی اول در شروع مرحله، الگوریتم امن پیشنهادی مقدار انرژی بیشتری جهت ارسال اطلاعات اولیه و شناسایی گره‌های غیرقابل‌اعتماد صرف میکند، ولی در پایان مرحله در مقایسه با الگوریتم‌های دیگر دارای مقدار انرژی باقیمانده مناسبی است.



شکل۱۹: درصد نرخ خطا در تشخیص گره‌های غیرقابل‌اعتماد در شکاف آخر مرحله آخر –سناریو دوم



شکل۲۰: مجموع هزینه ارتباط (تعداد بسته) در شبکه در شکاف آخر مرحله آخر– سناریو دوم

۵. نتیجه‌گیری

در این تحقیق به بررسی چالش‌های امنیتی در شبکه‌های حسگر بی‌سیم مبتنی‌بر نرم‌افزار تعریف‌شده و موارد کلیدی که باید برای دستیابی به امنیت حل‌شود، پرداخته‌شده‌است. در این راستا و در ابتدا، از ترکیب دو الگوریتم k-means و k NN، خوشه‌بندی بر اساس تعداد حسگرهای به‌کارگرفته‌شده توسط شبکه تعریف‌شده نرم‌افزاری انجام و سپس مسیریابی بهینه بر اساس مصرف انرژی و با اولویت اعتماد صورت‌گرفته‌است. شبیه‌سازی شبکه طراحی‌شده بر اساس سه سناریو متفاوت با شبیه‌ساز Wireless Sensor Network Simulator انجام‌گرفته‌است. برای مشخص‌کردن دقت و میزان اعتماد و انرژی مصرفی، الگوریتم امن پیشنهادی با الگوریتم‌های محلی‌سازی دیگری مانند محلی‌سازی مونت‌کارلو (MCL)، الگوریتم بهبودیافته مونت‌کارلو (IMCL) و الگوریتم محلی‌سازی فیلتر کالمان (KFL) در کنار الگوریتم محلی‌سازی پیش‌بینی تحرک (MPL) مقایسه‌شد. این مقایسه در زمینه درصد نرخ خطا، هزینه ارتباطات و مقدار انرژی مصرفی صورت‌گرفته‌است. از تحلیل‌ها و بررسی‌های به‌عمل‌آمده، الگوریتم امن پیشنهادی برای ایجاد شبکه حسگر بی‌سیم نرم‌افزارمحور قابل اعتماد، دارای نرخ خطای پایین‌تری است. این الگوریتم به‌علت استفاده از ارسال اطلاعات (بسته) بیشتر برای شناسایی گره‌های غیرقابل‌اعتماد دارای هزینه ارتباطی کمی بیشتر در مقایسه با سایر الگوریتم‌ها است که در مزایای آن می‌توان‌گفت الگوریتم پیشنهادی برای ایجاد شبکه قابل‌اعتماد، مناسب‌ترین الگوریتم است. همچنین در مجموع مصرف انرژی در مقایسه با سایر الگوریتم‌ها، انرژی کمتری مصرف‌می‌کند که برای شبکه‌های حسگر بی‌سیم از اهمیت بسیار بالایی برخوردار است.

مراجع

[1] Yick, J., B. Mukherjee, and D. Ghosal, Wireless sensor network survey. Computer networks, 2008.52(12): p. 2292-2330 .

[2] Yaeghoobi SB, K., M. Soni, and S. Tyagi, A Survey Analysis of Routing Protocols in Wireless Sensor

Networks. International Journal of Engineering and Technology (IJET), 2015.
[3] McKeown, N.J., How SDN will shape networking. Open Networking Summit, 2011 .
[4] Kirkpatrick, K., Software-defined networking. Journal of Communications of the ACM, 2013. 56(9): p. 16-19.
[5] Tang, M., et al. Coverage optimization algorithms based on voronoi diagram in software-defined sensor networks. in Wireless Communications & Signal Processing (WCSP), 2016 8th International Conference on. 2016. IEEE
[6] Christin, D., et al. Wireless sensor networks and the internet of things: selected challenges. in Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze. 2009.
[7] Curtis, A.R., et al. DevoFlow: scaling flow management for high-performance networks. in ACM SIGCOMM Computer Communication Review. 2011. ACM.
[8] Mahmood, M.A., W.K. Seah, and I.J.C.N. Welch, Reliability in wireless sensor networks: A survey and challenges ahead. 2015. 79: p. 166-187.
[9] Nunes, B.A.A., et al., A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys Tutorials, 2014. 16(3): p. 1617-1634.
[10] Luo, T., H.-P. Tan, and T.Q. Quek, Sensor OpenFlow: Enabling software-defined wireless sensor networks. IEEE Communications letters, 2012. 16(11): p. 1896-1899.
[11] Fernandez, M.P. Comparing openflow controller paradigms scalability: Reactive and proactive. in Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on. 2013. IEEE.
[12] Anastasi, G., et al., Energy conservation in wireless sensor networks: A survey. 2009. 7(3): p. 537-568.
[13] Mostafaei, H. and M.S. Obaidat. A Greedy Overlap-Based Algorithm for Partial Coverage of Heterogeneous WSNs. in GLOBECOM 2017-2017 IEEE Global Communications Conference. 2017. IEEE.
[14] Yaeghoobi, K.S., M. Soni, and S. Tyagi, Schedule communication routing approach to maximize energy efficiency in wireless body sensor networks. Smart Structures System, 2018. 21(2): p. 225-234.
[15] Wang, J., et al., Software defined network routing in wireless sensor network, in Cloud Computing, Security, Privacy in New Computing Environments. 2016, Springer. p. 3-11.
[16] Abdolmaleki, N., et al., Fuzzy topology discovery protocol for SDN-based wireless sensor networks. Simulation Modelling Practice Theory, 2017. 79: p. 54-68.
[17] Lee, S.H., et al. Wireless sensor network design for tactical military applications: Remote large-scale environments. in Military communications conference, 2009. MILCOM 2009. IEEE. 2009. IEEE.
[18] Kreutz, D., et al., Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 2015. 103(1): p. 14-76.
[19] Silva, R., J.S. Silva ,and F. Boavida, Mobility in wireless sensor networks–survey and proposal. Computer Communications, 2014. 52: p. 1-20
[20] Yu, H., et al. Energy Efficient Routing Algorithm Using Software Defining Network for WSNs via Unequal Clustering. in International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystems. 2016. Springer.
[21] Gong, N. and X. Huang. Reliability Analysis of Software Defined Wireless Sensor Networks. 2016. Singapore: Springer Singapore.
[22] Duan, Y., et al., A methodology for reliability of WSN based on software defined network in adaptive industrial environment. IEEE/CAA Journal of Automatica Sinica, 2018. 5(1): p. 74-82.
[23] Gante, A.D., M. Aslan, and A. Matrawy. Smart wireless sensor network management based on software-defined networking. in 2014 27th Biennial Symposium on Communications (QBSC). 2014.
[24] Jiang, J., et al., A trust cloud model for underwater wireless sensor networks :(۳)۵۵ .۲۰۱۷ .p. 110-116.
[25] Tajeddine, A., et al., CENTERA: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks. 2015. 15(2): p. 3299-3333.
[26] Wang, R., et al., ETMRM: An Energy-efficient Trust Management and Routing Mechanism for SDWSNs. Computer Networks, 2018. 139: p. 119-135.
[27] Galluccio, L., et al. SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks. in 2015 IEEE Conference on Computer Communications (INFOCOM), . 2015. IEEE.
[28] Lantz, B., B. Heller, and N. McKeown. A network in a laptop: rapid prototyping for software-defined networks. in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks .2010 .ACM.
[29] Charles, A.J .and P. Kalavathi, QoS Measurement of RPL using Cooja Simulator and Wireshark Network Analyser. 2018.
[30] Valenti, S., et al. A low cost wireless sensor node for building monitoring. in 2018 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS). 2018. IEEE.
[31] de Oliveira, B.T. and C.B. Margi. Distributed control plane architecture for software-defined Wireless Sensor Networks. in Consumer Electronics (ISCE), 2016 IEEE International Symposium on. 2016. IEEE.
[32] Kumar.G, Mehra.H, R Seth.A, N.HemavathiS.Sudha.P. An Hybrid ClusteringAlgorithm for OptimalClusters in Wireless Sensor Networks Conference on Electrical, Electronics and Computer Science.2014.
[33] CodeProject users worldwide 2016, URL: https://www.codeproject.com/Articles/606364/Wireless-Sensor-Network-Localization-Simulator-v2, Access Date: 17 Jun 2013.

پی‌نوشت

[1] Wireless Sensor Network
[2] Internet of Things
[3] Software Defined Network
[4] Transmission Control Protocol / Internet Protocol
[5] controller to switch
[6] asynchronous
[7] symmetric
[8] Open Flow Sensor
[9] CTMCs
[10] Single Point of Failure
[11] Network Operating System
[12] Middle Ware
[13] CENTERA
[14] Selective Forwarding Attack
[15] Grey hole
[16] Black hole
[۱۷] ETMRM
[۱۸] Packet-In
[۱۹] Sensor Flow
[20] Wise
[21] INPP
[22] Tiny
[23] Spoofing
[24] Overhearing
[25] Cluster Head Commander
[26] Orphan
[27] Intimacy
[28] Honesty
[29] Energy
[30] Unselfishness
[31] Trustor
[32] Trustee
[33] Maturity
[34] anomaly detection rules
[35] Beacon
[36] Wireless Sensor Network Simulator
[37] Spoofing
[38] Acknowledgment
[39] Slot