APJ. 6 (3):18-29, Autumn 2025

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Enhancing the Reliability of Wireless Sensor Networks Using Lightweight Machine Learning

M.najafijalalieh[*,1], *M.Shirmohammadi*[2]

[1] *Department of Computer Engineering, Hamedan Branch, Islamic Azad University, Hamedan, Iran*
[2] *Department of Computer Engineering, Hamedan Branch, Islamic Azad University, Hamedan, Iran*

RESEARCH PAPER

Received: 2025-9-1
Accepted: 2025-12-2

KEYWORDS:
Wireless sensor network,
Tiny ML,
Reliability,
Fault Detection,
Internet of Things

[1] Corresponding author:
m.najafi@iauh.ac.ir

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as one of the key technologies in recent decades due to their rapid deployability, low cost, and wide range of applications in fields such as the Internet of Things (IoT), environmental monitoring, smart agriculture, and critical systems. However, the hardware and software limitations of sensor nodes — including low processing power and limited energy resources — make these networks vulnerable to failures and disruptions, turning reliability into a fundamental challenge.

In this study, a novel framework based on Tiny Machine Learning (TinyML) is proposed to enhance reliability and optimize energy consumption in WSNs. The proposed architecture consists of four key modules — anomaly detection, failure prediction, intelligent data compression, and adaptive routing — which are deployed locally at the node level to enable fast processing, reduce communication overhead, and enable intelligent resource management.

Simulation results demonstrated that the proposed method not only increases the network lifetime and significantly reduces energy consumption but also improves data quality, communication stability, and responsiveness to abnormal events.

The findings of this research indicate that leveraging TinyML can open new horizons in the design of intelligent WSNs and provide a solid foundation for developing future large-scale applications in dynamic environments.

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۳، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

افزایش اتکا پذیری در شبکه های حسگر بی‌سیم با استفاده از یادگیری ماشین کوچک

مهدی نجفی جلالیه*[۱]، محمد مهدی شیر محمدی[۲]

[۱] گروه مهندسی کامپیوتر ،واحد همدان ، دانشگاه آزاد اسلامی ، همدان ، ایران

[۲] گروه مهندسی کامپیوتر ،واحد همدان ، دانشگاه آزاد اسلامی ، همدان ، ایران

چکیده

مقاله پژوهشی

شبکه‌های حسگر بی‌سیم (WSN) به دلیل قابلیت استقرار سریع، هزینه پایین و کاربردهای گسترده در حوزه‌هایی همچون اینترنت اشیا، پایش محیطی، کشاورزی هوشمند و سامانه‌های حیاتی، به یکی از فناوری‌های کلیدی در دهه‌های اخیر تبدیل شده‌اند. با این حال، محدودیت‌های سخت‌افزاری و نرم‌افزاری گره‌های حسگر، از جمله توان پردازشی و انرژی پایین، این شبکه‌ها را در برابر خرابی‌ها و اختلالات آسیب‌پذیر ساخته و موضوع اتکاپذیری را به چالشی اساسی بدل کرده است.

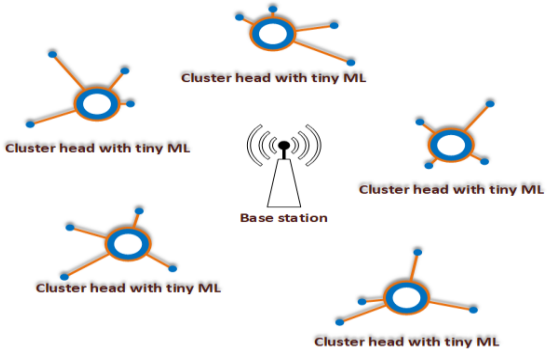
در این پژوهش، چارچوبی نوین مبتنی بر یادگیری ماشین کوچک (TinyML) برای افزایش اتکاپذیری و بهینه‌سازی مصرف انرژی در شبکه‌های حسگر بی‌سیم ارائه گردیده است. معماری پیشنهادی شامل چهار ماژول کلیدی تشخیص ناهنجاری، پیش‌بینی خرابی، فشرده‌سازی هوشمند داده و مسیریابی تطبیقی می‌باشد که با استقرار محلی در سطح گره‌ها، امکان پردازش سریع، کاهش بار ارتباطی و مدیریت هوشمند منابع را فراهم می‌سازد. نتایج شبیه‌سازی‌ها نشان داد که روش پیشنهادی علاوه بر افزایش طول عمر شبکه و کاهش چشمگیر مصرف انرژی، موجب بهبود کیفیت داده، پایداری ارتباطات و واکنش سریع به رخدادهای غیرعادی می‌گردد.

یافته‌های این تحقیق نشان می‌دهد که بهره‌گیری از یادگیری ماشین کوچک می‌تواند افق‌های جدیدی را در طراحی شبکه‌های حسگر بی‌سیم هوشمند بگشاید و بستر مناسبی برای توسعه کاربردهای آینده در مقیاس‌های کلان و محیط‌های پویا فراهم آورد.

واژگان کلیدی:
شبکه حسگر بی‌سیم،
یادگیری ماشین کوچک،
اتکاپذیری،
تشخیص خطا،
اینترنت اشیا.

۱– مقدمه

شبکه‌های حسگر بی‌سیم(Wireless Sensor Networks - WSNs) ، به عنوان یکی از فناوری‌های کلیدی در حوزه اینترنت اشیا(IoT) ، در سال‌های اخیر به طور گسترده‌ای مورد توجه قرار گرفته‌اند. این شبکه‌ها متشکل از تعداد زیادی گره حسگر با توان پردازشی، ذخیره‌سازی و ارتباطی محدود هستند که در محیط‌های مختلف برای پایش محیطی، کنترل هوشمند، مدیریت انرژی، کشاورزی دقیق و سلامت از راه دور به کار می‌روند. گره‌های حسگر پس از جمع‌آوری اطلاعات، آن‌ها را به یک گره مرکز یا ایستگاه پایه ارسال می‌کنند تا مورد تحلیل قرار گیرند. با توجه به ماهیت بی‌سیم، مصرف انرژی محدود و قرارگیری در محیط‌های نامساعد و غیرقابل کنترل، حفظ اتکاپذیری (Reliability)در این شبکه‌ها به یکی از چالش‌های اصلی و حیاتی تبدیل شده است.



شکل ۱: نمایی از شبکه سنسور بی‌سیم

اتکاپذیری در شبکه‌هایWSN ، به توانایی سیستم برای ارائه خدمات پیوسته، دقیق و بدون خطا در مواجهه با اختلالات گوناگون اشاره دارد. این اختلالات می‌توانند شامل خرابی گره‌ها، قطع ارتباط به دلیل موانع فیزیکی یا تداخلات محیطی، داده‌های نادرست ناشی از حسگرهای معیوب و یا حملات امنیتی باشند. از دست رفتن اتکاپذیری می‌تواند منجر به داده‌های ناقص، کاهش دقت در تصمیم‌گیری‌ها و حتی شکست کامل وظایف محوله شود. از این رو، طراحی و پیاده‌سازی سازوکارهایی که بتوانند خطاها را تشخیص دهند، با شرایط ناپایدار شبکه سازگار شوند و عملکرد کلی سیستم را حفظ کنند، ضروری است(1) .

در سال‌های اخیر، استفاده از الگوریتم‌های یادگیری ماشین (Machine Learning - ML)به عنوان ابزاری قدرتمند برای تحلیل داده‌ها، تشخیص الگو و پیش‌بینی رفتار سیستم‌ها مطرح شده است. این الگوریتم‌ها می‌توانند به افزایش خودمختاری سیستم‌های توکار (Embedded Systems)کمک کنند. با این حال، اجرای مستقیم مدل‌های پیچیده MLبر روی گره‌های حسگر با محدودیت‌های جدی مانند توان پردازشی پایین، مصرف انرژی محدود و حافظه اندک مواجه است. علاوه بر این، انتقال حجم زیاد داده‌های خام از گره‌ها به سرور مرکزی برای پردازش، پهنای باند شبکه را به شدت اشغال کرده و موجب افزایش مصرف انرژی می‌شود(2) .

در پاسخ به این محدودیت‌ها، حوزه نوظهور یادگیری ماشین کوچک یا TinyMLشکل گرفته است. این فناوری به توسعه و پیاده‌سازی مدل‌های یادگیری ماشین سبک، کم‌حجم و بهینه‌شده برای اجرا بر روی سخت‌افزارهای کم‌مصرف، مانند میکروکنترلرها(MCUs) ، می‌پردازد . TinyMLبه گره‌های حسگر امکان می‌دهد تا تحلیل‌های محلی و تصمیم‌گیری‌های بی‌درنگ انجام دهند و تنها در صورت لزوم اطلاعات مهم را به ایستگاه مرکزی منتقل کنند. از این طریق می‌توان تا حد زیادی در مصرف انرژی صرفه‌جویی کرد، تأخیر در پردازش را کاهش داد، حریم خصوصی داده‌ها را افزایش داد و عملکرد شبکه را پایدارتر نمود. این قابلیت‌ها به ویژه در سناریوهایی که نیاز به پاسخ‌دهی سریع و تحلیل آفلاین داده‌ها وجود دارد، بسیار حیاتی هستند(3) .

با وجود اهمیت TinyML، تحقیقات فعلی در زمینه کاربرد آن برای افزایش اتکاپذیری WSN هنوز کامل نیست. بیشتر مدل‌های موجود تنها برای پیش‌بینی یا طبقه‌بندی کاربرد دارند و کمتر به موضوعات پیچیده‌تر مانند تشخیص آنومالی، مسیریابی تطبیقی و نگهداری پیش‌بینانه با اجرای محلی پرداخته‌اند. پژوهش‌های پیشین به صورت جداگانه بر روی هر یک از این حوزه‌ها تمرکز کرده‌اند، اما یک چارچوب عملی و جامع که بتواند این قابلیت‌ها را در یک معماری یکپارچه پیاده‌سازی کند، هنوز ارائه نشده است. این شکاف در پژوهش‌های موجود، انگیزه اصلی ما برای انجام این تحقیق است(4) . در این مقاله، ما به دنبال ارائه یک معماری عملی مبتنی بر TinyML برای افزایش اتکاپذیری شبکه‌های حسگر بی‌سیم هستیم. معماری پیشنهادی ما شامل ماژول‌های تشخیص ناهنجاری برای شناسایی داده‌های غیرمعمول، پیش‌بینی خطا برای تشخیص زودهنگام مشکلات احتمالی، فشرده‌سازی هوشمند داده‌ها برای کاهش حجم داده‌های ارسالی و مسیریابی تطبیقی برای مدیریت بهینه جریان داده است. تمامی این ماژول‌ها برای پیاده‌سازی بر روی گره‌های حسگر سبک طراحی شده‌اند. هدف ما این است که نشان دهیم چگونه یک رویکرد یکپارچه مبتنی بر TinyMLمی‌تواند عملکرد کلی شبکه را در شرایط نامطمئن و با منابع محدود به طور قابل توجهی بهبود بخشد. کارایی این روش‌ها با تکیه بر نتایج شبیه‌سازی یا نمونه‌سازی اولیه بررسی و ارزیابی خواهد شد.

ساختار این مقاله به شرح زیر است: در بخش دوم، مروری بر پژوهش‌های پیشین و مفاهیم کلیدی مرتبط باWSN ، TinyMLو اتکاپذیری ارائه می‌شود. بخش سوم، به شرح معماری و روش پیشنهادی ما می‌پردازد. در بخش چهارم، نتایج ارزیابی عملکرد و تحلیل آن‌ها آورده شده و در نهایت، در بخش پنجم، جمع‌بندی و پیشنهاداتی برای پژوهش‌های آتی ارائه خواهد شد.

۲- بیان مسئله

شبکه‌های حسگر بی‌سیم (WSN) به دلیل قابلیت استقرار سریع، هزینه پایین، و انعطاف‌پذیری بالا، به‌طور گسترده در محیط‌های نامطمئن، غیرقابل دسترس یا حساس به انرژی مورد استفاده قرار می‌گیرند. با این حال، گره‌های حسگر در این شبکه‌ها اغلب از منابع محدودی از جمله پردازنده ضعیف، حافظه اندک، و باتری با ظرفیت محدود بهره‌مند هستند. این محدودیت‌ها سبب می‌شود که عملکرد این شبکه‌ها در برابر عوامل اختلال‌زا مانند خرابی گره‌ها، ناپایداری ارتباطات، خطاهای حسگر، یا حملات امنیتی به‌شدت آسیب‌پذیر باشد. چنین ضعف‌هایی، منجر به کاهش اتکاپذیری (Reliability) شبکه و تضعیف کیفیت خدمات آن در کاربردهای حیاتی می‌شود.

روش‌های سنتی برای افزایش اتکاپذیری، معمولاً متکی بر الگوریتم‌های متمرکز و ارسال داده‌های حسگر به ایستگاه پایه جهت تحلیل و تصمیم‌گیری هستند. این روش‌ها نه‌تنها با تأخیر بالا و مصرف انرژی زیاد همراه‌اند، بلکه در صورت قطعی ارتباط یا ازدحام شبکه، به‌کلی از کار می‌افتند. از سوی دیگر، استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی خطا و پیش‌بینی اختلالات نیز با چالش‌هایی جدی در محیط‌های دارای محدودیت منابع مواجه است؛ چرا که مدل‌های ML معمولاً نیاز به منابع محاسباتی و ذخیره‌سازی بالایی دارند.

در چنین شرایطی، استفاده از یادگیری ماشین کوچک (TinyML) به‌عنوان راهکاری نوظهور برای اجرای مدل‌های سبک یادگیری ماشین در سخت‌افزارهای کم‌مصرف، می‌تواند راه‌حلی مناسب برای افزایش هوشمندی و پایداری گره‌های حسگر باشد. با استقرار مدل‌های یادگیری سبک در گره‌های شبکه، امکان تصمیم‌گیری محلی، تشخیص سریع خطاها، و بهبود سازگاری شبکه با شرایط متغیر فراهم می‌شود، بدون آنکه به ارتباط مداوم با سرور مرکزی نیاز باشد.

مسئله اصلی که این پژوهش به آن می‌پردازد، چگونگی طراحی و پیاده‌سازی معماری مبتنی بر TinyML برای بهبود اتکاپذیری شبکه‌های حسگر بی‌سیم است، به‌گونه‌ای که با وجود محدودیت منابع، بتوان دقت، پایداری و طول عمر شبکه را افزایش داد. این پژوهش در تلاش است تا نشان دهد چگونه مدل‌های بهینه‌شده یادگیری ماشین می‌توانند به‌صورت مؤثر در لبه شبکه پیاده‌سازی شده و عملکرد سیستم را در برابر خطا و اختلال بهبود بخشند.

۳- کارهای مرتبط

شبکه‌های حسگر بی‌سیم (WSN) متشکل از تعداد زیادی گره حسگر با توان پردازشی، ارتباطی و ذخیره‌سازی محدود هستند که در محیط‌های مختلف برای پایش داده به‌کار می‌روند. یکی از چالش‌های اصلی در این شبکه‌ها، اتکاپذیری پایین در برابر خرابی گره‌ها، قطع ارتباط، یا تداخلات محیطی است. پژوهش (8) نشان داده است که ویژگی‌هایی مانند مصرف انرژی کم، تحمل خطا، و مدیریت مسیر، در طراحی WSN اهمیت کلیدی دارند و راهکارهای سنتی همچون الگوریتم‌های مسیریابی یا افزونگی داده نمی‌توانند به تنهایی عملکرد پایدار شبکه را تضمین کنند.

TinyMLبه عنوان حوزه‌ای نوظهور در یادگیری ماشین، امکان اجرای مدل‌های سبک و بهینه‌شده بر روی دستگاه‌های بسیار محدود مانند میکروکنترلرها را فراهم می‌سازد. طبق مرور(2) در حوزه‌هایی مانند کشاورزی هوشمند، پایش محیط، تشخیص ناهنجاری، و اینترنت حیوانات به کار گرفته شده و قابلیت‌هایی مانند مصرف انرژی بسیار پایین، زمان پاسخ سریع، حفظ حریم خصوصی داده‌ها و اجرای آفلاین را ارائه می‌دهد.

یکی از مسیرهای نوین پژوهش، استفاده از TinyML در گره‌های WSN برای انجام تحلیل‌های محلی و تصمیم‌گیری بی‌درنگ است. پژوهش (4)در مقاله‌ای در مجله *Information Fusion*، ترکیب یادگیری فدرال (Federated Learning)و یادگیری انتقالی (Transfer Learning) را برای آموزش مدل‌های TinyML درون‌گرا (on-board) پیشنهاد داده است. آن‌ها با آزمایش روی دستگاه‌های واقعی مثل Arduino و Raspberry Pi نشان دادند که این رویکرد می‌تواند دقت پیش‌بینی را افزایش داده، مصرف انرژی را کاهش دهد و در شرایط داده‌های نامتوازن نیز عملکرد مطلوبی داشته باشد.

این روش با حذف نیاز به ارسال داده‌های خام به سرور مرکزی، نه تنها مصرف انرژی و پهنای باند را کاهش می‌دهد بلکه به افزایش پایداری و اتکاپذیری شبکه کمک می‌کند. همچنین، وجود چارچوب‌هایی مانند TensorFlow Lite Microو TinyTrain زمینه را برای آموزش و استقرار مدل‌ها روی گره‌های بسیار سبک فراهم ساخته است.

یکی از مطالعات اولیه در زمینه امنیت شبکه‌های حسگر بی‌سیم، توسط (5) ارائه شده است. در این پژوهش، نویسندگان با بررسی کاربردهای گسترده WSN در حوزه‌های نظامی، پزشکی، محیط زیست و صنعت، بر چالش‌های امنیتی ناشی از ماهیت بی‌سیم شبکه و محدودیت منابع نودها تأکید کرده‌اند. در این مقاله انواع حملات مهم مانند DoS، Wormhole، Sybil، Sinkhole، Selective Forwarding، Hello Flood، Node Captureو حملات مبتنی بر درج نود مخرب تحلیل شده و راهکارهای مقابله‌ای متناسب با هر لایه از شبکه ارائه گردیده است. تمرکز ویژه این مطالعه بر حملات DoS و پیامدهای آن بر کاهش توان عملیاتی شبکه بوده است. همچنین نویسندگان پیشنهاد کرده‌اند که به جای راهکارهای جزیره‌ای در هر لایه، لازم است رویکردهای یکپارچه امنیتی توسعه داده شود تا بتوان امنیت WSN را به صورت کلی تضمین کرد

در حوزه امنیت شبکه‌های حسگر بی‌سیم ، پژوهش جامعی توسط (6) انجام شده است که در آن تهدیدات امنیتی متنوع همچون حملاتDoS ، Sinkhole، Wormhole، Sybil، Selective Forwardingو Jamming مورد بررسی قرار گرفته و برای هر یک از این تهدیدات، مکانیزم‌های دفاعی متناسب معرفی شده است. این مطالعه با مرور طیف وسیعی از الگوریتم‌ها و پروتکل‌های موجود، از جمله روش‌های رمزنگاری، توزیع کلید، احراز هویت چندعاملی و سامانه‌های تشخیص نفوذ، تصویری

جامع از وضعیت امنیتی WSN ارائه کرده است. نویسندگان همچنین چالش‌های باقی‌مانده و نیاز به توسعه راهکارهای کارآمدتر و سبک‌تر برای مقابله با حملات نوظهور را برجسته کرده‌اند.

مقاله «Exploring coverage and security challenges in wireless sensor networks: A survey» نوشته Moslehi et al. (2025) (14) به بررسی جامعی از چالش‌های پوشش و امنیت در شبکه‌های حسگر بی‌سیم می‌پردازد. این مقاله استراتژی‌های استقرار مختلف مانند روش‌های قطعی، تصادفی و سه‌بعدی را تحلیل کرده و تأثیر آن‌ها بر پوشش، اتصال و مصرف انرژی را بررسی می‌کند. همچنین، این پژوهش به چالش‌های امنیتی کلیدی مانند حملات DoS ، حملات black-hole و gray-hole ، و همچنین راه‌حل‌های مربوط به آن‌ها مانند سیستم‌های تشخیص نفوذ (IDS) مبتنی بر یادگیری ماشین و تکنیک‌های الهام گرفته از زیست می‌پردازد. این مقاله با مقایسه شبکه‌های حسگر همگن و ناهمگن، نشان می‌دهد که چگونه معیارهای متفاوت طراحی بر عملکرد و امنیت شبکه تأثیر می‌گذارند. بنابراین، این مقاله یک منبع ارزشمند برای درک مسائل پیچیده در زمینه استقرار و امنیت WSN است و می‌تواند به عنوان یک پایه نظری محکم برای پژوهش‌های مرتبط مورد استفاده قرار گیرد. مقاله «TinyML for Ultra-Low Power AI and Large Scale IoT Deployments: A Systematic Review» نوشته Schizas و همکاران (۲۰۲۲) یک مرور جامع بر TinyML ارائه می‌دهد. این پژوهش TinyML را به عنوان یک حوزه فناوری نوظهور معرفی می‌کند که هدف آن پیاده‌سازی الگوریتم‌های یادگیری ماشین بر روی دستگاه‌های با منابع محدود و میکروکنترلرها (MCUs) است. این فناوری با کاهش تأخیر، مصرف بهینه پهنای باند و بهبود امنیت و حریم خصوصی داده‌ها، عصر جدیدی را در اینترنت اشیا (IoT) رقم می‌زند.(25) این مقاله به بررسی چالش‌های کلیدی TinyML ، از جمله مصرف انرژی بسیار پایین، حافظه محدود، قدرت پردازش و ناهمگونی سخت‌افزار می‌پردازد. نویسندگان توضیح می‌دهند که چگونه این محدودیت‌ها بر عملکرد سیستم تأثیر می‌گذارند و نیاز به الگوریتم‌های بهینه‌سازی و سخت‌افزارهای تخصصی را برجسته می‌کنند. این مقاله همچنین چارچوب‌ها و کتابخانه‌های موجود مانند TensorFlow Lite را مورد بررسی قرار داده و نقش آن‌ها را در گسترش کاربرد یادگیری ماشین در دستگاه‌های تعبیه‌شده توضیح می‌دهد.

این تحقیق کاربردهای TinyML را در زمینه‌های مختلفی از جمله نظارت بر محیط زیست، ردیابی افراد، و تشخیص ناهنجاری بررسی می‌کند. این مقاله نشان می‌دهد که چگونه TinyML با پردازش داده‌ها در نزدیکی سنسورها، حریم خصوصی و پاسخگویی را افزایش داده و در عین حال هزینه‌های مرتبط با انتقال داده بی‌سیم را کاهش می‌دهد. این مقاله یک منبع اطلاعاتی مهم برای جامعه پژوهش اینترنت اشیا و رایانش ابری است و می‌تواند راه را برای مطالعات آینده در این زمینه هموار کند.

با پیشرفت الگوریتم‌های یادگیری ماشین، پژوهشگران تلاش کرده‌اند از آن‌ها برای افزایش هوشمندی WSN استفاده کنند؛ از جمله در کاربردهایی مانند تشخیص خطا، پیش‌بینی عمر باتری، و طبقه‌بندی رویدادها. با این حال، اجرای این الگوریتم‌ها در محیطی با منابع محدود مانند گره‌های WSN چالش‌برانگیز است، زیرا اغلب مدل‌ها نیازمند منابع محاسباتی، انرژی و حافظه بالا هستند.

اگرچه پژوهش‌های متعددی به بررسی TinyML و یادگیری ماشین در IoT و WSN پرداخته‌اند، اما هنوز چارچوب‌های عملی و جامعی برای افزایش اتکاپذیری WSN با استفاده مستقیم از TinyML در سطح گره‌های حسگر توسعه نیافته است. بیشتر مدل‌های موجود تنها برای پیش‌بینی یا طبقه‌بندی کاربرد دارند و کمتر به موضوعاتی مانند تشخیص آنومالی، مسیریابی تطبیقی و نگهداری پیش‌بینانه با اجرای محلی پرداخته‌اند. مقاله حاضر تلاش دارد این شکاف را با ارائه یک معماری کاربردی پوشش دهد.

جدول مقایسه کارهای مرتبط

جدول ۱: مقایسه کار های مرتبط

مرجع	موضوع اصلی	نکات کلیدی	نقاط قوت/تمرکز
García-Hernández et al. (2007)	اتکاپذیری در شبکه‌های WSN	بررسی چالش‌های اتکاپذیری و نقش تحمل خطا و مصرف انرژی کم	تأکید بر عدم کفایت راهکارهای سنتی
Kalpana Sharma (2010)	امنیت در شبکه‌های WSN	تحلیل حملات رایج مانند DoS و Sybil	بررسی اولیه حملات و ارائه راهکارهای لایه‌ای
Schizas et al. (2022)	مرور جامع TinyML	بررسی چالش‌های TinyML (حافظه و قدرت پردازش محدود) و چارچوب‌های آن (TensorFlow Lite)	مرور سیستماتیک بر TinyML و چالش‌های سخت‌افزاری آن
Abadade et al. (2023)	کاربرد IoT TinyML	ارائه کاربردهای TinyML در زمینه‌های مختلف (کشاورزی هوشمند)	تأکید بر مزایای TinyML مانند پاسخ سریع و حفظ حریم خصوصی
Ficco et al. (2024)	WSN TinyML	پیشنهاد ترکیب یادگیری فدرال و انتقالی برای افزایش دقت و کاهش مصرف انرژی	رویکرد نوین برای پیاده‌سازی TinyML در سطح گره‌های حسگر
Moslehi et al. (2025)	پوشش و امنیت WSN	بررسی استراتژی‌های استقرار و راهکارهای امنیتی مبتنی بر یادگیری ماشین	ارائه یک مرور جامع بر هر دو جنبه پوشش و امنیت
Elham Alotaibi et al. (2025)	امنیت پیشرفته WSN	بررسی تهدیدات متنوع و مکانیزم‌های دفاعی (رمزنگاری، احراز هویت)	مرور جامع بر مکانیزم‌های امنیتی در WSN

۴– پروتکل پیشنهادی

در این پژوهش، با هدف افزایش اتکاپذیری در شبکه‌های حسگر بی‌سیم، یک چارچوب نوین مبتنی بر یادگیری ماشین کوچک ارائه شده است که قادر است فرایندهای تصمیم‌گیری و تحلیل داده را به سطح گره‌های حسگر انتقال دهد .رویکرد سنتی مبتنی بر ارسال همه داده‌ها به ایستگاه مرکزی نه‌تنها مصرف انرژی را افزایش می‌دهد، بلکه در مواجهه با اختلالات شبکه (مانند قطع ارتباط یا تداخل)، باعث از دست رفتن داده یا تأخیر در واکنش سیستم می‌شود. در چارچوب پیشنهادی، هر گره حسگر به یک مدل یادگیری سبک مجهز شده که پس از آموزش خارج از شبکه(offline) ، به فرمت فشرده درآمده و بر روی میکروکنترلر گره مستقر می‌گردد. این مدل می‌تواند در محل (on-device) وظایفی نظیر تشخیص ناهنجاری، پیش‌بینی خرابی گره، و تصمیم‌گیری درباره ارسال یا عدم ارسال داده را برعهده بگیرد.

ایده اصلی این معماری بر این مبنا است که گره‌های حسگر، علی‌رغم محدودیت‌های جدی از نظر پردازش، حافظه و انرژی، می‌توانند با بهره‌گیری از مدل‌های یادگیری ماشین سبک، قابلیت‌های هوشمندانه‌ای در خود جای دهند. به جای تکیه صرف بر روش‌های سنتی مسیریابی یا مکانیزم‌های امنیتی که عمدتاً به‌صورت مجزا عمل می‌کنند، این معماری به دنبال آن است که چندین قابلیت کلیدی را در قالب یک راهکار منسجم و هماهنگ ترکیب نماید.

تمرکز اصلی این رویکرد بر طراحی ماژول‌های سبک و کارآمد است که بتوانند بدون ایجاد سربار سنگین محاسباتی یا مصرف انرژی بیش از حد، روی گره‌های کم‌منبع اجرا شوند. معماری پیشنهادی علاوه بر آنکه به نیازهای عملیاتی WSN پاسخ می‌دهد، با شرایط نامطمئن محیطی و محدودیت‌های ذاتی این شبکه‌ها نیز سازگار است.

این معماری با ادغام چهار ماژول اصلی یعنی تشخیص ناهنجاری، پیش‌بینی خطا، فشرده‌سازی هوشمند داده و مسیریابی تطبیقی، قادر است هم‌زمان چندین جنبه‌ی مهم از عملکرد شبکه را بهبود بخشد: کیفیت داده‌ها از طریق حذف یا علامت‌گذاری داده‌های غیرعادی ارتقا می‌یابد؛ پایداری شبکه با پیش‌بینی خرابی‌ها و فعال‌سازی مسیرهای جایگزین تضمین می‌شود؛ بهره‌وری انرژی از طریق کاهش داده‌های ارسالی افزایش می‌یابد؛ و در نهایت، مدیریت جریان داده با انتخاب پویا و هوشمند مسیرهای ارتباطی بهینه صورت می‌گیرد.

به بیان دیگر، هدف اصلی این معماری آن است که نشان دهد چگونه می‌توان با حداقل مصرف منابع سخت‌افزاری و نرم‌افزاری، حداکثر میزان پایداری، دقت و کارایی را در شبکه‌های حسگر بی‌سیم فراهم آورد. این رویکرد نه تنها امکان افزایش طول عمر شبکه را فراهم می‌سازد، بلکه بهبود کیفیت سرویس و اطمینان‌پذیری داده‌ها را نیز تضمین می‌کند.

معماری پیشنهادی

معماری پیشنهادی شامل چهار ماژول اصلی است که به صورت مکمل با یکدیگر عمل می‌کنند:

1. ماژول تشخیص ناهنجاری(Anomaly Detection)

در شبکه‌های حسگر، داده‌های جمع‌آوری‌شده همواره قابل اعتماد نیستند و ممکن است به دلیل نویز، خرابی سخت‌افزار یا حملات مخرب دچار انحراف شوند. این ماژول با استفاده از مدل‌های سبک TinyML داده‌ها را به صورت بلادرنگ تحلیل کرده و مقادیر غیرمعمول را شناسایی می‌کند. داده‌های ناهنجار بلافاصله علامت‌گذاری شده و با اولویت بالا در شبکه ارسال می‌شوند تا امکان واکنش سریع فراهم گردد. این قابلیت نه‌تنها کیفیت داده‌های جمع‌آوری‌شده را بهبود می‌بخشد، بلکه مانع از انتشار داده‌های بی‌ارزش یا مضر در شبکه می‌شود.

2. ماژول پیش‌بینی خطا (Fault Prediction)

یکی از نقاط ضعفWSN ، خرابی ناگهانی گره‌ها یا لینک‌های ارتباطی است که می‌تواند منجر به از دست رفتن داده‌ها یا قطع سرویس گردد. ماژول پیش‌بینی خطا با تحلیل شاخص‌های سلامت گره‌ها (مانند انرژی باقی‌مانده، دما، کیفیت لینک و نرخ از دست رفت بسته‌ها) احتمال خرابی آینده را تخمین می‌زند. در صورت پیش‌بینی خطر خرابی، گره مربوطه می‌تواند به‌طور خودکار داده‌های خود را تخلیه کرده یا مسیرهای جایگزین را فعال کند. این امر سبب می‌شود که اختلالات شبکه به حداقل برسد و زمان بازیابی کاهش یابد.

3. ماژول فشرده‌سازی هوشمند داده(Smart Data Compression)

ارسال داده به‌عنوان یکی از پرمصرف‌ترین عملیات‌ها در گره‌های حسگر، سهم زیادی در مصرف انرژی دارد. ماژول فشرده‌سازی هوشمند داده با بهره‌گیری از الگوریتم‌های سبک و تطبیقی، داده‌ها را بر اساس میزان تغییرپذیری آن‌ها فشرده می‌کند. برای داده‌های پایدار، از روش‌های ساده استفاده می‌شود، در حالی که برای داده‌های پرنوسان یا حیاتی، روش‌های دقیق‌تر با خطای کمتر به‌کار گرفته می‌شوند. این سازوکار سبب کاهش چشمگیر حجم ترافیک شبکه شده و در نتیجه طول عمر گره‌ها و کل شبکه افزایش می‌یابد.

4. ماژول مسیریابی تطبیقی(Adaptive Routing)

به منظور تضمین تحویل داده در شرایط متغیر شبکه، ماژول مسیریابی تطبیقی طراحی شده است. این ماژول با ارزیابی مداوم معیارهایی نظیر کیفیت لینک، میزان ترافیک، تأخیر و سطح اعتماد به همسایه‌ها، مسیر بهینه را برای ارسال داده انتخاب می‌کند. در شرایط بحرانی، مانند وقوع خطا یا شناسایی ناهنجاری، مسیرهای جایگزین فعال می‌شوند تا از اختلال در سرویس جلوگیری شود. این ویژگی پایداری و قابلیت‌اعتماد شبکه را به شکل قابل توجهی ارتقا می‌دهد.

ویژگی‌های کلیدی معماری

یکپارچگی **:**ترکیب چهار ماژول فوق در قالب یک معماری هماهنگ، امکان مدیریت جامع اتکاپذیری شبکه را فراهم می‌سازد.

سبک و بهینه :تمامی مدل‌ها و الگوریتم‌ها به‌گونه‌ای طراحی شده‌اند که روی گره‌های کم‌منبع با حداقل توان پردازشی قابل اجرا باشند.

تطبیق‌پذیری :ماژول‌ها به‌صورت پویا بر اساس شرایط محیطی و شبکه تنظیم می‌شوند.

صرفه‌جویی انرژی :کاهش ترافیک غیرضروری و جلوگیری از ارسال داده‌های بی‌ارزش، به طور مستقیم منجر به افزایش طول عمر شبکه می‌شود.

معماری سیستم شبکه سنسور بی‌سیم شامل دو لایه اصلی است:

۱. گره‌های حسگر هوشمند :شامل حسگر، میکروکنترلر کم‌مصرف، و مدل یادگیری.

۲. ایستگاه پایه :دریافت‌کننده داده‌های نهایی و هشدارها.

هر گره پس از دریافت داده از حسگر، ابتدا آن را نرمال‌سازی کرده و سپس مدل محلی را برای تحلیل داده اجرا می‌کند. در صورت شناسایی ناهنجاری، بسته اطلاعاتی حاوی داده و هشدار به ایستگاه مرکزی ارسال می‌شود. در غیر این صورت، داده حذف یا فشرده شده و تنها در صورت نیاز ارسال می‌گردد.

همچنین، در نسخه توسعه‌یافته این چارچوب، یک ماژول ساده برای مدل‌سازی مصرف انرژی و پیش‌بینی زوال عملکرد گره‌ها نیز افزوده شده است تا از طریق تحلیل وضعیت گره، امکان نگهداری پیشگیرانه فراهم گردد.

این روش موجب می‌شود:

از ارسال غیرضروری داده‌ها جلوگیری شود،

مصرف انرژی کاهش یابد،

واکنش سریع به رخدادهای مهم در محل انجام شود،

و طول عمر عملیاتی شبکه افزایش یابد.

مراحل گام‌به‌گام

۱ .تولید و نرمال‌سازی داده‌ها

داده‌های حسگر (مثلاً دما، رطوبت) به صورت مصنوعی یا واقعی جمع‌آوری شده و برای ورود به مدل یادگیری نرمال‌سازی می‌شوند:

$$X_{norm} = \frac{x-\min(x)}{\max(x)-\text{main}(x)} \quad (1)$$

۲ .آموزش مدل Autoencoder

از یک مدل Autoencoder سبک برای یادگیری الگوی نرمال داده استفاده می‌شود. مدل تلاش می‌کند ورودی x را بازسازی کند:

$$\hat{x} = f_{decoder}(f_{encoder}(x)) \quad (2)$$

و تابع زیان مدل به صورت میانگین مربع خطای بازسازی است:

$$\iota = \frac{1}{n}\sum_{i=1}^{n}(xi - \hat{xi})^2 \quad (3)$$

۳ .تشخیص ناهنجاری(Anomaly Detection)

پس از آموزش، برای هر داده ورودی، خطای بازسازی محاسبه می‌شود:

$$e_i = |x_i - \hat{x_i}| \quad (4)$$

اگر این خطا از آستانه تجربی θ بیشتر باشد، داده به عنوان ناهنجاری در نظر گرفته می‌شود:

$$Label_i = \begin{cases} 1 & \theta < e_i \text{ (ناهنجاری)} \\ 0 & \text{در غیر این صورت} \end{cases} \quad (5)$$

۴ .مدل مصرف انرژی گره

برای بررسی کارایی روش پیشنهادی، مدل مصرف انرژی به‌صورت زیر تعریف می‌شود:

$$E_{total} = E_{tx} \cdot N_{tx} + E_{comp} \cdot N_{inf} \quad (6)$$

که در آن:

جدول ۲: پارامترهای فرمول

نماد	توضیح	واحد
E_{tx}	انرژی ارسال هر بسته (مثلاً ۵۰۰۰ nJ)	nJ
N_{tx}	تعداد بسته‌های ارسالی به ایستگاه مرکزی	عدد صحیح
E_{comp}	انرژی هر بار اجرای inference	nJ
N_{inf}	دفعات اجرای مدل روی داده	عدد صحیح
E_{total}	انرژی کل مصرف‌شده توسط گره	nJ یا mJ

۵ .پیش‌بینی خرابی گره (در صورت داده کافی)

برای جلوگیری از خاموشی ناگهانی گره، می‌توان از یک مدل طبقه‌بندی ساده (مثلاً Logistic Regression) برای پیش‌بینی خرابی استفاده کرد. ورودی مدل برداری از ویژگی‌ها مانند ولتاژ، دما و نرخ افت بسته است:

$$X = [Voltage\ PacketLoss\ Rate\ Temperature] \quad (7)$$

تابع تصمیم مدل به صورت:

$$P(Failure) = \sigma(w^T X + b) = \frac{1}{1+E-(w^T X+b)} \quad (8)$$

که اگر مقدار خروجی بیش از ۰/۵ باشد، گره در معرض خرابی تشخیص داده می‌شود.

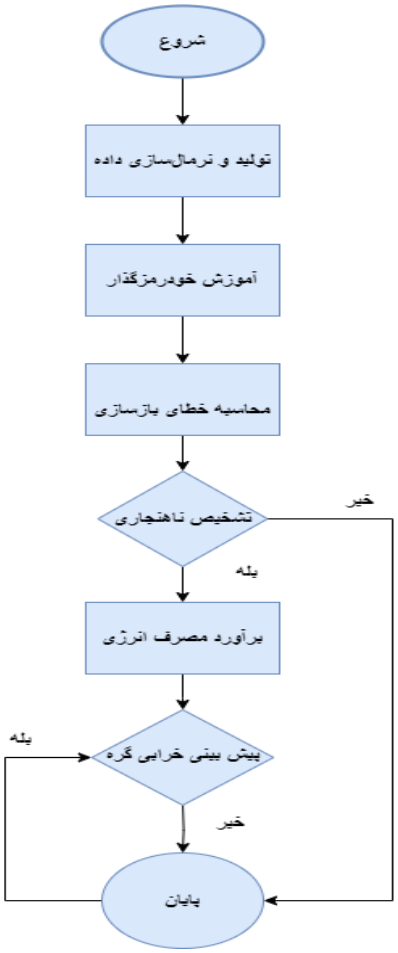
جدول ۳: نمادها و پارامترهای استفاده‌شده در فرمول‌های پروتکل پیشنهادی

نماد	توضیح	واحد
x	مقدار خام داده حسگر	C^0
x_{norm}	مقدار نرمال شده	بدون واحد
$\hat{X}$	مقدار بازسازی شده	مشابه x
E_i	خطای بازسازی	مشابه x
θ	آستانه تشخیص ناهنجاری	مشابه e_i
E_{tx}	انرژی ارسال یک بسته	nj
N_{tx}	تعداد بسته های ارسالی	عدد صحیح
E_{comp}	انرژی محاسبه inference	nj
N_{inf}	تعداد اجرای مدل	عدد صحیح

P(Failure)	احتمال خرابی گره	[0,1]

فلوچارت پروتکل پیشنهادی

فلوچارت کامل این فرآیند در شکل زیر نمایش داده شده است:



شکل ۲ : فلوچارت

توضیح مراحل فلوچارت روش پیشنهادی

۱ .شروع

فرآیند تحلیل داده در گره حسگر آغاز می‌شود. فرض بر این است که گره مجهز به حسگر، میکروکنترلر و مدل یادگیری از قبل آموزش‌دیده می‌باشد.

۲ .تولید و نرمال‌سازی داده

در این مرحله، داده‌های خام از حسگر (مانند دما، رطوبت یا ولتاژ باتری) دریافت شده و به مقیاس استاندارد تبدیل می‌شوند تا برای ورود به مدل یادگیری مناسب باشند. این مرحله باعث افزایش دقت پردازش مدل و کاهش حساسیت آن نسبت به نوسانات غیرمؤثر می‌شود.

۳ .آموزش خودرمزگذار

در این بخش، مدل یادگیری که از نوع خودرمزگذار یا Autoencoder است. با استفاده از داده‌های سالم و نرمال آموزش داده می‌شود. هدف از آموزش، یادگیری الگوی رفتاری معمول داده‌ها است. این آموزش معمولاً خارج از گره و یک‌بار برای همیشه انجام شده، سپس مدل در قالب فشرده بر روی گره بارگذاری می‌شود.

۴ .محاسبه خطای بازسازی

هنگامی که داده جدیدی توسط گره دریافت می‌شود، مدل یادگیری تلاش می‌کند آن داده را بازسازی کند. میزان اختلاف بین داده اصلی و بازسازی‌شده اندازه‌گیری می‌شود تا مشخص شود آیا این داده مطابق الگوهای نرمال است یا خیر.

۵ .تشخیص ناهنجاری

در این مرحله، تصمیم‌گیری انجام می‌شود که آیا داده‌ای که دریافت شده، رفتاری غیرعادی دارد یا خیر. اگر مدل یادگیری آن را مشابه الگوهای معمول تشخیص ندهد، گره آن را به عنوان ناهنجاری شناسایی کرده و به ایستگاه مرکزی ارسال می‌کند. در غیر این صورت، از ارسال آن صرف‌نظر می‌شود.

۶ .برآورد مصرف انرژی

با توجه به تعداد دفعات پردازش و میزان داده‌های ارسال‌شده، میزان مصرف انرژی گره برای این دوره عملکرد برآورد می‌شود. این برآورد به ما کمک می‌کند تا میزان بهینه‌سازی انرژی در روش پیشنهادی را نسبت به روش‌های سنتی بسنجیم.

۷ .پیش‌بینی خرابی گره

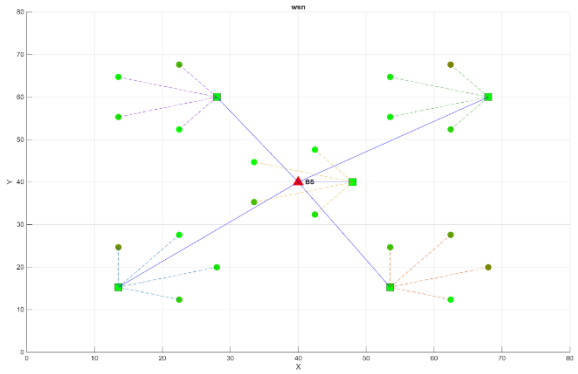
در این مرحله، با بررسی برخی ویژگی‌های فنی مانند افت ولتاژ، دمای بالا یا ضعف در برقراری ارتباط، یک مدل یادگیری دیگر بررسی می‌کند که آیا گره در معرض خرابی یا خاموشی قریب‌الوقوع قرار دارد یا خیر. در صورت مثبت بودن پیش‌بینی، هشدار لازم ارسال می‌شود.

۸ .پایان

پس از اتمام پردازش و ارسال (در صورت لزوم)، گره به وضعیت آماده‌باش بازمی‌گردد و منتظر داده بعدی می‌ماند.

۵– شبیه سازی پروتکل

برای ارزیابی عملکرد پروتکل پیشنهادی، شبیه‌سازی کامپیوتری در محیط MATLAB انجام شد. هدف اصلی این شبیه‌سازی بررسی مصرف انرژی، کارایی انتقال داده و پایداری شبکه در طول زمان است. پارامترهای اصلی مانند تعداد نودها، تعداد خوشه‌ها، مکان استگاه پایه (BS)، و میزان انرژی اولیه نودها تعریف شده‌اند. همچنین روش انتخاب سرخوشه‌ها، فشرده‌سازی داده و انتقال چندمرحله‌ای برای بهبود مصرف انرژی در نظر گرفته شده است (شکل ۱).



شکل ۳:مختصات شبکه حسگر بی‌سیم

تنظیمات اولیه شبیه‌سازی

در این شبیه‌سازی، شبکه شامل ۲۵ نود حسگر است که به ۵ خوشه تقسیم شده‌اند. هر خوشه دارای ۵ نود است که به صورت شعاعی و در اطراف مرکز خوشه (centroid) قرار گرفته‌اند. مختصات مراکز خوشه‌ها به صورت ثابت و پیش‌تعریف‌شده در نظر گرفته شده‌اند. ایستگاه پایه در مرکز میدان با مختصات (۴۰، ۴۰) قرار دارد. هر نود دارای انرژی اولیه متغیر بین ۰٫۵ تا ۱ ژول است که به صورت تصادفی تخصیص داده شده است، به جز سرخوشه‌ها که انرژی بیشتری (۳ ژول) دارند تا توانایی پردازش و ارسال داده‌های خوشه را داشته باشند. پارامترهای مورد استفاده در این پروتکل در جدول ۳ نشان داده شده است.

جدول ۴: پارامترهای مورد استفاده در پروتکل

پارامتر	مقدار
تعداد سنسورها	۲۵ عدد
محیط شبکه	۸۰*۸۰ متر
انرژی اولیه سرخوشه‌ها	۳ ژول
انرژی اولیه سنسورها	۰٫۵ تا ۱ ژول
جایگاه ایستگاه پایه	۴۰*۴۰ متر

مراحل شبیه‌سازی

در هر راند، مراحل زیر اجرا شدند:

۱. تشخیص ناهنجاری :سرخوشه‌ها داده‌های حسگرهای عضو خود را جمع‌آوری کرده و مقادیر غیرعادی بر اساس آستانه مشخص علامت‌گذاری شدند. سرخوشه‌هایی که داده نامعمول دریافت کردند، به‌طور موقت غیرفعال شدند. این ماژول نشان‌دهنده قابلیت TinyML در تحلیل اولیه داده‌ها و افزایش کیفیت آن‌ها است.

۲. انتقال داده و مصرف انرژی :انرژی مصرفی نودها و سرخوشه‌ها با در نظر گرفتن فشرده‌سازی هوشمند داده، مصرف اضافی ناشی از پردازش (ML) و مدل انرژی محاسبه شد. این مرحله شامل انتقال داده از نودها به سرخوشه و از سرخوشه به (BS) یا مسیر رله بود.

۳. مسیریابی تطبیقی :اگر فاصله سرخوشه تا (BS) بیشتر از آستانه تعیین‌شده بود، مسیر ارسال داده از طریق یک سرخوشه دیگر با انرژی کافی به عنوان رله انتخاب می‌شد. این مکانیزم باعث بهبود پایداری شبکه و کاهش مصرف انرژی کل می‌گردد.

۴. به‌روزرسانی انرژی و ثبت داده‌ها :انرژی باقی‌مانده نودها پس از هر راند ثبت شد و تعداد نودهای مرده محاسبه گردید.

الگوریتم خوشه‌بندی و انتخاب سرخوشه با استفاده از (K-means)

در این مدل، خوشه‌بندی نودهای شبکه با استفاده از الگوریتم مشهور k-meansانجام شده است. الگوریتم k-means یکی از روش‌های یادگیری بدون نظارت برای تقسیم داده‌ها به (k) خوشه است که در اینجا برای گروه‌بندی نودهای حسگر بی‌سیم به کار رفته است. در ابتدا، مختصات نودهای حسگر به صورت تصادفی یا طبق یک الگوی خاص در فضای دوبعدی شبکه (با ابعاد ۸۰×۸۰ متر) قرار می‌گیرند. سپس الگوریتم k-means اجرا می‌شود. در این فرآیند، ابتدا مراکز اولیه خوشه‌ها به صورت تصادفی تعیین می‌گردند و سپس به صورت تکراری نودها به نزدیک‌ترین مرکز تخصیص داده شده و مراکز جدید محاسبه می‌شوند تا جایی که همگرایی حاصل شود.

استفاده از k-means باعث خوشه‌بندی تطبیقی و واقع‌گرایانه‌تر در مقایسه با روش‌های دستی می‌شود، چرا که تقسیم‌بندی نودها به طور پویا و بر اساس موقعیت مکانی واقعی آن‌ها صورت می‌گیرد.

پس از تشکیل خوشه‌ها، برای هر خوشه، سرخوشه (Cluster Head) از میان نودهای عضو انتخاب می‌شود. معیار انتخاب سرخوشه، کمترین فاصله به مرکز خوشه k-means است. به بیان دیگر، نودی که نزدیک‌ترین مختصات به مرکز ثقل خوشه دارد، به عنوان سرخوشه تعیین می‌شود. برای اطمینان از توان عملیاتی بالای سرخوشه‌ها، به آن‌ها انرژی اولیه بیشتری (۳ ژول) نسبت به سایر نودها تخصیص داده می‌شود، در حالی که انرژی اولیه نودهای معمولی در بازه ۰٫۵ تا ۱ ژول تعیین شده است.

وظایف اصلی سرخوشه‌ها شامل موارد زیر است:

- جمع‌آوری داده از نودهای عضو خوشه؛
- اعمال فشرده‌سازی داده‌ها برای کاهش حجم انتقالی؛
- ارسال مستقیم داده‌های فشرده به ایستگاه پایه(BS) ، یا استفاده از سرخوشه‌های دیگر به‌عنوان رله در صورت زیاد بودن فاصله از (BS) مسیریابی چندمرحله‌ای.

جهت ارزیابی صحت عملکرد سرخوشه‌ها، مکانیزم شناسایی ناهنجاری (Anomaly Detection)نیز پیاده‌سازی شده است. هر سرخوشه در هر راند مقداری داده تصادفی تولید می‌کند که اگر خارج از بازه معین (مثلاً کمتر از ۱۰ یا بیشتر از ۵۰ واحد) باشد، به عنوان داده مشکوک تلقی شده و سرخوشه مربوطه به صورت موقت غیرفعال می‌شود. این رویکرد

به جلوگیری از ارسال اطلاعات نادرست و افزایش پایداری داده‌های نهایی کمک می‌نماید. به طور کلی، استفاده از الگوریتم k-means در فرآیند خوشه‌بندی، موجب توزیع متعادل‌تر نودها در خوشه‌ها، کاهش مجموع فاصله ارتباطی بین نودها و سرخوشه‌ها، و افزایش بازدهی مصرف انرژی در سطح شبکه می‌شود. این الگوریتم خصوصاً در محیط‌هایی با توزیع نودهای نامتوازن عملکرد مؤثری از خود نشان می‌دهد.

مدل مصرف انرژی

در شبیه‌سازی، مدل انرژی شامل موارد زیر است:

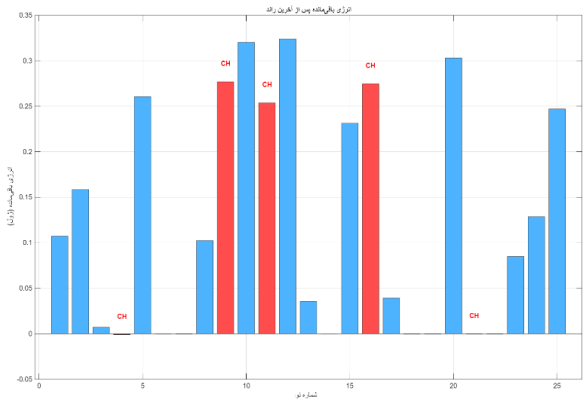
- انرژی مصرفی برای ارسال داده‌ها شامل انرژی الکترونیکی و انرژی آمپلیفایر است که متناسب با اندازه بسته داده و فاصله ارسال محاسبه می‌شود.
- انرژی مصرفی برای دریافت داده‌ها به صورت انرژی الکترونیکی محاسبه شده است.
- مصرف انرژی برای فشرده‌سازی داده‌ها با توجه به نسبت فشرده‌سازی و انرژی مصرفی به ازای هر بیت تعریف شده است.
- علاوه بر این، هزینه انرژی مربوط به یادگیری ماشین (ML) نیز برای پردازش داده‌ها در سرخوشه‌ها لحاظ شده است.

پروسه انتقال داده و مدیریت انرژی

در هر راند از شبیه‌سازی، اعضای هر خوشه داده‌های خود را به سرخوشه ارسال می‌کنند که انرژی مصرفی این انتقال برای هر نود به روز می‌شود. سرخوشه‌ها داده‌ها را فشرده کرده و سپس بسته به فاصله خود تا استگاه پایه تصمیم می‌گیرند که داده‌ها را مستقیم ارسال کنند یا از طریق سرخوشه‌های دیگر به صورت چندمرحله‌ای انتقال دهند. این روش باعث کاهش مصرف انرژی در سرخوشه‌های دور از استگاه پایه می‌شود. همچنین مصرف انرژی مربوط به انتقال چندمرحله‌ای و پردازش داده در سرخوشه‌ها محاسبه و کسر می‌شود.

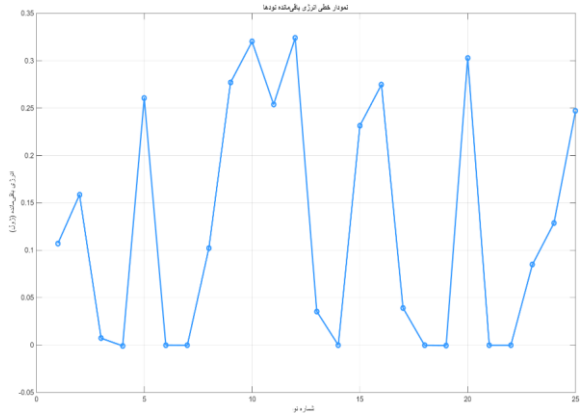
نتایج و تحلیل انرژی

شکل ۳ نمودار انرژی باقی‌مانده نودها را پس از آخرین راند نشان می‌دهد. همانطور که مشاهده می‌شود، سرخوشه‌ها به دلیل مصرف بالاتر انرژی برای ارسال و پردازش داده، انرژی کمتری نسبت به نودهای عادی دارند. با این وجود، مدیریت انتقال چندمرحله‌ای به حفظ انرژی برخی سرخوشه‌ها کمک می‌کند.



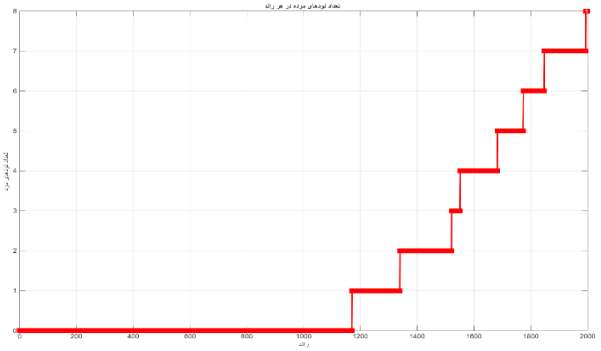
شکل ۴:انرژی باقی مانده در آخرین راند

نمودار تغییرات انرژی در طول راندها (شکل ۴) روند تدریجی کاهش انرژی در شبکه را نمایش می‌دهد. این نمودار نشان می‌دهد که انرژی نودها به تدریج کاهش می‌یابد و برخی نودها زودتر از بقیه به پایان عمر خود می‌رسند. این روند طبیعی برای شبکه‌های حسگر بی‌سیم است و اهمیت طراحی الگوریتم‌های صرفه‌جویانه در مصرف انرژی را نشان می‌دهد.



شکل ۵: نمودارخطی انرژی باقی مانده سنسورها

شکل ۵ تعداد نودهای مرده در هر راند را نمایش می‌دهد. مشاهده می‌شود که تعداد نودهای مرده با افزایش راندها افزایش می‌یابد، اما به دلیل مکانیزم‌های انتخاب سرخوشه و مسیریابی چندمرحله‌ای، این افزایش به صورت تدریجی بوده و پایداری شبکه حفظ شده است.



شکل ۶: تعداد نود های مرده

نتایج شبیه‌سازی

نتایج شبیه‌سازی نشان می‌دهد که معماری پیشنهادی با ترکیب ماژول‌های تشخیص ناهنجاری، پیش‌بینی خطا، فشرده‌سازی داده و

مسیریابی تطبیقی، توانسته عملکرد شبکه را در جنبه‌های مختلف بهبود دهد:

۱. توزیع انرژی نودها :نمودار انرژی نشان می‌دهد که سرخوشه‌ها با مصرف هوشمند انرژی و استفاده از فشرده‌سازی داده، قادر به فعالیت طولانی‌تر نسبت به نودهای عادی هستند.

۲. تغییرات انرژی در طول زمان :نمودار انرژی در طول ۲۰۰۰ راند کاهش تدریجی انرژی را نشان می‌دهد، که بیانگر افزایش طول عمر شبکه در مقایسه با شبکه‌های بدون مدیریت هوشمند است.

۳. تعداد نودهای مرده :تعداد نودهای مرده با گذر زمان به آرامی افزایش می‌یابد، که نشان‌دهنده پایداری بالای شبکه است.

۴. کارایی TinyML در WSN: ترکیب ماژول‌ها امکان تحلیل و پیش‌بینی هوشمند داده‌ها، فشرده‌سازی مؤثر و مسیریابی بهینه را فراهم می‌کند و نشان می‌دهد که گره‌های کم‌منبع می‌توانند با حداقل مصرف انرژی، قابلیت‌های هوشمند داشته باشند.

جدول ۵: جدول مقایسه‌ای روش پیشنهادی با سایر روش‌ها

معیار ارزیابی	روش پیشنهادی (tiny ml)	روش‌های سنتی مانند(LEACH/HEED)
مصرف انرژی	کاهش چشمگیر به دلیل پردازش محلی	بالا به دلیل ارسال مداوم داده‌ها
دقت تشخیص ناهنجاری	بالا، به دلیل پردازش محلی و یادگیری	پایین، وابسته به ایستگاه پایه
طول عمر شبکه	افزایش یافته (تا چند برابر)	کوتاه‌تر
واکنش به رخدادها	سریع، تصمیم‌گیری در گره	کند به دلیل تأخیر در انتقال
میزان داده ارسالی به سرور	بسیار کمتر (فقط داده مهم)	زیاد

این نتایج نشان می‌دهند که معماری یکپارچه TinyML قادر است همزمان کیفیت داده، طول عمر شبکه و پایداری و اتکا پذیری آن را بهبود دهد و امکان استفاده از یادگیری ماشین سبک را در شبکه‌های حسگر با منابع محدود فراهم می‌کند.

۶– نتیجه گیری

در این پژوهش، رویکردی نوین مبتنی بر یادگیری ماشین کوچک (TinyML)برای افزایش اتکاپذیری و بهبود مدیریت انرژی در شبکه‌های حسگر بی‌سیم ارائه شد. معماری پیشنهادی با ادغام ماژول‌های تشخیص ناهنجاری، پیش‌بینی خرابی، فشرده‌سازی هوشمند داده و مسیریابی تطبیقی توانست به شکل موثری چالش‌های ناشی از محدودیت منابع پردازشی و انرژی را کاهش دهد. نتایج شبیه‌سازی نشان داد که استفاده از این چارچوب، علاوه بر افزایش طول عمر شبکه، موجب ارتقای کیفیت داده، کاهش بار ارتباطی، و حفظ پایداری شبکه در شرایط نامطمئن می‌شود. یکی از نوآوری‌های اصلی این مطالعه، به‌کارگیری TinyML (یادگیری ماشین فوق‌سبک) در سرخوشه‌ها برای پردازش و تحلیل محلی داده‌ها بود .TinyML با استفاده از مدل‌های بسیار کم‌حجم و بهینه‌شده، امکان اجرای الگوریتم‌های یادگیری ماشین را بر روی سخت‌افزارهای با منابع محدود فراهم می‌کند. یک پروتکل خوشه‌بندی و مدیریت انرژی برای شبکه‌های حسگر بی‌سیم با هدف افزایش طول عمر شبکه و بهبود کارایی انتقال داده ارائه و شبیه‌سازی شد. با استفاده از الگوریتم خوشه‌بندی k-means، تقسیم‌بندی بهینه‌تری از نودها به خوشه‌ها ایجاد کرده و با انتخاب سرخوشه بر اساس کمترین فاصله به مرکز خوشه، ارتباطات درون‌خوشه‌ای را بهینه نموده است. همچنین، تخصیص انرژی اولیه بیشتر به سرخوشه‌ها، بهره‌گیری از فشرده‌سازی داده‌ها، و مسیریابی چندمرحله‌ای باعث کاهش بار ارتباطی و توزیع متوازن‌تر مصرف انرژی گردید. در این پروتکل، TinyMLبرای شناسایی ناهنجاری در داده‌های جمع‌آوری‌شده به کار رفت و باعث شد که تنها داده‌های معتبر به ایستگاه پایه ارسال شوند. این امر علاوه بر افزایش کیفیت داده‌ها، موجب صرفه‌جویی بیشتر در مصرف انرژی شد، زیرا داده‌های غیرضروری و مشکوک حذف گردیدند.

تحلیل نتایج شبیه‌سازی، از جمله نمودارهای انرژی باقی‌مانده و نرخ ازکارافتادگی نودها، نشان داد که ترکیب خوشه‌بندیk-means ، فشرده‌سازی داده، مسیریابی چندمرحله‌ای، و پردازش محلی مبتنی بر TinyMLمی‌تواند طول عمر شبکه را به شکل قابل‌توجهی افزایش دهد و مصرف انرژی را به صورت تدریجی و متعادل کاهش دهد. به طور کلی، یافته‌های این تحقیق نشان می‌دهد که استقرار TinyML در سطح گره‌های حسگر، نه تنها امکان اجرای پردازش محلی و تصمیم‌گیری هوشمند را فراهم می‌کند، بلکه وابستگی به ایستگاه پایه را کاهش داده و تاب‌آوری شبکه را در برابر خطاها و اختلالات افزایش می‌دهد. این ویژگی‌ها می‌توانند زمینه‌ساز توسعه کاربردهای گسترده‌تر (WSN) در حوزه‌هایی نظیر اینترنت اشیا، کشاورزی هوشمند، پایش محیطی و سیستم‌های حیاتی شوند. برای آینده، پیشنهاد می‌شود پژوهش‌های تکمیلی به سمت استفاده از الگوریتم‌های تکاملی برای انتخاب پویا سرخوشه‌ها، ترکیب TinyML با یادگیری فدرال، و طراحی سازوکارهای امنیتی سبک حرکت کنند تا علاوه بر بهبود کارایی انرژی و طول عمر شبکه، قابلیت اطمینان و امنیت در مقیاس‌های بزرگ نیز تضمین گردد.

مراجع

1. SONAM LATA SSU. Secure and Reliable WSN for Internet of Things:Challenges and Enabling Technologies. IEEE. 2021.
2. ABADADE Y, TEMOUDEN A, BAMOUMEN H, BENAMAR N, CHTOUKI Y, SENHAJI HAFID A. A Comprehensive Survey on TinyML. ieee. 2023.
3. KEYAN CAO YL,MQS. An Overview on Edge Computing Research. IEEE. 2020.
4. Montaser N.A. Ramadan MAHASYKMA. Federated learning and TinyML on IoT edge devices: Challenges, advances, and future directions. ScienceDirect. 2025.
5. Kalpana Sharma MKG. Wireless Sensor Networks: An Overview on its Security and threats. IJCA Special Issue on “Mobile Ad-hoc Networks”. 2010.
6. Elham Alotaibi RBSMA. Assessment of cybersecurity threats and defense mechanisms in wireless. Journal of Cyber Security and Risk Auditing. 2025.
7. MF, AG, EM, FP, RP, SR. Federated learning for IoT devices: Enhancing TinyML with on-board. ELSEVIER. 2024.
8. F. García-Hernández C, H. Ibargüengoytia-González P, García-Hernández J, A. Pérez-Díaz. Wireless Sensor Networks and Applications: a Survey. IJCSNS International Journal of Computer Science and Network Security. 2007.
9. Salam Hamdan MA,A. Edge-Computing Architectures for Internet of Things. MDPI. 2020.
10. WEI YU FXHWGH. A Survey on the Edge Computing for the internet of things. IEEE. 2018.
11. YONGLI ZHAO WWYLCCMMJZ. Edge Computing and Networking: A Survey on infrastructures and applications. IEEE. 2019.
12. ZHIZHOU X,ZLJZ. Edge Intelligence: Paving the lasr mile of artificial intelligence with edge computing. IEEE. 2019.
13. yuan ai mpkz. Edge computing technologies for internet of Things: a primer. ELSEVIER. 2018.
14. Moslehi MM. Exploring coverageandsecuritychallenges in wireless sensor networks: A survey. ELSEVIER. 2025.
15. Jusuf Elfarahati TPEKAFEŠAA. Review of Wireless Sensor Network security. Defense and Security Studies. 2025.
16. Ghadeer Al Sukkar SAS. Enhancing Security in Wireless Sensor Networks: A Machine Learing-based Dos Attack Detection. Engineering, Technology & Applied Science Research. 2025.
17. HUYNH A. D. NGUYEN QPH. Wireless Sensor Network Dependable Monitoring for Urban Air Quality. IEEE. 2022.
18. ArashHeidari ZMN. Assessmentofreliability andavailability of wireless sensornetworksinindustrialapplications byconsidering permanentfaults. WILEY. 2024.
19. Athanasios Trigkas DP,P. Edge Intelligence in Urban Landscapes: Reviewing TinyML Applications for Connected and Sustainable Smart Cities. MDPI. 2025.
20. Spyridon Giazitzisa AAINBAMPDMRSBFREO. TinyML models for SoH estimation of lithium-ion batteries based on Electrochemical Impedance Spectroscopy. ScienceDirect. 2025.
21. Iyad Katib EASASMR. Safeguarding IoT consumer devices: Deep learning with TinyML driven real-time anomaly detection for predictive maintenance. ScienceDirect. 2025.
22. Dennis Agyemanh Nana Gookyi EAEAjOA. TinyML for smart agriculture: Comparative analysis of TinyML platforms and practical deployment for maize leaf disease identification. ScienceDirect. 2024.
23. Sergio Trillesa bSSHDI. AnomalydetectionbasedonArtificialIntelligence of Things: A Systematic Literature Mapping. ScienceDirect. 2024.
24. Franklin Oliveiraa DGCFAIS. Internet of Intelligent Things: A convergence of embeddedsystems,edgecomputingandmachinelearning. ScienceDirect. 2024.
25. Nikolaos Schizas AKCKSS. TinyML for Ultra-Low Power AI and Large Scale IoT Deployments: A Systematic Review. MDPI. 2022.

تعارض منافع

هیچ گونه تعارض منافع توسط نویسندگان بیان نشده است.