
بسم الله الرحمن الرحیم

دانشکده مهندسی کامپیوتر

رساله دکتری مهندسی هوش مصنوعی

یک معماری کارا برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

نگارنده

مهدی صادقی زاده

استاد راهنما

دکتر امید رضا معروضی

استاد مشاور

دکتر علی‌اکبر پویان

بهمن ۹۷

تقدیم به پدر و مادرم

و

تقدیم به همسر عزیزم

که همواره یار و پشتیبان من بودند و در کوره راه زندگی، با گرمی عشق و محبتشان، لحظه لحظه زندگیم را امید، اشتیاق و معنای دوباره بخشیدند.

تقدیم به پیشگاه استادانم

استادانم از نخستین دم تا بازپسین حیاتم
آموزگارانی که جز دهش ایشان بضاعتی ندارم.

خدایا تو را سپاس می‌گویم که مرا لایق آموختن گردانیدی

از استاد فرزانه و گران‌قدر جناب **آقای دکتر امیدرضا معروضی** که در طول انجام پایان‌نامه همواره از رهنمودهای ارزنده و تلاش‌های پی‌گیرشان بهره‌مند بودم، کمال تشکر را دارم.

از استاد بزرگوار جناب آقای دکتر علی‌اکبر پویان به خاطر مشاوره و راهنمایی‌های ارزشمندشان سپاسگذارم.

از اساتید محترم آقایان دکتر محسن رضوانی، پروفسور حمید حسن‌پور و دکتر اسدالله شاه‌بهرامی که زحمت بازخوانی و داوری این پایان‌نامه را بر عهده داشتند، قدردانی می‌کنم.

از جناب آقای دکتر منصور فاتح نماینده محترم تحصیلات تکمیلی به خاطر ایجاد هماهنگی‌های لازم سپاسگذارم.

از سایر اساتید محترم گروه مهندسی کامپیوتر نیز تشکر و قدردانی می‌نمایم.

از همه دوستان عزیزم که آشنایی و همراهی‌شان فرصتی تکرار ناشدنی بود، صمیمانه سپاسگذارم و برای هریک از آنها آرزوی کامیابی و پیروزی دارم.

از بهترین‌های زندگی‌ام، **پدر و مادر عزیزم** که ذره ذره‌ی وجودشان را با هیچ منت و ادعایی بر من ارزانی داشتند و **همسر عزیزم** که همواره مهر و محبتش دلگرمی‌ام و عشقش پایداری‌ام در زندگی بوده‌است، تشکر می‌کنم.

تعهد نامه

اینجانب **مهدی صادقی زاده** دانشجوی دوره **دکتری** رشته **مهندسی کامپیوتر** گرایش **هوش مصنوعی** دانشکده مهندسی کامپیوتر دانشگاه صنعتی شاهرود نویسنده رساله دکتری **"یک معماری کارا برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم"** تحت راهنمایی جناب آقای **دکتر امیدرضا معروضی** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان‌نامه تاکنون توسط خود و یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام "دانشگاه صنعتی شاهرود" و یا "Shahrood University of Technology" به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند در مقالات مستخرج از رساله رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است، اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

تاریخ

امضای دانشجو

مهدی صادقی زاده

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه فردوسی مشهد می‌باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

چکیده

شبکه‌های حسگر بی‌سیم یکی از فناوری‌های کاربردی و جذاب است که در سال‌های اخیر بسیار موردتوجه محققان قرارگرفته است. با توجه به این‌که این شبکه‌ها معمولاً در مکان‌های دور و فاقد حفاظت و یا اغلب در شرایط عملیاتی خصمانه به کار گرفته می‌شوند، برای تهاجم و حملات امنیتی بسیار مستعد هستند که این امر با توجه به منابع محدود آن‌ها باعث کاهش شدید عملکرد و کارائی آن‌ها می‌گردد. بنابراین تأمین امنیت در شبکه‌های حسگر در برابر حملات مختلف به یک موضوع مهم مبدل شده و عملاً به‌عنوان یکی از پارامترهای اساسی کیفیت سرویس در آن‌ها مطرح است، به‌ویژه اگر این شبکه‌ها در فرآیندهای بحرانی نیز دخیل باشند. بسیاری از راه‌حل‌های امنیتی برای شبکه‌های حسگر بی‌سیم برای حملات خاص، طراحی‌شده‌اند و نمی‌توانند اغلب حملات امنیتی را دفع نمایند. سیستم تشخیص نفوذ یکی از شیوه‌های تدافعی در برابر حملات است که در حقیقت بعد از سیستم‌های پیشگیری از نفوذ، به‌عنوان دومین خط دفاعی در برابر مهاجمان بوده و وظیفه آن شناسایی و گزارش حملات است. یکی از مزایای سیستم‌های تشخیص نفوذ در مقابل روش‌های امنیتی دیگر، پوشش طیف وسیعی از حملات در شبکه‌های حسگر بی‌سیم است. محققان سیستم‌های تشخیص نفوذ مختلفی را برای شبکه‌های حسگر بی‌سیم ارائه کردند، اما با توجه به محدودیت‌های موجود در شبکه‌های حسگر بی‌سیم، طراحی یک سیستم تشخیص نفوذ مؤثر و کارآ که قابل‌استفاده در آن‌ها باشد هنوز یک چالش بزرگ است. ما قصد داریم با بررسی انواع روش‌های ارائه‌شده، یک معماری کارآ برای سیستم‌های تشخیص نفوذ بر روی شبکه‌های حسگر بی‌سیم ارائه نماییم. منظور ما از معماری کارآ، بهبود در مصرف و اتلاف انرژی گره‌های شبکه حسگر به‌عنوان اصلی‌ترین پارامتر و همچنین ارتقاء دقت تشخیص حملات است. ایده اصلی معماری پیشنهادی، توجه به سطح اهمیت گره و حساسیت آن در شبکه است و بر این اساس از الگوریتم‌های تشخیص نفوذ مؤثری در سطوح مختلف استفاده خواهیم کرد. هدف ما در این معماری پوشش حملات لایه شبکه است که رایج‌ترین حملات در شبکه‌های حسگر هستند. به جهت اعتبارسنجی مناسب و مطلوب، با انجام شبیه‌سازی معماری پیشنهادی، تمامی معیارهای کارائی بر روی آن مورد ارزیابی قرارگرفته‌اند. نتایج به‌دست‌آمده از شبیه‌سازی‌ها نشان می‌دهد که معماری پیشنهادی به‌عنوان یک روش مؤثر و سبک برای شبکه‌های حسگر بی‌سیم مطرح است و با به‌کارگیری آن در شبکه‌های حسگر بی‌سیم، به‌خوبی می‌توان کارائی و عملکرد شبکه را در حد مطلوب حفظ نمود.

کلمات کلیدی: شبکه‌های حسگر بی‌سیم[1]، سیستم‌های تشخیص نفوذ[2]، حملات لایه شبکه و مسیریابی[3]، مکانیسم‌های امنیتی[4]، معیارهای کارائی.

[1] Wireless Sensor Networks (WSNs)
[2] Intrusion Detection Systems (IDSs)
[3] Routing and Network layer Attacks
[4] Security Mechanisms

لیست مقالات مستخرج از رساله

مجلات عملی – پژوهشی

[Paper 1]. M. Sadeghizadeh, O. R. Marouzi, **"A Lightweight Intrusion Detection System Based on Specifications to Improve Security in Wireless Sensor Networks",** Journal of Communication Engineering, Vol. 7, No. 2, pp.29-50, July-December 2018.

[Paper 2]. M. Sadeghizadeh, O. R. Marouzi, **"Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining",** Journal of Communication Engineering, Vol. 8, No. 1, pp.29-50, pp. 1-20, January-June 2019.

کنفرانس

[مقاله ۱]. مهدی. صادقی زاده، امید رضا. معروضی و علی‌اکبر. پویان، « **ارائه یک سیستم تشخیص نفوذ سبک برای تشخیص حملات انکار سرویس در شبکه‌های حسگر بی‌سیم** »، سومین کنفرانس پردازش سیگنال و سیستم‌های هوشمند، دانشگاه صنعتی شاهرود، شاهرود، ایران ۱۳۹۶.

[مقاله ۲]. مهدی. صادقی زاده، امید رضا. معروضی و علی‌اکبر. پویان، « **شبیه‌سازی، تحلیل رفتار و بررسی تأثیر حملات مختلف بر روی شبکه‌های حسگر بی‌سیم** »، سومین کنفرانس محاسبات تکاملی و هوش جمعی، کرمان، ایران، اسفند ۱۳۹۶.

[مقاله ۳]. مهدی. صادقی زاده، امید رضا. معروضی و علی‌اکبر. پویان، « **بهبود کارائی سیستم‌های‌تشخیص‌نفوذ مبتنی بر داده‌کاوی در شبکه‌های حسگر بی‌سیم با ارائه یک مدل پیش‌پردازش داده‌ها** »، سومین کنفرانس محاسبات تکاملی و هوش جمعی، کرمان، ایران، اسفند ۱۳۹۶.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

واژه‌های اختصاری

علامت اختصاری	واژه اصلی
WSNs	Wireless Sensor Networks
IDSs	Intrusion Detection Systems
GPS	Global Positioning System
CH	Cluster Head
BS	Base Station
SQTL	Sensor Query and Tasking Language
CBR	Constant Bit Rate
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
TDMA	Time-division multiple access
SMAC	sensor medium access control protocol
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
AODV	Ad hoc On-Demand Distance Vector
TORA	Temporally Ordered Routing Algorithm
QoS	Quality of Service
DoS	Denial of Service
ASF	Attack Simulation Frameworkn
ASL	Attack Specification Language
KBIDS	Knowledge Based IDS
OWIDS	Ontology-based Wireless IDS
SVM	Support Vector Machine
FAR	False Alarm Rate
ECOC	Error Correcting Output Codes
GHIDS	Global Hybrid IDS
BPN	Back Propagation Network
ART	Adaptive Resonance Theory
ACO	Ant Colony Optimization
IWD	Intelligent Water Drops
MCFA	Modified CuttleFish Algorithm
TDOA	Time Difference Of Arrival
RPC	Random Password Generation Algorithm
CAM-PVM	Compare And Match-Position Verification Method
MAP	Message Authentication and Passing
RADS	Rule-based Anomaly Detection System
IRP	Interval of Received Packets
RSSI	Received Signal Strength Indicator
RMI	Routing Messages Interval
NS2	Network Simulator 2
PART	Partial Decision Tree

۱– مقدمه

۱–۱– معرفی اجمالی شبکه‌های حسگر بی‌سیم

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم این امکان را برای ما فراهم کرده است که بتوانیم حسگرهایی را با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربردهای گوناگون طراحی و ایجاد نماییم. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی (بر اساس نوع حسگر)، پردازش و ارسال آن اطلاعات را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های حسگر بی‌سیم شده‌اند [۱].

شبکه‌های حسگر بی‌سیم به دلیل مزایای ذاتی خود مانند هزینه کمتر و استقرار راحت‌تر در محیط، برای ایفای نقش در طیف وسیع و متنوعی از کاربردها مانند کنترل و نظارت نظامی، کنترل آتش‌سوزی جنگل‌ها، مراقبت از سلامتی، نظارت بر ایمنی سازه‌ها و ساختمان‌ها و خانه‌های هوشمند، بسیار مطلوب و مقرون‌به‌صرفه می‌باشند [۱]. بااین‌وجود گره‌های موجود در این شبکه‌ها به دلیل توان پردازشی پایین، حافظه و انرژی محدودشان دارای محدودیت‌های منابع شدیدی هستند.

۱–۲– اهمیت مسئله امنیت در شبکه‌های حسگر بی‌سیم

با توجه به این‌که این شبکه‌های حسگر بی‌سیم معمولاً در مکان‌های دور و فاقد حفاظت و یا اغلب در جاهایی که شرایط عملیاتی نامطلوب و یا حتی خصمانه دارد به کار گرفته می‌شوند، برای تهاجم و حملات امنیتی بسیار مستعد هستند که این امر با توجه به منابع محدود آن‌ها باعث کاهش شدید عملکرد و کارائی آن‌ها می‌گردد [۲]. بنابراین تأمین امنیت در شبکه‌های حسگر بی‌سیم در برابر مهاجمان و حملات مختلف به یک موضوع مهم مبدل شده است، به‌ویژه اگر این شبکه‌ها در فرآیندهای بحرانی نیز دخیل باشند. شبکه‌های حسگر بی‌سیم امن در کاربردهای نظامی (تاکتیکی) دارای اهمیت بحرانی و حساسی هستند، به‌گونه‌ای که یک شکاف امنیتی در شبکه می‌تواند باعث تحریک و تضعیف نیروهای خودی در میدان جنگ گردد [۳]. ما در این رساله قصد داریم با در نظر گرفتن حساسیت این موضوع مهم، به ارائه یک راه‌کار امنیتی کارآ بپردازیم به‌گونه‌ای که امنیت در شبکه‌های حسگر بی‌سیم تأمین گردد.

۱-۳- بیان مسئله

در این پژوهش راهکاری نوین برای تأمین امنیت در شبکه‌های حسگر بی‌سیم از طریق ارائه یک معماری تشخیص نفوذ کارآ ارائه‌شده است. در راهکار ارائه‌شده تمرکز زیادی بر روی سطوح مختلف حساسیت گره‌ها ازلحاظ تأمین امنیت و محدودیت منابع مربوطه شده است. ما با در نظر گرفتن این منطق یک معماری سه سطحی را طراحی کردیم و تمهیدات مختلفی را برای هر سطح در نظر گرفتیم.

روند کار به‌این‌ترتیب است که در این رساله در ابتدا با شبیه‌سازی یک نمونه کامل از شبکه حسگر بی‌سیم و قرار دادن آن در معرض حملات مسیریابی، نحوه عملکرد و کارایی آن را در مواجه با حملات مختلف ارزیابی کرده و با تحلیل رفتار حملات به طراحی یک معماری کارا برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم پرداخته‌ایم به‌گونه‌ای که عملکرد شبکه را در برابر حملات مختلف به‌خوبی حفظ می‌نماید.

منظور ما از معماری کارا در عنوان رساله "یک معماری کارا برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم"، بهبود در مصرف و اتلاف انرژی گره‌های شبکه است که به‌عنوان اصلی‌ترین پارامتر در شبکه‌های حسگر بی‌سیم مطرح است تا بتوانیم از این طریق طول عمر شبکه مفروض را افزایش دهیم. معماری تشخیص نفوذ پیشنهادی ما مربوط به آن دسته از شبکه‌های حسگری است که نیازمند حساسیت امنیتی بالایی هستند مانند کاربردهای نظامی و امنیتی.

ایده اصلی معماری پیشنهادی ما توجه به سطح اهمیت گره و حساسیت آن در شبکه حسگر بی‌سیم است و بر این اساس الگوریتم‌های تشخیص نفوذ مؤثری را در سطوح مختلف ارائه کرده‌ایم. هدف ما در این معماری پوشش حملات لایه شبکه و فرایند مسیریابی است که رایج‌ترین حملات در شبکه‌های حسگر بی‌سیم هستند [۲] [۳].

تفاوت اصلی معماری پیشنهادی ما با کارهای موجود و همچنین نوآوری‌های ارائه‌شده در این رساله به شرح ذیل است:

۱. در معماری پیشنهادی خود از ایده ابتکاری یک روش مبتنی بر سطح اهمیت گره‌ها بهره بردیم که هر چه درجه اهمیت گره افزایش می‌یابد (مثلاً گره سرخوشه) ما نیز حساسیت سیستم تشخیص نفوذ را افزایش داده تا قدرت تشخیص بیشتری ایجاد نماییم و به‌این‌ترتیب تضمین بیشتری برای حفظ امنیت ایجاد نماییم.

۲. ارائه الگوریتم‌های ابتکاری مناسب در بخش‌های مختلف معماری پیشنهادی به جهت بهبود کارایی آن

۳. استخراج ویژگی‌های جدید به جهت استفاده در سیستم تشخیص نفوذ پیشنهادی که از طریق شبیه‌سازی یک نمونه کامل از شبکه‌های حسگر بی‌سیم به‌صورت پارامتری و همچنین شبیه‌سازی حملات لایه شبکه و فرایند مسیریابی بر روی آن و تحلیل دقیق رفتار آن‌ها در شبکه انجام گردید.

۴. بهبود میزان تفکیک‌پذیری ویژگی‌های استخراج‌شده و موجود برای بهبود دقت تشخیص شناسایی حملات در سیستم تشخیص نفوذ پیشنهادی از طریق تحلیل دقیق رفتار حملات تعیین مناسب‌تر حدود آستانه مربوط به ویژگی‌ها

۵. بهبود دقت تشخیص حملات مختلف با ارائه یک روش مبتنی بر اعتماد به جهت ارزشیابی هشدارهای صادرشده برای تشخیص حملات و ترکیب آن با سیستم تشخیص نفوذ مبتنی بر خصوصیات پیشنهادی اولیه

۶. ارائه یک روش پیش‌پردازش داده‌ها بر روی دادگان به جهت بهبود دقت تشخیص و مصرف انرژی در سیستم تشخیص نفوذ ترکیبی پیشنهادی برای تأمین امنیت سرخوشه‌ها

۷. بررسی و تحلیل خصوصیات مربوط به طبقه‌بندهای مختلف و انتخاب یک روش مناسب به جهت طبقه‌بندی دادگان

۸. بررسی و تحلیل خصوصیات مربوط به الگوریتم‌های مختلف کاهش ویژگی و انتخاب یک روش مناسب کاهش ابعاد دادگان به جهت بهبود دقت تشخیص و مصرف انرژی معماری پیشنهادی

۹. استفاده از امکانات گره چاهک به جهت بهبود امنیت و کارایی سیستم تشخیص نفوذ پیشنهادی و همچنین استفاده از یک روش یادگیری ماشین بر روی آن به جهت شناسایی الگوی حملات جدید

۱۰. پوشش تمامی حملات لایه شبکه و فرایند مسیریابی توسط سیستم پیشنهادی با ادغام ویژگی‌های موجود و استخراج‌شده

ارزشیابی سیستم پیشنهادی با همه معیارهای کارائی مربوط به شبکه‌های حسگر بی‌سیم

فرضیات ما در ارائه معماری پیشنهادی نیز به شرح زیر می‌باشند:

- استفاده از معماری خوشه‌بندی شبکه حسگر بی‌سیم به جهت ارائه روش پیشنهادی
- ارائه معماری تشخیص نفوذ سلسله‌مراتبی مبتنی بر حساسیت گره‌ها ازلحاظ تأمین امنیت و محدودیت منابع مربوطه
- سرخوشه‌ها از لحاظ انرژی و تجهیزات قدرتمندتر از گره‌های عادی هستند.
- همگن بودن گره‌های عادی شبکه از لحاظ منابع و انرژی
- سرخوشه ها مستقیما با ایستگاه پایه در ارتباط هستند.
- در نظر گرفتن حملات لایه شبکه و فرایند مسیریابی به جهت تشخیص نفوذ
- ارائه روش پیشنهادی برای انواع کاربردهای نظامی، صنعتی و امنیتی
- استفاده از شبیه‌ساز NS2 به جهت انجام شبیه‌سازی‌های مربوطه
- عدم اطلاع مهاجمان و هکرها از ویژگی‌های شبکه حسگر مانند گستره شبکه، نحوه توزیع و چگالی گره‌ها در محیط، نرخ ثبت وقایع، نرخ ارتباطات بین گره‌ها و ...
- استفاده از دادگان KDDcup'99 و NSL به جهت ارزیابی معماری پیشنهادی
- استفاده از هنجارسازی آماری داده‌ها به جهت بهبود کارائی معماری پیشنهادی

۱-۴- چالش‌های رساله

مهم‌ترین معیارها برای ارزشیابی سیستم‌های تشخیص نفوذ دقت تشخیص، میزان اعمال سربارهای ارتباطی و محاسباتی، میانگین مصرف انرژی گره‌ها و طول عمر شبکه، گستره حملات قابل‌شناسایی و طول دوره تشخیص است. متأسفانه در تمامی روش‌های ارائه‌شده قبلی که به‌طور کامل در بخش ۳ بررسی شدند، تمامی معیارهای فوق به‌صورت یکجا و به‌طور توأم مدنظر قرار نگرفته‌اند. به‌عبارت‌دیگر روش‌های پیشنهادی موجود اغلب یک یا چند پارامتر فوق را بررسی نکرده و از این حیث دارای ضعف هستند، که این امر در تشریح روش‌های موجود نیز بیان شده است. برای مثال در اغلب روش‌های پیشنهادی فقط حملات خاصی بررسی‌شده‌اند و یا در موارد زیادی مصرف انرژی و کارآ بودن آن در نظر گرفته نشده است. به‌طور دقیق‌تر می‌توان مشکلات ذیل را در روش‌های پیشنهادی قبلی مشاهده کرد که به عنوان چالش‌های اصلی در رساله مطرح هستند:

- پوشش محدود حملات در روش‌های موجود
- سربار محاسباتی نسبتاً بالا
- عدم توجه به مصرف انرژی
- پایین بودن دقت تشخیص
- بالا بودن نرخ هشدارهای نادرست
- عدم تطبیق با کاربرد
- بالا بودن زمان تشخیص

بنابراین با توجه به محدودیت‌های شبکه‌های حسگر بی‌سیم که در بخش ۱-۱ ذکر شد و همچنین با توجه به موانع امنیتی موجود در این شبکه‌ها، ارائه یک سیستم تشخیص نفوذ مطلوب و کارآ، هنوز یک چالش اساسی در شبکه‌های حسگر بی‌سیم است.

۱–۵– دستاوردهای تحقیق

ما در این رساله به جهت ارائه مناسب یک معماری کارا برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم، به شبیه‌سازی و تحلیل رفتار حملات لایه شبکه و مسیریابی پرداختیم و نحوه عملکرد و کارایی شبکه حسگر بی‌سیم را در مواجه با آن‌ها ارزیابی کردیم.

مهدی. صادقی زاده، امیدرضا. معروضی و علی‌اکبر. پویان، " شبیه‌سازی، تحلیل رفتار و بررسی تأثیر حملات مختلف بر روی شبکه‌های حسگر بی‌سیم "، سومین کنفرانس محاسبات تکاملی و هوش جمعی، کرمان، ایران، اسفند ۱۳۹۶.

بر اساس نتایج تحلیل صورت گرفته در مقاله بالا، خصوصیات اساسی حملات مسیریابی را استخراج کردیم و بر اساس آن نمونه‌های اولیه سیستم تشخیص نفوذ را برای شبکه‌های حسگر ارائه دادیم.

مهدی. صادقی زاده، امیدرضا. معروضی و علی‌اکبر. پویان، " ارائه یک سیستم تشخیص نفوذ سبک برای تشخیص حملات انکار سرویس در شبکه‌های حسگر بی‌سیم "، سومین کنفرانس پردازش سیگنال و سیستم‌های هوشمند، دانشگاه صنعتی شاهرود، شاهرود، ایران ۱۳۹۶.

در ادامه بر اساس نتایج مقاله فوق و تجمیع خصوصیات کلیه حملات مسیریابی، یک الگوریتم سبک و مؤثر را برای بهبود امنیت گره‌های عادی (تشخیص نفوذ سطح پایین) در شبکه‌های حسگر بی‌سیم ارائه کردیم.

M. Sadeghizadeh, O. R. Marouzi, "*A Lightweight Intrusion Detection System Based on Specifications to Improve Security in Wireless Sensor Networks*", Journal of Communication Engineering, Vol. 7, No. 2, pp.29-50, July-December 2018.

در ادامه کار به جهت تقویت نتایج سیستم تشخیص نفوذ پیشنهادی مقاله فوق و ارتقاء دقت تشخیص حملات مسیریابی، به کمک یک روش مبتنی بر اعتماد و با ارزشیابی هشدارهای تولیدشده نرخ تشخیص و نرخ هشدارهای نادرست را در سیستم پیشنهادی بهبود دادیم.

مهدی. صادقی زاده و امیدرضا. معروضی، " یک سیستم تشخیص نفوذ سبک مبتنی بر اعتماد دوسطحی برای شبکه‌های حسگر بی‌سیم "، نشریه مهندسی برق و مهندسی کامپیوتر ایران، (داوری شده در حال بازبینی داوران).

سیستم تشخیص نفوذ پیشنهادی با نرخ تشخیص بالای ۹۷/۱٪ و نرخ هشدار نادرست خیلی پایین ۱/۲٪ و همچنین میانگین مصرف انرژی کم ۰/۰۲ ژول، در مقایسه با کارهای موجود به‌عنوان یک روش مؤثر و سبک برای تشخیص نفوذ در سطح گره‌های عادی در شبکه‌های حسگر مطرح است و با به‌کارگیری آن در شبکه‌های حسگر، به‌خوبی می‌توان کارائی شبکه را در حد مطلوب حفظ نمود.

سپس با توجه به حساسیت بالای گره‌های سرخوشه و عملیات مهم آن‌ها در شبکه حسگر بی‌سیم، به جهت تأمین امنیت آن‌ها یک روش مبتنی بر داده‌کاوی را با ارائه یک مدل پیش‌پردازش داده‌ها طراحی کردیم. هدف ما از این طراحی کاهش هزینه محاسباتی بالای روش مبتنی بر داده‌کاوی برای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم است.

مهدی. صادقی زاده، امیدرضا. معروضی و علی‌اکبر. پویان، " بهبود کارائی سیستم‌های‌تشخیص‌نفوذ مبتنی بر داده‌کاوی در شبکه‌های حسگر بی‌سیم با ارائه یک مدل پیش‌پردازش داده‌ها "، سومین کنفرانس محاسبات تکاملی و هوش جمعی، کرمان، ایران، اسفند ۱۳۹۶.

بر اساس نتایج مقاله فوق، با بهبود هرچه بیشتر مدل پیش‌پردازش پیشنهادی، یک سیستم تشخیص نفوذ ترکیبی مبتنی بر داده‌کاوی را برای تضمین امنیت گره‌های سرخوشه (تشخیص نفوذ سطح میانی) طراحی کردیم که با کاهش چشمگیر مصرف انرژی، نرخ بالایی در تشخیص نفوذ و نرخ خیلی کمی در تولید هشدارهای نادرست را به ارمغان می‌آورد.

M. Sadeghizadeh, O. R. Marouzi, " *Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining*", Journal of Communication Engineering, Vol. 8, No. 1, pp.29-50, pp. 1-20, January-June 2019.

نتایج حاصل از شبیه‌سازی‌ها نشان می‌دهد که سیستم پیشنهادی در مقایسه با کارهای موجود که اغلب پیچیدگی محاسباتی و حافظه بالا دارند، علاوه بر پیچیدگی محاسباتی پایین، با نرخ تشخیص بالای ۹۹/۵۹٪، نرخ هشدار نادرست پایین ۰/۲۴٪ و همچنین زمان پایین اجرای مدل یعنی ۰/۰۲۵ ثانیه که تداعی‌گر مصرف انرژی حداقلی آن است، به‌عنوان یک سیستم تشخیص نفوذ مؤثر و سبک برای تأمین امنیت سرخوشه‌ها در شبکه‌های حسگر بی‌سیم مطرح است.

ما در ادامه کار قصد داریم با ارائه یک سیستم تشخیص نفوذ سطح بالا، از پتانسیل‌های ایستگاه پایه (عدم وجود محدودیت انرژی و قابلیت‌های سخت‌افزاری بالا)، برای ارتقاء سطح امنیت سرخوشه‌ها استفاده کنیم.

۱–۶– ساختار رساله

ادامه این رساله به این صورت سازمان‌دهی شده است:

- در بخش ۲، مروری بر موضوعات و مفاهیم مرتبط با رساله و معماری پیشنهادی را انجام می‌دهیم.
- در بخش ۳ نیز، مهم‌ترین کارهای انجام‌شده در زمینه تشخیص نفوذ را به همراه مزایا و معایب آن‌ها بررسی می‌کنیم.
- در بخش ۴ سیستم تشخیص نفوذ پیشنهادی خود را ارائه می‌نماییم.
- در بخش ۵ به شبیه‌سازی، ارائه نتایج و مقایسه روش پیشنهادی با کارهای موجود خواهیم پرداخت. در انتها نیز، نتیجه‌گیری و کارهای آینده را ارائه خواهیم نمود.
- در بخش ۶ نیز مراجع و منابع را معرفی می‌کنیم.

۱–۷– جمع‌بندی

در سال‌های اخیر با توسعه رو به رشد شبکه‌های حسگر بی‌سیم، و همچنین با توجه مستعد بودن آن‌ها برای تهاجم و حملات امنیتی، طراحی یک سیستم تشخیص نفوذ کارآ به جهت تامین امنیت آن در برابر حملات مختلف، به‌ویژه در کاربردهای نظامی و بحرانی، به یک موضوع مهم مبدل شده است. در همین راستا در این فصل، به بیان و تعریف مسئله معماری تشخیص نفوذ در شبکه‌های حسگر بی‌سیم پرداخته شد. سپس چالش‌ها، فرضیات و نوآوری‌های رساله بیان شد. همچنین دستاوردهای رساله به صورت کلی بیان شد و در انتهای نیز سازماندهی کلی رساله تشریح گردید.

۲–مروری بر موضوعات و مفاهیم مرتبط

۲-۱- شبکه‌های حسگر بی‌سیم[1]

شبکه‌های حسگر بی‌سیم متشکل از صدها و یا هزاران دستگاه کوچک همراه با قابلیت‌های حسگری، پردازشی و ارتباطی برای نظارت بر محیط‌های واقعی است. این شبکه‌ها برای ایفای نقش در طیف وسیع و متنوعی از کاربردها مانند کنترل و نظارت نظامی تا کنترل آتش‌سوزی جنگل‌ها و نظارت بر ایمنی سازه‌ها و ساختمان‌ها، بسیار مطلوب و مقرون‌به‌صرفه می‌باشند.

لزوماً مکان قرارگرفتن گره‌های حسگر، از قبل تعیین‌شده و مشخص نیست. چنین خصوصیتی این امکان را میسر می‌کند که بتوانیم آن‌ها را در مکان‌های متخاصم و یا غیرقابل‌دسترس و دورافتاده مستقر کنیم. از طرف دیگر این بدان معنی است که پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی خودسامان‌دهی[2] باشند. از دیگر ویژگی‌های منحصربه‌فرد این شبکه‌ها، توانایی همکاری و هماهنگی بین گره‌های حسگر است. هر گره حسگر دارای یک پردازشگر است و به‌جای ارسال تمامی اطلاعات خام به مرکز یا گره‌ای که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه[3] و ساده را روی اطلاعات انجام می‌دهد و سپس داده‌های نیمه پردازش‌شده را ارسال می‌کند. با انجام این عملیات در حقیقت حجم ارسال داده‌ها و ارتباطات بین گره‌ها کاهش چشمگیری می‌یابد که منجر به کاهش مصرف انرژی و افزایش طول‌عمر شبکه حسگر خواهد شد.

۲-۱-۱. معماری ارتباطات شبکه

قبل از ارائه ساختار کلی ابتدا تعدادی از تعاریف کلیدی را ذکر می‌کنیم.

حسگر: وسیله‌ای که وجود شئ، رخداد یک وضعیت یا مقدار یک کمیت فیزیکی را تشخیص داده و به سیگنال الکتریکی تبدیل می‌کند. حسگر انواع مختلف دارد مانند حسگرهای دما، فشار، رطوبت، نور، شتاب‌سنج، مغناطیس‌سنج و... .

میدان حسگر: ناحیه کاری که گره‌های شبکه حسگر در آن توزیع می‌شوند.

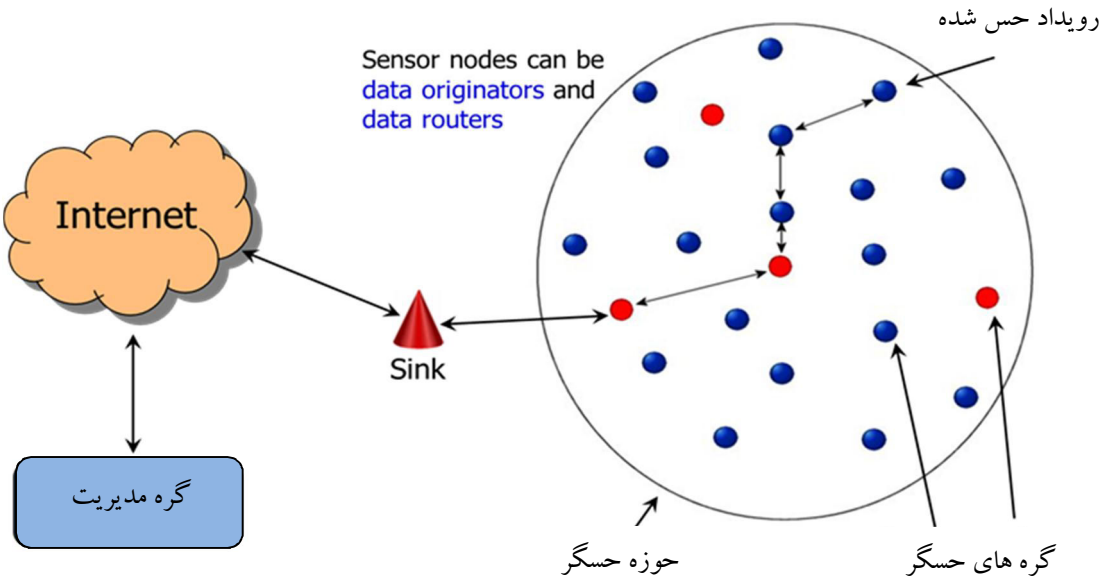
[1] Wireless Sensor networks (WSNs)
[2] Self-Organization
[3] In Network Processing

گره حسگر: به گره‌ای گفته می‌شود که شامل یک یا چند حسگر باشد. یک گره حسگر ممکن است با ابزارهای دیگری نیز همراه باشد. به‌عنوان نمونه می‌تواند شامل سیستم مکان‌یاب برای تشخیص موقعیت مکانی گره باشد و یا دارای محرک‌هایی جهت تعامل و تأثیر بر محیط باشد.

چاهک[1]: گره‌ای که جمع‌آوری داده‌ها را به عهده دارد و ارتباط بین گره‌های حسگر و گره مدیریت را برقرار می‌کند.

گره مدیریت: گره‌ای که یک شخصی به‌عنوان مدیر شبکه از طریق آن با شبکه ارتباط برقرار می‌کند. فرامین کنترلی و پرس‌وجوها از آن به شبکه ارسال‌شده و داده‌های جمع‌آوری‌شده به آن برمی‌گردد.

شبکه حسگر: شبکه‌ای متشکل از گره‌های حسگر است که در کاربردهایی که هدف جمع‌آوری اطلاعات و تحقیق در مورد یک پدیده است کاربرد دارد. به‌عبارت‌دیگر شبکه حسگر شبکه‌ای است با تعداد زیادی گره که هر گره می‌تواند در حالت کلی دارای تعدادی حسگر باشد. گره‌ها در ناحیه‌ای که میدان حسگر نامیده می‌شود با چگالی زیاد پراکنده می‌شوند. یک چاهک پایش کل شبکه را بر عهده دارد. اطلاعات به‌وسیله چاهک جمع‌آوری می‌شود و فرامین از طریق چاهک به گره‌های حسگر منتقل می‌شود. در شکل ۲-۱ نمایی از شبکه حسگر بی‌سیم همراه با معماری ارتباطات آن ارائه‌شده است.



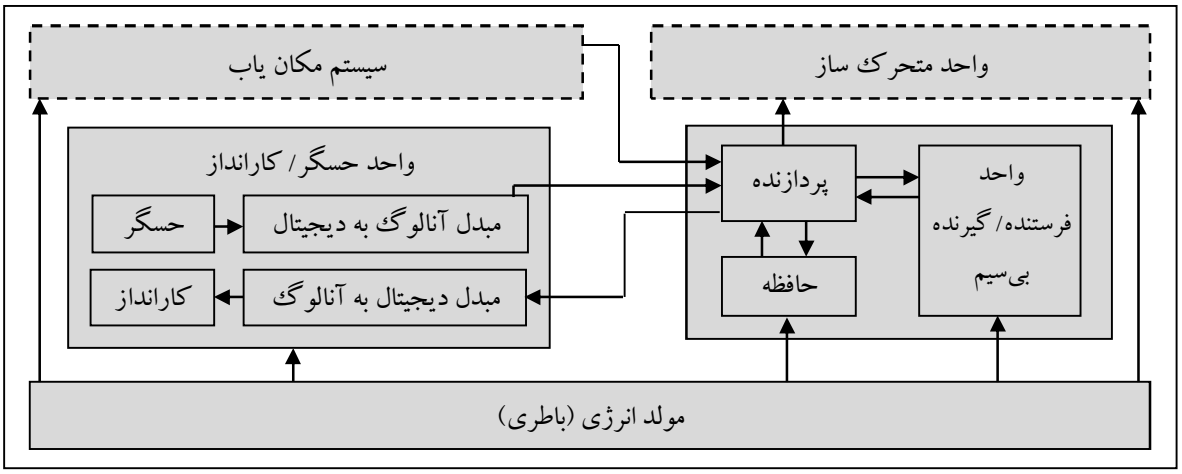
شکل (۲-۱) شبکه حسگر بی‌سیم و معماری ارتباطات آن [۱]

[1] Sink

۲-۱-۲. ساختار داخلی گره حسگر

شکل ۲-۲ ساختمان داخلی گره حسگر را نشان می‌دهد. هر گره شامل واحد حسگر، واحد پردازش داده‌ها، فرستنده/گیرنده بی‌سیم و منبع تغذیه است. بخش‌های اضافی واحد محرک[۱]، متحرک ساز[۲]، سیستم مکان‌یاب[۳] و تولید توان نیز ممکن است بسته به کاربرد در گره‌ها وجود داشته باشد.

- واحد پردازش داده شامل یک پردازندهٔ کوچک و یک حافظه با ظرفیت محدود است که داده‌ها را از حسگرها گرفته و بسته به کاربرد، پردازش محدودی روی آن‌ها انجام داده و از طریق فرستنده ارسال می‌کند.
- واحد فرستنده/گیرنده ارتباط گره با شبکه را برقرار می‌کند.
- واحد حسگر شامل یک سری حسگر و مبدل آنالوگ به دیجیتال است که اطلاعات آنالوگ را از حسگر گرفته و به‌صورت دیجیتال به پردازنده تحویل می‌دهد.
- واحد محرک در صورت وجود شامل محرک و مبدل دیجیتال به آنالوگ است که فرامین دیجیتال را از پردازنده گرفته و به محرک تحویل می‌دهد.
- واحد تأمین انرژی، توان مصرفی تمام بخش‌ها را تأمین می‌کند که اغلب یک باطری با انرژی محدود است.



شکل (۲-۲) ساختمان داخلی گره حسگر [۱]

[1] Actuator
[2] Mobilizer
[3] GPS

- در گره‌های متحرک واحدی برای متحرک‌سازی وجود دارد.
- مکان‌یاب موقعیت فیزیکی گره را تشخیص می‌دهد. تکنیک‌های مسیریابی و وظایف حسگری به اطلاعات مکان با دقت بالا نیاز دارند.

یکی از چالش‌های اساس در شبکه‌های حسگر بی‌سیم، محدودیت منابع و پردازشی در گره‌های آن‌ها می‌باشد. به‌منظور برآورد ذهنی مناسب و دقیقی از نوع پردازنده و قدرت پردازشی گره‌ها، حجم حافظه و همچنین میزان توان مصرفی آن‌ها، فهرستی از موارد فوق در جدول ۲-۱ ارائه گردیده است:

جدول ۲-۱ تحول در گره‌های شبکه حسگر بی‌سیم [۲]

Mote Type Year	WeC 1998	Rene 1999	Rene2 2000	Dot 2000	Mica 2001	Mica2Dot 2002	Mica2 2002	Telos 2004
Microcontroller								**مشخصات ریزپردازنده**
Type	AT90LS8535		Atmega163		ATmega128			T1 MSP430
Program Memory (KB)	8		16		128			60
RAM (KB)	0.5		1		4			2
Active Power (mW)	15		15		8		33	3
Sleep Power (µW)	45		45		75		75	6
Wakeup Time (µs)	1000		36		180		180	6
Nonvolatile storage (Flash)								**مشخصات حافظه غیر فرار**
Chip	24LC256				AT45DB041B			ST M24M01S
Connection type	I^2C				SPI			I^2C
Size (KB)	32				512			128
Communication								**مشخصات ارتباطی و تبادل اطلاعات**
Radio	TR1000				TR1000	CC1000		CC2420
Data rate (kbps)	10				40	38.4		250
Modulation type	OOK				ASK	FSK		O-QPSK
Receive Power (mW)	9				12	29		38
Transmit Power at 0dBm (mW)	36				36	42		35
Power Consumption								**مشخصات مصرف انرژی**
Minimum Operation (V)	2.7		2.7		2.7			1.8
Total Active Power (mW)	24				27	44	89	41
Programming and Sensor Interfacec								**مشخصات واسط حسگر و برنامه‌ریزی**
Expansion	none	51-pin	51-pin	none	51-pin	19-pin	51-pin	10-pin
Communication	IEEE 1284 (programming) and RS232 (requires additional hardware)							USB
Integrated Sensors	no	no	no	Yes	No	no	No	Yes

وجود برخی ویژگی‌ها در شبکه حسگر، آن را از سایر شبکه‌های سنتی و بی‌سیم متمایز می‌کنـد. از آن جمله عبارتند از:

- محدودیت‌های سخت‌افزاری[1] شامل محدودیت‌های اندازهٔ فیزیکی، منبع انرژی، قدرت پـردازش، ظرفیت حافظه
- تعداد بسیار زیاد گره‌ها
- چگالی بالا در توزیع گره‌ها در ناحیه عملیاتی
- وجود استعداد خرابی در گره‌ها
- تغییرات توپولوژی به‌صورت پویا و احیاناً متناوب
- استفاده از روش پخش همگانی[2] در ارتباط بین گره‌ها در مقابل ارتباط نقطه‌به‌نقطه
- داده محور بودن شبکه به این معنی که گره‌ها کد شناسایی ندارند.

۲-۱-۳. فاکتورهای طراحی در شبکه‌های حسگر

طراحی یک شبکه تحت تأثیر عوامل متعددی است. این عوامل عبارتند از: تحمل خرابی، قابلیت گسترش، هزینه تولید، محیط کار، توپولوژی شبکه حسگری، محدودیت‌های سخت‌افزاری، محیط انتقال و مصرف توان که در زیر به شرح آن‌ها می‌پردازیم [۱] [۲]. این عوامل از اهمیت بالایی در طراحی پروتکل‌های شبکه‌های حسگر برخوردار هستند.

- **تحمل خرابی**[3]: گره‌های حسگر موجود در شبکه حسگر بی‌سیم به دلایل مختلفی همچون اتمام انرژی، آسیب‌های فیزیکی و تأثیرپذیری از محیط پیرامونشان، ممکن است از کار بیفتند. ازکارافتادن گره‌های حسگر نباید تأثیری روی عملکرد کلی شبکه داشته باشد. بنابراین تحمل خرابی را می‌توانیم به‌صورت "توانایی تداوم عملیات شبکه حسگر علی‌رغم ازکارافتادن برخی از گره‌ها" تعریف نماییم.

[1] Hardware Constraints
[1] Broadcast
[2] Fault Tolerance

- **قابلیت گسترش**[3]**:** در یک شبکه حسگر بی‌سیم تعداد گره‌های حسگری که برای کنترل یک محیط و یا مطالعه یک پدیده مورداستفاده قرار می‌گیرند، ممکن است در حدود صدها و یا هزاران گره باشد. مسلماً تعداد گره‌ها به کاربرد و دقت موردنظر بستگی دارد؛ به‌طوری‌که در بعضی موارد این تعداد ممکن است به میلیون‌ها عدد نیز برسد. یک شبکه باید طوری طراحی شود که بتواند تعداد متغیری از گره‌ها را پوشش داده و چگالی بالای گره‌های حسگر را نیز تحقق بخشد. این چگالی می‌تواند از چند گره تا چند صد گره در یک منطقه که ممکن است کمتر از ۱۰ متر قطر داشته باشد، تغییر نماید. به‌عبارت‌دیگر شبکه حسگر از طرفی باید بتواند با تعداد صدها، هزارها و حتی میلیون‌ها گره کار کند و از طرف دیگر، چگالی توزیع متفاوت گره‌ها را نیز پشتیبانی کند. چگالی طبق رابطه (۲-۱) محاسبه می‌شود. که بیانگر تعداد متوسط گره‌هایی است که در برد یک گره نوعی (مثلاً دایره‌ای با قطر ۱۰ متر) قرار می‌گیرد.

$$\mu(R) = (N \,.\, \pi R^2) \,/\, A \qquad (۲-۱)$$

که در آن A مساحت ناحیه کاری، N تعداد گره در ناحیه کاری و R برد ارسال رادیویی است.

- **توپولوژی شبکه:** معمولاً توپولوژی یک شبکه حسگر بی‌سیم توسط یک گراف مشخص می‌شود. ارتباط گره‌ها توسط ارتباطات رادیویی بی‌سیم و به‌صورت انتشار عمومی است و هر گره با چند گره دیگر که در محدوده برد آن قرار دارد ارتباط دارد. برای افزایش کارایی الگوریتم‌ها در جمع‌آوری داده و کاربردهای ردگیری اشیاء، ساختار ارتباطی شبکه را یک درخت پوشا در نظر می‌گیرند. چون جریان داده‌ها اصولاً به شکلی است که داده‌ها از چند گره به سمت یک گره حرکت می‌کند مدیریت توپولوژی باید با دقت انجام شود. یک مرحله اساسی در مدیریت توپولوژی راه‌اندازی اولیه شبکه است به‌گونه‌ای که گره‌هایی که قبلاً هیچ ارتباط اولیه‌ای نداشته‌اند در هنگام جایگیری و شروع بکار اولیه باید بتوانند با یکدیگر ارتباط برقرار کنند. الگوریتم‌های مدیریت توپولوژی در راه‌اندازی اولیه باید امکان عضویت

[3] Scalability

گره‌های جدید و حذف گره‌هایی که به دلایل مختلف از کار می‌افتند را فراهم کنند. یکی از خصوصیات شبکه‌های حسگر بی‌سیم که امنیت آن را به چالش می‌کشد پویایی توپولوژی است.

- **محدودیت‌های سخت‌افزاری:** در یک شبکه حسگر هر گره درعین‌حال که باید کل اجزاء لازم را داشته باشد، همچنین باید تا حد ممکن کوچک، سبک و کم‌حجم نیز باشد. به‌عنوان‌مثال در برخی کاربردها گره‌ها باید به‌اندازه یک قوطی کبریت باشند و حتی گاهی حجم گره محدود به یک سانتیمتر مکعب است و ازنظر وزن آن‌قدر باید سبک باشد که بتواند همراه باد در هوا معلق شود. درعین‌حال هر گره باید توان مصرفی بسیار کم، قیمت تمام‌شده پایین داشته و با شرایط محیطی سازگار باشد. این‌ها همه محدودیت‌هایی است که کار طراحی و ساخت گره‌های حسگر را با چالش مواجه می‌کند. ارائه طرح‌های سخت‌افزاری سبک و کم‌حجم در مورد هر یک از اجزای گره بخصوص قسمت ارتباط بی‌سیم و حسگرها ازجمله موضوعات تحقیقاتی است که جای کار بسیار دارد.

- **قابلیت اطمینان**[1]: در یک شبکه حسگر، گره‌ها به دلایل مختلفی همچون تأثیر رویدادهای محیطی مثل تصادف یا انفجار و ... یا تمام شدن انرژی ممکن است از کار بیفتند. منظور از تحمل‌پذیری یا قابلیت اطمینان این است که خرابی گره‌ها نباید عملکرد کلی شبکه را تحت تأثیر قرار دهد. برای گره k با نرخ خرابی λ_k قابلیت اطمینان با رابطه (۲-۲) مدل می‌شود. که درواقع احتمال عدم خرابی است در زمان t به‌شرط اینکه گره در بازهٔ زمانی (0,t) خرابی نداشته باشد. بنابراین هرچه زمان می‌گذرد احتمال خرابی گره بیشتر می‌شود.

$$R_k(t) = e^{-\lambda_k t} \qquad (۲-۲)$$

- **هزینه تولید:** ازآنجایی‌که شبکه‌های حسگری از تعداد زیادی گره‌های حسگری تشکیل‌شده‌اند، هزینه یک گره در برآورد کردن هزینه کل شبکه بسیار مهم است. اگر هزینه یک شبکه حسگری گران‌تر از هزینه استفاده از شبکه‌های مشابه قدیمی باشد، در بسیاری موارد استفاده از آن مقرون‌به‌صرفه نیست. درنتیجه قیمت هر گره حسگری تا حد ممکن باید پایین نگه‌داشته شود.

[1] Reliability

- **شرایط محیطی**: در شبکه‌های حسگر بی‌سیم طیف وسیعی از کاربردها مربوط به محیط‌هایی می‌شود که امکان حضور انسان در آن وجود ندارد. نمونه‌هایی از این کاربردها عبارتند از: محیط‌های آلوده ازنظر شیمیایی، میکروبی، هسته‌ای و یا مطالعات در کف اقیانوس‌ها و فضا و یا محیط‌های نظامی به علت حضور دشمن و یا در جنگل و زیستگاه جانوران که حضور انسان باعث فرار آن‌ها می‌شود. در هر مورد، باید در طراحی گره‌ها شرایط محیطی آن در نظر گرفته شود. مثلاً در دریا و محیط‌های مرطوب گره حسگر در محفظه‌ای که رطوبت را منتقل نکند قرار می‌گیرد.

- **رسانه ارتباطی:** یکی از مشخصه‌های شبکه‌های حسگر این است که گره‌ها به‌صورت بی‌سیم و از طریق رسانه رادیویی، مادون‌قرمز، یا رسانه‌های نوری دیگر باهم ارتباط برقرار می‌نمایند. در این شبکه‌ها اکثراً از ارتباط رادیویی استفاده می‌شود، البته ارتباط مادون‌قرمز ارزان‌تر و ساختنش آسان‌تر است ولی فقط در خط مستقیم سیر می‌کند.

- **توان مصرفی گره‌ها:** با توجه به محدودیت منبع انرژی در گره‌های شبکه حسگر بی‌سیم، آن‌ها باید توان مصرفی کمی داشته باشند تا از این طریق بتوانیم طول عمر شبکه را افزایش دهیم. گاهی منبع تغذیه یک باتری ۱/۲ ولت با انرژی ۵/. آمپرساعت است که باید توان لازم برای مدت طولانی مثلاً ۹ ماه را تأمین کند. در بسیاری از کاربردها باتری قابل تعویض نیست لذا عمر باطری عملاً عمر گره را مشخص می‌کند. به‌علت اینکه یک گره علاوه‌بر گرفتن اطلاعات (توسط حسگر) یا اجرای یک فرمان (توسط محرک) به‌عنوان مسیریاب نیز عمل می‌کند، عملکرد نامناسب گره باعث حذف آن از شبکه شده که سازمان‌دهی مجدد شبکه و مسیردهی مجدد بسته عبوری را الزامی می‌کند. در طراحی سخت‌افزار گره‌ها استفاده از طرح‌ها و قطعاتی که مصرف کمی دارند و فراهم کردن امکان حالت خواب برای کل گره یا برای هر بخش به‌طور مجزا اهمیت زیادی دارد.

- **افزایش طول عمر شبکه:** در شبکه‌های حسگر بی‌سیم به دلیل این‌که طول عمر گره‌ها به علت محدودیت انرژی منبع تغذیه کوتاه است بنابراین عمر شبکه‌های حسگر نیز نوعاً کوتاه است. علاوه بر آن گاهی موقعیت ویژهٔ یک گره در شبکه این مشکل را تشدید می‌کند، مثلاً در گره‌های نزدیک به

گره چاهک، ازیک‌طرف به خاطر بار کاری زیاد خیلی زود انرژی خود را از دست می‌دهند و از طرفی ازکارافتادن هر یک از آن‌ها باعث قطع ارتباط چاهک با بخش بزرگی از شبکه می‌شود و ممکن است این امر باعث ازکارافتادن شبکه شود. برخی راه‌حل‌ها به ساختار برمی‌گردد. مثلاً در مورد مشکل فوق استفاده از ساختار خودکار راهکار مؤثری است. ازآنجاکه در ساختار خودکار بیشتر تصمیم‌گیری‌ها به‌طور محلی انجام می‌شود، ترافیک انتقالی از طریق گره بحرانی کم شده، طول عمر آن و درنتیجه طول عمر شبکه افزایش می‌یابد. مشکل تخلیه زودهنگام انرژی در مورد گره‌های نواحی کم تراکم در توزیع غیریکنواخت گره‌ها نیز صدق می‌کند. در این‌گونه موارد داشتن یک مدیریت توان در داخل گره‌ها و ارائه راه‌حل‌های توان آگاه به‌طوری‌که از گره‌های بحرانی کمترین استفاده را بکند مناسب خواهد بود.

- **ارتباط بلادرنگ و هماهنگی:** همان‌طور که می‌دانیم در سیستم‌های بلادرنگ علاوه بر تأمین پاسخ درست، زمان این پاسخگویی نیز اهمیت زیادی دارد. با توجه به این‌که برخی از کاربردهای شبکه‌های حسگر بی‌سیم به‌نوعی بلادرنگ هستند (مانند سیستم تشخیص و جلوگیری از گسترش آتش‌سوزی یا سیستم پیش‌گیری از سرقت) بنابراین سرعت پاسخگویی شبکه در آن‌ها از اهمیت زیادی برخوردار است. در کاربردهای بلادرنگ بر روی بسته‌های ارسالی باید به‌طور لحظه‌ای نظارت داشت تا روزآمد باشند. برای تحقق شرایط بلادرنگ، یک روش این است که برای بسته‌های ارسالی یک ضرب‌الاجل تعیین شود و در لایه کنترل دسترسی رسانه بسته‌های با ضرب‌الاجل کوتاه‌تر زودتر ارسال شوند که این ضرب‌الاجل به کاربرد بستگی دارد. مسئلهٔ مهم دیگر تحویل گزارش رخدادها به چاهک، به ترتیب وقوع آن‌هاست در غیر این صورت ممکن است شبکه واکنش درستی انجام ندهد.

- **امنیت و مداخلات:** یکی از موارد پر چالش در برخی از کاربردهای شبکه‌های حسگر بی‌سیم موضوع امنیت است، بخصوص این‌که امنیت در کاربردهای نظامی یک موضوع بحرانی است. همچنین به خاطر برخی ویژگی‌ها، شبکه‌های حسگر در مقابل مداخلات آسیب‌پذیرترند. یک مورد تأثیرگذار امنیتی، بی‌سیم بودن ارتباط شبکه است که کار دشمن را برای فعالیت‌های ضد امنیتی و مداخلات

آسان‌تر می‌کند. مورد دیگر استفاده از یک فرکانس مشترک ارتباطی برای کل شبکه است که شبکه را در مقابل استراق سمع آسیب‌پذیر می‌کند. مورد بعدی ویژگی متغیر بودن توپولوژی است که زمینه را برای پذیرش گره‌های دشمن فراهم می‌کند. اینکه پروتکل‌های مربوط به مسیردهی، کنترل ترافیک و لایه کنترل دسترسی شبکه سعی دارند با هزینه و سربار کمتری کار کنند مشکلات امنیتی بوجود می‌آورد. مثلاً برای شبکه‌های حسگر در مقیاس بزرگ برای کاهش تأخیر بسته‌هایی که در مسیر طولانی در شبکه حرکت می‌کنند، یک راه‌حل خوب این است که اولویت مسیردهی به آن بسته‌ها داده شود. همین روش باعث می‌شود حمله‌های سیلی مؤثرتر باشد. یکی از نقاط ضعف شبکه حسگر کمبود منبع انرژی است و دشمن می‌تواند با قرار دادن یک گره مزاحم که مرتب پیغام‌های بیدارباش به‌صورت پخش همگانی با انرژی زیاد تولید می‌کند باعث شود بدون دلیل گره‌های همسایه از حالت خواب خارج شوند. ادامهٔ این روند باعث به هدر رفتن انرژی گره‌ها شده و عمر آن‌ها را کوتاه می‌کند. با توجه به چنین محدودیت‌هایی باید دنبال راه‌حل‌های ساده و کارا مبتنی بر طبیعت شبکه حسگر بود.

– **عوامل پیش‌بینی‌نشده:** یک از مواردی که در شبکه‌های حسگر بی‌سیم مطرح است این است که این شبکه‌ها تابع تعداد زیادی از عدم قطعیت‌ها می‌باشند. نمونه‌هایی از این عدم قطعیت‌ها عوامل طبیعی غیرقابل‌پیش‌بینی مثل سیل، زلزله، مشکلات ناشی از ارتباط بی‌سیم و اختلالات رادیویی، امکان خرابی هر گره، تنظیم نبودن دستگاه اندازه‌گیری حسگرها، پویایی ساختار و مسیردهی شبکه، اضافه شدن گره‌های جدید و حذف گره‌های قدیمی، جابجایی گره‌ها به‌طور کنترل‌شده یا در اثر عوامل طبیعی و غیره می‌باشد. سؤالی که مطرح است این است که در این شرایط چگونه می‌توان چشم‌اندازی فراهم کرد که از دیدگاه لایه کاربرد، شبکه یک موجودیت قابل‌اطمینان در مقیاس بزرگ، دارای کارایی عملیاتی مشخص و قابل‌اعتماد باشد. باتوجه به اینکه شبکه‌های حسگر تا حدود زیادی به‌صورت مرکزی غیرقابل‌کنترل هستند و به‌صورت خودکار یا حداقل نیمه‌خودکار عمل می‌کنند باید بتوانند با مدیریت مستقل بر مشکلات غلبه کنند. ازاین‌رو باید ویژگی‌های خود بهینه‌سازی و خودسازمان‌دهی و خوددرمانی را داشته باشند.

۲-۱-۴. کاربردهای شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم طیف گسترده‌ای از کاربردها را شامل می‌شوند که در ۴ دسته کلی زیر تشریح شده‌اند [۱] [۲]:

- **کنترل محیط:** شبکه‌های حسگر بی‌سیم می‌توانند برای کنترل و نظارت بر محیط بکار بروند. برای نمونه می‌توانند برای کنترل مواد آلاینده در محیط‌های دفع زباله بکار بروند. نمونه دیگر، نظارت بر فرسایش خاک در یک محیط است. یک مثال دیگر می‌تواند برای شمارش تعداد گیاهان و حیواناتی که در یک مکان خاص زندگی می‌کنند، به کار رود. یکی دیگر از کاربردهای این شبکه‌ها در نظارت بر زیستگاه‌های حیوانات (مانند ردگیری حیوانات) برای حفاظت از آن‌ها می‌باشد.

- **کاربردهای نظامی و نظارت بر میدان نبرد**[1]: شبکه‌های حسگر بی‌سیم می‌توانند به‌عنوان بخش مهمی از سیستم‌های ارتباطی، نظارتی، ناوبری، هوشمند و پردازش نظامی مورداستفاده قرار گیرند. گاهی اوقات در این شبکه‌ها گره‌ها با فرستنده و گیرنده‌های ماهواره‌ای جهانی[2] همراه می‌شوند که در موقعیت‌یابی دقیق مناطق جنگی مورداستفاده واقع می‌شوند.

- **مراقبت بهداشتی و پزشکی**[3]: نصب حسگرها بر روی بدن بیماران جهت کنترل علائم حیاتی آن‌ها زمانی که نیاز است این بیماران برای مدت‌زمان زیادی تحت کنترل باشند و راهنمایی بیماران برای مصرف دارو (حسگرهای جاسازی‌شده در بسته‌های دارو تا زمانی‌که یک بیمار دارو را به‌صورت اشتباه مصرف کرد یک پیام هشدار ایجاد کند) از کاربردهای مهم شبکه‌های حسگر بی‌سیم در مراقبت پزشکی به شمار می‌آیند. همچنین در سیستم‌های مراقبت از بیماران ناتوان که مراقبی ندارند، محیط‌های هوشمند برای افراد سالخورده و نظارت بر بیماران ازجمله کاربردهای دیگر آن است.

- **کاربردهای تجاری:** کاربردهای تجاری طیف وسیعی از کاربردها را شامل می‌شود مانند سیستم‌های امنیتی تشخیص و مقابله با سرقت، آتش‌سوزی (در جنگل)، تشخیص آلودگی‌های

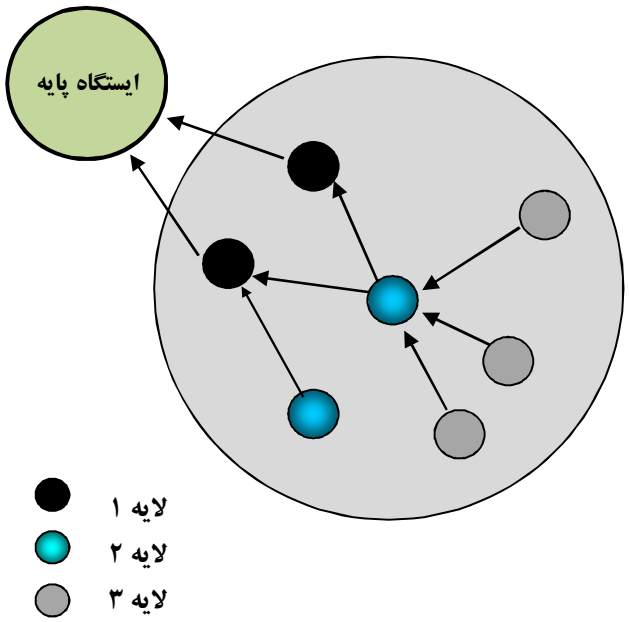
[1] Military, battlefield surveillance
[2] GPS
[3] Medical monitoring

زیست‌محیطی از قبیل آلودگی‌های شیمیایی، میکروبی، هسته‌ای، سیستم‌های ردگیری[1]، نظارت و کنترل وسایل نقلیه و ترافیک، کنترل کیفیت تولیدات صنعتی و ... . برای نمونه یک کاربرد تجاری این شبکه‌ها در کشاورزی مدرن است. استفاده از شبکه‌های بی‌سیم حسگر در کشاورزی اجازه می‌دهد آبیاری به‌طور دقیق انجام شود و بارور کردن خاک به‌وسیله قرار دادن حسگرها در داخل خاک انجام می‌شود.

۲-۱-۵. معماری شبکه

به لحاظ نحوه ارتباطات گره‌ها با هم در شبکه‌های حسگر بی‌سیم، دو معماری اصلی ارائه‌شده است [۲] که عبارتند از:

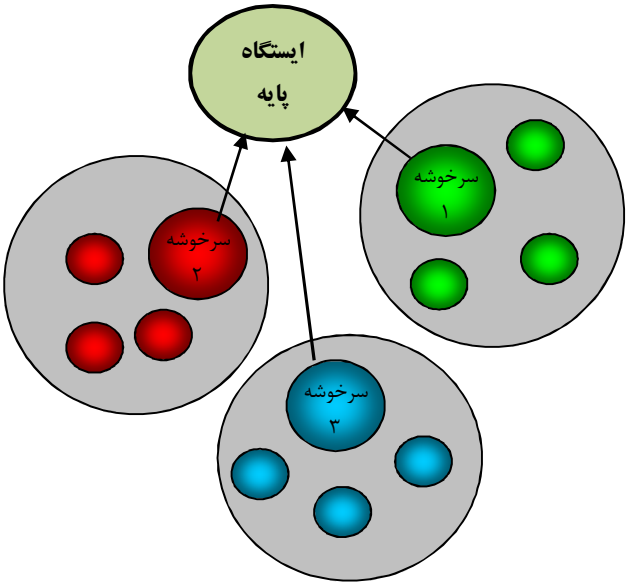
- **معماری لایه‌ای:** در این معماری که در شکل ۲-۳ نشان داده‌شده است، هر مجموعه از گره‌ها در یک لایه خاص تنها با گره‌های موجود در لایه‌های قبلی خود در ارتباط خواهند بود و این اطلاعات از لایه‌ای به لایه دیگر منتقل‌شده تا به ایستگاه پایه برسد.



شکل (۲-۳) معماری لایه‌ای [۲]

[1] Target Tracking

- **معماری خوشه‌بندی**[1]: در این معماری که در شکل ۲-۴ نشان داده‌شده است، در ابتدا گره-های موجود در شبکه به دسته‌هایی تقسیم می‌شوند که به آن‌ها خوشه گفته می‌شود. سپس برای هر خوشه یک گره به‌عنوان سرخوشه[2] انتخاب می‌گردد. در هر خوشه گره‌ها اطلاعات خود را به سرخوشه ارسال کرده و در مرحله بعدی سرخوشه‌ها اطلاعات را به ایستگاه پایه[3] منتقل می‌کنند.



شکل (۲-۴) معماری خوشه‌بندی [۲]

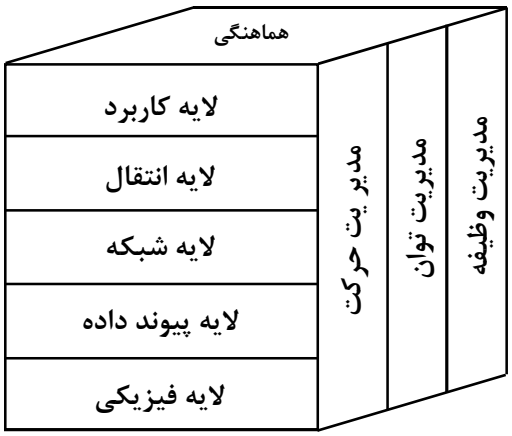
۲-۱-۶. پشته پروتکلی[4]

مطابق شکل ۲-۵ پشته پروتکلی ازیک‌طرف دارای پنج لایه افقی شامل لایه‌های فیزیکی، پیوند داده، شبکه، انتقال و کاربرد و از طرفی دارای سه لایه عمودی مدیریت توان، مدیریت جابجایی و مدیریت وظیفه است. لایه فیزیکی وظیفه‌اش عملیات مدولاسیون و ارسال و دریافت در سطح پایین است. لایه کنترل دسترسی رسانه باید قادر باشد با حداقل تصادم به روش پخش همگانی با هر گره همسایه ارتباط برقرار کند. لایه شبکه وظیفه مسیردهی داده‌هایی که از لایه انتقال می‌آیند را بر عهده دارد. لایه انتقال وظیفهٔ مدیریت جریان انتقال بسته‌ها را در صورت نیاز کاربرد، بر عهده دارد. بسته به کاری

[1] Clustered Architecture
[2] Cluster Head (CH)
[3] Base Station
[4] Protocol Stack

که شبکه برای آن طراحی‌شده انواع مختلف نرم‌افزارهای کاربردی می‌تواند روی لایه کاربرد استفاده شود و خدمات مختلفی را ارائه نماید.

یک زبان پردازه نویسی بنام زبان وظیفه و پرسشگری حسگر[1] پیشنهادشده که پرس‌وجوها و فرمان‌های آن مبتنی بر ویژگی داده محوری شبکه حسگر است [۱]. به‌عنوان‌مثال "چه تعداد لانه پرنده خالی در محدوده شمال شرقی جنگل وجود دارد" یا "اگر تا یک ساعت بعد تعداد لانه‌های خالی بیشتر از یک حد معینی شد اعلام شود".



شکل (۲-۵) پشته پروتکلی شبکه حسگر بی‌سیم [۱]

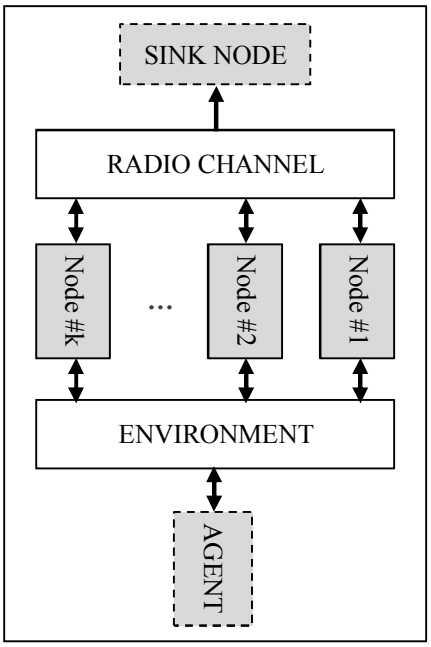
لایه عمودی مدیریت توان با دخالت در کلیه لایه‌های افقی چگونگی مصرف توان برای گره را تعیین می‌کند. درواقع برای کاهش مصرف انرژی به الگوریتم‌ها و پروتکل‌های توان آگاه[2] نیازمندیم. مثلاً اینکه یک گره پس از دریافت یک پیغام از یکی از همسایه‌هایش دریافت کننده‌اش را خاموش کند، باعث جلوگیری از دریافت دوباره پیغام و درنتیجه کاهش مصرف انرژی می‌گردد. ایده دیگری که می‌تواند هم‌زمان استفاده شود این است گره‌ای که به سطح پایین انرژی رسیده به همسایه‌هایش اعلام همگانی می‌کند که انرژی‌اش در حال اتمام است و نمی‌تواند در مسیردهی پیغام‌ها شرکت داشته باشد. گره‌های همسایه پس‌ازآن پیغام‌ها را از طریق گره‌های دیگر مسیردهی خواهند کرد. لایه عمودی مدیریت حرکت، روش‌های مکان‌آگاه[3] را به کار می‌گیرد. جابجایی گره را تشخیص داده و ثبت می‌کند.

[1] Sensor Query and Tasking Language (SQTL)
[2] Power-Aware
[3] Location Aware

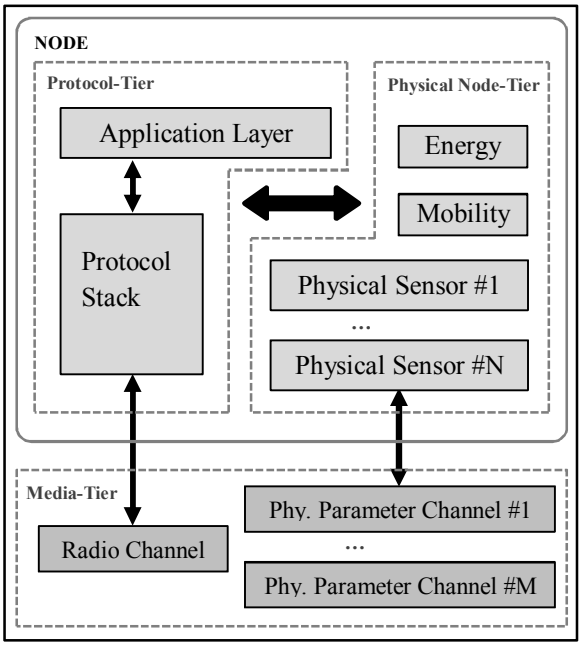
بدین ترتیب یک مسیر برگشت تا کاربر همیشه مدیریت می‌شود و رد گره متحرک دنبال می‌شود. مدیریت وظیفه، وظایف گره‌ها را زمان‌بندی و تنظیم می‌کند. مثلاً اگر وظیفهٔ حسگری به یک ناحیهٔ معین محول شد همهٔ گره‌های حسگر آن ناحیه لازم نیست عملیات حسگری را به‌طور هم‌زمان انجام دهند بلکه این وظیفه می‌تواند بسته به کاربرد به برخی گره‌ها مثلاً گره‌هایی که قابلیت اطمینان بیشتر یا ترافیک کمتر یا انرژی بیشتر دارند، محول شود. برای تضمین این نکته باید از الگوریتم‌های کارآگاه[1] استفاده نمود. با رعایت موارد فوق، گره‌ها در شبکه حسگر می‌توانند با روش‌های توان‌کارا[2] باهم کار کرده و داده‌ها را در یک شبکه سیار حسگر مسیردهی کنند و منابع را بین گره‌ها به اشتراک گذارند.

۲-۱-۷. تبیین نحوه شبیه‌سازی شبکه‌های حسگر بی‌سیم

برای شبیه‌سازی یک شبکه حسگر بی‌سیم با شبیه‌ساز NS2 ابتدا می‌بایست مدلی برای معماری شبکه و همچنین مدلی برای معماری ساختار گره‌ها ارائه نماییم تا بر اساس آن بتوانیم طراحی مناسبی از شبکه‌های حسگر بی‌سیم را در شبیه‌سازی ایجاد نماییم. به همین منظور در شکل ۲-۶ مدل معماری شبکه‌های حسگر بی‌سیم را ارائه نمودیم.



شکل (۲-۶): مدل معماری شبکه حسگر [۴]

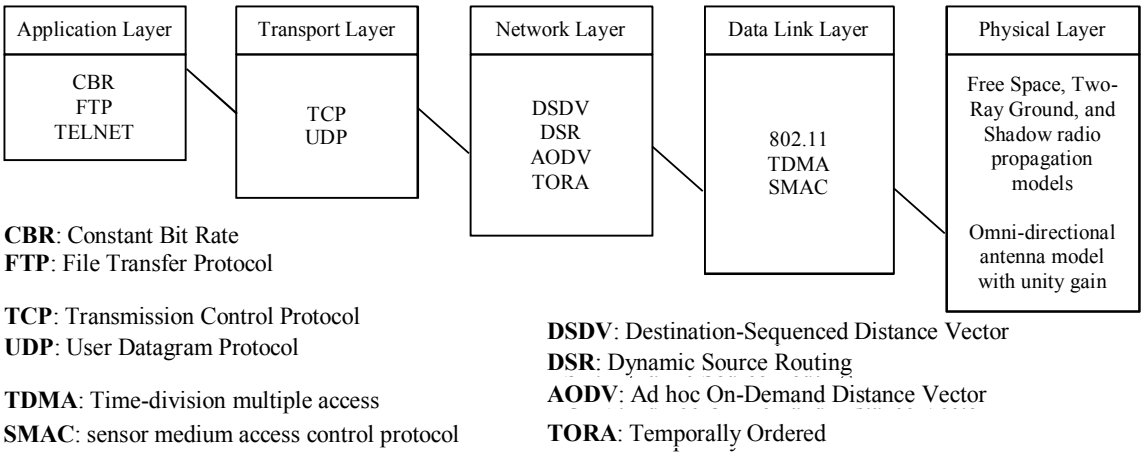


شکل (۲-۷): معماری لایه‌ای در طراحی گره‌های حسگر [۴]

[1] Application Aware
[2] Power Efficient

همان‌طور که در مدل ارائه‌شده دیده می‌شود، گره‌های حسگر وقایع محیط مورد نظارت توسط شبکه را حس کرده و با ارتباط با هم دیگر از طریق رسانه ارتباطی که همان کانال امواج رادیویی است، داده‌های حس شده را به گره چاهک ارسال می‌نمایند و در آنجا پردازش‌های اصلی بر روی داده‌های حس شده انجام‌شده و تصمیمات لازم اتخاذ می‌گردد.

در شکل ۲-۷ نیز مدل معماری لایه‌ای در طراحی و شبیه‌سازی گره‌های حسگر ارائه‌شده است. لایه پروتکل شامل همه پروتکل‌های ارتباطی اعم از پروتکل‌های کنترل دسترسی به رسانه، مسیریابی و لایه کاربرد است. لایه فیزیکی گره، پایه سخت‌افزاری و اثرات آن را بر روی کارایی تجهیزات ارائه می‌نماید. ترکیب و ساختار واقعی این بخش وابسته به کاربرد مربوطه در شبکه حسگر بی‌سیم است. همان‌طور که در شکل ۲-۷ مشاهده می‌شود، اجزاء معمول این لایه شامل حسگرهای فیزیکی، ماژول انرژی و ماژول متحرک‌سازی می‌باشد. در لایه رسانه نیز اتصال گره با محیط واقعی رسیدگی می‌گردد. پس از مشخص شدن مدل معماری شبکه و گره‌های آن، پروتکل‌های مربوطه برای هریک از لایه‌های مفروض در شبکه‌های حسگر بی‌سیم را باید تعیین کنیم. این پروتکل‌ها که به نوع کاربرد شبکه و نحوه تعامل گره‌های حسگر با محیط پیرامون وابستگی دارد در شکل ۲-۸ نشان داده‌شده‌اند.



شکل (۲-۸): پروتکل‌های لایه‌های مختلف در شبکه‌های حسگر بی‌سیم [۵]

برای شبیه‌سازی یک شبکه حسگر بی‌سیم باید تمامی پارامترهای لازم را که در بالا به آن‌ها اشاره کردیم در نظر بگیریم.

در شکل‌های (۲-۹)، (۲-۱۰) و (۲-۱۱) نمونه‌هایی از پارامترها برای شبیه‌سازی یک شبکه حسگر در مراجع مختلف ارائه‌شده‌اند:

Parameter	Default Value
N	1500 nodes
p	0.01
q	10^{-6}
e_j	[0.0001 – 0.1]
r	40 m
f	0.25
λ	15 nodes/(40 x 40 m^2)
λ_q	1 query/sec
λ_c	Once per 4 days to 28 days
$A \times A$	400m×400m
n_b	50 bits
E_{elec}	50 nJ/bit
E_{amp}	10 pJ/bit/m^2
E_o	10 Joule
$N_{iteration}$	3 iterations
$T_{clustering}$	60 sec
T_{req}	[0.3 – 1.0] sec
H_{pfp} , H_{pfn}	[0.01-0.05]

شکل (۲-۹) یک نمونه از پارامترهای شبیه‌سازی شبکه حسگر [۶]

Simulation Parameter

Sr.No	Parameters	Values
1.	Routing Protocol	AODV
2.	Mac Layer Protocol	802.11
3.	Total No. Of Nodes	50
4.	Traffic Type	CBR
5.	Simulation Topology	1024cm × 768cm
6.	Simulation Time	100 sec
7.	Packet Size	512 Kbytes

شکل (۲-۱۰) نمونه دوم از پارامترهای شبیه‌سازی شبکه حسگر [۷]

Nodes	100 (nodes)
Network size	100 X 100 (m^2)
Base station location	(50, 75)
Radio propagation speed	$3x10^8$ (m/s)
Processing delay	50 (µs)
Radio speed	1 (Mbps)
Starting energy	2 (J)
Cluster-head change time	20 (s)

شکل (۲-۱۱) نمونه سوم از پارامترهای شبیه‌سازی شبکه حسگر [۸]

۲-۲- امنیت در شبکه‌های حسگر بی‌سیم

با توجه به این‌که شبکه‌های حسگر بی‌سیم معمولاً در مکان‌های دور و فاقد حفاظت به کار گرفته می‌شوند، باید با یکسری سازوکارهای امنیتی برای دفاع در مقابل حملات موجود (مانند تسخیر گره[۱]، دست‌کاری فیزیکی[۲]، استراق سمع[۳]، رد سرویس[۴] و ...) مجهز شوند. متأسفانه به‌کارگیری سازوکارهای امنیتی سنتی و مرسوم که سربار محاسباتی بالایی دارند، برای گره‌های حسگر که با محدودیت منابع روبرو هستند، عملی و امکان‌پذیر نمی‌باشند.

برای تأمین امنیت در شبکه‌های حسگر بی‌سیم، طرح‌های امنیتی مختلفی با توجه به محدودیت‌های منابع موجود پیشنهاد شده‌اند [۲]. همچنین در راستای تأمین امنیت در شبکه‌های حسگر بی‌سیم، تعدادی پروتکل مسیریابی کارآ و ایمن و چندین پروتکل تجمیع داده ایمن[۵] نیز پیشنهاد شده‌اند.

۲-۲-۱. محدودیت‌های[۶] شبکه‌های حسگر

برای اینکه بتوانیم یک سازوکار امنیتی مناسب و مطلوب برای شبکه‌های حسگر بی‌سیم ارائه دهیم، ابتدا می‌بایست محدودیت‌های موجود در این شبکه‌ها را که مانعی بر سر راه برقراری امنیت هستند را شناسایی نماییم. در حقیقت اگر بخواهیم از رهیافت‌های امنیتی بکار رفته در شبکه‌های سنتی برای امنیت در شبکه‌های حسگر بی‌سیم استفاده نموده و یا ایده بگیریم، باید یک سری محدودیت‌ها را در آن‌ها بدانیم. این محدودیت‌ها در ادامه تشریح شده‌اند [۹] و [۱۰]:

- **محدودیت انرژی**: انرژی بزرگ‌ترین محدودیت در شبکه‌های حسگر بی‌سیم است. در کل مصرف انرژی در گره‌های حسگر در سه بخش زیر خواهد بود:
  - انرژی برای مبدل حسگر
  - انرژی برای ارتباط بین گره‌های حسگر

[1] Node capture
[2] Physical tampering
[3] Eavesdropping
[4] Denial of service
[5] Secure data aggregation protocols
[6] Constrains

- انرژی برای محاسبات پردازشگر

با توجه به بررسی‌های به‌عمل‌آمده مشخص‌شده است که در شبکه‌های حسگر بی‌سیم ارتباطات پرهزینه‌تر از محاسبات هستند. برای برآورد ذهنی دقیق‌تر کافی است مقایسه‌ای بر روی ارسال و دریافت اطلاعات توسط واحد ارتباطی و اجرای دستورالعمل‌ها توسط پردازنده داشته باشیم. رابطه‌های (۲-۳) و (۲-۴) میزان مصرف انرژی برای ارسال و دریافت n بیت اطلاعات را ارائه می-نمایند:

$$E_{\text{rcvd}} = T_{\text{start}}\, P_{\text{start}} + \frac{n}{R\, R_{\text{code}}} P_{\text{rxElec}} + n\, E_{\text{decBit}} \qquad (۲-۳)$$

$$E_{\text{tx}}\left(n, R_{\text{code}}, P_{\text{amp}}\right) = T_{\text{start}}\, P_{\text{start}} + \frac{n}{R\, R_{\text{code}}} \left(P_{\text{rxElec}} + P_{\text{amp}}\right) \qquad (۲-۴)$$

در رابطه‌های فوق پارامترها به شرح زیر هستند:

- T_{start} : میانگین زمان لازم برای خروج از حالت خواب و فعال شدن
- P_{start} : میانگین توان لازم برای خروج از حالت خواب و فعال شدن در واحد زمان
- R : نرخ نرمال ارسال و دریافت داده
- R_{code} : نرخ کدگذاری داده‌ها
- P_{rxElec} : توان مصرفی اجزاء الکترونیکی دریافت‌کننده
- P_{txElec} : توان مصرفی اجزاء الکترونیکی ارسال گر
- E_{decBit} : انرژی مصرفی برای رمزگشایی هر بیت از اطلاعات
- P_{amp} : توان مصرفی آمپلی‌فایر

درصورتی‌که بخواهیم میزان مصرف انرژی برای "ارسال یک بیت اطلاعات" را با "اجرای یک دستورالعمل" مقایسه نماییم، با توجه به فرمول‌های فوق انرژی مصرفی برای ارسال و دریافت یک کیلوبایت اطلاعات در مسافت ۱۰۰ متر معادل انرژی مصرفی برای محاسبات و اجرای سه میلیون دستورالعمل خواهد بود. بنابراین کاملاً واضح است که میزان مصرف انرژی در ارسال و دریافت اطلاعات (هزینه ارتباطات)، بسیار بالاتر از مصرف انرژی اجرای دستورالعمل‌ها (هزینه محاسبات)

می‌باشد. بنابراین سعی بر این است که تا حد ممکن محاسبات را جایگزین ارتباطات نماییم تا میزان مصرف انرژی کاهش یابد. برای مثال با اعمال الگوریتم‌های فشرده‌سازی قوی‌تر اطلاعات و یا اعمال الگوریتم‌های کدگذاری مناسب‌تر حجم داده‌ها و اطلاعات ارسالی را کاهش دهیم.

هر پیام ایجادشده با سازوکار امنیتی با هزینه قابل‌توجهی منتقل می‌گردد. در سطوح امنیتی بالاتر در شبکه‌های حسگر معمولاً مصرف انرژی بیشتری برای عملیات رمزنگاری نیاز خواهد بود. بنابراین بسته به هزینه مصرف انرژی، سطوح امنیتی مختلفی در شبکه‌های حسگر می‌تواند ارائه گردد.

- **محدودیت‌های حافظه:** یک حسگر درواقع یک دستگاه کوچک است که دارای حجم کمی از حافظه و فضای ذخیره‌سازی است (جدول ۲-۱). حافظه یک گره حسگر شامل حافظه RAM و حافظه فلش است. حافظه فلش برای ذخیره و بارگذاری کدهای کاربردی استفاده می‌گردد (حجم آن بین ۸ تا ۱۲۸ کیلوبایت است) و حافظه RAM برای ذخیره برنامه‌های کاربردی، داده‌های حسگر و نتایج محاسبات استفاده می‌شود (حجم آن بین ۰/۵ تا ۴ کیلوبایت است). معمولاً بعد از بارگذاری سیستم‌عامل و کدهای کاربردی در حافظه حسگر، فضای کافی برای اجرای الگوریتم‌های پیچیده وجود ندارد. بنابراین الگوریتم‌های امنیتی جاری بر روی این حسگرها معقول و قابل‌استفاده نیستند و باید تجدید نظرهای جدی در آن‌ها انجام شود تا در شبکه‌های حسگر بی‌سیم بتوان از آن‌ها استفاده کرد.
- **ارتباطات غیرقابل‌اعتماد:** ارتباطات نامطمئن تهدید جدی دیگری برای امنیت حسگرها است. به‌طور عادی مسیریابی داده محور در شبکه‌های حسگر بر پروتکل‌های بدون اتصال استوار است و بنابراین ذاتاً غیرقابل‌اعتماد هستند. بسته‌های ارسالی ممکن است به دلیل خطاهای کانال آسیب‌دیده و یا در گره‌هایی با ازدحام بالاتر حذف گردند. علاوه بر این کانال ارتباطی بی‌سیم غیرمطمئن ممکن است به خراب شدن بسته‌ها منجر شود. نرخ خطای بالاتر نیز نیازمند پیاده‌سازی طرح‌های رفع خطای قدرتمندتری می‌باشد که این امر منجر به سربار بیشتری به سیستم می‌گردد.

به‌طور خاص، حتی اگر کانال مطمئن باشد، ارتباطات ممکن است مطمئن نباشند. این امر به دلیل ماهیت انتشار همگانی اشتراکی ارتباطات بی‌سیم است. برای مثال بسته‌ها در هنگام انتقال ممکن است با هم برخورد کرده و نیازمند ارسال مجدد باشند.

- **ارتباطات با تأخیر بیشتر:** در یک شبکه حسگر بی‌سیم، عواملی نظیر مسیریابی چند پرشه، ازدحام شبکه و پردازش داده‌ها در گره‌های میانی منجر به تأخیر بیشتر در ارسال بسته‌ها می‌شود. این امر حصول همگام‌سازی را بسیار مشکل می‌نماید. موضوع همگام‌سازی بعضی‌اوقات در تأمین امنیت بسیار حیاتی است. برای مثال برخی سازوکارهای امنیتی مرتبط با گزارش پدیده‌های بحرانی و توزیع کلیدهای رمزنگاری هستند.
- **عملیات بدون حفاظ شبکه**[1]: در اغلب موارد، گره‌ها در یک شبکه حسگر بی‌سیم در یک ناحیه دوردست منتشرشده و بدون حفاظت رها می‌شوند. بنابراین در چنین محیطی احتمال مواجه‌شدن گره‌ها با حملات فیزیکی بسیار بالا خواهد بود. مدیریت از راه دور در این شبکه‌ها، تشخیص مداخلات فیزیکی را در آن‌ها مشکل می‌نماید. این امر فرایند تأمین امنیت در شبکه‌های حسگر بی‌سیم را بسیار مشکل می‌کند.

۲-۲-۲. نیازمندی‌های امنیتی

با توجه به محدودیت‌های بیان‌شده در بخش قبل، سرویس‌های امنیتی شبکه حسگر بی‌سیم به نحوی باید طراحی شوند که از اطلاعات منتقل‌شده تحت شبکه و منابع آن در مقابل حملات و رفتار نامطلوب گره‌ها محافظت نمایند. مهم‌ترین نیازمندی‌های امنیتی در شبکه‌های حسگر بی‌سیم در زیر ارائه‌شده‌اند [۹] [۱۰] [۳]:

- محرمانگی داده‌ها[2]: این اصل به ما اطمینان می‌دهد که یک پیام داده‌شده، به‌وسیله هیچ‌کسی جز دریافت‌کننده‌های مجاز، قابل‌فهم نخواهد بود.

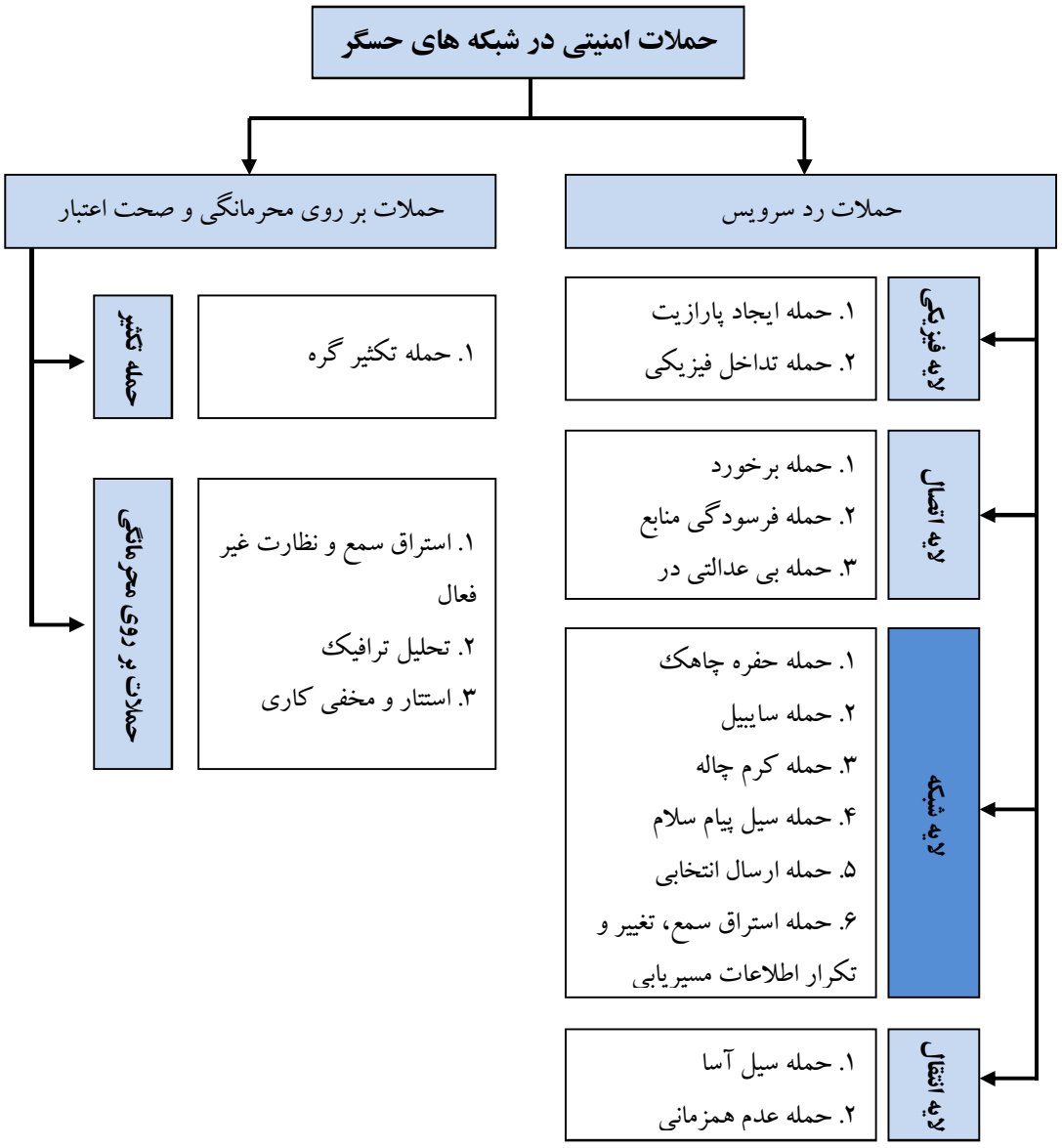
[1] Unattended operation of networks
[2] Data confidentiality

- جامعیت داده‌ها[1]: این اصل تضمین می‌کند که یک پیام ارسال‌شده از یک گره به یک گره دیگر، توسط گره‌های میانی معاند دچار تغییرات نمی‌گردد.
- در دسترس بودن[2] (موجودیت): این اصل این تضمین را به ما می‌دهد که خدمات مورد انتظار و مطلوب شبکه حتی در حضور حملات رد سرویس در دسترس خواهند بود.
- تازه‌سازی داده‌ها[3]: این اصل بر این امر دلالت دارد که داده‌ها تازه و جدید باشند و تضمین می‌کند که هیچ مهاجمی نمی‌تواند داده‌های قدیمی را بازپخش نماید.
- خودسازمان‌دهی: این اصل به این مفهوم است که هر گره در شبکه حسگر بی‌سیم باید قابلیت خودسازمان‌دهی، تنظیم کردن و حفظ سلامت خود را داشته باشد.
- مکان‌یابی امن: در بسیاری از شرایط این امر لازم است که هر گره حسگر به‌طور دقیق و خودکار محل استقرار خود را در شبکه حسگر بی‌سیم، تعیین نماید.
- همگام‌سازی زمان: در اغلب کاربردهای شبکه‌های حسگر نیازمند همگام‌سازی زمانی هستیم. به‌ویژه همه سازوکارهای امنیتی بر روی این شبکه‌ها نیز باید همگام‌سازی زمانی را انجام دهند.
- تأیید هویت[4]: این اصل به ما اطمینان می‌دهد که ارتباط از یک گره به گره دیگر موثق و مورد تأیید است، این امر به این مفهوم است که گره مهاجم با تظاهر کردن نمی‌تواند خود را به‌جای یک گره صحیح شبکه جا بزند.
- تنفیذ[5] (مجاز بودن): این اصل بر این امر اشاره می‌کند که تنها گره‌های مجاز می‌توانند در تأمین داده‌ها برای خدمات شبکه ورود پیدا نمایند.
- عدم انکار[6]: این اصل بیان می‌کند که یک گره نمی‌تواند ارسال پیامی را که قبلاً فرستاده است، انکار نماید.

[1] Data integrity
[2] Availability
[3] Data freshness
[4] Authentication
[5] Authorization
[6] Non repudiation

۲-۲-۳. آسیب‌های امنیتی و انواع حملات

شبکه‌های حسگر بی‌سیم برای انواع مختلفی از حملات مستعد هستند. یک مهاجم یا حمله‌کننده می‌تواند یک حمله را در سه مرحله سازمان‌دهی نماید: مرحله جمع‌آوری اطلاعات، مرحله پردازش و استخراج اطلاعات و مرحله ارتباطات. بنابراین مهاجم سعی می‌کند تا خصوصیات و نقاط ضعف شبکه حسگر بی‌سیم را به‌وسیله مکان‌یابی گره چاهک، تحلیل ترافیک و غیره، شناسایی نماید. حملات شبکه‌های حسگر بی‌سیم به‌طور کامل در شکل (۲-۱۲) ارائه‌شده‌اند. در ادامه ما به معرفی مهم‌ترین حملات موجود در شبکه‌های حسگر بی‌سیم می‌پردازیم [۲] [۹] [۱۱]:



شکل (۲-۱۲) انواع حملات امنیتی بر روی شبکه‌های حسگر بی‌سیم [۹]

همان‌طور که در شکل (۲-۱۲) نشان داده‌شده، به‌طورکلی حملات شبکه‌های حسگر بی‌سیم در دو دسته اصلی زیر طبقه‌بندی می‌شوند:

حملات بر روی دسترس‌پذیری به شبکه: این حملات اغلب تحت عنوان حملات رد سرویس شناخته می‌شوند. هدف اصلی این حملات اختلال در سرویس‌دهی و از کار انداختن شبکه است.

حملات بر روی محرمانگی و صحت اعتبار: تکنیک‌های استاندارد رمزنگاری می‌تواند محرمانگی و صحت اعتبار کانال‌های ارتباطی را در برابر مهاجمان خارجی (مانند استراق سمع، حملات تکرار بسته و حملات تغییر و یا جعل بسته‌ها) حفظ نماید. در این حملات حفظ دسترس‌پذیری شبکه حسگر برای سرویس‌دهی خدماتش ضروری است.

۲-۲-۳-۱- حملات رد سرویس[1]

ساده‌ترین نوع حمله رد سرویس، برای تخلیه منابع موجود در یک گره ضعیف تلاش می‌کند. دشمن با ارسال بیش‌ازحد بسته‌های غیرضروری، از دسترسی کاربران مشروع شبکه به سرویس‌های موجود و یا منابعی که مستحق آن‌ها هستند، جلوگیری می‌کند. حملات رد سرویس، تنها به معنی تلاش دشمن برای خرابکاری، مختل کردن کار و یا تخریب شبکه نیست، بلکه منظور هر حادثه‌ای است که باعث تنزل و یا نقصان ظرفیت شبکه در تأمین یک سرویس می‌شود.

تاکنون سازوکارهای تدافعی زیادی برای مقابله با انواع مختلفی از این حملات ارائه‌شده است اما اغلب آن‌ها دارای سربار محاسباتی بالایی هستند و بنابراین برای استفاده در شبکه‌های حسگر بی‌سیم که دارای محدودیت منابع می‌باشند، مناسب نیستند. به دلیل اینکه حملات رد سرویس در شبکه حسگر بی‌سیم برخی اوقات هزینه بالایی را به سیستم تحمیل می‌کنند، محققان زمان زیادی را صرف نموده‌اند تا انواع مختلف این حملات را شناسایی کرده و راهکارهایی را برای مقابله و دفاع در برابر آن‌ها ابداع نمایند. در ادامه برخی از مهم‌ترین انواع حملات رد سرویس در شبکه‌های حسگر بی‌سیم موردبررسی قرارگرفته‌اند.

[1] Denial of Service Attack (DoS)

حملات لایه فیزیکی: با توجه به این‌که در شبکه‌های حسگر گره‌ها ممکن است در محیط‌های ناامن و متخاصم قرار گیرند، بنابراین مهاجمان می‌توانند به‌صورت فیزیکی به گره‌ها دسترسی داشته باشند. دو نوع از حملات در لایه فیزیکی عبارتند از حمله ایجاد پارازیت و حمله تداخل فیزیکی.

- **حمله ایجاد پارازیت**[1]: نوعی از حمله است که در آن با فرکانس رادیویی که گره‌ها برای ارتباطات در شبکه حسگر بکار می‌برند تداخل ایجاد می‌کند. یک منبع پارازیت ممکن است آن‌قدر قوی باشد که کل شبکه را مختل نماید. حتی با منابع پارازیت با قدرت کمتر نیز یک مهاجم پتانسیل آن را دارد که به‌وسیله استراتژی توزیع مناسب منابع پارازیت، ارتباطات در کل شبکه را تحت تأثیر قرار دهد. درصورتی‌که شبکه حسگر بی‌سیم به زمان‌بندی ارتباط پیامی حساس باشد، یک منبع پارازیت متناوب نیز ممکن است تا حدودی مخرب باشد.
- **حمله دست‌کاری فیزیکی**[2]: شبکه‌های حسگر اساساً در محیط‌های دور از دسترس بکار گرفته می‌شوند. بدون حفاظ بودن و توزیع‌شدگی گره‌ها در یک شبکه حسگر، آن را در معرض حملات فیزیکی قرار می‌دهد. این حملات ممکن است باعث خسارت‌های جبران‌ناپذیری در گره‌ها بشوند. یک مهاجم می‌تواند کلیدهای رمزنگاری را از گره تسخیرشده استخراج و مدارات آن را دست‌کاری کرده، کدهای برنامه را تغییر دهد و یا حتی گره‌ها را با حسگرهای معاند جایگزین نماید. نشان داده‌شده است که گره‌های حسگری مانند ذره میکا[3] در زمان کمتر از یک دقیقه می‌توانند مورد تسخیر قرار بگیرند.

حملات لایه پیوند: لایه پیوند داده مسئول سهمیه‌بندی جریان داده‌ها، تشخیص فریم‌های داده، کنترل دسترسی به رسانه ارتباطی و کنترل خطا است. حملات این لایه عبارتند از: برخورد، فرسودگی منابع و بی‌عدالتی در اختصاص منابع.

[1] Jamming Attack
[2] Tampering Attack
[3] Mica Mote2

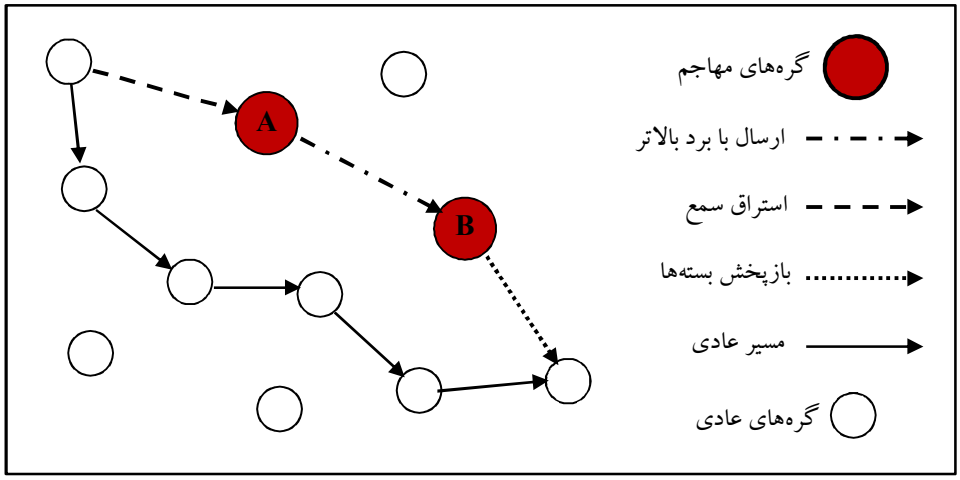
- **برخورد**[1]: تداخل یا برخورد زمانی رخ می‌دهد که دو گره به‌صورت هم‌زمان با فرکانس یکسانی اقدام به ارسال می‌نمایند. هنگامی‌که بسته‌ها با یکدیگر برخورد می‌کنند باید آن‌ها را حذف نموده و اقدام به ارسال مجدد آن‌ها نماییم. یک مهاجم ممکن است به‌صورت هدفمند باعث تداخل در بسته‌های خاصی مانند پیام‌های کنترلی ACK گردد. یکی از پیامدهای پرهزینه چنین تداخل‌هایی کاهش نمایی سرعت است. مهاجم به‌طور ساده ممکن است پروتکل ارتباطی را مختل نموده و به‌صورت پیاپی نیز پیام‌هایی را به جهت ایجاد تداخل ارسال نماید.
- **فرسودگی منابع**[2]: برخوردهای مکرر نیز می‌تواند توسط یک حمله‌کننده استفاده شود تا منجر به فرسودگی منابع گردد. برای مثال یک پیاده‌سازی ساده از لایه پیوند ممکن است به‌طور پیاپی اقدام به ارسال مجدد بسته‌های خراب‌شده نماید. اگر این ارسال‌های مجدد سریع کشف نشوند، سطح انرژی گره‌ها به‌سرعت تقلیل یافته و تمام می‌شود.
- **بی‌عدالتی در اختصاص منابع:** بی‌عدالتی یک شکل ضعیف از حمله رد سرویس است. یک مهاجم ممکن است با استفاده متناوب از حملات لایه پیوند ذکرشده در بالا باعث ایجاد بی‌عدالتی گردد. در این مورد مهاجم به‌وسیله قطع متناوب ارسال فریم‌ها، موجب تنزل اجرای کاربردهای بلادرنگ بر روی سایر گره‌ها می‌گردد.

حملات لایه شبکه: مهم‌ترین وظیفه لایه شبکه مسیریابی بسته‌ها در بین گره‌های شبکه است. بنابراین حملات این لایه به حملات مسیریابی نیز مشهور هستند و عبارتند از:

- **حمله کرم‌چاله**[3]: حمله کرم‌چاله، یک حمله بحرانی است به‌نحوی‌که حمله‌کننده بسته‌ها را در مکانی از شبکه ضبط می‌کند و از طریق تونل‌سازی آن‌ها را به مکان دیگری می‌برد. تونل سازی و یا ارسال مجدد بیت‌ها می‌تواند به‌صورت انتخابی انجام شود. این حمله یک تهدید مهم برای

[1] Collision
[2] Resource Exhaustion
[3] Wormhole

شبکه‌های بی‌سیم حسگر محسوب می‌شود، چون این حمله نیازی به سازش با حسگرها در شبکه ندارد و می‌تواند در زمانیکه حسگرها شروع به کشف اطلاعات همسایه می‌کنند، انجام گیرد. طرحواره این حمله در شکل ۲-۱۳ نشان داده‌شده است.

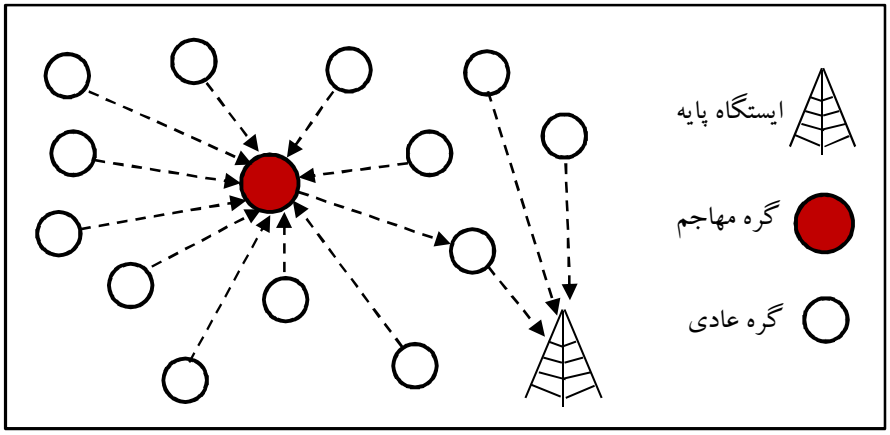


شکل (۲-۱۳) حمله کرم‌چاله [۲]

- **حمله سیاه‌چاله**[1] **(حفره چاهک**[2]**)**: در این حمله که در شکل (۲-۱۴) ارائه‌شده، گره مهاجم به‌گونه‌ای عمل می‌کند که برای همسایه‌هایش در مواردی چون پارامترهای مسیریابی (مانند توان ارسال بالاتر) جذاب بوده و یا به‌عنوان ایستگاه پایه به نظر برسد، بنابراین گره‌های همسایه در مسیریابی داده‌هایشان، بیشتر و بیشتر گره مهاجم را انتخاب می‌کنند. به این شکل این حمله یک چاهک دروغی را ایجاد کرده و بدون احراز هویت از داده‌های ارسالی بهره‌برداری می‌نماید و درنتیجه اطلاعات به ایستگاه پایه نرسیده و بنابراین به خدمات شبکه آسیب می‌رسد. به‌عبارت‌دیگر در این حمله یک گره مهاجم به‌عنوان یک حفره سیاه حمله می‌کند تا تمام ترافیک شبکه حسگر را جذب کند. حمله‌کننده به درخواست‌های روی مسیر گوش می‌دهد. سپس به گره‌های هدف به نحوی پاسخ می‌دهد که وانمود سازد دربرگیرنده کیفیت بالا و یا بهترین مسیر به سمت ایستگاه پایه است. این حمله به‌خصوص در پروتکل‌های ارتباطی اتصال گرا مبتنی بر ترافیک جریانی به‌طور مؤثری عمل می‌کند. چراکه کافی است تنها یک‌بار

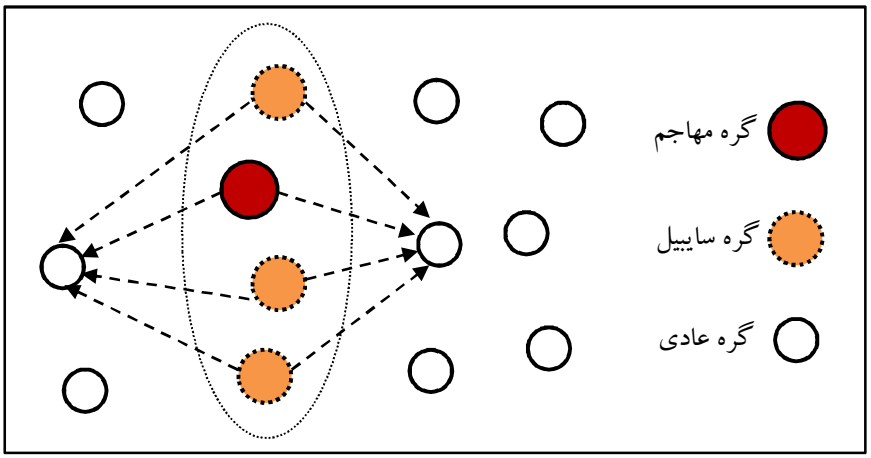
[1] Blackhole
[2] Sinkhole

گره مهاجم خود را بین گره‌هایی که باهم ارتباط دارند، مثل گره حسگر و چاهک، جای دهد و بعد تمام بسته‌های در حال عبور بین آن‌ها را در اختیار خود بگیرد.



شکل (۲-۱۴) حمله حفره چاهک [۱۱]

- **حمله سایبیل**[1]: حمله سایبیل به‌عنوان یکی از حملات مخرب در شبکه‌های حسگر بی‌سیم در مراجع زیادی موردتوجه محققان بوده است و به‌طور ساده به‌عنوان "یک وسیله مهاجم که به‌طور نامشروع و نادرست چندین شناسه می‌گیرد" تعریف می‌گردد. این حمله برای اولین بار بر روی شبکه‌های نظیر به نظیر معرفی گردید [۱۲]. این حمله می‌تواند آمار فراوانی و توزیع داده‌ها را در سیستم‌های ذخیره‌سازی توزیع‌شده مختل سازد. طرحواره این حمله در شکل ۲-۱۵ نشان داده‌شده است.



شکل (۲-۱۵) حمله سایبیل [۱۱]

[1] Sybil attack

نحوه عملکرد حمله سایبیل به این صورت است که یک گره مهاجم به‌طور غیرقانونی و با شیوه‌های مختلفی چندین شناسه را در شبکه حسگر بی‌سیم به خود اختصاص می‌دهد. در چنین شرایطی به گره مهاجم به همراه همه شناسه‌های تحت کنترل آن (که معمولاً چندین گره را شامل می‌شود) گره‌های سایبیل اطلاق می‌گردد. در ادامه گره مهاجم به همراه شناسه‌های در اختیار خود اقدام به تضعیف و تخریب عملکرد پروتکل‌های مختلف شبکه حسگر (مانند پروتکل توزیع داده‌ها، پروتکل مسیریابی و ...) کرده و از این طریق عملکرد شبکه را تحت تأثیر خود به‌شدت تنزل می‌دهد.

به جهت درک بهتر از پیامدهای حمله سایبیل و چگونگی دفاع در برابر آن در ابتدا باید انواع شیوه‌های مختلف آن را موردبررسی قرار دهیم. سه شیوه مختلف از حمله سایبیل عبارتند از: حمله مستقیم در برابر حمله غیرمستقیم، حمله مبتنی‌بر ساخت در برابر حمله مبتنی‌بر سرقت و حمله هم‌زمان در برابر حمله ناهم‌زمان. در ادامه به تشریح این شیوه‌ها می‌پردازیم.

حمله مستقیم در برابر حمله غیرمستقیم: در حمله مستقیم گره‌های سایبیل به‌طور مستقیم با گره‌های واقعی شبکه ارتباط برقرار می‌کنند درحالی‌که در حمله غیرمستقیم گره‌های سایبیل از طریق یک گره مهاجم با گره‌های واقعی شبکه ارتباط برقرار می‌نمایند.

حمله مبتنی‌بر ساخت در برابر حمله مبتنی بر سرقت: در حمله مبتنی‌بر ساخت، گره مهاجم با تکیه‌بر الگوی ساخت شناسه‌های مجاز گره‌ها در شبکه اقدام به ساخت شناسه‌های جدید غیرمجاز می‌نماید. برای مثال اگر هر گره به‌وسیله یک عدد صحیح ۳۲ بیتی شناخته می‌شود، گره مهاجم می‌تواند به‌سادگی و به‌صورت تصادفی به هر گره سایبیل یک شناسه صحیح ۳۲ بیتی اختصاص دهد. درصورتی‌که یک مکانیسم تشخیص برای شناسه گره‌های مجاز در شبکه وجود داشته باشد، امکان ساخت شناسه‌های جدید از مهاجم سلب می‌گردد. برای مثال فرض کنید فضای نام شناسه‌ها به‌صورت هدفمند محدودشده باشد تا از درج شناسه‌های جدید توسط مهاجمین جلوگیری شود.

در حمله مبتنی بر سرقت گره مهاجم شناسه‌های مجاز (شناسه گره‌های واقعی) موجود در شبکه را به گره‌های سایبیل اختصاص می‌دهد. در این حالت اگر مهاجم گره‌های جعلی را از بین ببرد و یا موقتی آن‌ها را غیرفعال نماید احتمال عدم‌تشخیص آن وجود دارد.

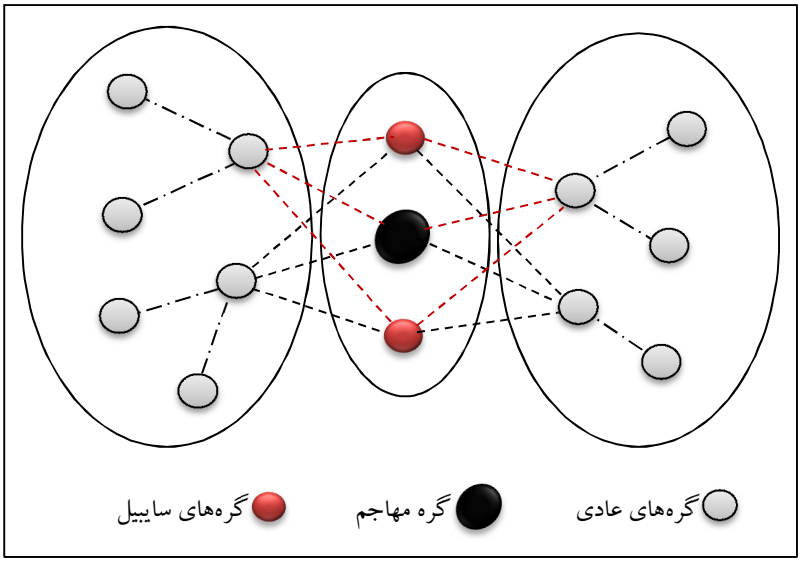
حمله هم‌زمان در برابر حمله ناهم‌زمان: در حمله هم‌زمان، همه شناسه‌های سایبیل در یک‌زمان در شبکه فعال بوده و به‌صورت هم‌زمان در عملیات حمله شرکت می‌نمایند. ازآنجایی‌که هر گره در هرلحظه فقط با یک شناسه می‌تواند فعالیت کند، گره مهاجم می‌تواند با استفاده حلقه-وار از این شناسه‌های سایبیل، تصور حضور هم‌زمان همه آن‌ها را در شبکه القا نماید. در حالت ناهم‌زمان، گره مهاجم ممکن است تعداد زیادی از شناسه‌ها را تحت یک پریود زمانی استفاده نماید به‌گونه‌ای که در هر زمان مشخصی فقط تعداد کمی از شناسه‌ها فعال باشند. گره مهاجم می‌تواند این کار را از طریق القای تصور خروج یک شناسه از شبکه و پیوستن یک شناسه دیگر به آن انجام دهد. در این شرایط یک شناسه خاص ممکن است چندین بار شبکه را ترک کرده و دوباره به آن ملحق شود و یا مهاجم ممکن است هر شناسه را فقط یک بار استفاده کند.

یک امکان دیگر به این صورت است که مهاجم بتواند چندین گره فیزیکی مجزا در شبکه داشته باشد و همچنین در آن‌ها بتواند شناسه‌ها را تعویض نماید. در این حالت تعداد شناسه‌هایی را که مهاجم استفاده می‌کند برابر است با تعداد گره‌های سایبیل موجود، به‌گونه‌ای که هر گره در زمان‌های مختلف شناسه‌های متفاوتی را بکار می‌برد.

یک حمله سایبیل با استفاده از شناسه‌های در اختیارش می‌تواند پروتکل‌های مختلف شبکه حسگر را دچار مشکل نماید. در ادامه انواع پروتکل‌های شبکه حسگر که از طریق حمله سایبیل موردحمله قرار می‌گیرند را به همراه چگونگی طرح‌ریزی عملیات آن موردبررسی و تشریح قرار می‌دهیم.

- **پروتکل ذخیره‌سازی توزیع‌شده:** این حمله با تکیه‌بر گره‌های سایبیل تحت کنترل خود، بر روی معماری ذخیره‌سازی داده‌ها در شبکه تأثیر گذاشته و سازوکار تکثیر داده‌ها و ذخیره توزیع‌شده آن‌ها را در شبکه با شکست مواجه می‌کند.

- **پروتکل مسیریابی:** حمله سایبیل تهدیدی برای سازوکار مسیریابی در شبکه‌های حسگر است [۱۳]. حمله سایبیل با تکیه‌بر گره‌های سایبیل تحت کنترل خود، چندین مسیر جعلی را بین گره‌های شبکه ایجاد کرده و این‌گونه عملکرد پروتکل مسیریابی را در شبکه مختل می‌نماید. این امر در شکل ۲-۱۶ نشان داده‌شده است.
- **پروتکل تجمیع داده‌ها:** به جهت صرفه‌جویی در مصرف انرژی، پروتکل‌های پرس‌وجوی مؤثری برای تجمیع داده‌ها ارائه‌شده‌اند که اطلاعات خوانده‌شده توسط حسگرهای مختلف را با انجام محاسباتی تجمیع می‌نمایند [۱۴]. حمله سایبیل می‌تواند با ارائه داده‌های نادرست توسط گره‌های سایبیل تحت کنترل خود، عملکرد این پروتکل را دچار مشکل نماید.



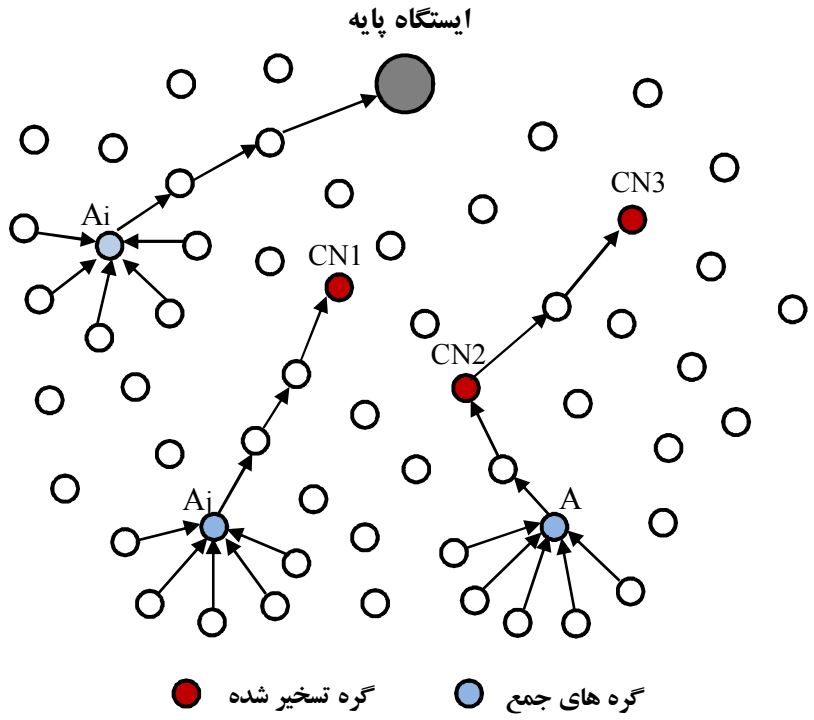
شکل (۲-۱۶): حمله سایبیل به پروتکل مسیریابی

- **پروتکل رأی‌گیری:** در شبکه حسگر بی‌سیم برای برخی از فرایندها لازم است عملیات رأی‌گیری انجام گیرد. برای مثال فرایند انتخاب سرخوشه‌ها در هر بازه زمانی مشخص و یا فرایند تصمیم‌گیری درباره وضعیت ناهنجاری در یک گره مجاز شبکه، معمولاً از طریق عملیات رأی‌گیری در گره‌های شبکه انجام می‌شود. یک حمله سایبیل به‌راحتی و با تکیه‌بر گره‌های سایبیل تحت کنترل خود می‌تواند در نتایج رأی‌گیری تأثیر گذاشته و آن را به نفع خود تغییر دهد.

- **پروتکل تشخیص ناهنجاری:** روال برخی از سیستم‌های تشخیص ناهنجاری در شبکه به این صورت است که هشدارهای رسیده از گره‌های مختلف را مبنی بر وجود ناهنجاری در گره مشخص را ارزیابی کرده و در صورت تجاوز از حد آستانه آن گره را به‌عنوان مهاجم شناخته و آن را از شبکه حذف می‌کند. حمله سایبیل با ایجاد چند هشدار توسط گره‌های سایبیل تحت کنترل خود می‌تواند گره‌های مجاز شبکه را به‌عنوان گره مهاجم معرفی کرده و موجبات حذف آن را از شبکه فراهم کرده و متعاقباً طول‌عمر شبکه را کاهش دهد.
- **پروتکل تخصیص عادلانه منابع:** برخی از منابع شبکه ممکن است بر اساس نیاز گره‌ها به‌صورت عادلانه بین آن‌ها تخصیص داده شوند. برای مثال گره‌های نزدیک به هم در شبکه از یک کانال رادیویی یکسان برای ارسال و دریافت داده‌ها به‌صورت اشتراکی در طول زمان استفاده می‌کنند. حمله سایبیل با کمک شناسه‌های مختلف در اختیار خود می‌تواند روی تخصیص منابع شبکه تأثیر گذاشته و با مصرف طولانی‌مدت آن موجب تحلیل منابع شبکه شده و همچنین باعث عدم سرویس‌دهی مناسب به گره‌های مجاز شبکه شود.
- **حمله ارسال انتخابی**[1]: شبکه‌های چند گام بر مبنای این فرض کار می‌کنند که گره‌های شرکت‌کننده میانی در مسیریابی، پیام‌های دریافت شده را به‌صورت کامل و دست‌نخورده به گره بعدی ارسال می‌کنند. در یک حمله ارسال انتخابی، گره‌های غیرمجاز ممکن است پیام‌های خاص را به گره بعدی ارسال نکنند و آن‌ها را حذف کنند تا مطمئن شوند که این پیام‌ها درهرصورت انتشار نخواهند یافت. یک شکل ساده از این حمله بدین‌صورت است که گره غیرمجاز به‌عنوان یک سیاه‌چاله عمل می‌کند و هر بسته‌ای را که به آن می‌رسد به گره بعدی ارسال نمی‌کند و آن‌ها حذف می‌کند. اگر یک نفوذگر از طرف گره‌های همسایه‌اش تهدید شود و نتیجه بگیرد که دارد از مسیر حذف می‌شود، تصمیم می‌گیرد که یک مسیر دیگر را جستجو کند. یک فرم خیلی زیرکانه از این حمله زمانی است که یک نفوذگر به‌طور انتخابی بسته‌ها را

[1] Select forwarding

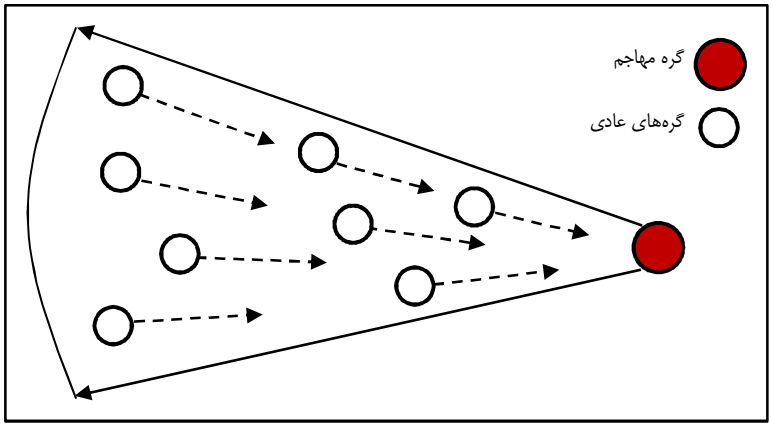
ارسال می‌کند. یک نفوذگر تمایل دارد که بسته‌های منتشرشده از تعدادی گره‌های خاص را حذف یا تغییر دهد و بقیه بسته‌ها را به شکل صحیح ارسال کند و با این کار باعث شود که بدگمانی و سوءظن نسبت به کارهای غیرمجازش کاهش یابد. طرحواره این حمله در شکل ۲-۱۷ نشان داده‌شده است.



شکل (۲-۱۷) حمله ارسال انتخابی [۱۱]

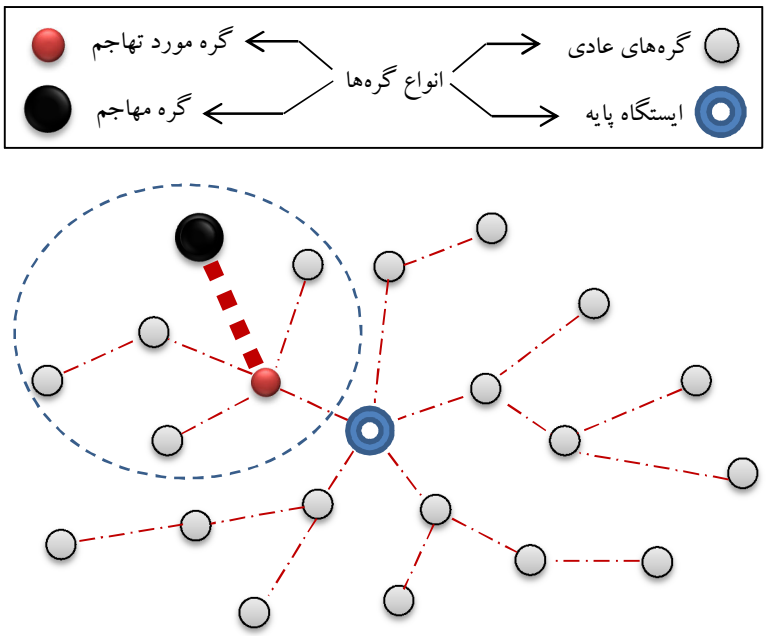
- **حمله سیل پیام Hello**[1]: این حمله از بسته‌های Hello به‌عنوان یک سلاح برای قانع کردن حسگرها در شبکه‌های بی‌سیم استفاده می‌کند. در این نوع حمله، حمله‌کننده با توانی بالا بسته‌های Hello را به تعدادی از گره‌های حسگر که در ناحیه وسیعی از محدوده شبکه بی‌سیم حسگر پخش‌شده‌اند، ارسال می‌کند. بدین ترتیب، حسگرها متقاعد می‌شوند که دشمن همسایه آن‌هاست. درنتیجه در زمان ارسال اطلاعات به ایستگاه پایه، گره‌های ضعیف سعی می‌کنند تا با حمله‌کننده کار کنند، به این دلیل که حمله‌کننده را همسایه خود می‌دانند و سرانجام توسط مهاجم از بین می‌روند. طرحواره این حمله در شکل ۲-۱۸ نشان داده‌شده است.

[1] Hello Flood Attack



شکل (۲-۱۸) حمله سیل پیام Hello [۲]

- **حمله رد سرویس:** حمله رد سرویس به‌عنوان یکی از رایج‌ترین حملات در شبکه‌های حسگر بی‌سیم در مراجع زیادی [۱۸-۱۵] موردتوجه محققان بوده است. نحوه عملکرد آن به این صورت است که گره مهاجم که معمولاً گره‌ای با قدرت و انرژی بالا است، با سرعت خیلی زیاد بسته‌های داده را در شبکه به گره‌های دیگر ارسال می‌نماید. این کار موجب می‌گردد که گره-های موردتهاجم، به دلیل حجم بالای پیام‌های رسیده از گره مهاجم، درگیر این امر شده و عملاً از سرویس‌دهی به بقیه گره‌های شبکه و انجام وظایف دیگر خود بازبمانند.



شکل (۲-۱۹): حمله رد سرویس

همان‌طور که در شکل ۲-۱۹ مشاهده می‌گردد، گره مهاجم با ارسال سیلی از پیام‌ها به سمت گره هدف، باعث می‌شود گره موردتهاجم امکان سرویس‌دهی به گره‌های دیگر شبکه را نداشته باشد و درنتیجه کار کل خوشه مشخص‌شده به‌طور کامل مختل می‌گردد. گاهی اوقات این حمله با تهاجم به چندین گره مهم در شبکه حتی می‌تواند کار کل شبکه را نیز مختل نماید.

- **حمله استراق سمع، تغییر و تکرار اطلاعات مسیریابی:** رایج‌ترین حمله مستقیم علیه یک پروتکل مسیریابی، هدف قرار دادن اطلاعات مسیریابی است که بین گره‌ها مبادله می‌شود. به‌وسیله استراق سمع، تغییر، یا تکرار اطلاعات مسیریابی، نفوذگران می‌توانند باعث ایجاد حلقه‌های مسیریابی، ایجاد پیام‌های خطای اشتباه، تقسیم‌بندی شبکه، افزایش تأخیر انتها به انتها، افزایش یا کوتاه کردن مسیرهای منبع و غیره، بشوند.

حملات لایه انتقال: حملاتی که بر روی لایه انتقال داده‌ها در شبکه‌های حسگر بی‌سیم می‌توانند طرح‌ریزی شوند عبارتند از: حمله سیل‌آسا و حمله عدم هم‌زمانی.

- **حمله سیل‌آسا:** هر وقت پروتکلی برای حفظ وضعیت دو انتهای یک اتصال موردنیاز باشد، در این حالت برای مصرف بی‌رویه حافظه توسط حمله سیل‌آسا مستعد می‌گردد. یک مهاجم ممکن است به‌طور مکرر درخواست‌های اتصال جدیدی ایجاد نماید تا جایی که منابع موجود به‌وسیله همه اتصالات ایجادشده به اتمام رسیده و یا به یک حد بیشینه برسند. در چنین شرایطی، بیشتر درخواست‌های قانونی و معمول به علت عدم وجود منابع کافی، رد خواهند شد.
- **حمله عدم هم‌زمانی**[1]: این حمله به تخریب یک اتصال موجود می‌پردازد. یک مهاجم ممکن است به‌صورت پیاپی پیام‌های ارسالی به یک میزبان را تغییر دهد و باعث شود تا آن درخواست ارسال مجدد بسته‌های گم‌شده را بنماید. اگر به‌موقع این حمله کشف نگردد، یک مهاجم ممکن است توانایی میزبان‌ها را برای مبادله موفقیت‌آمیز داده‌ها از بین ببرد یا تنزل دهد، زیرا آن‌ها انرژی زیادی را صرف می‌کنند تا خطاهایی را رفع کنند که هرگز وجود نداشته‌اند.

[1] De-synchronization

۲-۲-۳-۲- حملات روی محرمانگی و صحت اعتبار

با توجه به اینکه در شبکه‌های حسگر بی‌سیم حجم وسیعی از اطلاعات به‌آسانی در دسترسی از راه دور قرار می‌گیرند، بنابراین مسئله محرمانگی اطلاعات در این شبکه‌ها حساس‌تر از شبکه‌های دیگر است. انواع مختلفی از حملات تحت این دسته در ادامه موردبررسی قرارگرفته‌اند.

حمله تکثیر گره[1]: در یک حمله تکثیر گره، یک مهاجم برای افزودن یک گره به شبکه حسگر بی‌سیم موجود از طریق تکثیر (مثلاً کپی‌برداری) شناسه گره از روی یک گره‌ای که قبلاً در شبکه موجود بوده، تلاش می‌نماید. یک گره تکثیرشده و ملحق شده به شبکه با این روش می‌تواند به‌طور بالقوه باعث تخریب شدید در ارتباط پیامی به‌وسیله منحرف کردن و هدایت بسته‌ها در مسیرهای نادرست در شبکه حسگر بی‌سیم گردد.

حملات بر روی محرمانگی: در زیر برخی حملاتی که بر روی محرمانگی انجام می‌شوند ارائه‌شده‌اند:

- **استراق سمع و نظارت غیرفعال**[2]: این حمله مرسوم‌ترین و آسان‌ترین شکل حمله بر روی اطلاعات محرمانه است. درصورتی‌که پیام‌ها به‌وسیله تکنیک‌های پنهان نگاری محافظت نشده باشند، مهاجم به‌راحتی می‌تواند به محتوی آن‌ها پی ببرد. بسته‌های حاوی اطلاعات کنترلی در یک شبکه حسگر بی‌سیم اطلاعات بیشتری را از مکان‌های قابل‌دسترس به خدمات ارائه می‌نمایند، ازین رو استراق سمع بر روی چنین پیام‌هایی برای یک مهاجم مؤثرتر واقع می‌گردد.
- **تحلیل ترافیک:** به‌منظور سازمان‌دهی یک حمله مؤثر بر روی اطلاعات محرمانه، عملیات استراق سمع باید با عمل تحلیل ترافیک ادغام گردد. از طریق یک عملیات مؤثر تحلیل ترافیک، یک مهاجم می‌تواند برخی از گره‌ها با وظایف و فعالیت‌های خاص را در شبکه حسگر بی‌سیم شناسایی نماید. برای مثال یک افزایش ناگهانی در پیام‌های ارتباطی بین گره‌های معینی، نشان می‌دهد که آن گره‌ها دارای فعالیت‌ها و رویدادهای خاصی برای بهره‌برداری هستند. دانگ و

[1] node replication attack
[2] Eavesdropping and passive monitoring

همکاران دو نوع از حملاتی را تشریح نمودند که می‌توانند ایستگاه پایه را در شبکه حسگر بی‌سیم، بدون حتی نادیده گرفتن اطلاعات ناچیز در محتوی بسته‌های جستجو شده در یک تحلیل ترافیک، شناسایی نمایند [۱۹].

۲-۲-۴. معرفی محدودیت‌های مهاجمان و هکرها

در طراحی یک سیستم امنیتی مناسب برای شبکه‌های حسگر بی‌سیم، علاوه بر شناسایی دقیق حملات مختلف و تحلیل رفتار آن‌ها، می‌بایست محدودیت‌های مربوط به مهاجمان و هکرها را نیز معرفی کرده و در نظر بگیریم. این محدودیت‌ها در ذیل ارائه شده‌اند:

۱. عدم آگاهی هکر به حساسیت‌ها و ویژگی‌های سیستم موجود مانند حدود آستانه، نرخ ارتباطات، نرخ ثبت وقایع توسط حسگرها، نوع داده‌ها و ...
۲. عدم آگاهی هکر از گستره شبکه موجود و نحوه توزیع گره‌ها در محیط و چگالی توزیع آن‌ها
۳. عدم آگاهی هکر از فعالیت‌ها و عملیات موجود در گزه‌ها و شبکه مربوطه
۴. عدم اطلاع و دسترسی هکر به ویژگی‌های امنیتی شبکه حسگر و گره‌های موجود در آن مانند وجود روش‌های امنیتی پیشگیرانه به عنوان اولین خط تدافعی در برابر حملات
۵. عدم اطلاع از رمزگذاری پیام‌ها و نحوه آن و عدم دسترسی به کلیدهای امنیتی و ...

۲-۲-۵. تبیین نحوه شبیه‌سازی حملات لایه شبکه و مسیریابی

در بخش ۲-۸ نحوه شبیه‌سازی شبکه حسگر بی‌سیم مطلوب خود را همراه با پارامترهای کاملی معرفی کردیم. مرحله دوم شبیه‌سازی انواع حملات مفروض برای ارزیابی روش تشخیص نفوذ پیشنهادی است. در حقیقت ما برای شبیه‌سازی‌ها و ارائه نتایج روش پیشنهادی، نیازمند مجموعه‌ای از حملات به‌عنوان مجموعه دادگان هستیم که قبلاً در بخش‌های قبلی آن‌ها را تشریح نمودیم. مهم‌ترین حملاتی که در این مورد نیازمند آن‌ها هستیم حملات لایه شبکه و مسیریابی هستند که بیشترین

استفاده را در حملات و مهاجمان به‌خود اختصاص می‌دهند و بسیاری از مراجع نیز در طرح‌های پیشنهادی خود برروی آن‌ها متمرکزشده‌اند. این حملات که در بخش قبلی تشریح شده‌اند، عبارتند از:

- حمله رد سرویس
- حمله کرم‌چاله
- حمله حفره چاهک
- حمله سایبیل
- حمله ارسال انتخابی
- حمله سیل ارسال سلام

به جهت ارزیابی روش تشخیص نفوذ پیشنهادی ابتدا باید حملات مطرح‌شده در بالا را شبیه‌سازی نماییم. مثلاً برای شبیه‌سازی حمله ارسال انتخابی باید یک یا چند گره در شبکه به‌عنوان گره مهاجم در نظر گرفته شوند به‌گونه‌ای که پیام‌های دریافتی از گره‌های حقیقی شبکه را به‌صورت تصادفی و یا انتخابی به گره‌های دیگر شبکه ارسال نمایند. در شکل‌های (۲-۲۰) و (۲-۲۱) نمونه‌های مختلفی از سناریوهای حمله ارسال انتخابی ارائه‌شده است.

a

```
Receive(Packet,Source-Node);
Random-generate(X,1,10);
If(X<=5) Then
    Drop(Packet);
Else
    Send(Packet, Destination_Node);
```

(b

```
Receive(Packet,Source-Node);
Random-generate(X,1,10);
If(X<=3) Then
    Drop(Packet);
Else
    Send(Packet, Destination_Node);
```

شکل (۲-۲۰) نمونه کد حمله ارسال انتخابی a) با احتمال حذف ۵۰٪ و b) احتمال حذف ۳۰٪ بسته‌ها

a

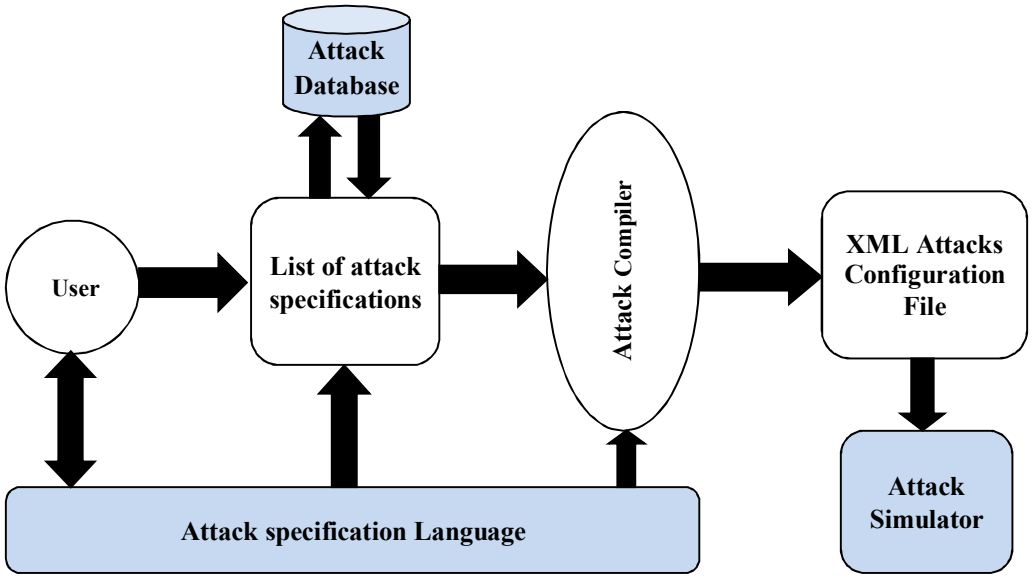
```
Receive(Packet,Source-Node);
If(Time>=200 && Time<= 400) Then
    Drop(Packet);
Else
    Send(Packet, Destination_Node);
```

b

```
Receive(Packet,Source-Node);
If(Source-Node IN Filter-List) Then
    Drop(Packet);
Else
    Send(Packet, Destination_Node);
```

شکل (۲-۲۱) کد حمله ارسال انتخابی a) با حذف زمانی بسته‌ها b) حذف بسته‌ها بر اساس گره‌های خاص

همچنین در شکل ۲-۲۲ یک قالب و چهارچوب[1] برای شبیه‌سازی حملات در شبکه‌های حسگر بی-سیم ارائه‌شده است:



شکل (۲-۲۲) معماری چهارچوب شبیه‌سازی حملات در شبکه‌های حسگر بی‌سیم [۲۰]

در این قالب، تعریف حملات مختلف با استفاده از یک زبان توصیف حمله[2] که مجموعه‌ای از توابع اولیه و پیش‌ساخته می‌باشد امکان‌پذیر است. ازنظر معماری، یک حمله به‌عنوان یک دنباله از رویدادها[3] تعریف می‌گردد که به‌صورت اتمیک[4] و مجزا رخ می‌دهند. بنابراین یک کاربر با تکیه‌بر توابع موجود در زبان توصیف حملات می‌تواند با تعریف دنباله‌ای از رویدادها یک حمله خاص را ایجاد نماید.

درنهایت با توجه به موارد فوق و همچنین با توجه به این‌که حملات لایه شبکه با ایجاد اختلال در فرایند مسیریابی، شبکه حسگر بی‌سیم را دچار مشکل می‌کنند، با ایجاد تغییراتی در پروتکل مسیریابی گره‌های مهاجم که در نرم‌افزار شبیه‌سازی NS2 در فایل‌های AODV.h و AODV.cc قرار دارند، عملکرد مربوط به آن‌ها را می‌توانیم شبیه‌سازی نماییم [۲۱]، [۲۲].

[1] Attack Simulation Framework (ASF)
[2] Attack Specification Language (ASL)
[3] Events
[4] Atomical

۲-۲-۶. سازوکارهای امنیتی

به‌طورکلی سازوکارهای تأمین امنیت در شبکه‌های حسگر بی‌سیم به شش دسته اصلی زیر تقسیم می‌شوند [۹]، [۱۰] و [۲۳]:

- پنهان‌نگاری[۱]
- مدیریت کلید[۲]
- مسیریابی امن[۳]
- ترکیب داده امن[۴]
- مدیریت اطمینان[۵]
- تشخیص نفوذ[۶]

در زیر به‌طور مختصر به تشریح هر یک از سازوکارها می‌پردازیم:

پنهان نگاری: پنهان نگاری در حقیقت روشی است که از طریق آن داده‌های تبادلی بین گره‌های حسگر قابل‌شناسایی توسط گره‌های مهاجم و حمله‌کننده‌ها نباشند. برحسب کاربردهای متفاوت روش‌های مختلفی برای پنهان نگاری ارائه‌شده است. انتخاب مناسب‌ترین روش پنهان نگاری در شبکه‌های حسگر بی‌سیم امری حیاتی است زیرا همه سرویس‌های امنیتی به‌وسیله پنهان نگاری از حصول امنیت مطمئن می‌شوند. تکنیک‌های پنهان نگاری‌ای که در شبکه‌های حسگر بی‌سیم بکار می‌روند باید محدودیت‌های گره‌های حسگر را برآورده کرده و ازلحاظ طول کد، حجم داده‌ها، زمان پردازش و توان مصرفی مناسب باشند. دو روش اساسی در پنهان نگاری بر روی شبکه‌های حسگر بی‌سیم عبارتند از:

[1] Cryptography
[2] Key management
[3] Secure routing
[4] Secure data aggregation
[5] Trust management
[6] Intrusion detection

- پنهان نگاری با کلید عمومی: بسیاری از محققان معتقدند که تکنیک‌های کلید عمومی به دلیل طول کد، حجم داده‌ها، زمان پردازشی و توان مصرفی‌شان، برای استفاده در شبکه‌های حسگر بی‌سیم نامناسب هستند.
- پنهان نگاری با کلید متقارن: محدودیت‌های محاسباتی و مصرف انرژی در گره‌های حسگر، به‌کارگیری پنهان نگاری با کلید عمومی را در شبکه‌های حسگر با مشکل مواجه می‌نماید. بنابراین در شبکه‌های حسگر بی‌سیم اغلب مطالعات پژوهشی بر روی پنهان نگاری با کلید متقارن معطوف شده است.

پروتکل‌های مدیریت کلید: مدیریت کلید به‌عنوان یک سازوکار محوری برای اطمینان از امنیت سرویس‌های شبکه و کاربردهای آن در شبکه‌های حسگر بی‌سیم مطرح است. هدف مدیریت کلید ایجاد و تصدیق کلیدهای موردنیاز در هنگام مبادله داده‌ها در بین گره‌های حسگر می‌باشد. بعلاوه یک طرح مدیریت کلید باید در حین کار کردن در محیط‌هایی با آرایش و چیدمان از پیش تعریف‌نشده، درج و حذف پویای گره‌های حسگر را نیز در شبکه پشتیبانی نماید. به دلیل محدودیت‌های گره‌های حسگر، راهکارهای مدیریت کلید در شبکه‌های حسگر بی‌سیم تفاوت‌های زیادی با روش‌های شبکه‌های معمولی دارند. همان‌طور که در بالا ذکر شد، پنهان نگاری با کلید عمومی محدودیت‌های موجود در شبکه حسگر بی‌سیم را تحمل نمی‌کند. بنابراین اغلب طرح‌های پیشنهادی برای مدیریت کلید مبتنی بر پنهان نگاری با کلید متقارن هستند. ولی استفاده از روش اشتراک صریح زوج کلید خصوصی در بین هر جفت از گره‌ها در شبکه حسگر بی‌سیم غیرعملی است. چراکه این روش نیازمند توزیع و ذخیره‌سازی n کلید در هر گره است که در آن n تعداد گره‌ها در شبکه حسگر را نشان می-دهد. روش‌های زوج کلیدی زمانی که اندازه شبکه بزرگ باشد به دلیل حجم زیاد حافظه موردنیاز در هر گره، مناسب نیستند. بعلاوه اغلب زوج کلیدها نیز بلااستفاده خواهند بود زیرا ارتباطات مستقیم فقط در بین گره‌های همسایه ممکن است. همچنین این روش‌ها برای درج و حذف پویای گره‌ها در

شبکه انعطاف‌پذیر نیستند. بنابراین با توجه به محدودیت‌های موجود در شبکه حسگر باید پروتکل‌های مناسبی برای مدیریت کلید در این شبکه‌ها ارائه گردد.

مسیریابی امن: پروتکل‌های مسیریابی زیادی به‌طور خاص برای شبکه‌های حسگر بی‌سیم طراحی‌شده‌اند. این پروتکل‌های مسیریابی بر طبق ساختار شبکه می‌توانند در سه دسته تقسیم‌بندی شوند: مسیریابی مسطح، مسیریابی سلسله مراتبی و مسیریابی مبتنی بر مکان. در مسیریابی مسطح، نوعاً همه گره‌ها دارای نقش یا عملکرد یکسانی هستند. در مسیریابی سلسله مراتبی، گره‌ها نقش‌های متفاوتی را در شبکه اجراء می‌کنند. در مسیریابی مبتنی بر مکان، از موقعیت‌های مکانی گره‌های حسگر برای مسیریابی داده‌ها در شبکه استفاده می‌گردد. اگرچه در مقالات پروتکل‌های مسیریابی زیادی برای شبکه‌های حسگر پیشنهادشده‌اند، اما تعداد کمی از آن‌ها با اهداف امنیتی طراحی‌شده‌اند. فقدان سرویس‌های امنیتی در پروتکل‌های مسیریابی، شبکه‌های حسگر بی‌سیم را برای انواع زیادی از حملات مستعد کرده است. اغلب حملات لایه شبکه که قبلاً در بخش ۲-۲-۳ تشریح شده‌اند، به‌عنوان حملات مسیریابی در شبکه حسگر بی‌سیم مطرح هستند. بنابراین با طراحی پروتکل‌های مؤثر مسیریابی امن در شبکه‌های حسگر بی‌سیم می‌توان تا حدودی تأثیر حملات فوق را در شبکه کاهش داد.

ترکیب امن داده‌ها: ارتباطات و انتقال داده‌ها بخش مهمی از کل انرژی مصرفی را در شبکه حسگر به خود اختصاص می‌دهند. بنابراین ترکیب داده‌ها می‌تواند به‌طور قابل‌ملاحظه‌ای به ذخیره و حفظ انرژی محدود گره‌های حسگر و منابع انرژی از طریق حذف داده‌های اضافی کمک نماید. برای مثال یک سیستم ممکن است میانگین دمای هوای یک ناحیه جغرافیایی را محاسبه نموده، مقادیر حسگرها را برای محاسبه مکان و سرعت یک شئ متحرک ادغام نماید و یا داده‌ها را برای جلوگیری از تولید هشدارهای اشتباه در تشخیص رویدادهای طبیعی با هم ترکیب نماید. بسته به معماری شبکه حسگر بی‌سیم، ترکیب داده‌ها ممکن است در مکان‌های مختلفی از شبکه انجام پذیرد. با توجه به اهمیت

بالای عملیات ترکیب داده‌ها به دلیل تشخیص و حذف داده‌های اضافی، باید امنیت همه مکان‌های ترکیب داده‌ها و گره‌هایی که برای این منظور در نظر گرفته‌شده‌اند، برآورده و تضمین گردد.

مدیریت اعتماد: کاربرد چارچوب‌های مبتنی بر اعتماد به جهت ایجاد سطح بالایی از امنیت در شبکه‌های حسگر بی‌سیم، شیوه دیگری برای تأمین امنیت در این شبکه‌ها است. درواقع طرح‌های مبتنی بر اعتماد می‌توانند در برابر حملاتی که فراتر از توانایی‌ها و سطوح امنیتی پنهان نگاری هستند، شبکه را محافظت نمایند. برای مثال موضوعاتی مانند کنترل کیفیت و قابلیت اطمینان گره‌های حسگر و لینک‌های ارتباطی شبکه، قابلیت اطمینان در ترکیب داده‌ها و بررسی صحت گره‌های ادغام داده‌ها و غیره می‌توانند به‌طور مؤثری با یک روش باقاعده و با کمک یک قالب مبتنی بر اعتماد نشان داده شوند. بااین‌وجود مدل‌های مبتنی بر اعتماد معمولاً سربار محاسباتی بالایی دارند و ایجاد یک طرح مؤثر با توجه به محدودیت منابع موجود در شبکه‌های حسگر بی‌سیم یک فرایند بسیار چالشی است.

تشخیص نفوذ: در یک شبکه یا یک سیستم، هر نوعی از فعالیت‌های غیرمجاز و نامطلوب، نفوذ نامیده می‌شوند. یک سیستم تشخیص نفوذ یک مجموعه از ابزار، روش‌ها و منابع برای کمک به شناسایی، ارزیابی و گزارش نفوذها است. سیستم‌های تشخیص نفوذ به جهت شناسایی و آشکارسازی نفوذها (قبل از این‌که آن‌ها بتوانند منابع سیستم و اطلاعات امنیتی را فاش نمایند) طراحی‌شده‌اند.

ما با توجه به تحقیقات و بررسی‌هایمان بر روی مقالات مختلف و مقایسه روش‌های فوق بر آن شدیم تا بر روی سازوکارهای تشخیص نفوذ کارمان را ادامه دهیم. در ادامه ما به‌طور کامل بر روی سیستم‌های تشخیص نفوذ و راهکارهای پیشنهادشده در این زمینه خواهیم پرداخت.

۲-۳- تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

امنیت در شبکه‌های حسگر بی‌سیم یک موضوع مهم است. به‌ویژه اگر این شبکه‌ها شامل فرایندهایی با عملیات بحرانی باشند. برای مثال اطلاعات محرمانه درباره سلامتی یک بیمار نباید برای بیماران دیگر فاش گردد. شبکه‌های حسگر بی‌سیم امن در کاربردهای نظامی (تاکتیکی) دارای اهمیت بحرانی و حساسی هستند، به‌گونه‌ای که یک شکاف امنیتی در شبکه می‌تواند باعث تحریک و تضعیف نیروهای خودی در میدان جنگ گردد.

همان‌طور که در فصل قبل بیان گردید، انواع حملات متنوعی نسبت به شبکه‌های حسگر بی‌سیم وجود دارند که امنیت این شبکه‌ها را به مخاطره می‌اندازند. راه‌حل‌هایی برای تأمین امنیت شبکه‌های حسگر بی‌سیم در مقابل این حملات ارائه‌شده‌اند که در سه مرحله اصلی دسته‌بندی می‌شوند که عبارتند از [۲۴]:

- **مرحله پیشگیری**[1] (دفاع در مقابل حملات): هدف این مرحله جلوگیری و پیشگیری از هر حمله‌ای قبل از وقوع آن است. بنابراین هر روش پیشنهادی در این گام باید در مقابل حملات موردبحث قابلیت تدافعی داشته باشد. به جهت پیشگیری از نفوذ و حملات، پروتکل‌های مسیریابی[1] مختلفی مانند SAR[۱۷]، SPINS[۲۵]، UDSR[۲۶] و S-LEACH[۲۷] برای شبکه‌های حسگر بی‌سیم ارائه‌شده که همه آن‌ها محدودیت‌هایی را به جهت افزایش امنیت، به شبکه اعمال می‌کنند. بنابراین با توجه به‌احتمال بسیار پایین انجام حمله، در شرایطی که حمله‌ای وجود نداشته باشد مصرف انرژی شبکه را افزایش خواهند داد.
- **مرحله تشخیص**[2] (اطلاع از یک حمله مفروض که در حال حاضر فعال است): درصورتی‌که یک مهاجم با مدیریت مطلوب بتواند از مرحله پیشگیری عبور نماید، این امر به مفهوم وجود ایراد دفاعی در مقابله با حمله است. در این زمان، راه‌حل برقراری امنیت در شبکه حسگر بی-

[1] Prevention
[2] Detection

سیم، سوئیچ فوری به مرحله تشخیص حمله در حال پیشرفت و به‌ویژه شناسایی گره‌هایی است که موردحمله قرارگرفته‌اند.

- **مرحله تسکین**[1] (تقابل با حمله شناسایی‌شده): مرحله نهایی قصد دارد تا از طریق حذف (از جداول مسیریابی شبکه) گره‌های آلوده‌شده، تأثیر هر حمله‌ای را بعد از وقوع آن کاهش داده و دوباره امنیت را برقرار نماید.

نفوذ یک فعالیت غیرمجاز در شبکه است که به دو صورت فعال (مانند هدایت اشتباه بسته‌ها، حذف بسته‌ها، حملات حفره) و یا غیرفعال (مانند جمع‌آوری اطلاعات، استراق سمع[2]) انجام می‌گردد. در یک سیستم امنیتی، اگر خط نخست دفاعی یعنی "پیشگیری از نفوذ" مانع نفوذها نگردد، در این صورت خط دوم تدافعی یعنی "تشخیص نفوذ" به اجرا درمی‌آید. در این مرحله هر رفتار مشکوک[3] موجود در شبکه که توسط اعضای آن انجام می‌شود، شناسایی می‌گردد.

در هر طرح امنیتی، برخی یا همه اطلاعات زیر توسط سیستم‌های تشخیص نفوذ برای حمایت و پشتیبانی سیستم‌های دیگر تأمین می‌گردند [۲۸]:

- شناسایی مهاجم (نفوذ گر)
- تعیین محدوده تهاجم (برای نمونه یک گره تک و یا یک ناحیه)
- تعیین زمان نفوذ (مثلاً تاریخ رخداد آن)
- نحوه فعالیت مهاجم (این‌که نفوذگر فعال یا غیرفعال است)
- تعیین نوع نفوذ (برای مثال حملاتی مانند کرم‌چاله، سیاه‌چاله، حفره چاهک، ارسال انتخابی)
- تعیین لایه‌ای که نفوذ در آن واقع‌شده است (برای مثال لایه شبکه، اتصال داده و یا فیزیکی)

[1] Mitigation
[2] Eavesdropping
[3] Suspicious behavior

این اطلاعات برای تسکین دادن و اصلاح اثرات حمله خیلی مفید خواهند بود، ازینرو هر اطلاعات خاصی در رابطه با مهاجم جمع‌آوری می‌گردد. بنابراین سیستم‌های تشخیص نفوذ برای برقراری امنیت شبکه بسیار حائز اهمیت هستند.

شبکه حسگر بی‌سیم دارای خصوصیات منحصربه‌فردی می‌باشند که عبارتند از:

- منبع انرژی محدود
- پهنای باند پایین
- اندازه حافظه و حجم ذخیره‌سازی کم

به دلیل همین شرایط عملیاتی بغرنج موجود در شبکه‌های حسگر بی‌سیم (محدودیت‌های محاسباتی و منابع انرژی همراه با محیط ارتباطی موردی[1])، اغلب روش‌های امنیتی (شامل روش‌های تشخیص نفوذ) ارائه‌شده برای شبکه‌های سیمی / بیسیم سنتی، به‌صورت مستقیم برای محیط شبکه‌های حسگر بی‌سیم قابل‌استفاده نیستند. طراحی یک تکنیک تشخیص نفوذ مؤثر و کاراً که قابل‌استفاده برای شبکه‌های حسگر بی‌سیم باشد، امری دشوار و بسیار چالش‌برانگیز است. از طرف دیگر با توجه به جدید بودن مبحث و حساسیت بالای وجود یک چنین سیستمی در شبکه‌های حسگر که بتواند با محدودیت‌های آن سازگار گردد، انگیزه اصلی ما برای کار در این زمینه گردید.

۲-۳-۱. سیستم‌های تشخیص نفوذ

در یک شبکه یا یک سیستم، هر نوعی از فعالیت‌های غیرمجاز و نامطلوب، نفوذ نامیده می‌شوند. یک سیستم تشخیص نفوذ یک مجموعه از ابزار، روش‌ها و منابع برای کمک به شناسایی، ارزیابی و گزارش نفوذها می‌باشد. تشخیص نفوذ یک واحد حفاظتی منفرد و جداگانه نیست بلکه معمولاً بخشی از یک سیستم حفاظت کلی‌تر است که در کنار یک سیستم یا دستگاه نصب می‌گردد. در مرجع [۲۹]، نفوذ به‌صورت: "هر مجموعه از فعالیت‌ها که تلاش می‌کند تا جامعیت، محرمانگی و یا موجودیت یک منبع

[1] Ad-Hoc

را به خطر بیندازد" تعریف می‌شود و روش‌های پیشگیری از نفوذ (مانند رمزنگاری، تأیید هویت، کنترل دسترسی، مسیریابی امن) به‌عنوان اولین خط تدافعی در برابر نفوذها ارائه می‌شوند.

بااین‌وجود، باید توجه داشت که در هر نوع سیستم امنیتی، نمی‌توان نفوذها را به‌طور کامل پیشگیری نمود. نفوذ و تسخیر یک گره منجر به افشای اطلاعات محرمانه مانند کلیدهای امنیتی برای نفوذگرها شده و شکست سازوکار امنیتی پیشگیرانه را بدنبال دارد. بنابراین بسیار مهم است که سیستم‌های تشخیص نفوذ به نحوی طراحی‌شده باشند که قبل از این‌که مهاجم بتواند منابع سیستم و اطلاعات امنیتی را فاش نمایند، نفوذ را شناسایی و آشکارسازی کنند. سیستم‌های تشخیص نفوذ ازنقطه‌نظر امنیتی به‌عنوان دومین دیوار تدافعی موردتوجه بوده‌اند. البته باید متذکر شد که سیستم‌های تشخیص نفوذ بدون وجود روش‌های پیشگیرانه نیز می‌توانند به‌تنهایی امنیت شبکه را تأمین نمایند. این سیستم‌ها در فضاهای سایبری معادل آژیرهای خطر سرقت هستند که امروزه در سیستم‌های امنیتی فیزیکی به کار می‌روند. شرایط عملیاتی مورد انتظار در یک سیستم تشخیص نفوذ به‌صورت زیر خواهد بود [۲۹]:

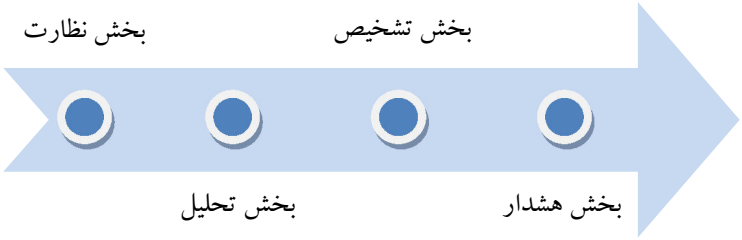
- نرخ کم f-P[1] که معادل است با درصد فعالیت‌های عادی که به‌عنوان ناهنجاری شناخته می‌شوند.
- نرخ بالای T-P[2] که معادل است با درصد ناهنجاری‌هایی که به‌درستی کشف‌شده‌اند.

همان‌طور که در شکل (۲-۲۳) نشان داده‌شده است، هر سیستم تشخیص نفوذ داری سه بخش اصلی است [۳۰] که عبارتند از:

- **بخش نظارت**[3]: این بخش برای نظارت بر رخدادهای محلی و کنترل همسایه‌ها به کار می‌رود. این بخش غالباً الگوهای ترافیک، رخدادهای داخلی و بهره‌وری منابع را کنترل می‌نماید.

[1] False-Positive
[2] True-Positive
[3] Monitoring

- **بخش تحلیل و تشخیص**[1]: این واحد بخش اصلی سیستم تشخیص نفوذ است که وابسته به الگوریتم مدل‌سازی است. در این بخش عملیات، رفتار و فعالیت‌های شبکه تجزیه‌وتحلیل شده و تصمیم‌گیری می‌گردد که آن‌ها را به‌عنوان یک نفوذ اعلان نماید یا خیر.
- **بخش هشدار**[2]: این بخش مسئول واکنش در برابر نفوذ است که هشداری در مورد تشخیص یک نفوذ تولید می‌نماید.



شکل (۲-۲۳) اجزاء سیستم‌های تشخیص نفوذ

۲-۳-۲. نیازمندی‌های سیستم‌های تشخیص نفوذ

هر سیستم تشخیص نفوذ که طراحی می‌گردد باید ملزومات و شرایط زیر را برآورده نماید [۳۱]:

- نباید معایب و نقاط ضعف جدیدی به سیستم اضافه نماید.
- منابع سیستم را کمتر مصرف نماید و همچنین نباید با سربارهایی که به سیستم تحمیل می‌کند، کارایی آن را تنزل دهد.
- به‌صورت پیوسته و مداوم اجرا شود و برای سیستم و کاربران به‌صورت نامحسوس عمل نماید.
- طراحی آن مطابق استانداردها باشد تا امکان مشارکت و گسترش آن در آینده ممکن باشد.
- قابل‌اعتماد باشد و در فاز تشخیص نرخ‌های F-p و F-n را به حداقل برساند.

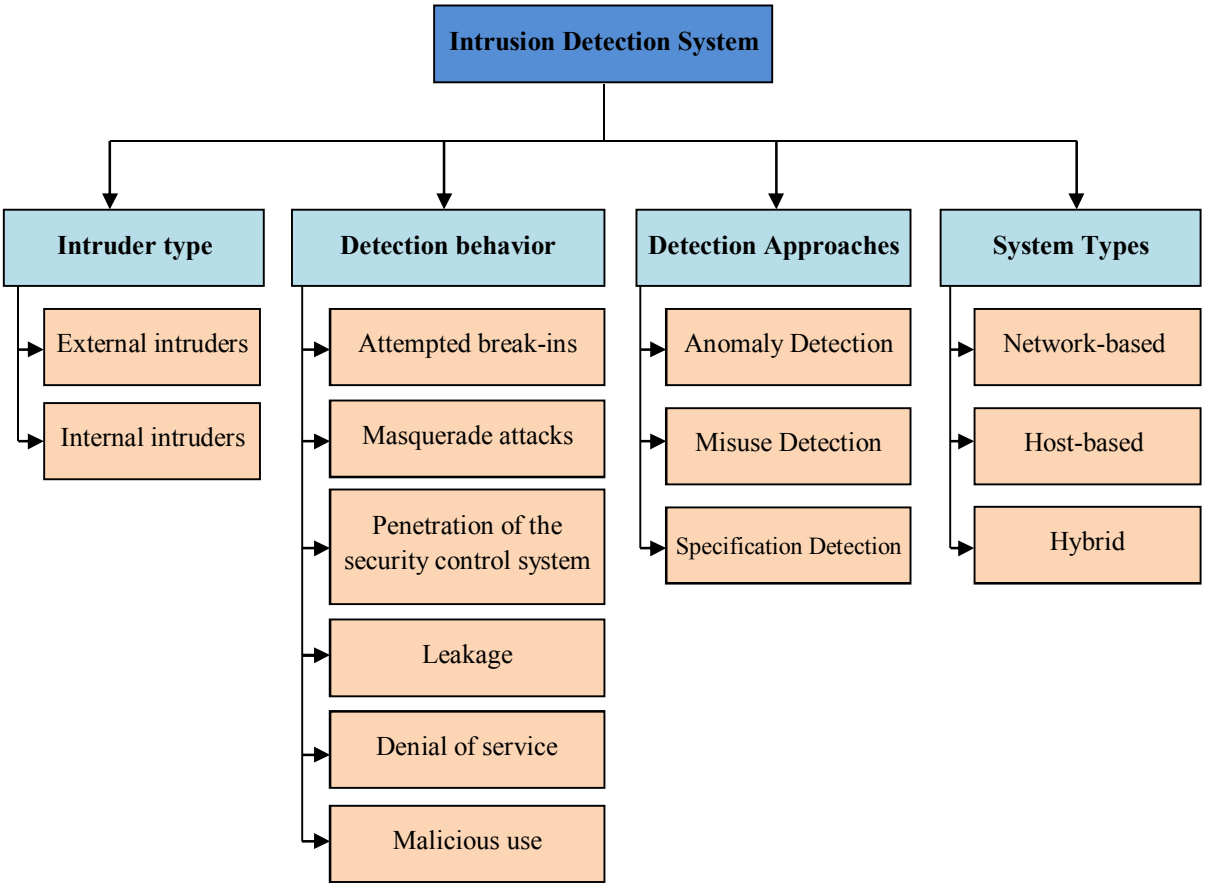
[1] Analysis & Detection
[2] Alarm

۲-۳-۳. دسته‌بندی‌های سیستم‌های تشخیص نفوذ

در شکل (۲-۲۴) انواع دسته‌بندی‌های مختلف بر روی سیستم‌های تشخیص نفوذ ارائه‌شده است.

سیستم‌های تشخیص نفوذ بر اساس نحوه عملکرد به سه گروه دسته‌بندی می‌شوند که عبارتند از [۲۸] [۳۰] [۳۱]:

- تشخیص مبتنی بر ناهنجاری[۱]
- تشخیص مبتنی بر قانون[۲] (مبتنی بر سوءاستفاده[۳] و یا مبتنی بر ردپا[۴])
- تشخیص مبتنی بر خصوصیات[۵]

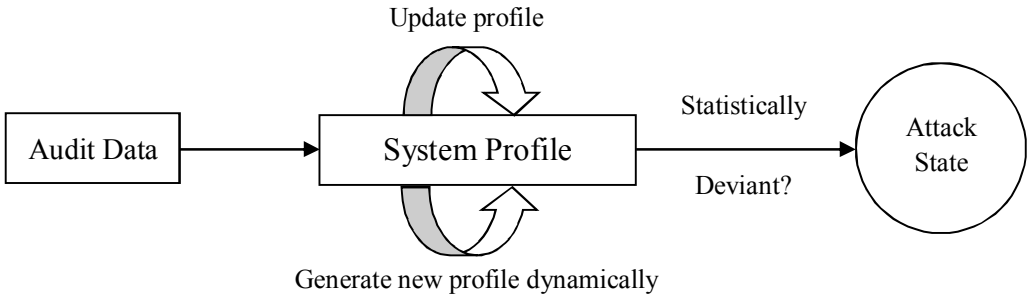


شکل (۲-۲۴) انواع دسته‌بندی‌های مختلف بر روی سیستم‌های تشخیص نفوذ [۳۱]

در ادامه نحوه عملکرد هر یک از روش‌های فوق‌الذکر به‌تفصیل ارائه می‌گردد.

[1] Anomaly based detection
[2] Rule Based detection
[3] Misuse based detection
[4] Signature based detection
[5] Specification based detection

- **تشخیص مبتنی بر ناهنجاری:** این روش که در شکل (۲-۲۵) نشان داده‌شده است، مبتنی بر مدل کردن رفتار آماری است که در آن عملیات بهنجار اعضای شبکه ثبت‌شده و در صورت مشاهده انحراف مشخصی نسبت به آن، آن را به‌عنوان ناهنجاری معرفی می‌نماید. عیب این روش تشخیص این است که چون رفتار شبکه ممکن است سریع تغییر نماید، بنابراین اطلاعات وضعیت بهنجار اعضاء باید به‌صورت دوره‌ای بروز رسانی گردد. این امر باعث می‌شود بار کاری گره‌ها افزایش‌یافته و سرباری بر منابع محدود گره‌های حسگر اضافه نماید.

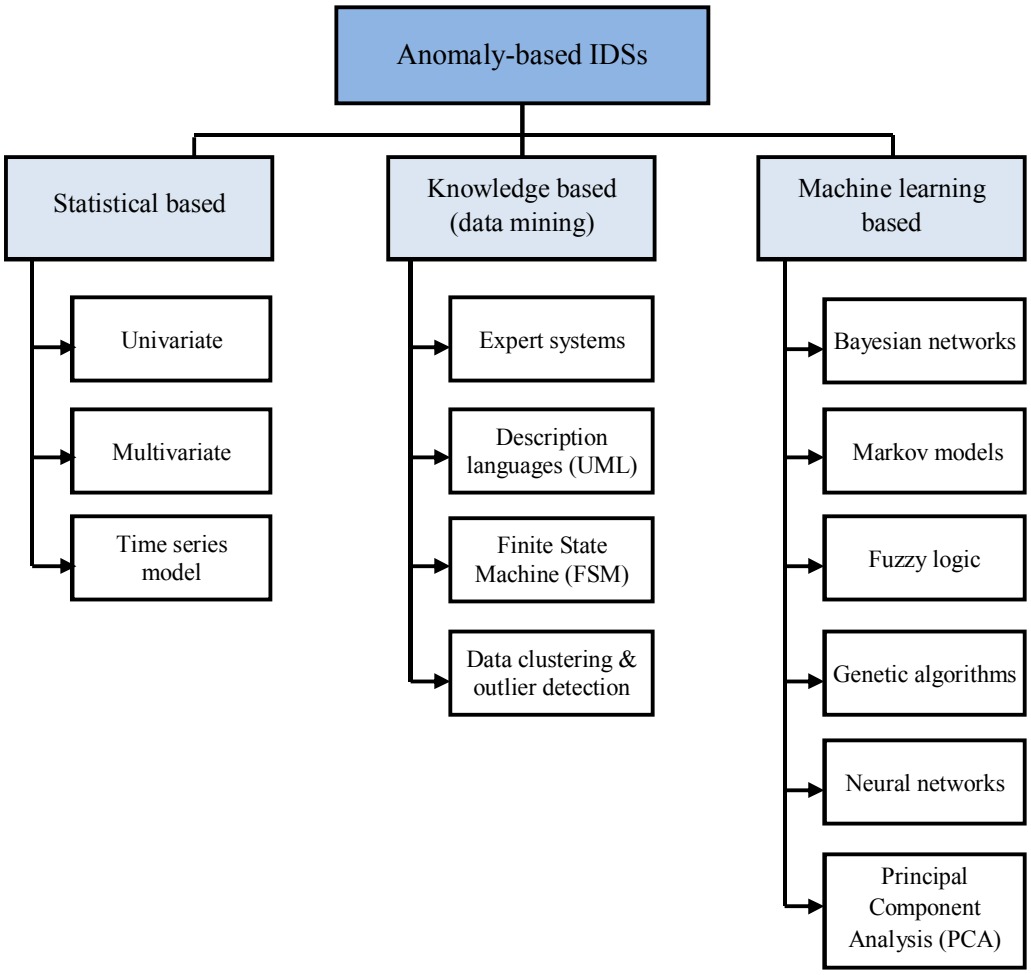


شکل (۲-۲۵) یک نمونه از سیستم‌های تشخیص ناهنجاری [۳۱]

این روش نفوذهایی را که در آن‌ها شبکه از الگوهای رفتاری ایستا[1] تبعیت می‌نماید، به‌صورت خیلی دقیق و به‌طور مداوم همراه با نرخ‌های پایینی برای F-P و F-N تشخیص می‌دهد [۲۹]. مزیت این نوع از تشخیص در این است که کاملاً برای تشخیص حملات ناشناخته و یا حملاتی که قبلاً با آن‌ها مواجه نشدیم، مناسب است. سیستم‌های تشخیص مبتنی بر ناهنجاری، بسته به ماهیت پردازشی مرتبط با مدل رفتاری مطرح‌شده به سه دسته زیر تقسیم می‌شوند که در شکل (۲-۲۶) ارائه‌شده‌اند:

- مبتنی بر آمار[2]
- مبتنی بر دانش[3]
- مبتنی بر یادگیری ماشین[4]

[1] Static behavioral patterns
[2] Statistical based
[3] Knowledge based
[4] Machine learning based



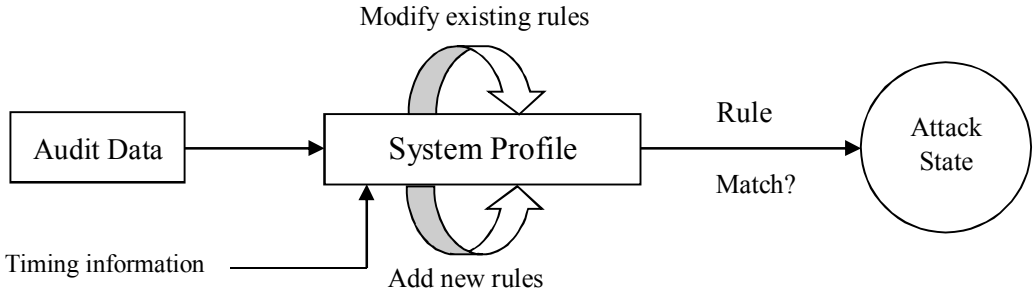
شکل (۲-۲۶) انواع سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری [۲۸]

- **تشخیص نفوذ مبتنی بر قانون:** در این روش که در شکل (۲-۲۷) نشان داده‌شده است، پروفایل‌های مربوط به حملات شناخته‌شده قبلی تولیدشده و به‌عنوان مرجعی برای تشخیص و شناسایی حملات آینده استفاده می‌گردند. برای نمونه یک مثال معمول از یک رد پای[۱] یک رفتار نامطلوب به‌صورت زیر می‌باشد:

"وجود سه بار تلاش نادرست برای ورود به سیستم در ۵ دقیقه" به‌عنوان حمله کلمه عبور با کاربرد ناشیانه[۲] شناخته می‌شود. مزیت این روش تشخیص در این است که می‌تواند حملات شناخته‌شده را به‌طور دقیق و کارائی تشخیص دهد. بنابراین این روش‌ها دارای نرخ پایینی از F-P

[1] Signature
[2] Brute force password attack

هستند. عیب این روش نیز این است که اگر حمله یک نوع جدیدی باشد (که اطلاعات آن قبلاً ثبت‌نشده باشد)، در این صورت قادر به شناسایی و رسیدگی به آن نخواهد بود.



شکل (۲-۲۷) یک نمونه از سیستم‌های تشخیص نفوذ مبتنی بر قانون [۳۱]

این سیستم‌ها خیلی مشابه سیستم‌های ویروس‌یاب هستند که می‌توانند اغلب یا همه الگوهای حمله شناخته‌شده را تشخیص دهند، اما از کارائی خیلی کمی برای تشخیص حملاتی که هنوز ناشناخته هستند، برخوردار است [۳۱].

برخی از انواع قوانین به جهت تشخیص و شناسایی حملات مختلف به‌صورت زیر ذکرشده‌اند [۷] و [۳۲]:

- **قانون فاصله:** تأخیر بین دو پیام دریافتی پشت سر هم باید در یک حد معینی باشد. درصورتی‌که این زمان از حد مجاز بیشتر و یا کمتر گردد به‌عنوان یک عیب گزارش می‌شود. دو حمله‌ای که احتمالاً توسط این قانون شناسایی می‌شوند عبارتند از حمله سهل‌انگاری و حمله فرسودگی منابع. در حمله سهل‌انگاری گره مهاجم پیام‌های تولیدشده به‌وسیله یک گره دیگر را ارسال نمی‌نماید. درحالی‌که در حمله فرسودگی، مهاجم نرخ ارسال پیام‌ها را به‌منظور افزایش مصرف انرژی گره‌های دیگر موجود در خوشه افزایش می‌دهد.
- **قانون ارسال به جلو:** یک پیام ارسالی باید توسط گره‌های میانی به سمت جلو هدایت شود.
- **قانون تأخیر:** ارسال مجدد یک پیام باید بعد از یک زمان انتظار مشخصی انجام گردد.

- **قانون اصالت:** پیام اصلی ارسال‌شده توسط فرستنده نباید هنگامی‌که به گیرنده می‌رسد دچار تغییرات شده باشد.
- **قانون تکرار:** یک پیام خاص تنها می‌تواند به تعداد دفعات معینی توسط یک گره یکسان تکرار و ارسال گردد.
- **قانون محدوده ارسال رادیویی:** یک پیام تنها باید از گره‌های همسایه دریافت گردد.
- **قانون پارازیت:** تعداد برخوردها برای ارسال یک بسته باید کمتر از حد آستانه باشد.

- **تشخیص مبتنی بر خصوصیات:** در این روش یک مجموعه از خصوصیات و محدودیت‌ها که عملیات صحیح یک برنامه یا پروتکل را توصیف می‌نمایند، تعریف می‌شود. سپس اجرای آن برنامه با توجه به خصوصیات و محدودیت‌های تعریف‌شده مورد نظارت قرار می‌گیرد. این فناوری به‌گونه‌ای است که قابلیت تشخیص حملات شناخته‌شده قبلی را با نرخ پایین F-P فراهم می‌نماید. تمایز اصلی بین دو روش تشخیص مبتنی بر ناهنجاری و مبتنی بر قانون را می‌توان به‌صورت زیر بیان کرد [۳۱]:

"سیستم‌های تشخیص مبتنی‌بر ناهنجاری تلاش دارند تا اثر رفتار بد[1] را تشخیص دهند، اما سیستم‌های تشخیص مبتنی بر قانون سعی دارند تا رفتار بد از پیش شناخته‌شده را آشکارسازی نمایند."

روش‌های تشخیص نفوذ مبتنی بر خصوصیات، مزایای هر دو روش تشخیص مبتنی بر ناهنجاری و مبتنی بر قانون را با استفاده از توسعه دستی خصوصیات و محدودیت‌های موجود برای توصیف رفتار قانونی و مشروع سیستم، ادغام می‌نمایند. روش‌های مذکور ازاین‌جهت مشابه روش‌های مبتنی بر ناهنجاری هستند که هردوی آن‌ها حملات را به‌عنوان انحرافی از حالت بهنجار سیستم تشخیص می‌دهند.

[1] Effect of bad behavior

ازآنجایی‌که روش‌های تشخیص نفوذ مبتنی بر خصوصیات وابسته به توسعه دستی خصوصیات و محدودیت‌ها هستند، بنابراین دارای نرخ پایین هشدار اشتباه در مقایسه با نرخ بالای هشدار اشتباه در روش‌های تشخیص مبتنی بر ناهنجاری هستند. از طرف دیگر هزینه بدست آوردن چنین نرخ پایینی برای هشدار اشتباه وابسته به توسعه و ایجاد خصوصیات و محدودیت‌های تفصیلی بوده که بسیار زمان‌بر خواهد بود.

۲-۳-۴. سازوکارهای تصمیم‌گیری

دو نوع سازوکار اتخاذ تصمیم در سیستم‌های تشخیص نفوذ وجود دارند:

- **اتخاذ تصمیم مشارکتی و مبتنی بر همکاری**[1]: در این روش همه (یا برخی) اعضای شبکه در اتخاذ تصمیم درباره یک پدیده همکاری می‌نمایند. برای نمونه، در مورد رأی‌گیری اکثریت، تصمیم نهایی سرانجام به نفع اکثریت اعضاء بر روی دو تصمیم اتخاذ می‌شود: "پدیده یک نفوذ است" یا "پدیده یک نفوذ نیست".
- **اتخاذ تصمیم مستقل:** در این روش هر عضو بر اساس وقایع و پدیده‌های اطراف خودش تصمیمی را اتخاذ می‌کند.

یک سیستم تشخیص نفوذ، یکی از چهار تصمیم زیر را به‌عنوان نتیجه فرایند تصمیم‌گیری خود تحت یک پدیده، بیان می‌نماید:

- نفوذ رخداده اما ناهنجاری تشخیص داده نشده (False-Negative): در این‌حالت نفوذ به‌عنوان یک حالت مجاز شناخته می‌شود.
- نفوذ رخ نداده اما تشخیص وجود ناهنجاری است (False-Positive): در این‌حالت یک وضعیت مجاز به‌عنوان نفوذ گزارش می‌شود.
- نفوذ رخ نداده و تشخیص عدم وجود ناهنجاری است (True-Negative): در این‌حالت وضعیت مجاز سیستم درست تشخیص داده می‌شود.

[1] Collaborative decision making

- نفوذ رخ‌داده و تشخیص وجود ناهنجاری است (True-Positive): در این حالت نفوذ درست شناسایی می‌گردد.

در سیستم‌های تشخیص نفوذ مربوط به شبکه‌های حسگر بی‌سیم، با توجه به ماهیت ارتباطات بی‌سیم موجود، وضعیت‌های زیر به‌عنوان F-P استنباط می‌شوند، بنابراین در مدل اتخاذ تصمیم نیازمند توجه به آن‌ها هستیم:

- برخوردها[1]
- حذف بسته‌ها
- توان ارسال محدود
- تخلیه توان باطری

برای مثال با توجه به ماهیت ارتباطات نامطمئن بی‌سیم که در آن امکان وجود برخورد در ارسال به‌طور طبیعی بین گره‌ها وجود دارد، امکان دارد سیستم تشخیص نفوذ این برخوردهای طبیعی را به‌عنوان یک حمله برخورد تشخیص داده و گره‌ای سالم را به‌اشتباه به‌عنوان مهاجم شناسایی نماید.

همچنین در زمانی که حجم ارسال اطلاعات در بین گره‌ها زیاد شود، در شرایطی که در شبکه (مخصوصاً در نزدیکی گره‌های چاهک) به دلیل حجم بالای اطلاعات ارسالی، ازدحام بوجود می‌آید، به‌طور طبیعی ممکن است برخی از بسته‌ها به دلایل مختلفی همچون سرریز شدن بافرها، حذف شوند که درصورتی‌که سیستم تشخیص نفوذ از دقت کافی برخوردار نباشد ممکن است آن را به‌عنوان یک حمله (برای مثال در حملاتی مانند حفره چاهک، کرم‌چاله و ارسال انتخابی، عمل حذف بسته‌ها رایج است) تلقی نموده و تشخیص اشتباه بدهد.

بنابراین سیستم تشخیص نفوذ باید به‌گونه‌ای طراحی شود که تا حد ممکن F-P را به حداقل برساند تا با تشخیص اشتباه رفتارهای بهنجار و عادی به‌عنوان حمله، باعث محدود کردن سیستم و حذف گره‌های سالم در شبکه نگردد.

[1] Collisions

۲-۳-۵. تبیین نحوه شبیه‌سازی سیستم‌های تشخیص نفوذ

در این بخش مهم‌ترین نکات مربوط به شبیه‌سازی سیستم‌های تشخیص نفوذ را موردبررسی قرار می-دهیم. پس از شبیه‌سازی شبکه حسگر بی‌سیم و حملات لایه شبکه بر روی آن، مرحله سوم شبیه‌سازی سیستم تشخیص نفوذ روی آن است که باید بر روی گره‌های شبکه حسگر بی‌سیم نصب‌شده و سیستم را در مقابل حملات مفروض محافظت نماید. در این مرحله سیستم تشخیص نفوذ با تمامی پارامترهای مربوطه و جزئیات دقیق آن بر روی شبکه حسگر بی‌سیم شبیه‌سازی‌شده نصب می‌گردد و نتایج اجرایی آن در قالب نمودارهای آماری ترسیم خواهد شد. معمولاً نتایج اجرایی حاصل از شبیه‌سازی‌ها با دو فاکتور درصد تشخیص حملات و میزان مصرف انرژی ارائه می‌شوند. در اینجا به جهت درک دقیق‌تری از ارائه نتایج، نمونه‌هایی از نتایج روش‌های موجود در شکل‌های زیر ارائه‌شده‌اند.

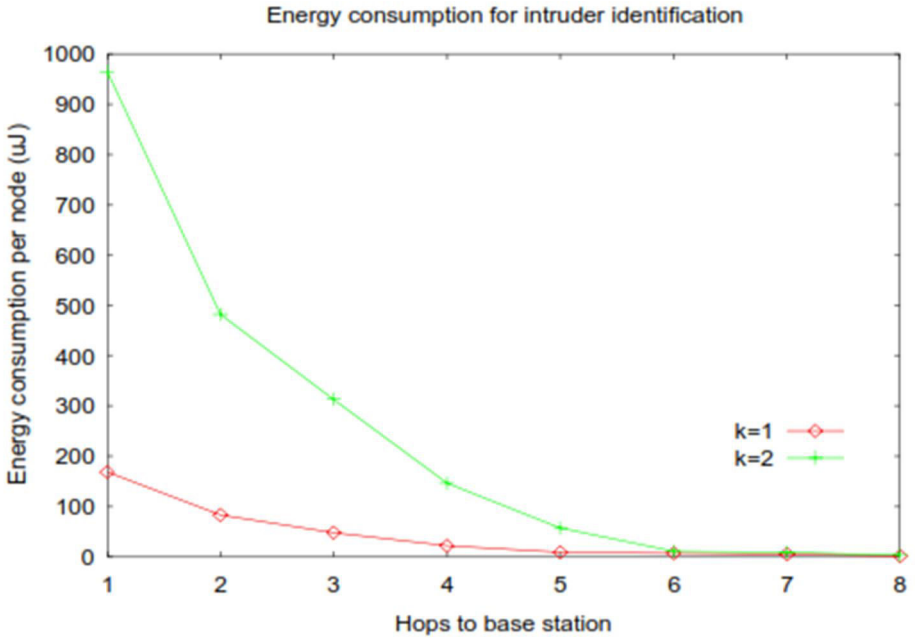
ازنقطه‌نظر درصد تشخیص حملات: در برخی از مقالات میانگین نرخ تشخیص در برابر حملات گوناگون توسط روش‌های مختلف تشخیص نفوذ به‌صورت جدول ارائه‌شده است [۳۳].

ازنقطه‌نظر میزان مصرف انرژی: ما برای اینکه بتوانیم تصور مناسبی نسبت به میزان مصرف انرژی در روش تشخیص نفوذ پیشنهادی داشته باشیم باید سناریوهای مختلفی را شبیه‌سازی نماییم.

- سناریوی اول در نظر گرفتن شبکه حسگر بی‌سیم مفروض بدون سیستم تشخیص نفوذ و با یک بارکاری بهنجار و بدون حضور هیچ مهاجمی می‌باشد.
- سناریوی دوم در نظر گرفتن شبکه حسگر بی‌سیم مفروض بدون سیستم تشخیص نفوذ و با یک بارکاری بهنجار و همراه با سناریوی حملات مشخص‌شده است.
- سناریوی سوم در نظر گرفتن شبکه حسگر بی‌سیم مفروض همراه با سیستم تشخیص نفوذ پیشنهادی و با یک بارکاری بهنجار و بدون حضور هیچ مهاجمی می‌باشد.
- سناریوی چهارم نیز در نظر گرفتن شبکه حسگر بی‌سیم مفروض همراه با سیستم تشخیص نفوذ پیشنهادی و با یک بارکاری بهنجار و همراه با سناریوی حملات مشخص‌شده است.

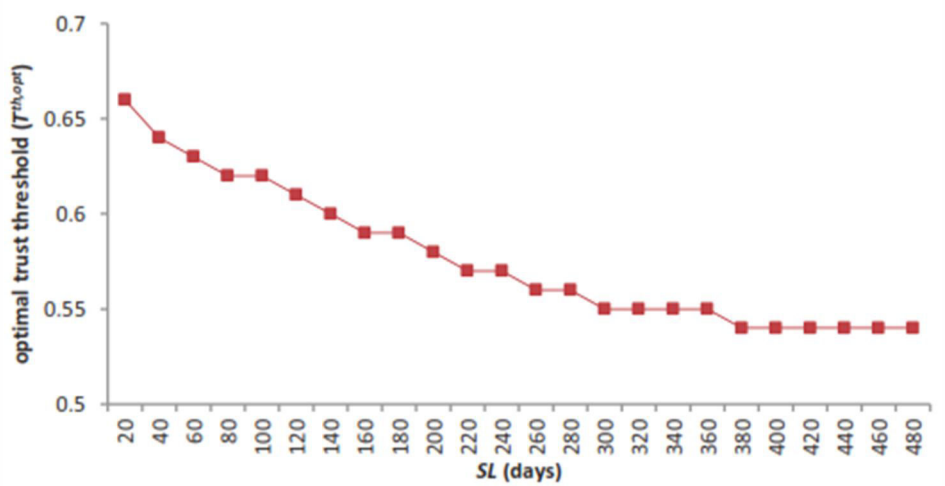
بنابراین ما با توجه به میزان مصرف انرژی در سناریوهای فوق و مقایسه آن‌ها باهم به‌راحتی می‌توانیم مصرف انرژی در روش پیشنهادی را محاسبه کرده و با روش‌های تشخیص نفوذ موجود مقایسه نماییم. برای نمونه به جهت درک ذهنی مناسب‌تری از میزان مصرف انرژی، نمودارهای آماری مربوط به میزان مصرف انرژی سیستم تشخیص نفوذ ارائه‌شده در برخی از مقالات در شکل‌های زیر نشان داده‌شده‌اند. در شکل (۲-۲۸) نمودار میانگین مصرف انرژی سیستم تشخیص ارائه‌شده در گره‌های شبکه بر اساس روش پیشنهادی نگای و همکاران [۳۴] برحسب تعداد پرش تا ایستگاه پایه ارائه‌شده است.

در شکل (۲-۲۹) نیز نمودار طول عمر گره‌های شبکه در پژوهش ارائه‌شده توسط بائو و همکاران نشان داده‌شده است [۳۵]. آن‌ها در سیستم تشخیص نفوذ پیشنهادی از یک حد آستانه برای تشخیص نفوذ استفاده کرده‌اند. در این نمودار سطح حساسیت و تشخیص سیستم تشخیص نفوذ پیشنهادی بر اساس تغییرات پارامتر سطح آستانه، تغییر می‌کند. همان‌طور که در شکل (۲-۲۹) مشاهده می‌شود، هرچه سطح حساسیت سیستم تشخیص نفوذ آن‌ها بالاتر برود به‌طبع میزان مصرف انرژی گره‌های شبکه افزایش‌یافته و بنابراین طول عمر شبکه نیز کاهش می‌یابد.



شکل (۲-۲۸) نمونه‌ای از نمودار میانگین مصرف انرژی سیستم تشخیص نفوذ [۳۴]

در جدول (۲-۲) نیز در ابتدا میزان مصرف انرژی گره‌های شبکه در عدم حضور حملات توسط دیاز و همکاران [۳۶] اندازه‌گیری شده و سپس درصد افزایش مصرف انرژی آن‌ها برای تشخیص نفوذ در برابر حملات مختلف ارائه گردیده است.



شکل (۲-۲۹) نمودار طول عمر شبکه بر اساس تغییرات پارامتر سطح آستانه [۳۵]

جدول (۲-۲) مصرف انرژی سیستم تشخیص نفوذ در گره‌های مختلف شبکه در برابر حملات مختلف [۳۶]

	Mesh Network				Linear Network			
	Gateway	*Node [0-6]*	*Node 7*	*Total*	*Gateway*	*Node [0-6]*	*Node 7*	*Total*
Without attacks	3.614 J	0.713 J	0.713 J	9.319 J	0.563 J	1.598 J	1.598 J	13.354 J
Collision attack	-28.01%	+192.95%	+192.95%	+108.92%	-9.48%	0%	+90.56%	+9.4 %
Interrogation attack	333.51%	0%	0%	+90.65%	+1390.9%	0%	0%	+65.02%
Sybil Attack	0%	0%	+563.2%	+68.21%	0%	0%	314.53%	+20.44%

۲-۴- جمع‌بندی

ما در این بخش به طرح و بررسی مفاهیم پایه‌ای و مسائل مرتبط با موضوع رساله پرداختیم. در ابتدا شبکه‌های حسگر بی‌سیم را همراه با معماری ارتباطات، ساختار داخلی گره‌ها، فاکتورهای طراحی و کاربردهای گسترده آن و ... معرفی کردیم، که بستر اصلی ما در ارائه معماری تشخیص نفوذ پیشنهادی برای تأمین امنیت در برابر حملات مختلف می‌باشد. سپس به تشریح مقوله امنیت و روش-های تأمین آن در شبکه‌های حسگر بی‌سیم پرداخته و انواع مختلف حملات امنیتی را بر روی این شبکه‌ها معرفی کردیم. در انتها نیز سیستم‌های تشخیص نفوذ را به همراه انواع مختلف آن، به‌عنوان یکی از روش‌های مناسب تأمین امنیت در این شبکه‌ها به‌طور کامل تشریح کردیم.

۳–پیشینه تحقیق

در این بخش به بررسی روش‌های تشخیص نفوذ موجود خواهیم پرداخت. به‌طورکلی روش‌های پیشنهادی بر اساس نحوه عملکرد و معماری قابل‌استفاده به دسته‌های زیر تقسیم‌بندی می‌شوند:

۳-۱- سیستم‌های تشخیص نفوذ مبتنی بر خوشه‌بندی (سلسله مراتبی)

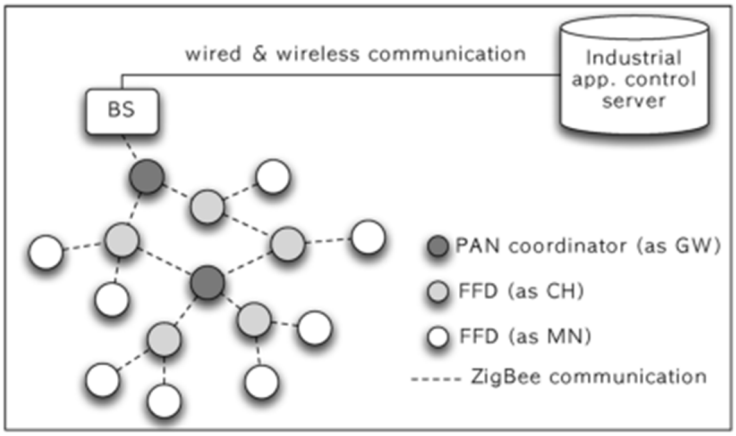
لِی و چن یک سیستم تشخیص نفوذ مبتنی بر خوشه‌بندی برای حمله رد سرویس ارائه کرده‌اند که در آن یک مجموعه گره ویژه به نام گره‌های محافظ[1]، عملیات بررسی و تحلیل ترافیک شبکه و کشف و گزارش حملات رد سرویس را به گره‌های سرخوشه برعهده دارند [۳۷]. مشکل اساسی این روش عدم توجه به پارامتر انرژی و مصرف آن است که در شبکه‌های حسگر دارای اهمیت بالایی است. در این مقاله گره‌های محافظ به‌صورت ثابت در کل زمان کاری شبکه در نظر گرفته‌شده‌اند و تنها به‌منظور انجام فرایند تشخیص نفوذ استفاده می‌شوند.

برای اصلاح مشکل یادشده، می‌توان گره‌های محافظ را به‌صورت دوره‌ای و بر اساس انرژی باقیمانده انتخاب کرد تا علاوه بر اعمال معمول، عملیات تحلیل ترافیک و تشخیص نفوذ را نیز انجام دهند و بدین ترتیب یک راه‌حل پویا برای افزایش طول عمر شبکه ارائه خواهد شد [۳۸]. البته باید توجه داشت که خود الگوریتم انتخاب و تعویض گره‌های محافظ دارای سربار انرژی و محاسبات خواهد بود.

در روشی دیگر، یک معماری سلسله مراتبی برای تشخیص نفوذ همراه با پردازش داده به شیوه سلسله مراتبی توسط شین و همکاران پیشنهادشده است [۳۳]. آن‌ها یک خوشه‌بندی دوسطحی را ارائه کردند که در سطح اول سرخوشه ها مدیریت خوشه‌ها را بر عهده‌دارند و در سطح دوم سرخوشه‌ها با دروازه‌ها در ارتباط خواهند بود و از طریق آن‌ها با ایستگاه پایه مرتبط می‌شوند (شکل ۳-۱).

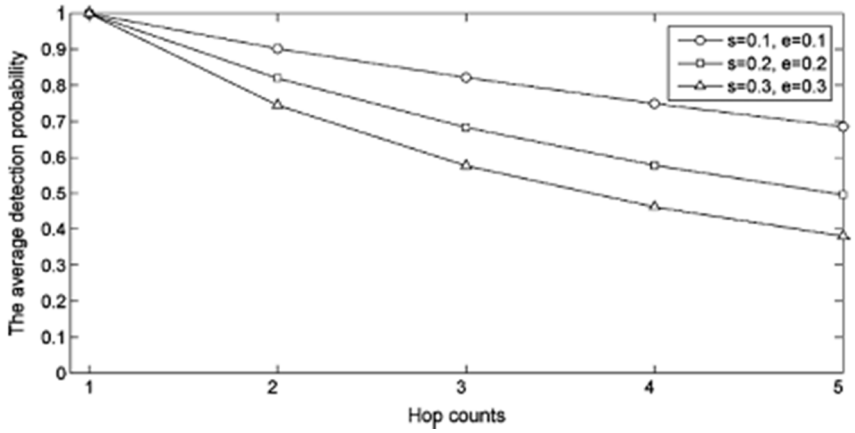
آن‌ها در تمام آزمایش‌های مرتبط با معماری پیشنهادی خود بر روی مفهوم خوشه‌بندی تک پرشه متمرکزشده‌اند. دلیل اصلی تمرکز آن‌ها بر روی خوشه‌بندی تک پرشه این‌گونه عنوان‌شده است که بالاترین نرخ تشخیص زمانی است که گره‌ها به‌صورت تک پرشه با سرخوشه در ارتباط باشند و هرچه تعداد پرش‌ها بیشتر گردد نرخ تشخیص نفوذ نیز به‌صورت خطی کاهش خواهد یافت.

[1] Guarding Nodes



شکل (۳-۱) خوشه‌بندی دوسطحی بر اساس استاندارد زیگ بی [۳۳]

این امر در شکل (۳-۲) نشان داده‌شده است که در آن s نمایانگر نرخ خواب و e نشانگر نرخ خطا است. آن‌ها معتقدند که معماری پیشنهادشده برای تأمین امنیت کاربردهای صنعتی در شبکه‌های حسگر بی‌سیم با توجه به دو خط دفاعی، قابل‌استفاده خواهد بود.



شکل (۳-۲) اثر تعداد پرش در خوشه‌بندی بر روی میانگین احتمال تشخیص نفوذ [۳۳]

چن و همکاران یک جدول تفکیک[1] برای تشخیص نفوذها در شبکه‌های حسگر بی‌سیم سلسله مراتبی پیشنهاد کردند که ازلحاظ مصرف انرژی کارآ است [۳۹]. این روش نیازمند خوشه‌بندی دو سطحی است. بر اساس نتایج آزمایش‌ها، روش تشخیص نفوذ بر اساس جدول تفکیک، حملات را به‌طور مؤثری می‌تواند تشخیص دهد. مشکل این روش این است که: محققان ادعا کردند که هر سطح بر سطح دیگر نظارت نموده و گزارش هر نوع از ناهنجاری را به ایستگاه پایه ارسال می‌کنند. بنابراین این یک شبکه

[1] Isolation table

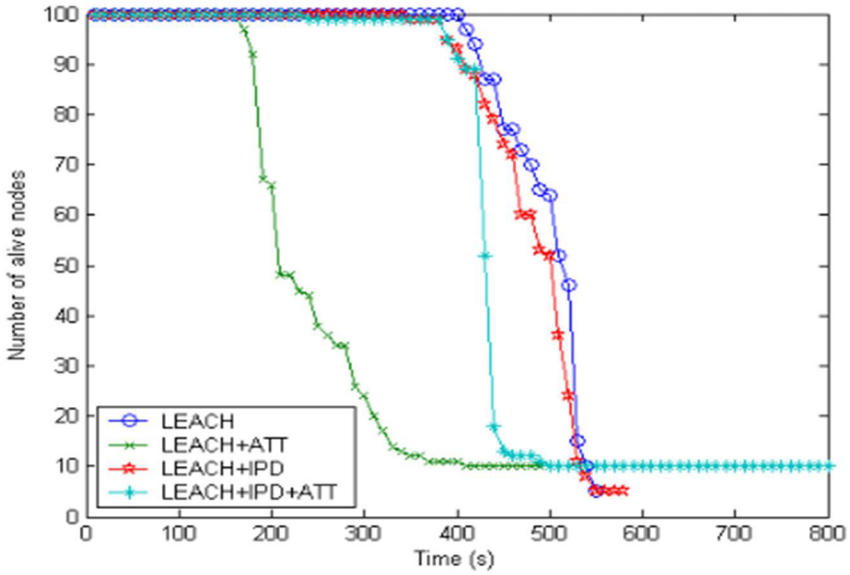
سلسله مراتبی است که هر هشدار تولیدشده توسط گره‌های سطح پایین‌تر می‌بایست از گره‌های سطح بالاتر عبور نماید. درصورتی‌که گره سطح بالاتر یک مهاجم باشد، به‌طور ساده از طریق مسدود کردن پیام‌های هشداری که از گره‌های سطح پایین‌تر دریافت می‌کند، اجازه نخواهد داد تا ایستگاه پایه از ناهنجاری‌های موجود آگاه گردد.

یک سیستم تشخیص نفوذ مبتنی بر شیوه خوشه‌بندی نیز توسط سوو و همکاران پیشنهادشده است [۸]. روش پیشنهادی آن‌ها امنیت سرخوشه ها را نیز تأمین می‌کند. در شیوه آن‌ها، اعضای خوشه به‌صورت زمان‌بندی‌شده بر سرخوشه نظارت می‌کنند. با این روش، در مصرف انرژی همه اعضای خوشه صرفه‌جویی می‌گردد. در مقابل، اعضای خوشه نه از طریق همکاری بین اعضای خوشه بلکه به‌وسیله سرخوشه نظارت می‌شوند و این امر موجب صرفه‌جویی انرژی بیشتری در اعضای خوشه می‌گردد. نتایج شبیه‌سازی‌های انجام‌شده که در شکل (۳-۳) نشان داده‌شده است به‌خوبی تأثیر الگوریتم پیشنهادی آن‌ها را در افزایش طول عمر شبکه و کارایی بهتر آن در میزان مصرف انرژی را بیان می‌کند. محققان برای مقایسه و ارزیابی الگوریتم خود، چهار حالت زیر را شبیه‌سازی نموده‌اند:

- الف: حالت معمول استفاده از الگوریتم LEACH
- ب: حالت استفاده از الگوریتم LEACH در حضور سناریوی حمله ATT[1]
- ج: حالت استفاده از الگوریتم LEACH در حضور سیستم تشخیص نفوذ IPD[2]
- د: استفاده از الگوریتم LEACH در حضور سیستم تشخیص IPD و سناریوی حمله ATT[3]

همان‌طور که در شکل (۳-۳) دیده می‌شود، بدون وجود هیچ حمله‌ای در شبکه، سیستم تشخیص نفوذ ازلحاظ مصرف انرژی سربار خیلی کمی ایجاد می‌نماید، اما در حضور حمله در شبکه سیستم تشخیص نفوذ به‌خوبی می‌تواند میزان مصرف انرژی را به‌شدت نسبت به حالتی که هیچ سیستم تشخیص نفوذی وجود ندارد کاهش دهد.

[1] Leach+ATT
[2] Leach+IPD
[3] Leach+IPD+ATT



شکل (۳-۳) تأثیر الگوریتم تشخیص نفوذ پیشنهادی در طول عمر شبکه [۸]

مشکل این شیوه، سازوکار مدیریت‌کلید آن است. این سازوکار بخشی از سیستم تشخیص نفوذ بوده و به آن کمک می‌کند تا ارتباط جفت کلیدها را در بین گره‌ها برقرار نماید. سیسم تشخیص نفوذ این کلیدها را به‌منظور احراز هویت پیام‌ها بکار می‌برد. مدیریت کلید فرض می‌کند که گره‌ها ثابت هستند (غیر سیار) و گره‌های جدید بعدازاین که جفت کلیدها تثبیت شدند، دیگر نمی‌توانند به شبکه اضافه شوند. با توجه به این‌که شبکه‌های حسگر بی‌سیم ممکن است به‌طور دوره‌ای نیازمند انتشار گره‌های جدید باشد، این امر باعث ایجاد یک نقص در مدلشان می‌شود.

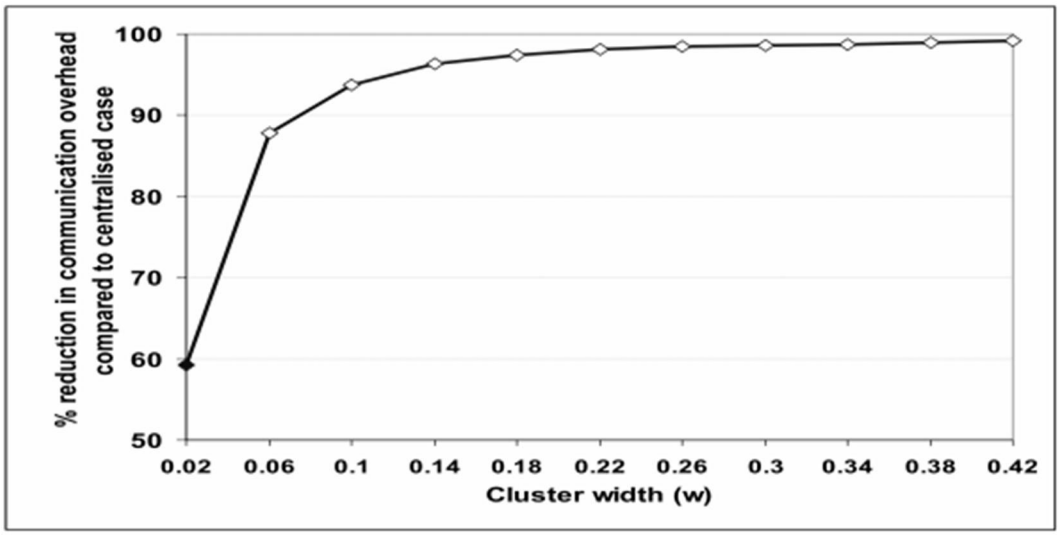
استریکس یک سیستم تشخیص نفوذ سلسله‌مراتبی را پیشنهاد کرده است که شبکه را به دو خوشه تقسیم می‌کند و برای هر خوشه با رأی‌گیری یک سرخوشه انتخاب می‌شود [۴۰]. همچنین او یک روش مسیریابی متمرکز را ارائه داده که هر بسته داده‌ی ارسالی ابتدا به سمت سرخوشه هدایت‌شده و سپس به ایستگاه پایه ارسال می‌شود. این طرح تشخیص‌دهنده‌های نفوذ در سرخوشه ها را به‌گونه‌ای جایابی می‌کند که کل شبکه را با حداقل تعداد تشخیص‌دهنده‌ها پوشش دهد. مؤلف هیچ نتایجی از شبیه‌سازی و یا داده‌هایی از آزمایش واقعی ارائه نکرده است، بنابراین مشخص نیست که آیا سیستم پیشنهادی وی به آن صورتی که تشریح نموده اجرا می‌شود یا خیر.

یک الگوریتم تشخیص ناهنجاری مبتنی بر خوشه‌بندی توزیع‌شده توسط راجاسگارار و همکاران پیشنهادشده است [۴۱]. آن‌ها به‌وسیله خوشه‌بندی مقادیر حسگرها و ادغام آن‌ها قبل از ارسال آن به گره‌های دیگر، سربار ارتباطات را به حداقل رسانده‌اند. محققان مدل پیشنهادی خود را در یک پروژه واقعی پیاده‌سازی کردند. آن‌ها نشان دادند که طرحشان در کنار کاهش قابل‌توجهی در سربار ارتباطات، دقت قابل‌مقایسه‌ای را نیز در قیاس با طرح‌های متمرکز بدست می‌آورد. در شکل (۳-۴) درصد کاهش سربار ارتباطات الگوریتم تشخیص ناهنجاری مبتنی بر خوشه‌بندی توزیع‌شده را در مقایسه با یک الگوریتم متمرکز نشان می‌دهد. برای این کار آن‌ها از رابطه (۳-۱) برای بدست آوردن درصد کاهش مذکور استفاده نمودند:

$$x = \frac{NVDTcentralised - NVDTdistributed}{NVDTcentralised} \qquad (۳-۱)$$

- $NVDT_{centralised}$: تعداد بردارهای داده انتقال داده‌شده در حالت الگوریتم متمرکز
- $NVDT_{distributed}$: تعداد بردارهای داده انتقال داده‌شده در حالت الگوریتم توزیع‌شده

ایراد اساسی موجود این است که در طرح پیشنهادی آن‌ها مشخص نشده است که چه حملاتی پوشش می‌یابند و نتایج به‌صورت کلی بوده و فقط دقت تشخیص را ارائه کرده‌اند.



شکل (۳-۴) درصد کاهش سربار ارتباطات در مقابل پارامتر طول خوشه‌ها [۴۱]

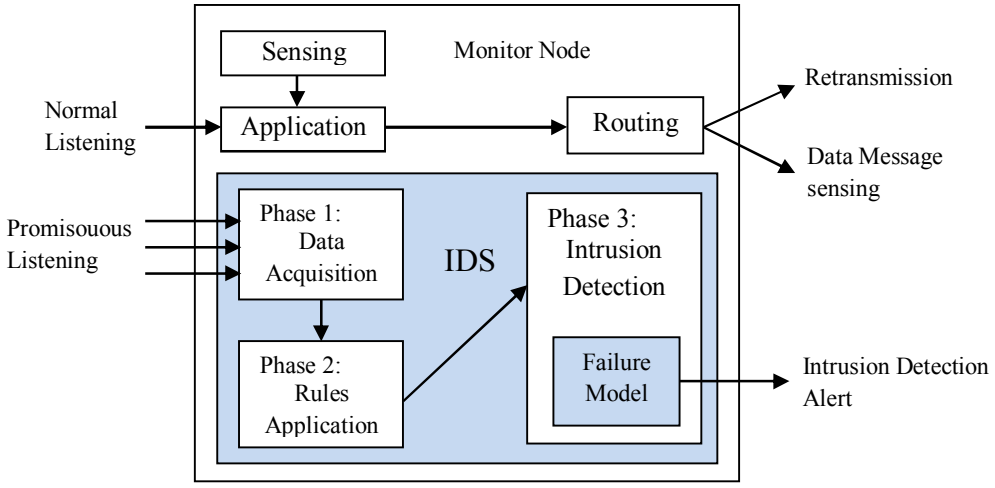
۳-۲- سیستم‌های تشخیص نفوذ مبتنی بر همکاری[1] (توزیع‌شده)

کرونتیریس و همکاران یک سیستم تشخیص نفوذ توزیع‌شده برای شبکه‌های حسگر بی‌سیم ارائه کردند که مبتنی بر همکاری گره‌های همسایه برای نظارت است. در یک محیط شبیه‌سازی، محققان اثرات طرح سیستم تشخیص نفوذشان را در مقابل حملات سیاه‌چاله و ارسال انتخابی ارزیابی نمودند [۴۲].

در تحقیقی دیگر کرونتیریس و همکاران یک راه‌حل برای مشکل تشخیص نفوذ مشارکتی در شبکه-های حسگر بی‌سیم پیشنهاد داده‌اند که در آن، گره‌ها با واحدهای تشخیص‌دهنده محلی مجهز شده‌اند و می‌بایست نفوذگر را به یک شیوه توزیع‌شده شناسایی نمایند [۴۳]. واحدهای تشخیص‌دهنده حدس‌های خود درباره یک نفوذگر را با حسگرهای همسایه در میان می‌گذارند. محققان با بررسی شرایط لازم و کافی برای شناسایی موفقیت‌آمیز مهاجم، الگوریتمی بر اساس مدل تهدید عمومی[2] را طراحی و ارائه داده‌اند. متأسفانه آن‌ها در این مدل تهدید مشخص نکرده‌اند که چه حملاتی را با چه دقتی پوشش می‌دهند. همچنین طرح پیشنهادی آن‌ها تنها قابلیت تشخیص یک مهاجم را دارد و اگر چند مهاجم باهم و به‌صورت هماهنگ حمله نمایند، قدرت تشخیص بقیه مهاجمان را ندارد. نتایج واضحی نیز به‌صورت شفاف برای ارزیابی ارائه نشده است. علاوه بر موارد یادشده آن‌ها هیچ بحثی در مورد مصرف انرژی نکرده‌اند.

داسیلوا و همکاران از یک الگوریتم تشخیص مبتنی بر خصوصیات به‌منظور تشخیص نفوذ استفاده کرده‌اند [۴۴]. محققان یک شیوه تشخیص توزیع‌شده را استفاده کردند که در آن تشخیص‌دهنده‌های نفوذ در میان شبکه به‌گونه‌ای توزیع‌شده‌اند که فواصل بین آن‌ها تک پرشه[3] بوده و کل شبکه را پوشش می‌دهند. سپس اطلاعات جمع‌آوری‌شده و پردازش آن‌ها در یک وضعیت توزیع‌شده انجام می‌شود. الگوریتم پیشنهادی آن‌ها عملیات خود را در سه مرحله اجرا می‌کند که به‌صورت زیر است:

[1] Collaborative
[2] General threat model
[3] One-hop



شکل (۳-۵) مراحل تشخیص نفوذ از معماری پیشنهادی داسیلوا و همکاران [۴۴]

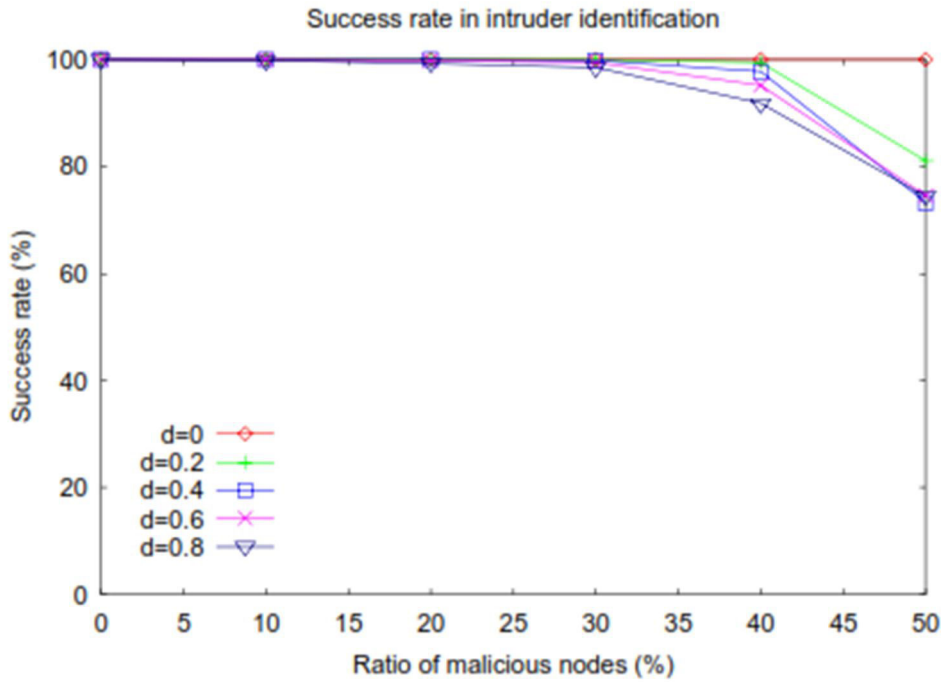
- **مرحله اکتساب داده‌ها:** در این مرحله پیام‌ها به شکل بی‌قاعده و تصادفی جمع‌آوری‌شده و قبل از ذخیره از میان آن‌ها اطلاعات مهم برای تجزیه‌وتحلیل بعدی، فیلتر می‌گردد.
- **مرحله اعمال قوانین:** این گام در حقیقت مرحله پردازشی است که در آن قوانین بر روی داده‌های ذخیره‌شده اعمال می‌شوند. اگر تحلیل پیام در تست‌های اعمال‌شده ناموفق باشد، در این صورت یک هشدار عدم موفقیت تولید خواهد شد.
- **مرحله تشخیص نفوذ:** این مرحله‌ای از تحلیل است که در آن تعداد هشدارهای تولیدشده با مقدار مورد انتظار از هشدارهای مرتبط در شبکه مقایسه می‌شود. اگر این تعداد از حد آستانه بیشتر باشد در این حالت یک هشدار تشخیص نفوذ تولید می‌شود.

ازآنجاکه در این شیوه توزیع‌شده، تشخیص‌دهنده‌های نفوذ در کل شبکه پخش‌شده‌اند، دید کامل‌تری نسبت به آن خواهند داشت و درنتیجه این شیوه در مقایسه با یک شیوه متمرکز هم مقیاس‌پذیرتر است و هم قدرت تشخیص بیشتری دارد. یکی از معایب طرح پیشنهادی آن‌ها وابسته بودن آن به اندازه بافر موردنیاز تشخیص‌دهنده‌های نفوذ است. به‌گونه‌ای که در اندازه بافر پایین دقت تشخیص کم می‌شود و برای افزایش دقت تشخیص نیاز به افزایش اندازه بافرها است، که این امر باعث می‌شود میزان مصرف انرژی و منابع مصرفی تشخیص‌دهنده‌های موجود در گره‌ها افزایش‌یافته و بنابراین طول

عمر شبکه کاهش می‌یابد که با توجه به منابع محدود شبکه‌های حسگر به‌ویژه حافظه و انرژی، مناسب و مطلوب نیست.

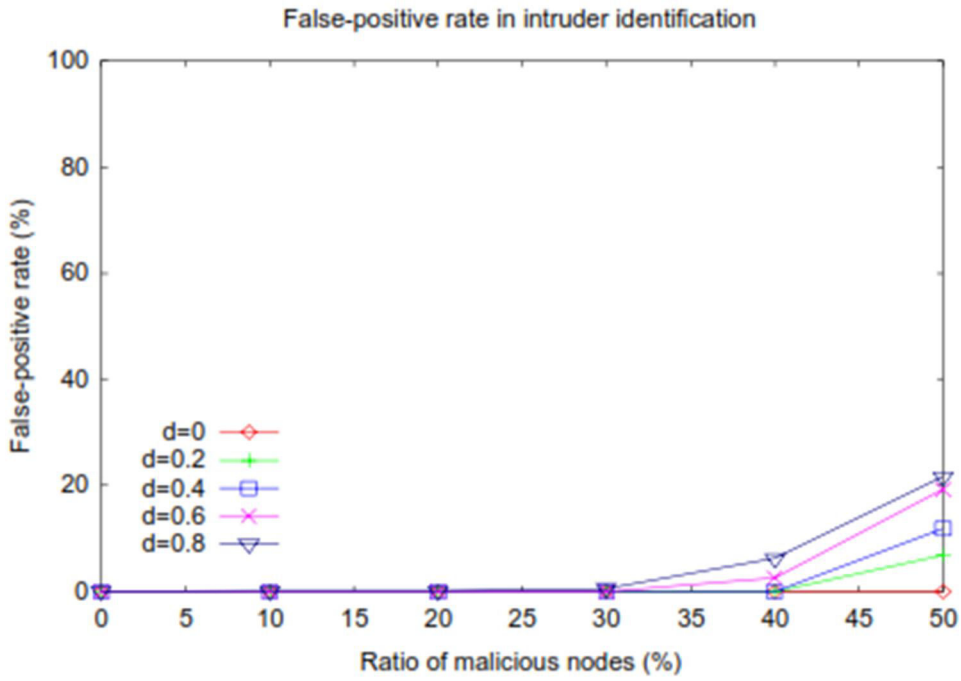
۳-۳- سیستم‌های تشخیص نفوذ مبتنی بر تشخیص آماری[1]

نگی و همکاران یک الگوریتم برای تشخیص نفوذگر در یک حمله حفره چاهک ارائه نمودند [۳۴]. الگوریتم پیشنهادی ابتدا یک لیست از گره‌های مشکوک را یافته و سپس نفوذگر را به‌صورت مؤثری از طریق یک گراف جریان شبکه[2] در لیست شناسایی می‌کند. الگوریتم یک تکنیک چند متغیره (تکنیک پارامتریک آماری) مبتنی بر آزمون Chi-Square را پیاده‌سازی می‌نماید. کارایی و دقت الگوریتم پیشنهادی به‌وسیله هر دو روش تحلیل عددی و شبیه‌سازی ارزیابی‌شده است. در شکل‌های (۳-۶) و (۳-۷) به ترتیب نرخ موفقیت و نرخ تشخیص نادرست الگوریتم تشخیص نفوذ پیشنهادی برحسب نسبت درصدی گره‌های مهاجم به کل گره‌ها ارائه‌شده است. پارامتر d نیز نشانگر نرخ حذف بسته‌ها می‌باشد که در شبکه وجود دارد.



شکل (۳-۶) نمودار نرخ موفقیت در شناسایی نفوذگر در مرجع [۳۴]

[1] Statistical detection based IDSs
[2] Network flow graph



شکل (۳-۷) نمودار نرخ شکست F-P در تشخیص نفوذگر [۳۴]

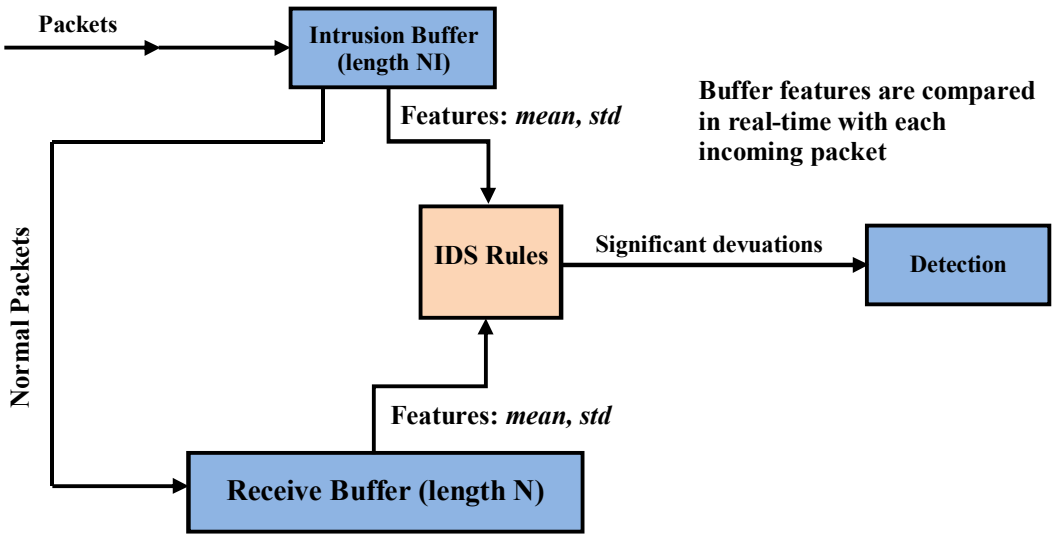
همچنین محققان ادعا کردند که میزان ارتباطات و سربار محاسباتی الگوریتمشان برای شبکه‌های حسگر بی‌سیم معقول است. ایراد اساسی طرح پیشنهادی آن‌ها در این است که فقط برای تشخیص حمله حفره چاهک ارائه‌شده است.

در الگوریتم پیشنهادشده توسط دومیت و آگراوال، شبکه حسگر متناسب با شرایط محیط موجود در آن، یک حد بهنجاری از پویایی را می‌پذیرد، به‌گونه‌ای که هر فعالیت غیر نابهنجار را بتواند بر اساس آن تمایز دهد [۴۵]. بدین منظور، آن‌ها یک مدل زنجیر مارکوف مخفی[1] را به کار گرفته‌اند. محققان ادعا کردند که الگوریتم پیشنهادی‌شان ازلحاظ استفاده آسان بوده و ازلحاظ پردازش و ذخیره‌سازی داده‌ها نیز حداقل منابع را احتیاج دارد. عملکرد و کارائی این الگوریتم از طریق سناریوهای آزمایشی برآورد شده است. الگوریتم پیشنهادی با استفاده از شیوه آماری هر رفتار غیرعادی را دفع می‌نماید. این روش نوع خیلی خاص از سیستم‌های تشخیص نفوذ است که به‌جای تمرکز بر روی امنیت گره‌ها یا لینک‌ها، اساساً بر روی داده‌های جمع‌آوری‌شده تمرکز دارد. متأسفانه آن‌ها مشخص نکرده‌اند که این

[1] Hidden Markov mode

الگوریتم چه نوع حملاتی را پوشش می‌دهد و این‌که آیا اصولاً تمرکز روی داده‌ها به‌جای فعالیت گره‌ها و لینک‌ها، قابلیت تشخیص انواع مختلف حملات را با چه دقتی خواهد داشت.

اونات و میری یک الگوریتم تشخیص ناهنجاری بلادرنگ مبتنی بر گره[1] پیشنهاد کرده‌اند [۴۶] که همه فرآیندهای انجام‌شده توسط یک گره را بررسی می‌نماید (شکل ۳-۸). آن‌ها مدل ترافیک ورودی یک گره حسگر را بدست آوردند و همچنین طرحی را برای تشخیص تغییرات غیرعادی در آن ترافیک ورودی ابداع کردند. الگوریتم تشخیص، آمارهای کوتاه‌مدتی را با استفاده از طرح ذخیره‌سازی وقایع مبتنی بر یک پنجره لغزان چند سطحی، نگهداری می‌نماید. با این شیوه الگوریتم می‌تواند ترافیک ورودی را در دوره‌های زمانی مختلفی مقایسه نماید. محققان ادعا کردند که الگوریتم آن‌ها ازلحاظ منابع کارا بوده و پیچیدگی پایینی دارد. طرح پیشنهادی آن‌ها با توجه به این‌که تشخیص‌دهنده‌های نفوذ به‌صورت محلی بر روی داده‌های گره‌ها فعالیت می‌کنند، قابلیت تشخیص حملات عمومی و سراسری که توسط چند مهاجم انجام شود را ندارد. همچنین فقط برای شبکه‌های حسگر با فعالیت ایستا که تغییر و پویایی کمی در ترافیک دریافتی دارند مناسب است.

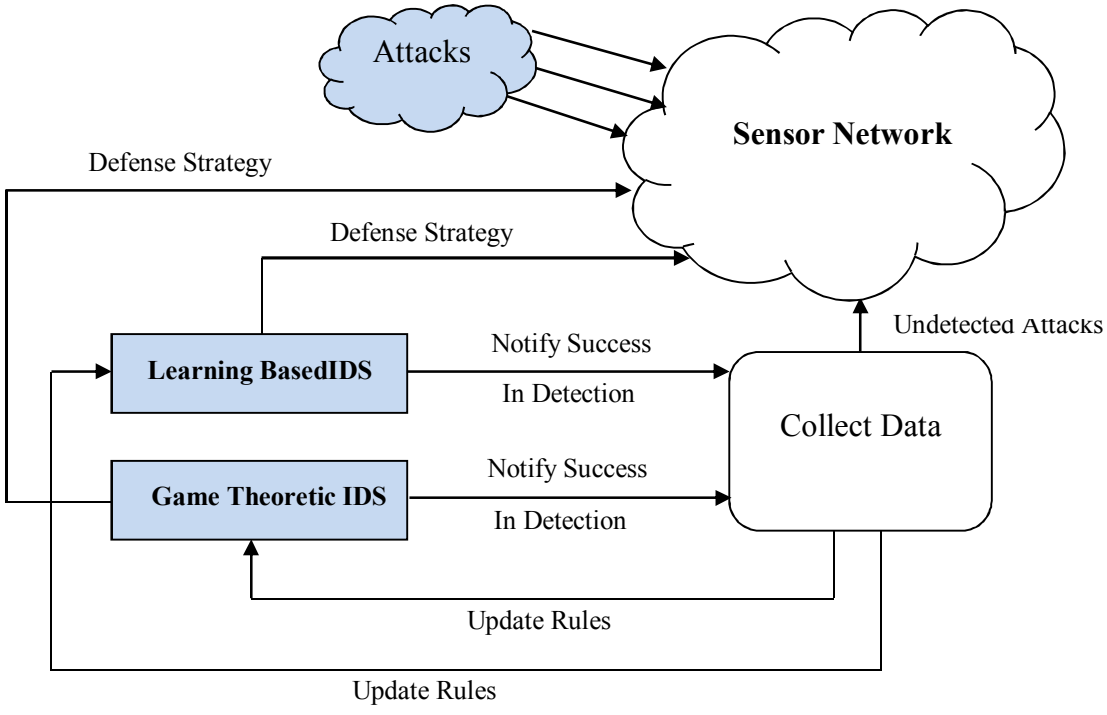


شکل (۳-۸) تشخیص ناهنجاری بلادرنگ مبتنی بر ترافیک ورودی [۴۶]

[1] Real time node based anomaly detection algorithm

۳-۴- سیستم‌های تشخیص نفوذ مبتنی بر نظریه بازی[1]

برخی از محققان حمله و تشخیص آن را به‌عنوان طرفین یک بازی در نظر گرفته‌اند و تدابیری را برای هر دو طرف بازی تنظیم نموده‌اند [۴۷] و [۴۸]. چنین طرح‌هایی بر روی شناسایی ضعیف‌ترین گره در شبکه و ایجاد تدابیری برای دفاع از آن گره تمرکز دارند. بر طبق مفروضات روش پیشنهادی آن‌ها (شکل ۳-۹)، در هرلحظه فقط یکی از خوشه‌ها نظارت می‌شود و مابقی شبکه بدون حفاظت رها می‌شود. بنابراین در صورت وجود چندین مهاجم در شبکه حسگر بی‌سیم، تنها یکی از آن‌ها توسط سیستم تشخیص نفوذ شناسایی می‌گردد درحالی‌که مابقی مهاجمان بدون شناسایی رها می‌شوند. یکی دیگر از مشکلات اساسی روش‌های مبتنی بر نظریه بازی این است که این سیستم‌ها غیر وفقی هستند و همچنین برای یک عملیات پایدار نیازمند دخالت انسان می‌باشند.



شکل (۳-۹) یک دید کلی به سیستم شخیص نفوذ مبتنی بر نظریه بازی‌ها [۴۷]

[1] Game theory based IDSs

۳–۵– سیستم‌های تشخیص نفوذ مبتنی بر تشخیص ناهنجاری

راجاسگارار و همکاران در مقاله خود جدیدترین تکنیک‌های تشخیص ناهنجاری برای شبکه‌های حسگر بی‌سیم را مرور کرده‌اند [۳۲]. جمع‌بندی آن‌ها در این مقاله این است که در طراحی روش‌های تشخیص ناهنجاری برای کمینه‌سازی مصرف انرژی در گره‌های حسگر و بیشینه‌سازی عمر شبکه باید به محدودیت‌های ذاتی شبکه‌های حسگر توجه داشت.

همان محققان راه‌حلی را برای مسئله کمینه‌سازی سربار ارتباطات در شبکه در هنگام انجام محاسبات درون‌شبکه‌ای برای تشخیص ناهنجاری‌ها پیشنهاد کرده‌اند [۴۹]. بدین منظور آن‌ها از رده‌بند بردار پشتیبان (SVM) تک‌کلاسه با هسته ربع-کروی quarter-sphere توزیع‌شده در گره‌های مختلف شبکه، جهت شناسایی ناهنجاری‌های موجود در داده‌های اندازه‌گیری‌شده بهره می‌گیرند. جهت بررسی‌های بیشتر بردارهای داده از فضای ورودی به یک فضای با ابعاد بیشتر نگاشت داده می‌شوند. ایشان طرح خود را در یک پروژه واقعی پیاده‌سازی و نشان دادند که این طرح درعین آنکه ازلحاظ دقت با یک طرح متمرکز قابل‌مقایسه است، به لحاظ سربار ارتباطات و کاهش مصرف انرژی نیز کارآ است. متأسفانه آن‌ها بیشتر بر روی پیچیدگی محاسباتی مدلشان بحث کرده و درباره پوشش حملات مختلف هیچ بحثی نشده و مشخص نیست این روش چه حملاتی را با چه درصدی تشخیص می‌دهد.

جهت شناسایی و تشخیص حملات رد سرویس درون خوشه‌ای، روشی به نام MOM ارائه‌شده است [۵۰]. روال کار آن به این صورت است که دو لیست از پیام‌های عادی و پیام‌های نامعتبر ایجاد می‌کند و برای هر پیام جدید ورودی، ابتدا آن را با لیست پیام‌های نامعتبر مقایسه کرده و عدم اعتبار آن را تشخیص می‌دهد. همچنین در صورت معتبر بودن پیام آن را با لیست پیام‌های عادی نیز مقایسه می‌کند تا تکراری بودن آن را تشخیص دهد. دو مشکل اساسی این روش، نیازمندی به حافظه بالا به جهت نگهداری لیست پیام‌های عادی و نامعتبر و دیگری عدم‌تشخیص پیام‌های نامعتبر جدید و غیرتکراری است.

بهوس و گوپتا متدهای سبک‌وزنی[1] را برای تشخیص نفوذهای غیرعادی در شبکه‌های حسگر بی‌سیم پیشنهاد کرده‌اند [۵۱]. ایده اصلی آن‌ها مبتنی بر استفاده مجدد از اطلاعات سیستمی قبلی و موجود در شبکه مبتنی است. اطلاعاتی مانند لیست همسایه‌ها، جداول مسیریابی، زمان‌بندی‌های فعال و غیرفعال شدن، اطلاعات شدت سیگنال دریافتی، زمان‌بندی ارسال در لایه MAC که در لایه‌های مختلف پشته پروتکلی شبکه به‌ویژه در لایه‌های فیزیکی، MAC و مسیریابی، تولیدشده‌اند. به‌منظور ارتقاء نرخ تشخیص، آن‌ها استفاده از چندین تشخیص‌دهنده را برای نظارت بر لایه‌های مختلف شبکه پیشنهاد داده‌اند. البته به‌کارگیری این روش برای شبکه‌های حسگر امکان‌پذیر نیست، زیرا نظارت بر نفوذ در لایه‌های مختلف و حفظ هماهنگی بین این ناظرها می‌تواند به‌سرعت منابع محدود موجود در شبکه حسگر را مصرف نموده و تخلیه کند. از طرف دیگر، این طرح تنها برای شناسایی حملات خارجی مؤثر است و حملات داخلی را در نظر نمی‌گیرد. این امر نقص بزرگی است چراکه گره‌های حسگر در یک شبکه حسگر بی‌سیم برای حملات داخلی (مانند حمله تسخیر فیزیکی گره‌ها، حمله سایبیل و غیره) بسیار مستعد هستند.

روش اونات و میری حملات را با آشکارسازی ناهنجاری‌های توان بسته‌های دریافتی تشخیص می‌دهد [۵۲]. طرح تشخیص آن‌ها بر روی رفتار فرستنده/گیرنده و نرخ ورود بسته‌ها از گره‌های همسایه به یک گره خاص نظارت دارد. پیش‌فرض محققان در این روش این است که هر گره شبکه الگوی ارتباطی ثابتی در حین عملیات دارد و درنتیجه "هر گره یک مدل آماری ساده از رفتار همسایه‌های خودش ایجاد می‌نماید و آن را برای تشخیص تغییرات غیرعادی رفتار آینده آن‌ها به کار می‌برد." مدل پیشنهادی برای تشخیص حملات جعل هویت[2] خوب کار می‌کند. البته باید توجه داشت که این فرض تنها برای شبکه‌های حسگر بی‌سیم غیر سیار و دارای محیطی با شرایط عملیاتی به لحاظ آماری ایستان صادق است و در شبکه‌های سیاری مانند MANET و کاربردهایی که شرایط عملیاتی آن دستخوش تغییرات ناگهانی باشد، نمی‌تواند برقرار باشد.

[1] Lightweight methods
[2] Impersonation attacks

در تحقیقی دیگر یک رهیافت تشخیص نفوذ مبتنی بر دانش[1] (KBIDS) برای تشخیص چندین نوع از حملات تحت ساختار مختلف شبکه ارائه‌شده که هدف از آن طراحی یک مدل تشخیص مستقل از ساختار شبکه برای شبکه‌های حسگر بی‌سیم است [۵۳]. سازوکار پیشنهادی بر این واقعیت استوار است که انواع مختلف حملات به‌احتمال‌زیاد دارای اشکال مختلف تراکم در فضای ویژگی هستند. بنابراین پس از استخراج بردار ویژگی ترافیک شبکه از آن به‌عنوان مشخصه رفتار تصادفی شبکه برای تشخیص حملات مختلف در فضای ویژگی استفاده کرده‌اند. الگوی تراکم بردار مشخصات در حملات مختلف می‌تواند به‌عنوان یک شاخص برای تمایز رفتار عادی و غیرعادی شبکه موردتوجه قرار گیرد. نتایج حاصل از شبیه‌سازی بر روی سه حمله سیاه‌چاله، سیل ارسال پیام و رد سرویس نشان‌دهنده دقت تشخیص مناسب و سازگاری بالا با ساختار شبکه نسبت به سایر کارهای موجود است [۵۳].

۳-۶- سیستم‌های تشخیص نفوذ مبتنی بر مراقب[2]

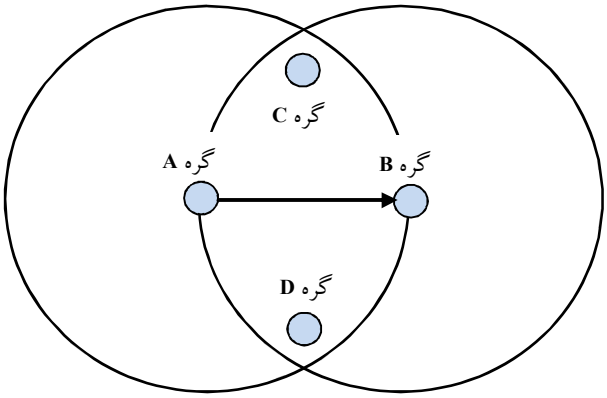
رومن و همکاران راهکارهایی را درباره کاربرد سیستم‌های تشخیص نفوذ برای شبکه‌های اقتضایی سیار (MANET) ارائه داده‌اند [۵۴]. آن‌ها یک سیستم تشخیص نفوذ برای شبکه‌های حسگر پیشنهاد کردند که "مراقب فوری[3]" نامیده می‌شود. در این طرح، به جهت صرفه‌جویی و بهینه‌سازی مصرف انرژی، بجای آنکه تمام گره‌ها درصدد کشف الگوی ارتباطی گره‌های همسایه باشند، در هر بخش از شبکه برخی گره‌ها به‌عنوان ناظر انتخاب می‌شوند تا به‌طور مستقل بر ارتباطات موجود در گره‌های همسایه-شان نظارت نمایند. با توجه به محدودیت‌های منابع موجود در شبکه‌های حسگر و به‌منظور افزایش بهره‌وری انرژی، در طراحی سیستم تشخیص نفوذ از دو نوع عامل استفاده‌شده که عبارتند از:

عامل محلی: این عامل بر فعالیت‌های محلی و ارسال و دریافت اطلاعات توسط حسگر نظارت می-کند. این عامل فقط زمانی که حسگر فعال باشد اجرا می‌شود و در آن حسگر تنها ارتباطات خودش را مدیریت می‌کند. بنابراین سربارهای تحمیلی به حسگر کم خواهد بود.

[1] Knowledge Based IDS (KBIDS)
[2] Watchdog based IDS
[3] Pontaneous watchdogs

عامل سراسری: این عامل باید بر ارتباطات همسایگانش نظارت نماید و به‌عنوان یک مراقب رفتار می‌کند. با توجه به سربار بالای این عامل‌ها، آن‌ها فقط بر روی برخی گره‌های منتخب اجرا می‌شوند.

با تکیه‌بر ماهیت پخش همگانی در ارتباطات حسگرها، روش مراقب فوری از مزیت چگالی بالای حسگرهای مستقرشده در محیط استفاده می‌نماید. در شکل (۳-۱۰) این امر نشان داده‌شده است که در هر بخش از شبکه مجموعه‌ای از گره‌ها وجود دارند که می‌توانند هم بر بسته‌های ارسالی از گره‌های همسایه و هم بر ارسال آن‌ها از گره بعدی نظارت نمایند. بنابراین این گره‌ها می‌توانند گزینه مناسبی برای انتخاب به جهت استقرار عامل‌های سراسری برای نظارت بر بسته‌های مبادله شده در همسایگان باشند.



شکل (۳-۱۰) گزینه‌های ممکن برای انتخاب گره ناظر برای استقرار مراقب فوری [۵۴]

هرچند محققان ادعا دارند که با به‌کارگیری عامل‌های تشخیص نفوذ بر اساس طرح فوق، کارایی و بهره‌وری سیستم تشخیص نفوذ شبکه‌های حسگر بی‌سیم معقول خواهد بود ولی چند نقد بر این طرح وارد است. اول آنکه طرح پیشنهادی آن‌ها برای شبکه‌های حسگر بی‌سیم ایستا ارائه‌شده است که با توجه به پویایی ذاتی شبکه‌های حسگر، مناسب نیست و مهم‌تر اینکه با توجه به مصرف انرژی بالای عامل‌های سراسری، گره‌های هدف این عامل‌ها به‌سرعت منابع را مصرف می‌نمایند.

در مقاله بیگ مدلی مبتنی بر شناسایی الگو[1] برای حملات فرسودگی منابع ارائه‌شده که می‌تواند برای حملات رد سرویس نیز بکارگرفته شود [۵۵]. در این مقاله از یک سری گره‌های خاص به جهت

[1] Pattern Recognition

نظارت بر ترافیک شبکه استفاده‌شده است تا بر اساس مدل الگوی خاصی که شناسایی‌شده ترافیک عادی را از ترافیک غیرعادی تشخیص دهد.

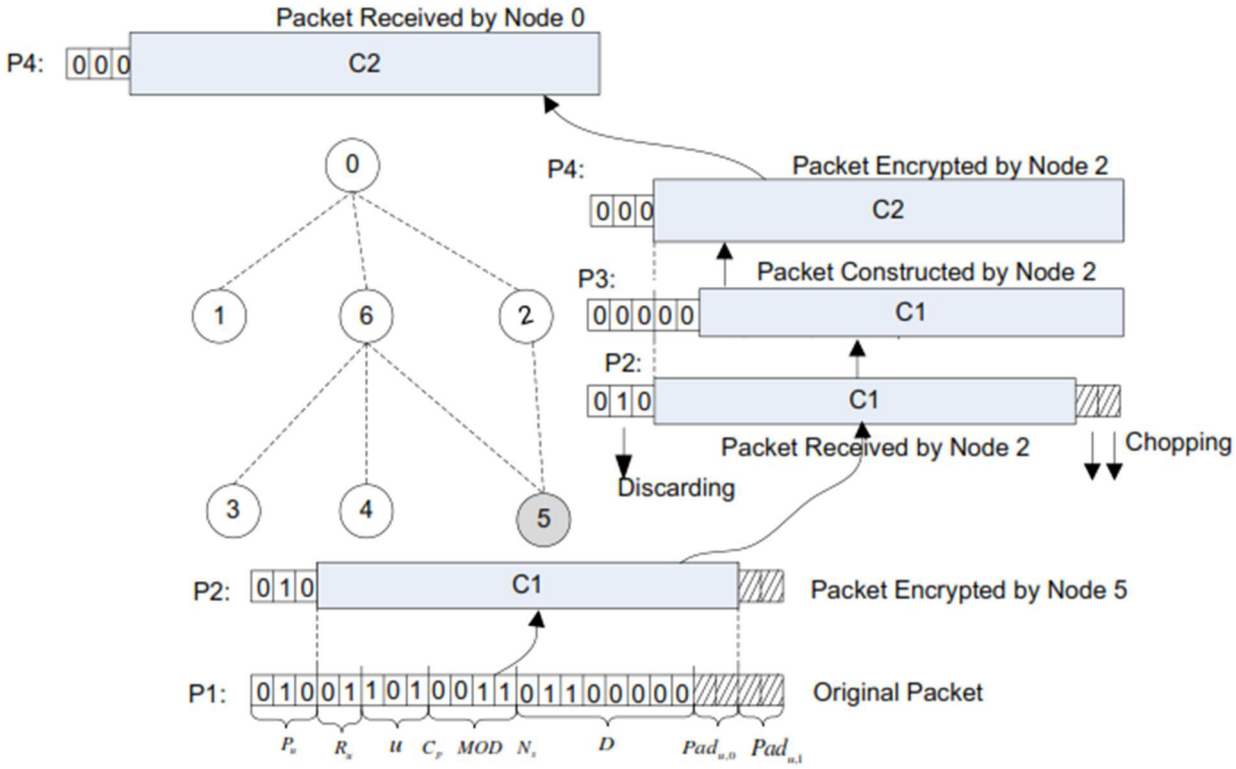
هسیه و همکاران یک سیستم تشخیص نفوذ سبک مبتنی بر دانش تشخیص[1] (OWIDS) ارائه داده‌اند که از یک سری گره‌های نگهبان برای تشخیص نفوذ استفاده می‌کند [۵۶]. گره نگهبان درواقع یک گره حسگری است که دانش چگونگی تشخیص حملات را در خود دارد. این گره‌ها از طریق جمع‌آوری اطلاعات از گره‌های حسگر و اعمال دانش تشخیص روی آن‌ها، بر گره‌های دیگر نظارت می‌کنند. این روش برای بالا بردن قدرت تشخیص نفوذ گره‌های نگهبان، روابط بین گره‌های حسگر را نیز در دانش تشخیص تعریف می‌کند. روش آن‌ها ازلحاظ مصرف انرژی سبک است اما با توجه به استفاده از گره-های نگهبان که عملاً یک سربار برای شبکه است، هزینه مصرف انرژی شبکه در کل افزایش خواهد یافت. همچنین دقت تشخیص نیز بسته به تعداد گره‌های نگهبان در شبکه تغییر می‌کند.

۳-۷- سیستم‌های تشخیص نفوذ مبتنی بر شهرت[2] (اعتماد[3])

یک مدیریت اعتماد سلسله مراتبی برای شناسایی گره‌های خودخواه و بدرفتار در شبکه‌های حسگر بی‌سیم پیشنهادشده است [۳۵]. مدل احتمالی ارائه‌شده در این تحقیق برای تجزیه‌وتحلیل کارایی پروتکل مذکور از روش مدل‌سازی شبکه‌های پتری تصادفی استفاده می‌کند. این مدل، اعتماد مورد انتظار را با اعتماد واقعی بدست آمده بر اساس وضعیت گره موجود مقایسه و خروجی مدل را بر این اساس ارزیابی می‌نماید. این الگوریتم تشخیص نفوذ مبتنی بر اعتماد، در شرایطی که نرخ عدم‌تشخیص نفوذ را به‌اندازه کافی پایین نگه می‌دارد، دقت تشخیص بهتری هم نسبت به الگوریتم‌های تشخیص نفوذ مبتنی بر ناهنجاری دارد. در این طرح دقت تشخیص وابسته به یک حد آستانه است که با افزایش آن، مصرف انرژی بالا رفته و طول عمر شبکه کاهش می‌یابد. همچنین هیچ صحبتی درباره حملات قابل پوشش نشده و ارزیابی کلی بر روی درصد تشخیص انجام‌شده است.

[1] Ontology-based Wireless IDS (OWIDS)
[2] Reputation based IDS
[3] Trust

روش دیگر تشخیص نفوذ برای شبکه‌های حسگر مبتنی بر اعتماد توسط ونگ و همکاران پیشنهادشده است [۵۷]. همان‌طور که در شکل (۳-۱۱) نشان داده‌شده در این روش بسته‌های داده علامت‌گذاری می‌شوند و سپس الگوریتم‌های رتبه‌بندی اکتشافی را برای شناسایی محتمل‌ترین گره‌های بد در شبکه به کار می‌برد. به دلیل این‌که مبدأ بسته مخفی بماند هر بسته همراه با اطلاعات ساختگی رمزگذاری می‌شود. در ادامه علامت مشخصه‌ای در هر بسته اضافه می‌گردد به‌گونه‌ای که گره چاهک بتواند مبدأ بسته را بازیابی نموده و سپس نرخ حذف مرتبط با هر گره حسگر را تعیین می‌کند. بر طبق شبیه‌سازی‌ها، اغلب گره‌های بد به‌وسیله الگوریتم رتبه‌بندی آن‌ها همراه با نرخ پایینی از نرخ تشخیص نادرست، می‌توانند شناسایی شوند. ایراد اصلی طرح پیشنهادی آن‌ها این است که فقط برای حملات حذف بسته ارائه‌شده و تنها روی انواع مختلفی از سناریوهای حذف بسته امتحان شده است.



شکل (۳-۱۱) مثالی از رمزنگاری و ارسال بسته [۵۷]

۳-۸- سیستم‌های‌تشخیص‌نفوذ مبتنی بر داده‌کاوی[1]

در تحقیق ژو یک چارچوب[2] وفقی مبتنی بر یادگیری ماشین برای تشخیص نفوذ ارائه‌شده است [۵۸]. او در طرح خود، از ماشین‌های بردار پشتیبان چندکلاسه[3] برای رده‌بندی حملات استفاده‌کرده است.

صفیر و همت‌یار با استفاده از تئوری مجموعه راف، بهترین زیر مجموعه از ویژگی‌های لایه مک را که بتوان توسط آن‌ها با سرعت بیشتری به تشخیص نفوذ پرداخت را استخراج کرده‌اند[۵۹]. همچنین برای بهبود دقت تشخیص یک مدل تشخیص بر مبنای سیستم ایمنی مصنوعی مبتنی بر تئوری خطر را ارائه کرده‌اند. آن‌ها ادعا کرده‌اند که روش پیشنهادی برای کاهش ویژگی، دارای کاهش شدید زمان یادگیری و محاسبه الگوریتم طبقه‌بندی حملات بدون کاهش چشمگیر در دقت تشخیص می‌باشد.

در تحقیقی دیگر باغچه‌بند و همکاران روش‌های داده‌کاوی را برای انتخاب ویژگی‌های مهم بکار برده و با ترکیب شبکه عصبی و الگوریتم ژنتیک در راستای کاهش بار محاسباتی، وضعیت ارتباط مربوطه را از لحاظ ناهنجاری تشخیص می‌دهد [۶۰].

معیارهای ارزیابی سیستم‌های تشخیص نفوذ برای رده‌بندهای دوکلاسه توسط الحمامی و همکاران بررسی‌شده‌اند [۶۱] و با توجه به مناسب نبودن این معیارها برای ارزیابی سیستم‌های تشخیص نفوذ چند کلاسه، معیارهای ارزیابی جدیدی ارائه‌شده است. در انتها نیز بررسی و ارزیابی رده‌بندی حملات بر پایه معیارهای پیشنهادشده، بر روی مجموعه‌دادگان KDDCup'99 صورت گرفته است.

جهت افزایش کارائی سیستم‌های تشخیص نفوذ می‌توان اطلاعات موجود در مجموعه‌دادگان KDDCup'99 را تحلیل و انواع مختلفی از ویژگی‌ها را استخراج کرد [۶۲]. آگراوال و شارما ویژگی‌های استخراج‌شده را در چهار کلاس پایه، محتوا، ترافیک و میزبان رده‌بندی کرده‌اند. آن‌ها ویژگی‌های ترکیبی این کلاس‌ها را باهم در نظر گرفته و با رده‌بندی آن‌ها با الگوریتم درخت تصادفی نتایج بدست آمده را با نتایج روش‌های دیگر بر اساس نرخ تشخیص و نرخ هشدار اشتباه[4] مقایسه نموده‌اند.

---

[1] Datamining Base IDSs
[2] Framework
[3] Multi-class Support Vector Machines (SVMs)
[4] False Alarm Rate (FAR)

در روشی مشابه پس از استخراج ویژگی با تمرکز بر خصوصیات آماری مربوط به ویژگی‌های استخراج‌شده از مجموعه‌داده، به‌منظور بهبود دقت و کارائی سیستم تشخیص نفوذ، ویژگی‌های متمایزکننده حملات مختلف شناسایی و انتخاب می‌شوند تا مجموعه پیرایش شده و هدفمندی از ویژگی‌های مؤثر بدست آیند [۶۳]. در همین راستا، یک سری روش‌های پیش‌پردازش داده‌ها مانند پر کردن مقادیر گم‌شده، حذف نمونه‌های داده‌های تکراری و هنجارسازی نمونه‌ها، پیشنهادشده و بر اساس الگوریتم‌های مختلف داده‌کاوی بر روی مجموعه‌دادگان اعمال‌شده‌اند.

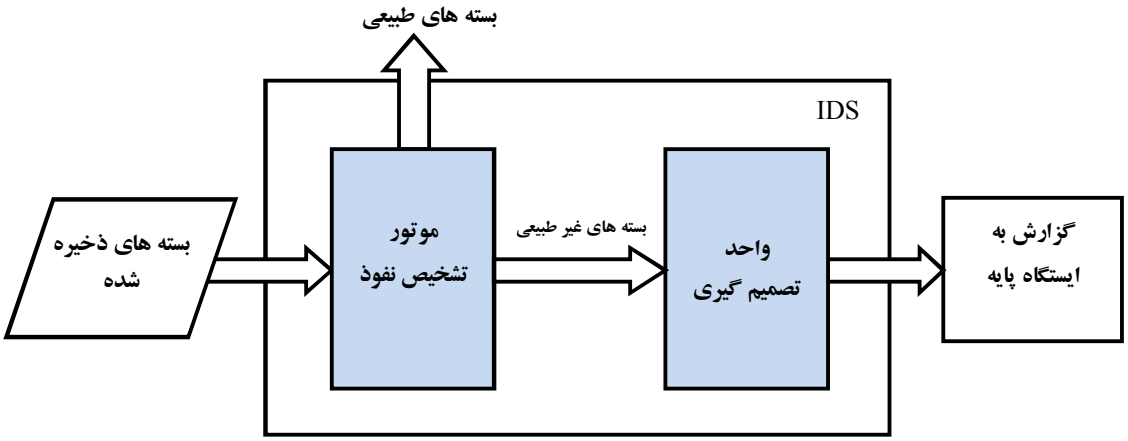
هنجارسازی[1] ویژگی‌ها همواره به‌عنوان یک گام اساسی در پیش‌پردازش داده‌ها مطرح بوده است. اثر روش‌های مختلف هنجارسازی در بهبود کارائی و افزایش دقت سیستم‌های تشخیص نفوذ، توسط ونگ و همکاران موردتوجه قرارگرفته است [۶۴]. در این تحقیق، چهار طرح مختلف برای هنجارسازی ویژگی‌ها در مرحله پیش‌پردازش داده‌ها در سیستم‌های تشخیص نفوذ معرفی‌شده است که توسط رده‌بندهای مختلف بر روی مجموعه‌دادگان KDDCup'99 مورد ارزیابی و مقایسه قرارگرفته‌اند. بر اساس نتایج حاصل از شبیه‌سازی‌ها مدل هنجارسازی آماری به‌عنوان بهترین انتخاب برای مجموعه داده‌های بزرگ معرفی‌شده است.

یک روش چند کلاسه تشخیص حملات در شبکه‌های حسگر بی‌سیم با هدف بهبود کارائی توسط ژو و همکاران ارائه‌شده است [۶۵]. الگوریتم ارائه‌شده بر پایه کدهای خروجی اصلاح خطا (ECOC[2]) مکار می‌کند. این روش می‌تواند برای رده‌بندی داده‌های ترافیکی جمع‌آوری‌شده به‌وسیله گره‌های شبکه استفاده گردد تا تعیین نماید که آیا سیستم موردتهاجم حملات قرارگرفته یا خیر. در این روش از رده‌بند چند کلاسه‌ای بر پایه ماتریس هادامارد و همین‌طور ماشین بردار پشتیبان دو کلاسه استفاده‌شده است. همچنین از روش کدگذاری تُنُک[3] به‌منظور کمینه‌سازی پیچیدگی الگوریتم پیشنهادی استفاده‌شده است.

[1] Features Normalization
[2] Error Correcting Output Codes (ECOC)
[3] sparse coding method

۳-۹- سیستم‌های تشخیص نفوذ ترکیبی[1]

یک روش ترکیبی برای تشخیص توسط دشموک و همکاران ارائه‌شده است [۷]. همان‌طور که در شکل ۳-۱۲ نشان داده‌شده است، آن‌ها از ادغام دو روش خوشه‌بندی و مبتنی بر قانون به جهت رسیدن به مزایای هر دو روش، استفاده کرده و روش پیشنهادی ترکیبی خود را ایجاد نمودند. آن‌ها ادعا کردند که این ترکیب، سهولت در عملکرد، کاهش در مصرف انرژی و امنیت بالا را به ارمغان می‌آورد. با توجه به سه نوع از گره‌ها در سیستم خوشه‌بندی، یعنی گره‌های عادی، سرخوشه‌ها و ایستگاه پایه، عملیات متفاوتی را برای تشخیص نفوذ در آن‌ها تعریف‌شده‌اند. متأسفانه آن‌ها در شبیه‌سازی‌های انجام‌شده نتایج واضحی را برای ارزیابی ادعاهای خود ارائه نکرده‌اند.



شکل (۳-۱۲) معماری ترکیبی برای تشخیص نفوذ [۷]

در روشی دیگر، یک سیستم تشخیص نفوذ ترکیبی سراسری[2] (GHIDS) ارائه‌شده است [۶۶] که ترکیبی از یک روش تشخیص ناهنجاری مبتنی بر رده‌بند ماشین بردار پشتیبان (SVM) و یک مجموعه از قوانین مبتنی بر خوشه‌بندی را برای تشخیص حملات در شبکه‌های حسگر بی‌سیم به‌منظور دستیابی به‌دقت تشخیص بالا و نرخ هشدار نادرست پایین، بکار می‌گیرد. نتایج حاصل از شبیه‌سازی‌ها نشان می‌دهد که روش پیشنهادی آن‌ها ازلحاظ نرخ تشخیص و نرخ هشدار نادرست در

[1] Hybrid IDSs
[2] Global Hybrid IDS (GHIDS)

وضعیت مطلوبی قرار دارد. اما مشکل اساسی آن‌ها بالا بودن مصرف انرژی به جهت استفاده از روش مبتنی بر تکنیک ماشین بردار پشتیبان (SVM) است که سربار آن برای شبکه حسگر مناسب نیست.

یک سیستم تشخیص نفوذ مشابه با GHIDS توسط سجلماچی و فهام ارائه‌شده است [۶۷] که به جهت کاهش پیچیدگی محاسباتی و مصرف انرژی، ویژگی‌های موجود به چهار ویژگی کاهش داده‌شده‌اند. هرچند با این روش بهبود چشمگیری در مصرف انرژی ایجادشده است، اما باید توجه داشت که دقت تشخیص آن از روش قبلی پایین‌تر است.

یک سیستم تشخیص نفوذ ترکیبی دیگر نیز ارائه‌شده که برای شناسایی گره‌های مهاجم روش تشخیص نفوذ مبتنی بر خوشه‌بندی را با روش قوانین تشخیص رفتار سوء و اعتبارسنجی عملکرد ترکیب می‌کند [۶۸]. ایده اصلی روش پیشنهادی این است که بجای اینکه حملات فقط در سطح گره‌ها تشخیص داده شوند، یک طرح متمرکز مبتنی بر همکاری گره‌ها و با استفاده از ارزیابی اعتماد متقابل بین همه اجزاء شبکه این کار را برعهده بگیرد. بدین منظور باید هر گره حسگر مقادیر مربوط به اعتبار عملکرد همسایه‌های خود را به‌وسیله مشاهده فعالیت‌های آن‌ها (نقل و انتقالات و تجمیع داده‌ها) محاسبه کند. برای رسیدن به این هدف آن‌ها پنج معیار اعتبارسنجی عملکرد تعریف کرده و از مزیت نرخ تشخیص بالای شیوه تشخیص رفتار سوء نیز با اعمال قوانین مربوطه بهره برده‌اند. مشکل اصلی روش آن‌ها این است که صرفاً نتایج خود را ازلحاظ مصرف انرژی بیان کرده‌اند و هیچ بحثی بر روی انواع حملات قابل‌شناسایی و نرخ تشخیص آن‌ها ارائه نکرده‌اند.

در تحقیقی دیگر، یک سیستم تشخیص نفوذ یکپارچه[1] (IIDS) برای شبکه‌های حسگر بی‌سیم ناهمگن ارائه‌شده است [۶۹]. در این تحقیق، با توجه به قابلیت‌های متفاوت گره‌های شبکه و همچنین احتمالات متفاوت تهاجم به آن‌ها، سه سیستم تشخیص نفوذ جداگانه برای گره چاهک، سرخوشه و گره‌های عادی طراحی‌شده است. در گره‌های عادی از یک روش تشخیص ناهنجاری مبتنی بر قانون

[1] Integrated IDS

استفاده‌شده است، اما جزئیات روش بیان‌نشده و نتایجی نیز در این مورد ارائه نداده‌اند. برای سرخوشه-ها نیز یک روش تشخیص ترکیبی از روش‌های مبتنی بر ناهنجاری و مبتنی بر رفتار سوء ارائه‌شده که با استفاده از روش انتخاب ویژگی SVM، ویژگی‌های موجود به ۲۴ ویژگی کاهش داده‌شده است. درنهایت از رده‌بند شبکه عصبی سه لایه با الگوریتم یادگیری انتشار به عقب[1] برای رده‌بندی نمونه‌ها استفاده کرده‌اند. در گره چاهک نیز روشی یکسانی با سرخوشه‌ها استفاده‌شده با این تفاوت که در انتهای کار به آن یک الگوریتم یادگیری ART[2] برای رده‌بندی حملات تشخیص داده نشده در مرحله قبل، اضافه کرده‌اند. این روش به دلیل نرخ پایین هشدارهای نادرست و همچنین پیچیدگی محاسباتی کم، قابل‌استفاده در شبکه‌های حسگر بی‌سیم است، اما مشکل اصلی آن نرخ نسبتاً پایین تشخیص است که مخصوصاً برای گره‌های سرخوشه با توجه به اهمیت عملیات آن‌ها، نامناسب خواهد بود.

چندین سیستم تشخص نفوذ ترکیبی هم پیشنهادشده‌اند که در ابتدا به‌منظور کاهش پیچیدگی محاسباتی از الگوریتم‌های ابتکاری برای انتخاب ویژگی‌ها سود برده و سپس از ماشین بردار پشتیبان برای رده‌بندی نمونه‌ها استفاده می‌کنند [۷۰]، [۷۱] و [۷۲]. ژینگژو روش بهینه‌سازی کلونی مورچگان[3] را با رده‌بندی SVM ترکیب ساخته تا با امتیازدهی به ویژگی‌های مختلف، مؤثرین آن‌ها را انتخاب کند. با این روش او توانست درنهایت تعداد ویژگی‌ها را به ۲۵ ویژگی کاهش دهد [۷۰]. اصلحی و همکاران از الگوریتم ژنتیک برای انتخاب ویژگی‌ها استفاده می‌کنند که تعداد ویژگی‌ها را به ۱۰ ویژگی کاهش داده‌اند [۷۱]. آچاریا و سینق نیز الگوریتم قطره آب هوشمند[4] (IWD) را برای انتخاب ویژگی‌ها بکار می‌برند و درنهایت تعداد ویژگی‌ها را به ۹ ویژگی کاهش می‌دهند [۷۲].

ایراد اصلی هر سه روش فوق پیچیدگی محاسباتی نسبتاً بالا به جهت استفاده از الگوریتم رده‌بندی SVM است که با مصرف انرژی بالا شبکه‌های حسگر بی‌سیم را با مشکل مواجه می‌کند.

[1] Back Propagation Network (BPN)
[2] Adaptive Resonance Theory (ART) Network
[3] Ant Colony Optimization (ACO)
[4] Intelligent Water Drops (IWD) Algorithm

الگوریتم CuttleFish تغییریافته[1] (MCFA) با انتخاب یک زیرمجموعه مناسب از مرتبط‌ترین ویژگی‌ها از میان حجم بالایی از مجموعه دادگان نقش تعیین‌کننده‌ای در روش تشخیص نفوذ پیشنهادی کئور و همکاران دارد [۷۳]. در این روش، تابع هدف Griewank، برای محاسبه مقدار هدف MCFA و الگوریتم رده‌بندی بیزی ساده نیز برای رده‌بندی نمونه‌ها استفاده‌شده است.

راماکریشنان و دواراجو یک روش انتخاب مبتنی بر آنتروپی برای انتخاب ویژگی‌های مهم، زبان کنترل فازی لایه‌ای برای تولید قوانین فازی و الگوریتم رده‌بندی لایه‌ای را برای تشخیص حملات مختلف شبکه پیشنهاد داده‌اند [۷۴].

در مقاله‌ای دیگر، الگوریتم بهبودیافته بهینه‌سازی چند هدفه (I-NSGA-III) با استفاده از یک فرایند حفاظتی جدید پیشنهادشده است [۷۵]. یک فرایند انتخاب بایاس که وضعیتی با کمترین ویژگی‌های انتخاب‌شده را در نظر گرفته و همچنین یک فرایند متناسب‌سازی انتخاب که وضعیتی با بیشترین وزن مجموع اهداف را انتخاب می‌کند، شالوده این الگوریتم را شکل می‌دهند. محققان ادعا کرده‌اند که نتایج تجربی حاکی از آن است که این الگوریتم می‌تواند مشکل عدم تعادل در دقت رده‌بندی را برای کلاس‌هایی که نمونه‌های کمتری دارند، کاهش دهد.

خلاصه روش‌های بررسی‌شده در این بخش همراه با معایب و مشکلات آن‌ها در جدول ۳-۱ ارائه‌شده است:

[1] Modified CuttleFish Algorithm (MCFA)

جدول (۳-۱): بررسی معایب روشهای تشخیص نفوذ موجود

معماری	سیستم پیشنهادی	معایب و چالش‌های موجود
خوشه‌بندی (سلسله مراتبی)	مرجع [۳۳]	فقط بر خوشه‌بندی تک پرشه استوار است. همچنین تنها برای کاربردهای صنعتی مفید است. (WISN)
	مرجع [۳۹]	عدم تضمین امنیت گره‌های سطوح بالاتر که رابط گره‌های سطوح پایین‌تر با ایستگاه پایه هستند.
	مرجع [۸]	با توجه به فرض موجود در آن، فقط برای شبکه‌های حسگر ایستا مناسب است، درصورتی‌که اغلب شبکه‌های حسگر پویا هستند.
	مرجع [۴۰]	عدم ارائه هیچ‌گونه نتایج شبیه‌سازی و یا پیاده‌سازی برای ارزشیابی طرح پیشنهادی
	مرجع [۴۱]	اینکه چه حملاتی را پوشش می‌دهد مشخص نشده و نتایج به‌صورت کلی فقط دقت تشخیص را ارائه کرده‌اند.
همکاری (توزیع‌شده)	مرجع [۴۲]	فقط برای تشخیص حملات سیاه‌چاله و ارسال انتخابی طراحی‌شده است.
	مرجع [۴۳]	تنها قابلیت تشخیص یک مهاجم را دارد و اگر چند مهاجم باهم و به‌صورت هماهنگ حمله نمایند، قدرت تشخیص بقیه مهاجمان را ندارد. همچنین مشخص نکرده‌اند که چه حملاتی را با چه دقتی پوشش می‌دهند. درباره مصرف انرژی هم بحثی نشده است.
	مرجع [۴۴]	طرح پیشنهادی آن‌ها وابسته به‌اندازه بافر موردنیاز تشخیص گرهای نفوذ است. در اندازه بافر پایین دقت تشخیص کم بوده و برای افزایش دقت تشخیص نیاز به افزایش اندازه بافرها است که این امر باعث می‌شود میزان مصرف انرژی و منابع مصرفی تشخیص گرهای موجود در گره‌ها افزایش‌یافته و بنابراین طول عمر شبکه کاهش می‌یابد.
تشخیص آماری	مرجع [۳۴]	فقط برای تشخیص حمله حفره چاهک ارائه‌شده است.
	مرجع [۴۵]	متأسفانه آن‌ها مشخص نکرده‌اند که چه حملاتی را پوشش می‌دهند و این‌که آیا اصولاً تمرکز روی داده‌ها به‌جای فعالیت گره‌ها و لینک‌ها، قابلیت تشخیص انواع مختلفی از حملات را خواهد داشت یا خیر. اگر جواب مثبت است با چه دقتی.
	مرجع [۴۶]	با توجه به این‌که تشخیص گرهای نفوذ به‌صورت محلی بر روی داده‌های گره‌ها فعالیت می‌کنند، قابلیت تشخیص حملات عمومی و سراسری که توسط چند مهاجم انجام شود را ندارند. همچنین فقط برای شبکه‌های حسگر با فعالیت ایستا که تغییر و پویایی کمی در ترافیک دریافتی دارند مناسب است.
نظریه بازی	مرجع [۴۷] و [۴۸]	بر طبق مفروضات روش پیشنهادی آن‌ها، در هرلحظه فقط یکی از خوشه‌ها نظارت می‌شود و مابقی شبکه بدون حفاظت رها می‌شود. بنابراین در صورت وجود چندین مهاجم در شبکه حسگر بیسیم، تنها یکی از آن‌ها توسط سیستم تشخیص نفوذ شناسایی می‌گردد درحالی‌که مابقی مهاجمان بدون شناسایی رها می‌شوند.
تشخیص ناهنجاری	مرجع [۳۲]	فقط حاوی یک سری پیشنهادات برای طراحان سیستم های تشخیص نفوذ است.
	مرجع [۴۹]	بیشتر بر روی پیچیدگی محاسباتی مدلشان بحث کرده‌اند و درباره پوشش حملات هیچ بحثی نشده و مشخص نیست چه حملاتی را با چه درصدی تشخیص می‌دهد.
	مرجع [۵۱]	محققان پیشنهاد کردند که چندین تشخیص گر به لایه‌های مختلف مدل OSI نظارت نمایند. این برای شبکه‌های حسگر امکان‌پذیر نیست، زیرا به‌سرعت منابع محدود موجود را مصرف می‌کند. طرح آن‌ها تنها برای حملات خارجی ارائه‌شده و حملات داخلی مانند حمله تسخیر فیزیکی گره، حمله سایبیل را در نظر نمی‌گیرد.
	مرجع [۵۲]	مدل پیشنهادی فقط برای تشخیص حملات جعل هویت ارائه‌شده و خوب عمل می‌نماید.
مراقب	مرجع [۵۴]	طرح پیشنهادی آن‌ها برای شبکه‌های حسگر بیسیم ایستا ارائه شده‌است که با توجه به پویایی ذاتی شبکه‌های حسگر، مناسب نیست. با توجه به مصرف انرژی بالای عامل‌های سراسری، گره‌های هدف این عامل‌ها به‌سرعت منابع را مصرف می‌نمایند.
شهرت	مرجع [۵۷]	طرح پیشنهادی آن‌ها فقط برای حملات حذف بسته ارائه‌شده و تنها بر روی انواع مختلف سناریوهای حذف بسته تست‌شده است.
	مرجع [۳۵]	در این طرح دقت تشخیص وابسته به حد آستانه است که با افزایش آن، مصرف انرژی بالا رفته و طول عمر شبکه کاهش می‌یابد. همچنین هیچ صحبتی درباره حملات قابل پوشش نشده و ارزیابی کلی بر روی درصد تشخیص انجام‌شده است.

۳–۱۰– سیستم‌های تشخیص نفوذ در برابر حملات سایبیل

هر گره فیزیکی موجود در شبکه در برخی از امکانات و منابع خود دارای محدودیت است. بنابراین بررسی منابع می‌تواند شیوه مناسبی در جهت دفاع در برابر حمله سایبیل باشد [۱۲]. بر طبق این روش جهت شناسایی حمله سایبیل، منابع پردازشی، حافظه و ارتباطی موردبررسی قرار می‌گیرند.

نیوسام و همکاران برای اولین بار حمله سایبیل را در شبکه‌های حسگر بی‌سیم به شیوه‌ای سامان‌مند موردبررسی و تحلیل قراردادند [۷۶]. آن‌ها نشان داده‌اند که منابع پردازشی و حافظه به جهت شناسایی حمله سایبیل در شبکه‌های حسگر بی‌سیم مناسب نیستند؛ زیرا در این شبکه‌ها مهاجم می‌تواند منابع پردازشی و حافظه به‌مراتب بزرگ‌تری را نسبت به گره‌های مجاز شبکه استفاده نماید. در عوض طرح بررسی منابع رادیویی را پیشنهاد کردند که در آن فرض بر این است که هر گره تنها از یک منبع رادیویی استفاده می‌کند و امکان ارسال و دریافت هم‌زمان روی بیشتر از یک کانال را ندارد. حالا اگر یک گره بخواهد وجود گره‌های سایبیل را در همسایه‌هایش بررسی کند، باید به هر یک از آن‌ها یک کانال متفاوت برای همه‌پخشی پیام‌ها اختصاص دهد. سپس گره به‌طور تصادفی کانالی را به‌قصد شنود انتخاب کرده و اگر پیامی را بر روی کانال اختصاصی مرتبط با آن همسایه بشنود، آن همسایه جزء گره‌های مجاز خواهد بود و در غیر این صورت آن گره به‌عنوان گره سایبیل شناسایی می‌گردد. البته چگونگی اختصاص کانال‌های رادیویی به گره‌های همسایه هنوز یک مسئله حل‌نشده است. همچنین فرایند بررسی نیز ممکن است انرژی زیادی را هدر دهد.

برای شناسایی گره‌های سایبیل، الگوریتم‌های مبتنی بر قدرت سیگنال دریافتی (RSSI) در شبکه‌های حسگر بی‌سیم مبتنی بر پروتکل مسیریابی LEACH ارائه‌شده است [۷۷] و [۷۸]. در این مقالات، مدلی از حمله سایبیل در نظر گرفته‌شده که در آن گره مهاجم با تکیه‌بر گره‌های سایبیل خود به‌عنوان گره سرخوشه عمل می‌نماید.

می‌توان مدلی از حمله سایبیل را در نظر گرفت که مهاجم با حمله به پروتکل خوشه‌بندی مبتنی بر کمترین شناسه (LID) روند انتخاب سرخوشه را مختل می‌نماید [۷۹]. در ادامه نیز به‌صورت اجمالی روش‌های مختلفی برای مقابله با این حمله ارائه‌شده است.

ژونگ و همکاران یک طرح مکان‌یابی مبتنی بر RSSI ارائه داده‌اند که بر اساس نسبت قدرت سیگنال دریافتی از چند گره در شبکه مکان گره جدید را تعیین می‌کند [۸۰]. در این مقاله قضیه‌ای بنام قضیه نظارت پنج‌گانه بیان‌شده مبنی بر اینکه اگر در هر ناحیه از شبکه، امواج رادیویی توسط حداقل چهار گره نظارت شوند، در این صورت هیچ گره‌ای نمی‌تواند مکان خود را مخفی کند. در اینجا بنا به اهمیت قضیه نظارت پنج‌گانه آن‌را اثبات می‌کنیم [۸۰]:

فرض کنید در یک ناحیه با شرایط فوق یک گره با قدرت P_0 سیگنالی را ارسال کند. در این حالت قدرت سیگنال دریافتی (RSSI) در گره i به‌صورت زیر خواهد بود:

$$R_i = P_0.K / {d_i}^{\alpha} \quad (۲-۳)$$

که در آن K یک ثابت و d_i فاصله اقلیدسی گره مفروض تا گره i و α فاکتور تضعیف سیگنال است. بنابراین نسبت RSSI برای هر دو گره i و j عبارت است از:

$$R_i/R_j = (P_0.K/{d_i}^{\alpha})/(P_0.K/{d_j}^{\alpha}) = (d_i/d_j)^{\alpha} \quad (۳-۳)$$

$$\xrightarrow{(2)} \quad d_i/d_j = (R_i/R_j)^{\frac{1}{\alpha}} \quad (۴-۳)$$

حالا با قرار دادن مختصات دکارتی گره‌ها در معادله فوق و با فرض اینکه مکان گره مفروض (x,y) و مکان گره i (x_i,y_i) باشد و همچنین چهار گره ناظر دریافت‌کننده سیگنال از گره مفروض به ترتیب i، j، f و p باشند، داریم:

$$\begin{cases} (x-x_i)^2+(y-y_i)^2 = \left(\frac{R_i}{R_j}\right)^{\frac{1}{\alpha}} \left((x-x_j)^2+(y-y_j)^2\right) \\ (x-x_i)^2+(y-y_i)^2 = \left(\frac{R_i}{R_f}\right)^{\frac{1}{\alpha}} \left((x-x_f)^2+(y-y_f)^2\right) \\ (x-x_i)^2+(y-y_i)^2 = \left(\frac{R_i}{R_p}\right)^{\frac{1}{\alpha}} \left((x-x_p)^2+(y-y_p)^2\right) \end{cases} \quad (۵-۳)$$

در ادامه با حل دستگاه معادله (۳-۵)، مکان گره مفروض تعیین می‌گردد. روش کار برای تشخیص حمله سایبیل به این صورت خواهد بود که هرگاه پیام‌هایی توسط دو گره مختلف ارسال گردد، چهار گره ناظر در آن ناحیه، مکان گره‌های ارسال‌کننده پیام را با استفاده از رابطه (۳-۵) محاسبه نموده و درصورتی‌که مکان آن‌ها یکسان باشد، آن‌ها را به‌عنوان یک حمله سایبیل تشخیص خواهند داد [۸۰].

مشکلات اساسی روش فوق برای تشخیص حمله سایبیل، محاسبات سنگین برای تعیین مکان با استفاده از رابطه (۳-۵)، نیاز به تعداد زیادی گره ناظر برای پوشش کل شبکه با مکان از پیش مشخص‌شده و نیز تبادل زیاد پیام بین گره‌های ناظر است.

به‌منظور رفع محاسبات سنگین روش فوق، به این نکته دقت شده است که با توجه به عدم‌تغییر مکان گره‌های ناظر در شبکه می‌توان بدون تعیین مکان گره‌های دیگر و صرفاً بر اساس ذخیره و مقایسه نسبت قدرت سیگنال دریافتی (RSSI) برای پیام‌های دریافت شده از آن‌ها، حمله سایبیل را تشخیص داد [۸۱]. روش کار الگوریتم پیشنهادی آن‌ها به این صورت است که هرگاه دو گره S_1 و S_2 پیام‌هایی را در شبکه ارسال کنند بر اساس رابطه (۳-۵) و یکسان بودن مختصات گره‌های ناظر فقط کافی است برای آن‌ها نسبت RSSI را محاسبه کنیم که به‌صورت زیر خواهد بود:

$$R_i^{S_1}/R_j^{S_1} \ , \ R_i^{S_1}/R_f^{S_1} \ , \ R_i^{S_1}/R_p^{S_1} \qquad (۶-۳)$$

$$R_i^{S_2}/R_j^{S_2} \ , \ R_i^{S_2}/R_f^{S_2} \ , \ R_i^{S_2}/R_p^{S_2} \qquad (۷-۳)$$

در روابط فوق فرض کنید نماد R_i^k قدرت سیگنال دریافتی باشد هنگامی‌که گره k پیامی را ارسال کرده و گره i آن را دریافت نموده است. در ادامه کار به جهت تشخیص حمله سایبیل کافی است بررسی گردد که آیا نسبت قدرت سیگنال‌های دریافتی به‌دست‌آمده از روابط (۳-۶) و (۳-۷) باهم برابر هستند یا خیر. به‌عبارت‌دیگر:

$$\left(\frac{R_i^{S_1}}{R_j^{S_1}} = \frac{R_i^{S_2}}{R_j^{S_2}}\right) And \left(\frac{R_i^{S_1}}{R_f^{S_1}} = \frac{R_i^{S_2}}{R_f^{S_2}}\right) And \left(\frac{R_i^{S_1}}{R_p^{S_1}} = \frac{R_i^{S_2}}{R_p^{S_2}}\right) \qquad (۸-۳)$$

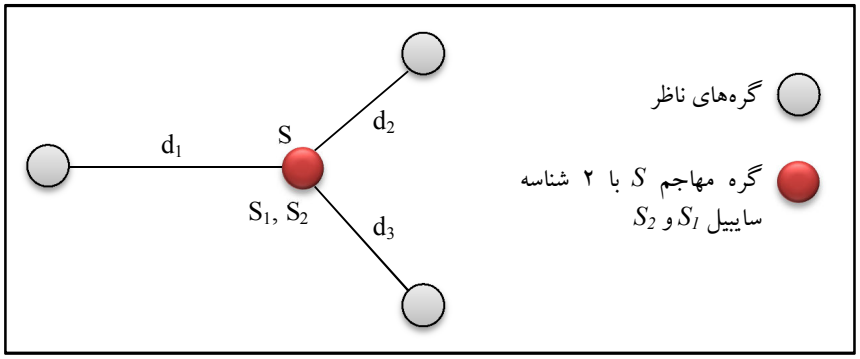
اگر حاصل عبارت منطقی فوق درست باشد در این صورت گره‌های S_1 و S_2 به‌عنوان حمله سایبیل شناخته خواهند شد.

هرچند این روش تا حدود زیادی مشکل محاسبات سنگین روش اول را رفع می‌کند اما کماکان دو مشکل دیگر آن یعنی نیاز به تعداد زیادی گره ناظر برای پوشش کل شبکه (که باعث افزایش چشمگیر هزینه شبکه حسگر می‌گردد) و همچنین تبادل زیاد پیام بین گره‌های ناظر برای تعیین مقادیر نسبت قدرت سیگنال‌های دریافتی (که باعث افزایش اتلاف انرژی گره‌ها و به‌تبع آن باعث کاهش طول عمر شبکه حسگر می‌گردد)، همچنان وجود دارند.

سازوکاری دیگری پیشنهادشده است که مشابه با روش قبلی بر اساس اختلاف‌زمان ورود پیام‌ها (TDOA) بین گره مهاجم و گره‌های ناظر[1] عمل می‌نماید [۸۲]. در این روش همان‌طور که در شکل ۳-۱۳ دیده می‌شود، حداقل به سه گره ناظر نیاز است که یکی از آن‌ها به‌عنوان گره ناظر اصلی مطرح می‌شود. فرض کنید گره ۱ گره ناظر اصلی و نماد d_i^s فاصله بین گره ناظر i با گره مهاجم است، بنابراین داریم:

$$\Delta d_{i,1}^s = c\,\Delta t_{i,1}^s = d_i^s - d_1^s \qquad (۹-۳)$$

در رابطه ۳-۹، $\Delta d_{i,1}^s$ اختلاف فاصله بین گره ناظر i و گره ناظر اصلی نسبت به گره منبع و $\Delta_{i,1}^s$ نیز مقدار TDOA بین گره ناظر اصلی و گره ناظر i نسبت به گره مهاجم و c سرعت انتشار سیگنال است.



شکل (۳-۱۳): موقعیت گره مهاجم نسبت به گره‌های ناظر [۸۲]

[1] Time Difference Of Arrival (TDOA)

هنگامی‌که یک گره مهاجم با یکی از شناسه‌های سایبیل خود (مانند S_1) پیامی را ارسال می‌کند، همه گره‌های ناظر زمان ورود آن را ثبت می‌کنند. سپس همه گره‌های ناظر اطلاعات زمان ورود پیام خود را به گره ناظر اصلی ارسال می‌کنند. گره ناظر اصلی نیز به کمک رابطه ۳-۹ اختلاف‌زمان ورود پیام از گره‌های ناظر دیگر را با خودش محاسبه می‌نماید؛ بنابراین داریم:

$$\Delta t_{i,1}^{S_1} = t_i^{S_1} - t_1^{S_1} = \left(d_i^{S_1} - d_1^{S_1}\right) / c \qquad (۱۰-۳)$$

در رابطه ۳-۱۰، $t_i^{S_1}$ زمان ورود پیام به گره ناظر i از گره مهاجم با شناسه سایبیل S_1 است. سپس نسبت اختلاف‌زمان‌های فوق برای گره‌های ناظر نسبت به گره ناظر اصلی محاسبه می‌شود.

حالا در دفعه بعد اگر گره مهاجم با یک شناسه سایبیل دیگر (مانند S_2) پیامی را ارسال نماید، فرایند فوق برای محاسبه نسبت اختلاف‌زمان ورود مجدداً تکرار می‌گردد. حالا همان‌طور که در رابطه ۳-۱۱ مشاهده می‌شود، اگر این نسبت به‌طور تقریبی با نسبت قبلی یکسان باشد در این صورت حمله سایبیل شناسایی می‌شود.

$$\Delta t_{2,1}^{S_1} / \Delta t_{3,1}^{S_1} = \Delta t_{2,1}^{S_2} / \Delta t_{3,1}^{S_2} \qquad (۱۱-۳)$$

در این روش هر خوشه باید دارای گره‌های ناظر کافی باشد و آن‌ها نیز باید از مکان دقیق خود اطلاع داشته باشند. بنابراین اولاً نیازمندی این روش به گره‌های ناظر و ثانیاً تعیین مکان دقیق آن‌ها موجب افزایش هزینه و انرژی در شبکه حسگر می‌گردد. همچنین باید بین گره‌های ناظر یک هماهنگ‌سازی زمانی نیز وجود داشته باشد. علاوه بر مشکلات فوق درصورتی‌که خود گره‌های ناظر موردتهاجم واقع شوند دیگر این روش درست عمل نخواهد کرد. البته باید یادآور شویم که هزینه ارتباطات آن نیز مانند روش قبلی هنوز بالا است.

طرحی برای تشخیص حمله سایبیل ارائه‌شده است که در آن هویت گره‌ها بر اساس تحلیل اطلاعات گره‌های همسایه هر گره، موردبررسی قرار می‌گیرد [۸۳]. این روش تشخیص بر پایه این واقعیت استوار است که در یک شبکه متراکم، دو گره مختلف نمی‌توانند دارای مجموعه همسایه‌های یکسانی باشند. در یک حمله سایبیل به دلیل این‌که همه گره‌های سایبیل توسط یک گره مهاجم ایجادشده‌اند،

بنابراین همه آن‌ها دارای مجموعه همسایگی یکسانی خواهند بود. این ویژگی از گره‌های سایبیل می-تواند برای تشخیص وجود حمله سایبیل استفاده گردد. مهم‌ترین مشکل این روش نیازمندی آن به ارتباطات زیاد و به‌تبع آن مصرف بالای انرژی آن است. با توجه به محاسبات موجود در [۸۳] تعداد کل پیام‌های ردوبدل شده برای این روش به ازای هر گره در شبکه برابر با $O(\alpha*|NB_{AVG}|^2)$ است؛ که در آن $|NB_{AVG}|$ میانگین تعداد همسایه گره‌های شبکه و α تعداد دفعات انجام بررسی برای تشخیص است. همان‌طور که مشاهده می‌گردد سربار ارتباطات برای تشخیص بالا است. البته ما در اینجا محاسبات مربوط به تعیین گره‌های سایبیل را در هر گره نادیده گرفتیم که با افزودن آن به هزینه ارتباطات، وضعیت مصرف انرژی بدتر خواهد شد.

جهت تشخیص حمله سایبیل در شبکه‌های اقتضایی سیار می‌توان از حرکت گره‌ها به‌عنوان یک ویژگی استفاده کرد [۸۴]. این سازوکار بر اساس این واقعیت پایه‌ریزی شده که گره‌های سایبیل مربوط به یک گره مهاجم همیشه با همدیگر حرکت خواهند کرد. اگر یک مجموعه از گره‌ها در یک دوره زمان طولانی توسط یک گره ناظر با همدیگر دیده شوند، آن‌ها احتمالاً شناسه‌های مربوط به یک مهاجم سایبیل هستند. دقت این روش با به‌کارگیری چندین گره ناظر مطمئن می‌تواند بهبود یابد. اگر گره مهاجم به‌طور مداوم شناسه گره‌های سایبیل خود را تغییر دهد، این روش دچار خطا خواهد شد. همچنین به جهت بالا بودن مصرف انرژی این روش برای شبکه‌های حسگر بی‌سیم مناسب نیست.

همچنین یک طرح هوشمند ترکیبی برای پیش‌بینی حمله سایبیل نیز پیشنهادشده است [۸۵]. در این روش از الگوریتم هوش جمعی[1] برای جمع‌آوری اطلاعات از هر مسیر استفاده‌شده است. یک گره مهاجم از طریق تغییرات انرژی می‌تواند شناسایی گردد. اطلاعات جمع‌آوری‌شده به‌وسیله عامل‌های هوشمند به‌عنوان داده‌های آموزشی برای شبکه بیزین[2] بکار می‌روند تا حد آستانه را برای تغییرات انرژی تنظیم نمایند.

[1] Swarm Intelligence
[2] Bayesian Networks

در روشی دیگر، مفهوم کلیدهای رمزنگاری مبتنی بر مکان معرفی‌شده است [۸۶]. در این روش کلید خصوصی هر گره با شناسه و مکان جغرافیایی آن ترکیب می‌گردد. کلیدهای مبتنی بر مکان بر اساس رمزنگاری مبتنی بر شناسه و توسط یک مرجع معتبر تولید می‌گردد. هنگامی‌که یک گره مهاجم سعی می‌کند تا یک گره مجاز را جعل نماید، با توجه به این‌که کلید معتبری ندارد، بنابراین نمی‌تواند عملیات تأیید هویت متقابلی را با گره‌های مجاز دیگر با موفقیت به پایان برساند. روش احراز هویت مشابه دیگری توسط ژانگ و همکاران ارائه‌شده است [۸۷]. در کل روش‌های احراز هویت نیاز به فضای حافظه قابل‌توجهی برای ذخیره اطلاعات هویتی (مانند کلیدهای رمزنگاری مشترک و گواهی هویت و غیره) و همچنین شامل پردازش‌های سنگین الگوریتم‌های تأیید هستند.

روش دیگری تحت عنوان الگوریتم تولید کلید تصادفی[1] (RPC) ارائه‌شده است که بر سطوح مختلف ترافیک و امنیت در حین انتقال داده‌ها در شبکه‌های حسگر متمرکز است [۸۸]. این الگوریتم یک جدول مسیریابی برای نگهداری اطلاعات استقرار گره‌ها تولید می‌کند. گره‌های میانی نیز در مسیر بین مبدأ و مقصد شناسایی می‌شوند. در طول ارتباطات بین گره‌ها اطلاعات گره‌های میانی با پایگاه داده RPC مقایسه‌شده و بر اساس نتایج، الگوریتم در مورد سایبیل یا عادی بودن گره تصمیم‌گیری می‌کند.

ترکیبی از روش CAM-PVM (روش مقایسه و مطابقت موقعیت[2]) با روش MAP (تأیید هویت و انتقال پیام[3]) را برای شناسایی، حذف و درنهایت جلوگیری از ورود گره‌های سایبیل در شبکه پیشنهادشده است [۸۹]. در این روش به جهت تطبیق موقعیت باید گره‌ها از موقعیت مکانی خودآگاه باشند که عملاً مستلزم هزینه و محاسبات سنگین برای گره‌ها است. همچنین نیازمند تأیید هویت توسط بررسی کلید از طریق گره ایستگاه‌پایه است که این امر نیز مستلزم ارتباطات و حافظه بالا است.

الگوریتم دیگری برای تشخیص حمله سایبیل ارائه‌شده است که از مختصات مکانی گره‌ها استفاده می‌کند [۹۰]. این الگوریتم به‌طور ساده با ارسال یک پیام همگانی توسط سرخوشه به جهت تعیین

[1] Random Password Generation Algorithm (RPC)
[2] Compare and match-position verification method (CAM-PVM)
[3] Message Authentication and Passing (MAP)

موقعیت گره‌های خوشه شروع می‌شود. سپس همه گره‌ها پیامی حاوی شناسه و موقعیت مکانی خود به سرخوشه ارسال می‌کنند و سرخوشه نیز با عدم پاسخ‌گویی و یا تطبیق مکانی گره‌هایی با شناسه-های متفاوت، حمله سایبیل را شناسایی می‌کند. در این الگوریتم هیچ صحبتی نسبت به نحوه محاسبه موقعیت مکانی گره‌ها نشده است که عملاً الگوریتم به‌طور کامل تحت تأثیر آن است.

عندلیب و همکاران ادعا کرده‌اند که یک الگوریتم سبک برای تشخیص حمله سایبیل برای شبکه‌های حسگر بی‌سیم سیار ارائه کرده‌اند [۹۱]. این الگوریتم در دو مرحله پیکره‌بندی و آزمون، عملیات خود را انجام می‌دهد. در مرحله پیکره‌بندی که قبل از توزیع گره‌ها در محیط انجام می‌شود، بر اساس سازوکار ویژه‌ای به هر گره حسگر یک شناسه منحصربه‌فرد اختصاص داده می‌شود [۹۲]. سپس در هر گره یک جدول برای ذخیره اعداد تصادفی مربوط به هر گره چاهک و در هر گره چاهک نیز جدولی برای ذخیره اعداد تصادفی مربوط به گره‌های عادی در نظر گرفته‌شده است. در مرحله آزمون که پس از توزیع گره‌ها در شبکه است، بر اساس حرکت گره‌ها و ارتباط با گره‌های چاهک، اعداد تصادفی توسط چاهک مربوطه برای آن‌ها تولیدشده و در جداول مربوطه در آن‌ها ذخیره می‌گردد. در ادامه هر گره بر اساس اعداد تصادفی تولیدشده احراز هویت می‌شود و از این طریق گره‌های سایبیل نیز شناسایی می‌شوند. با توجه به نیاز به مرحله پیکره‌بندی امکان افزودن گره‌ها به شبکه در آینده وجود ندارد و عملاً شبکه ایستا خواهد بود. همچنین به دلیل این‌که این روش بر اساس حرکت گره‌ها و ارتباط آن با گره‌های چاهک پایه‌ریزی شده، متأسفانه صرفاً برای شبکه‌های حسگر بی‌سیم سیار قابل‌استفاده خواهد بود. علاوه بر این حمله سایبیل با تکیه‌بر عملیات شنود امکان دستیابی به اعداد تصادفی مربوط به گره‌ها را داشته که متعاقباً کاهش نرخ تشخیص را در پی خواهد داشت.

شی و همکاران ادعا کردند که یک سازوکار تشخیص سبک برای حمله سایبیل ارائه کرده‌اند [۹۳]. آن‌ها به جهت پایین آوردن پیچیدگی محاسباتی صرفاً به قدرت سیگنال دریافتی (RSSI) بسنده کرده و بر اساس آن تشخیص خود را انجام می‌دهند. روش آن‌ها به این صورت است که در ابتدا هر گره

سرخوشه با تبادل پیام‌هایی با گره‌های داخل خوشه‌اش، جدول RSSI دریافتی را برای آن‌ها تشکیل می‌دهد. سپس هر سرخوشه اطلاعات خود را به همراه جدول RSSI مربوطه به گره چاهک ارسال می‌نماید. در ادامه گره چاهک با بررسی RSSI دریافتی از سرخوشه و اطلاعات مربوط به آن و همچنین بررسی جدول RSSI خوشه، صرفاً بر اساس یکسان بودن RSSI موجود در جدول خوشه، تشخیص سایبیل بودن گره سرخوشه و یا گره‌های درون خوشه را می‌دهد. ایراد اساسی این روش این است که اگر گره مهاجم با توان‌های متفاوتی از گره‌های سایبیل تحت اختیار خود پیام‌ها را ارسال نماید، در این صورت با توجه به تفاوت در RSSI دریافتی از آن‌ها، امکان تشخیص حمله سایبیل وجود نخواهد داشت. همچنین این روش به جهت مقایسه ساده RSSI دریافتی دارای نرخ هشدار نادرست بالایی است. یک ایراد دیگر نیز میزان ارتباطات بالا در ارسال جداول RSSI از سرخوشه‌ها به گره چاهک در بازه‌های زمانی کوتاه است.

یک سیستم تشخیص ناهنجاری مبتنی بر قانون[1] (RADS) ارائه‌شده است [۹۴] که در چهار مرحله و بر اساس یک الگوریتم تشخیص مبتنی بر محدوده با پهنای باند بالا، در یک شرایط توزیع‌شده و بدون نیاز به همکاری و یا اطلاعات اشتراکی بین گره‌های حسگر عملیات خود را انجام می‌دهد. در فاز اول هر گره به اکتشاف همسایه‌های خود از طریق تبادل پیام hello می‌نماید. در فاز دوم هر گره به‌وسیله یک سری محاسبات محلی یک جدول شامل تخمین فاصله همسایه‌ها با خودش را ایجاد می‌کند. در فاز سوم هر گره به‌طور مستقل و بر اساس جدول تولیدشده در فاز قبل عملیات تطابق فاصله را بین همسایگان خود انجام داده و درصورتی‌که اختلاف هر زوج از فواصل از حد مجازی کمتر باشد آن‌ها را به‌عنوان گره‌های سایبیل می‌شناسد. این امر در رابطه ۳-۱۲ نشان داده‌شده است که در آن d_{ij}^{e} فاصله گره j از گره i است که توسط گره i با خطای e تخمین زده‌شده است.

$$if \begin{cases} \left|d_{ij}^{e} - d_{ik}^{e}\right| < e, & then\, raise\, an\, alarm \\ \left|d_{ij}^{e} - d_{ik}^{e}\right| \geq e, & else\, continue\, normal\, operation \end{cases} \qquad (۱۲-۳)$$

[1] Rule-based Anomaly Detection System (RADS)

مهم‌ترین مشکلات این روش تشخیص نفوذ این است که اولاً در فاز دوم هیچ توضیحی درباره محاسبات تخمین فاصله گره‌های همسایه داده نشده است که این مسئله به جهت پیچیدگی محاسباتی و تخمین میزان خطا بسیار حائز اهمیت است. ثانیاً نرخ هشدار نادرست این روش نسبت به سایر کارهای موجود بالا است. همچنین آن‌ها به‌هیچ‌وجه به این مسئله نپرداخته‌اند که اگر یک گره مهاجم با توان‌های ارسال مختلفی از گره‌های سایبیل تحت اختیار خود تبادل پیام نماید الگوریتم تخمین فاصله درست کار خواهد کرد یا خیر.

روش مشابهی با RADS هم ارائه‌شده است که صرفاً نتایج عملیاتی روش مفروض با معیارهای ارزیابی جدیدی همچون دقت، $F1$و ضریب همبستگی متیو[1] (Mcc) تحلیل‌شده است [۹۵].

$$Mcc = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP) * (TP + FN) * (TN + FP) * (TN + FN)}} \quad (۱۳-۳)$$

در رابطه ۳-۱۳ ضریب همبستگی متیو ارائه‌شده است که درجه همبستگی بین گره‌های سایبیل واقعی با گره‌های سایبیل تشخیص داده‌شده را تعیین می‌کند.

۳-۱۱- جمع‌بندی

سیستم‌های تشخیص نفوذ پیشنهادشده برای شبکه‌های حسگر بی‌سیم به‌صورت خلاصه در جدول (۳-۱) ارائه‌شده‌اند به‌گونه‌ای که در آن برای هر طرح پیشنهادی، معماری شبکه موردنیاز، تکنیک تشخیص نفوذ و ویژگی‌های برجسته آن نیز بیان‌شده است. بنابراین در یک جمع‌بندی می‌توانیم نتایج زیر را برای سیستم‌های تشخیص نفوذ پیشنهادی در شبکه‌های حسگر بی‌سیم، استنباط نماییم [۲۸]:

- در سیستم‌های تشخیص نفوذ مبتنی بر خوشه‌بندی و سلسله مراتبی، الگوریتم‌های خوشه‌بندی شبکه به‌منظور دسته‌بندی گره‌ها در خوشه‌ها، انرژی قابل‌توجهی از شبکه را مصرف می‌کنند. بعد از این‌که خوشه‌ها شکل گرفتند و سرخوشه‌ها انتخاب شدند، سرخوشه ها مشکل نقطه

[1] Matthews correlation coefficient (Mcc)

منفرد را ایجاد می‌کنند و بنابراین باید امن شوند. از طرف دیگر اگر گره سرخوشه یک گره متمایز ازلحاظ قدرت نباشد در این صورت سربار سرخوشه بودن خیلی سریع منابع آن را کاهش می‌دهد.

- سیستم‌های تشخیص نفوذ مبتنی بر عامل، بارکاری و تأخیر شبکه را کاهش می‌دهند. اما از طرف دیگر موجب مصرف بالای انرژی گره‌هایی می‌شوند که بر روی آن‌ها فعالیت می‌کنند. هزینه ارتباطات بین عامل‌ها و هماهنگ‌کننده، یا ارتباطات بین خود عامل‌ها می‌تواند باعث ایجاد ازدحام و گلوگاه در شبکه گردد.
- سیستم‌های تشخیص نفوذ مبتنی بر قانون از جهت نصب و عملکرد ساده هستند، اما به جهت مقابله با حملات جدید به‌طور مداوم نیازمند بروز رسانی قوانین هستند.
- سیستم‌های تشخیص نفوذ مبتنی بر داده‌کاوی می‌توانند حملات ناشناخته را تشخیص دهند. ولی متأسفانه پیچیدگی محاسباتی و مصرف انرژی بالایی دارند و نیازمند مقادیر زیادی از داده‌های نمونه هستند. از طرف دیگر آن‌ها همچنین نیازمند ابزار تحلیلی کارایی برای تحلیل مقادیر زیادی از داده‌های مورد کاوش بوده و ظرفیت حافظه بالایی نیز برای ذخیره آن‌ها نیاز دارند.
- در سیستم‌های تشخیص نفوذ مبتنی بر نظریه بازی، نرخ تشخیص می‌تواند توسط مدیر امنیت شبکه و از طریق تغییر پارامترهای آن، تنظیم گردد. مشکل موجود در این سیستم‌ها غیر وفقی بودن آن است و همچنین برای یک عملیات پایدار نیازمند دخالت انسان می‌باشند.

۴–راهکار پیشنهادی

۴-۱- مقدمه

تاکنون روش‌های مختلفی برای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه‌شده است. اما چالش اساسی در روش‌های موجود همچنان در مصرف انرژی بالا و عدم پوشش اغلب حملات است. راهکار پیشنهادی ما با عنوان ارائه "یک معماری کارآ برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم[1]" به دنبال ارائه روشی است که بتواند عملکرد بهتری نسبت به روش‌های موجود ارائه دهد. همان‌طور که می‌دانیم برای ارائه یک معماری باید موارد زیر به‌خوبی تشریح گردند:

- دید کلی: ارائه بخش‌های مختلف یک معماری
- دید جزئی: ارائه جزئیات دقیق هر بخش و سازوکار عملیاتی آن‌ها
- دید ارتباطی: تبیین نحوه ارتباطات بین بخش‌های مختلف معماری

ما در ادامه به تشریح موارد فوق برای معماری پیشنهادی در بخش‌های ۴-۲ تا ۴-۳ خواهیم پرداخت. منظور ما از معماری کارآ در عنوان پیشنهادی، بهبود در مصرف و اتلاف انرژی گره‌های شبکه است که به‌عنوان اصلی‌ترین پارامتر در شبکه‌های حسگر بی‌سیم مطرح است تا بتوانیم از این طریق طول عمر شبکه مفروض را افزایش دهیم. معماری تشخیص نفوذ پیشنهادی ما مربوط به آن دسته از شبکه‌های حسگری است که نیازمند حساسیت امنیتی بالایی هستند (مانند کاربردهای نظامی و امنیتی). ایده اصلی معماری پیشنهادی ما توجه به سطح اهمیت گره و حساسیت آن در شبکه است و بر این اساس از الگوریتم‌های تشخیص نفوذ مؤثری در سطوح مختلف استفاده خواهیم کرد. هدف ما در این معماری پوشش حملات لایه شبکه است که رایج‌ترین حملات در شبکه‌های حسگر هستند.

تکنیک پیشنهادی ما با توجه به پارامترهای طراحی موجود در شبکه‌های حسگر بی‌سیم و نگرش مبتنی بر کارایی، قصد دارد تا مشکلات موجود در روش‌های قبلی (بخش ۳-۱۲) را کاهش دهد. در ادامه به ارائه کلیاتی از منطق معماری پیشنهادی می‌پردازیم که متضمن دلایل کارایی آن نیز هستند:

[1] An Efficient Architecture for Intrusion Detection Systems in Wireless Sensor Networks

- **ازنقطه‌نظر طراحی سیستم،** مصرف انرژی توسط سیستم تشخیص نفوذ یک موضوع بسیار مهم است. گره‌های موجود در یک شبکه حسگر بی‌سیم به‌منظور وظایف ثبت وقایع و پدیده‌ها در محیط مربوطه، پردازش اطلاعات جمع‌آوری‌شده و ارسال نتایج و ارتباطات، نیازمند مصرف انرژی هستند. بنابراین به جهت پشتیبانی از انجام وظایف و عملیات اصلی آن‌ها، سیستم‌های تشخیص نفوذ به عنوان یک عملیات سربار باید حداقل انرژی ممکن را مصرف نمایند. با توجه به ایجاب مصرف انرژی پایین در این شبکه‌ها، می‌توان استنباط کرد که استفاده از روش خوشه‌بندی گره‌ها برای ارتباطات درون شبکه‌ای و استفاده از مدل سلسله مراتبی برای سیستم‌های تشخیص نفوذ مرتبط با آن‌ها سودمند است. بنابراین با این نگرش و پرهیز از ارسال داده‌ها در فواصل طولانی و مستقیم به ایستگاه پایه توسط گره‌ها، مصرف انرژی در آن‌ها به حداقل خواهد رسید. ما نیز در معماری پیشنهادی به‌صورت پایه‌ای از این منطق استفاده کردیم تا از مزایای آن برای کاهش مصرف انرژی سود ببریم.

- **ازلحاظ گستره تشخیص حملات** ما با استفاده از ارائه یک روش مبتنی بر سطح اهمیت گره‌ها از جهت عملیات مربوطه و با در نظر گرفتن حساسیت مصرف انرژی در آن‌ها، یک روش تشخیص نفوذ سلسله‌مراتبی با بیشترین کارایی ارائه خواهیم داد. ما از این نکته کلیدی بهره خواهیم برد که برای مهاجمان انتخاب گره‌های مهم‌تر و بحرانی‌تر از لحاظ سطح وظایف و عملیات مربوطه، معمولاً در اولویت قرار دارد و از طرفی دیگر این گره‌ها نیز معمولاً با توجه به معماری سلسله مراتبی از منابع بیشتری برخوردار هستند. به عبارت ساده‌تر ما بر روی انواع مختلف گره‌ها بر اساس سطح اهمیت آن‌ها ازلحاظ حساسیت و میزان منابع موجود، الگوریتم‌های متفاوتی را برای تشخیص نفوذ ارائه خواهیم کرد. با این کار هم گستره تشخیص حملات را افزایش داده و هم تا حد ممکن مصرف انرژی را کاهش داده و متعاقباً طول عمر شبکه را نیز افزایش می‌دهیم.

- **ازلحاظ دقت تشخیص** نیز با توجه به موارد گفته‌شده هر چه سطح اهمیت گره از لحاظ وظایف و عملیات مربوطه افزایش می‌یابد، با توجه به منطق الگوریتم پیشنهادی، با به کار گرفتن الگوریتم‌های قوی‌تر دقت تشخیص هم بالطبع افزایش خواهد یافت. این امر در شبکه-های حسگر بی‌سیم امری معقول و منطقی است. به‌عبارت‌دیگر درجه و سطح اهمیت گره، درجه قدرت الگوریتم تشخیص نفوذ پیشنهادی را مشخص می‌کند.

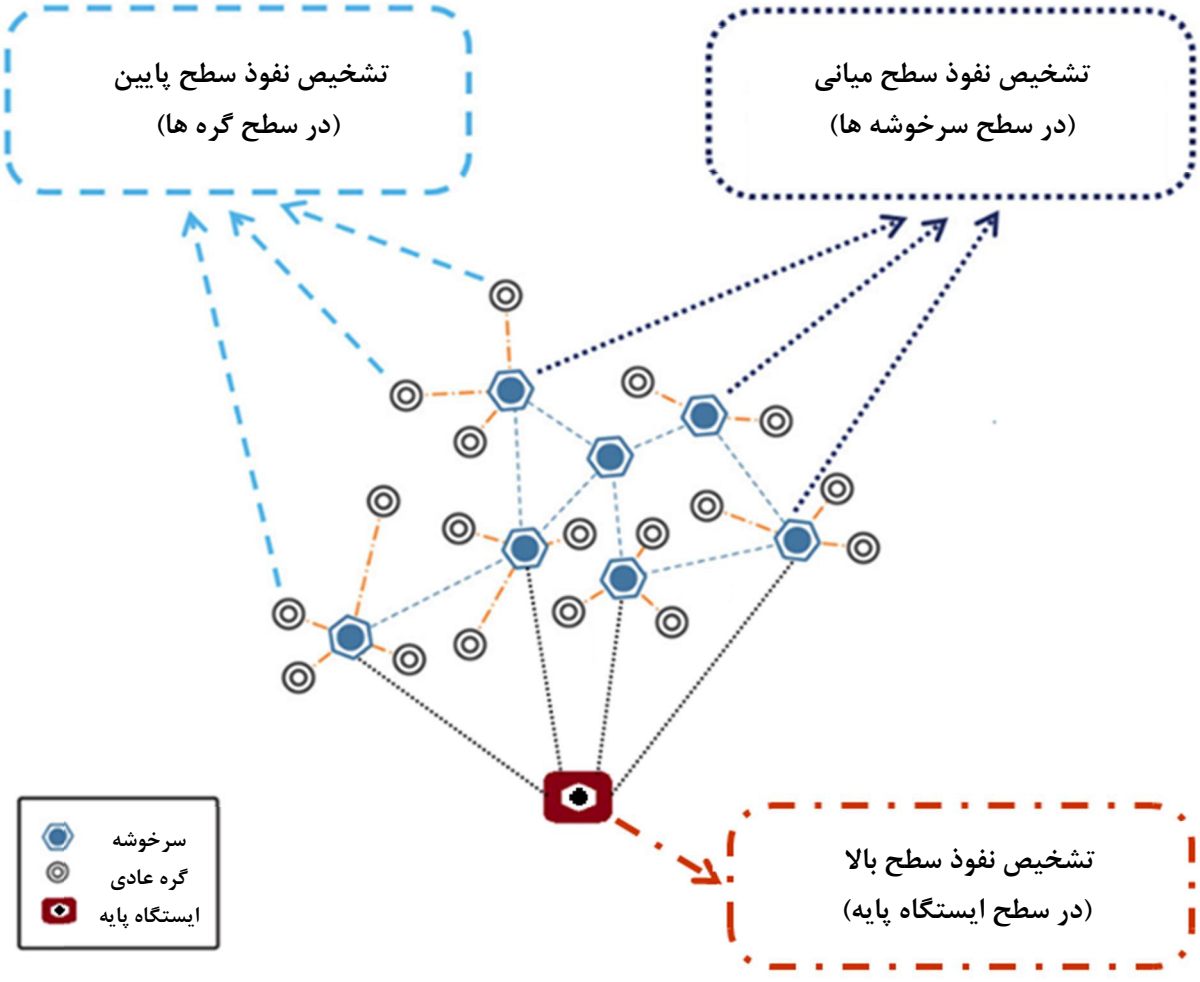
تفاوت اصلی معماری پیشنهادی ما با کارهای موجود در موارد ذیل می‌باشد:

- ما در معماری پیشنهادی خود از ایده یک روش مبتنی بر سطح اهمیت گره‌ها بهره می‌بریم که هر چه اهمیت گره افزایش می‌یابد (مثلاً گره سرخوشه) ما نیز حساسیت سیستم تشخیص نفوذ را افزایش داده تا قدرت تشخیص بیشتری ایجاد نماییم و به‌این‌ترتیب تضمین بیشتری برای حفظ امنیت ایجاد نماییم.
- ما در معماری پیشنهادی با در نظر گرفتن سطح و امکانات ایستگاه پایه سعی داریم قدرت تشخیص نفوذ در سطح سرخوشه ها را افزایش و میزان مصرف انرژی را در آن‌ها کاهش دهیم.
- ما با ارائه الگوریتم‌های متفاوت و مناسب در بخش‌های مختلف معماری پیشنهادی قصد داریم حداکثر کارایی را در آن ایجاد نماییم. مثلاً در سطح گره‌های معمولی ما با یک روش مبتنی بر خصوصیات قصد داریم الگوریتمی سبک و مؤثر را برای این گره‌ها ارائه نماییم.
- پوشش همه حملات لایه شبکه و حملات مسیریابی توسط معماری پیشنهادی.
- ارزشیابی معماری پیشنهادی با همه معیارهای کارائی (بخش ۵-۳) در شبکه‌های حسگر.
- ما در معماری پیشنهادی به جهت بهبود دقت تشخیص و کارایی، به شبیه‌سازی یک شبکه-حسگر بی‌سیم با پارامترهای کامل مربوطه و همچنین شبیه‌سازی حملات لایه شبکه بر روی آن پرداختیم، تا با تجزیه و تحلیل دقیق رفتار حملات بر روی شبکه، به استخراج خصوصیات کلیدی آن‌ها برای استفاده در معماری پیشنهادی دست‌یابیم.

۴-۲- ارائه بخش‌های مختلف معماری پیشنهادی (دید کلی)

همان‌طور که در شکل ۴-۱ نشان داده‌شده است، سطوح مختلف معماری تشخیص نفوذ پیشنهادی که مبتنی بر سطح اهمیت گره‌ها است به‌صورت ذیل خواهد بود:

- تشخیص نفوذ سطح پایین[1] (در سطح گره‌های عادی)
- تشخیص نفوذ سطح میانی[2] (در سطح سرخوشه ها)
- تشخیص نفوذ سطح بالا[3] (در سطح ایستگاه پایه)



شکل (۴-۱) معماری پیشنهادی برای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

در ادامه به تشریح هر یک از سطوح سیستم تشخیص نفوذ پیشنهادی خواهیم پرداخت:

[1] Low Level Intrusion Detection
[2] Mid Level Intrusion Detection
[3] High Level Intrusion Detection

- **تشخیص نفوذ سطح پایین (در سطح گره‌های عادی)**

با توجه به حساسیت کم و منابع محدود گره‌های عادی، اولین سطح از معماری تشخیص نفوذ پیشنهادی با نگرش کمترین میزان پردازش، ارتباطات و انرژی مصرفی طراحی شده است که تحت عنوان تشخیص محلی از آن یاد می‌کنیم. در این سطح هر گره صرفاً بر عملکرد خود و همسایه‌های بلافصل خود نظارت دارد و نیازی به ارتباطات وجود ندارد. ما در این سطح با توجه به حساسیت پایین‌تر این گره‌ها و منابع محدودشان، یک روش مبتنی بر خصوصیات را با توجه به تحلیل دقیق رفتار حملات مسیریابی ارائه می‌نماییم که بتوانیم این حملات را در گره‌های عادی با حداکثر کارایی و حداقل مصرف انرژی پوشش دهیم.

- **تشخیص نفوذ سطح میانی (در سطح سرخوشه ها)**

این سطح از معماری پیشنهادی وظیفه تأمین امنیت گره‌های سرخوشه را بر عهده دارد. علاوه بر آن مواردی هم که در تشخیص نفوذ سطح پایین در گره‌های عادی قابلیت تشخیص نداشته و نیازمند بررسی‌های بیشتری هستند، مورد بررسی قرار می‌گیرند. با توجه به حساسیت بالای گره‌های سرخوشه از لحاظ عملیات و وظایف مربوطه، ما با ارائه یک روش تشخیص مبتنی بر داده‌کاوی به همراه یک روش پیش پردازش داده‌ها، روش قدرتمندتری را به نسبت گره‌های عادی ارائه می‌نماییم. بنابراین میزان سربار محاسبات و ارتباطات در این سطح از سطح گره‌های عادی بیشتر خواهد بود که با در نظر گرفتن منابع بیشتر در سرخوشه‌ها، اجرای آن منطقی و معقول خواهد بود. البته ما با ارائه یک روش پیش پردازش داده‌ها، تا حد امکان پردازش‌ها و به تبع آن سربار و مصرف انرژی را در آن کاهش داده ایم.

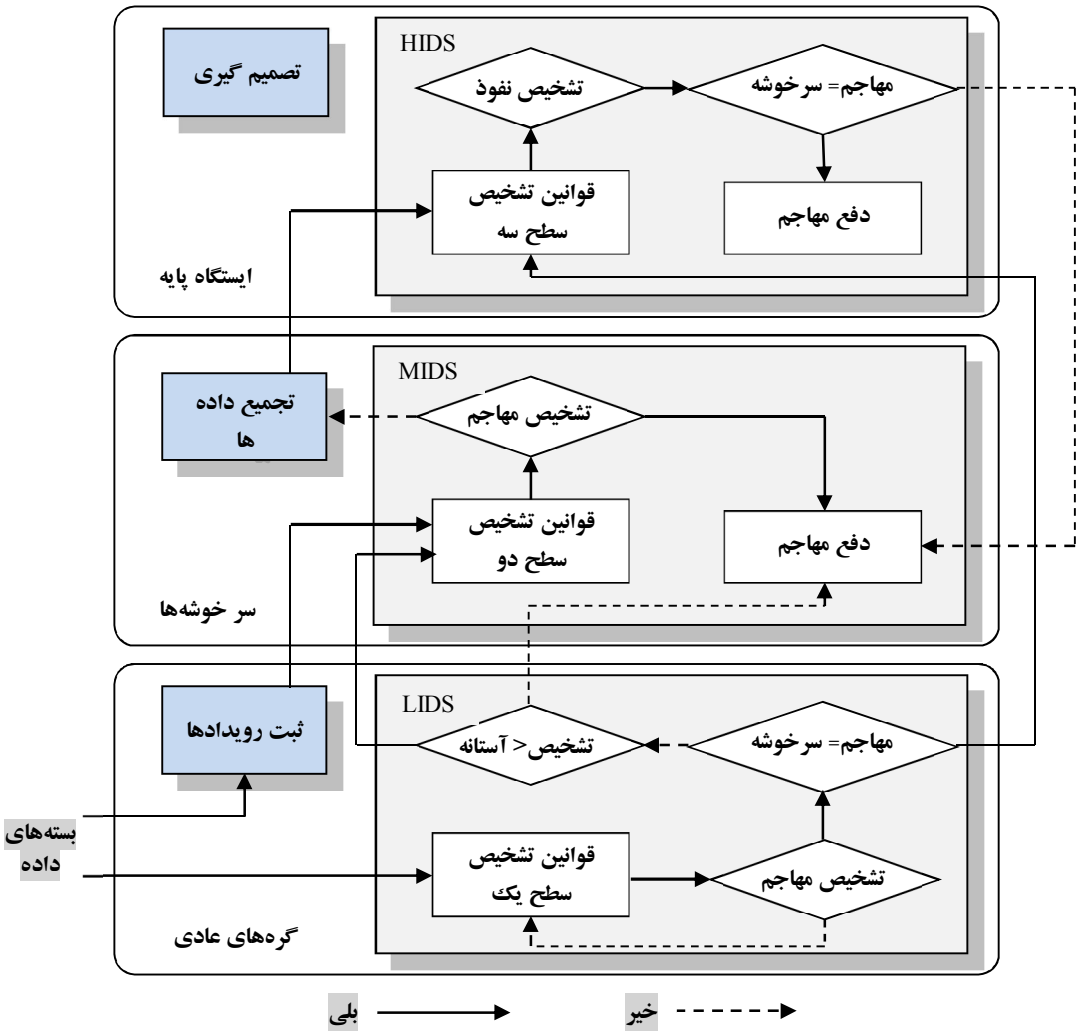
- **تشخیص نفوذ سطح بالا (در سطح ایستگاه پایه)**

در این مرحله با توجه به منابع بالای ایستگاه پایه و عدم وجود محدودیت منابع و انرژی، و همچنین به دلیل اهمیت بالای امنیت سرخوشه‌ها، از الگوریتم‌های تشخیص نفوذ قدرتمند ترکیبی استفاده می‌کنیم، به‌گونه‌ای که عملاً امنیت سرخوشه‌ها تضمین گردد. البته این امر

مستلزم مصرف انرژی زیادی است که با توجه به عدم محدودیت منابع و انرژی بر روی ایستگاه پایه منطقی بوده، و امنیت در سرخوشه‌ها را تضمین می‌کند.

۴-۳-تبیین ارتباطات بین بخش‌ها در معماری پیشنهادی

در شکل (۴-۲) نمودار جریان ارتباطی معماری پیشنهادی ارائه‌شده است.

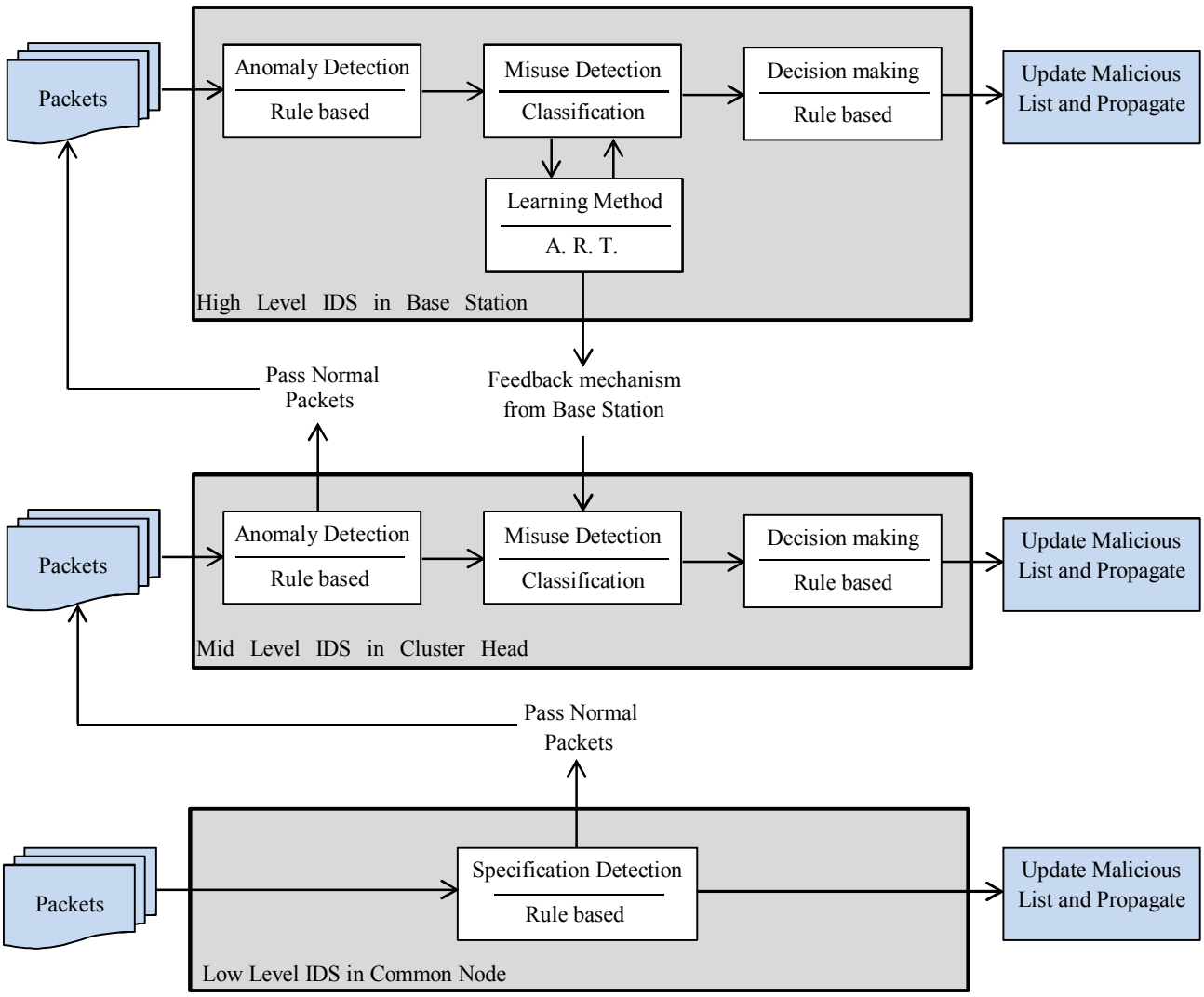


شکل (۴-۲) نمودار جریان ارتباطی معماری پیشنهادی

در تشخیص نفوذ سطح پایین که بر روی گره‌های عادی اجرا می‌گردد، قوانین مربوط به خصوصیات حملات مختلف بررسی‌شده و در صورت وجود هرگونه ناهنجاری آن را به گره سرخوشه به جهت بررسی‌های بیشتر ارجاع می‌دهند. در تشخیص نفوذ سطح میانی نیز که بر روی گره‌های سرخوشه اجرا می‌گردد، مواردی که در تشخیص نفوذ سطح پایین قابلیت تشخیص نداشته و نیازمند بررسی‌های

بیشتری هستند، به‌وسیله ارتباطات به سرخوشه‌ها ارسال می‌شوند تا از جهت تشخیص نفوذهای احتمالی موردبررسی بیشتری قرار گیرند. همچنین در این مرحله ترافیک عادی ارسالی به خود سرخوشه نیز به جهت وجود ناهنجاری و تشخیص حملات بررسی می‌گردد. درنهایت در تشخیص نفوذ سطح بالا که در ایستگاه پایه اجرا می‌شود، کل ترافیک ارسالی به آن، همراه با مواردی که در سطوح قبلی قابلیت تشخیص نداشته‌اند مورد بررسی‌های دقیق‌تر قرار می‌گیرند. همچنین با به‌کارگیری الگوریتم‌های یادگیری در این سطح امکان تشخیص حملات ناشناخته و جدید نیز فراهم گردیده است.

۴-۴- تشریح جزئیات سیستم تشخیص نفوذ پیشنهادی



شکل (۴-۳): نمودار کامل سیستم تشخیص نفوذ پیشنهادی همراه با جزئیات مربوطه

در شکل (۴-۳) نمودار کامل سیستم تشخیص نفوذ پیشنهادی همراه با جزئیات مربوطه به‌طور دقیق ارائه‌شده است. در شکل ۴-۳، برای هر بخش از سطوح سه‌گانه تشخیص نفوذ پیشنهادی، مراحل کاری و الگوریتم بکار گرفته‌شده در آن‌ها و نحوه ارتباط زیر بخش‌ها باهم نشان داده‌شده است.

در ادامه به تشریح سطوح مختلف سیستم تشخیص نفوذ پیشنهادی با ارائه جزئیات آن‌ها و نحوه عملکرد و الگوریتم‌های مربوطه بر اساس شکل ۴-۳ می‌پردازیم.

۴-۴-۱- تشخیص نفوذ سطح پایین[1] (در سطح گره‌های عادی)

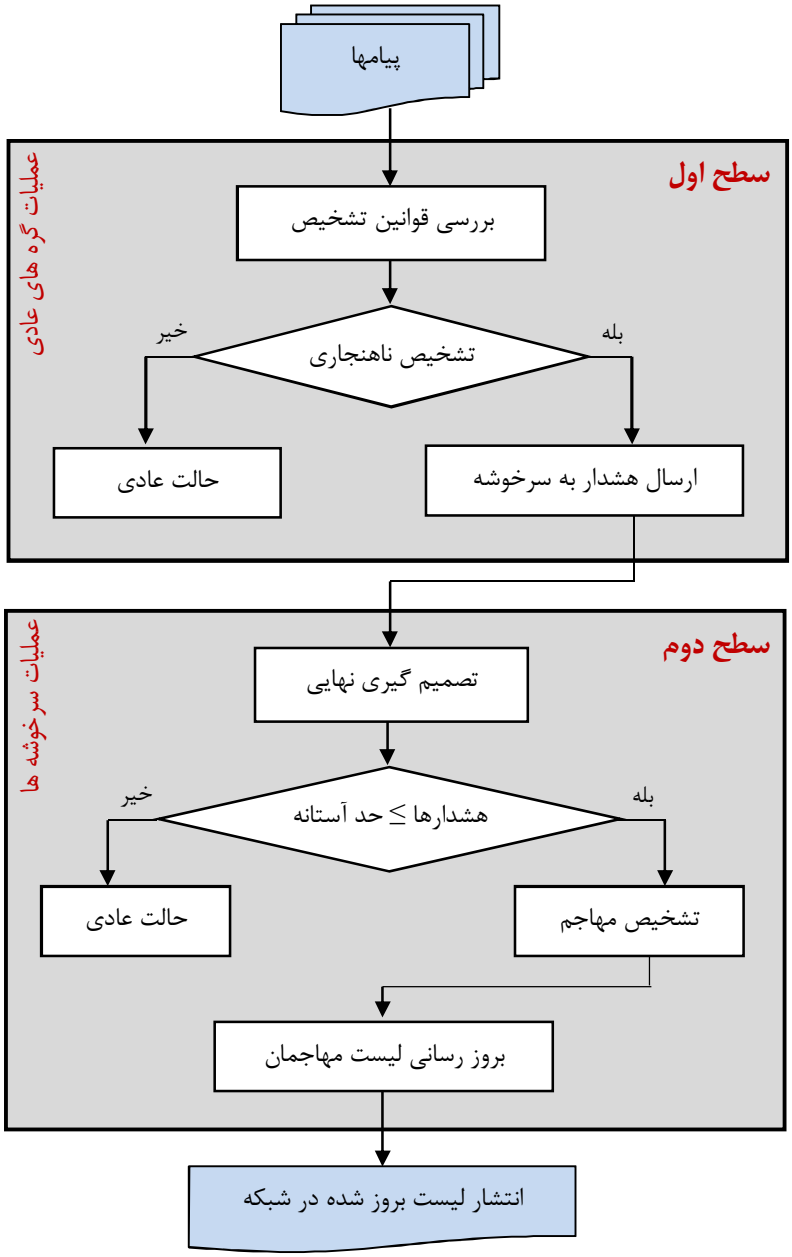
در این بخش می‌خواهیم با ارائه یک سیستم تشخیص نفوذ سبک، در سطح گره‌های عادی شبکه حسگر بی‌سیم، حتی‌الامکان حملات مفروض را به‌صورت مؤثری تشخیص دهیم.

اولین سطح از معماری تشخیص نفوذ در گره‌های عادی اجرا خواهد شد که تحت عنوان تشخیص محلی از آن یاد می‌کنیم. با توجه به حساسیت کم و منابع محدود این گره‌ها، در این سطح هر گره صرفاً بر عملکرد خود و همسایه‌های بلافصل خود نظارت دارد. در این حالت نیازی به ارتباطات وجود ندارد. با توجه به بررسی روش‌های موجود در این سطح، استفاده از یک روش مبتنی بر خصوصیات را پیشنهاد می‌کنیم که بتوانیم حملات لایه شبکه و مسیریابی را در گره‌های عادی پوشش دهیم.

بنابراین در سطح گره‌های عادی شبکه (تشخیص نفوذ سطح پایین)، ما از یک تشخیص نفوذ مبتنی بر خصوصیات استفاده می‌کنیم که هم به جهت سرعت عمل آن و کاهش انرژی مصرفی در تشخیص و هم به دلیل پایین بودن خطا در تشخیص، می‌تواند کارائی شبکه را در حد مطلوبی نگه دارد. همان‌طور که در شکل ۴-۳ مشاهده می‌شود ما به جهت پیاده‌سازی تشخیص نفوذ مبتنی بر خصوصیات در این سطح از یک مجموعه قوانین استفاده می‌کنیم که منطبق بر خصوصیات حملات لایه شبکه و مسیریابی ارائه‌شده‌اند.

[1] Low Level Intrusion Detection

همچنین به جهت بهبود دقت تشخیص ما از یک روش مبتنی بر اعتماد سبک نیز بهره خواهیم برد به‌گونه‌ای که بتواند بر اساس سطح اعتماد گره‌ها، پیام‌های هشدار تولیدشده توسط آن‌ها را ارزشیابی نماید. این ارزشیابی می‌تواند سیستم تشخیص نفوذ را در تشخیص گره‌های مهاجم و حملات یاری نماید و دقت تشخیص‌های آن را نیز ارتقاء دهد. همچنین در سیستم پیشنهادی از تکنیک خوشه‌بندی گره‌ها استفاده کردیم تا از مزایای آن در روند تشخیص نفوذ در شبکه استفاده نماییم.



شکل (۴-۴): نمودار جریان مربوط به تشخیص نفوذ سطح پایین

نمودار جریان روش پیشنهادی که در شکل ۴-۴ ارائه‌شده، در دو سطح گره‌های عادی (سطح اول) و گره‌های سرخوشه (سطح دوم) سازمان‌دهی می‌گردد. در سطح اول، ابتدا گره‌های عادی قوانین مربوط به خصوصیات حملات مختلف را بررسی نموده و در صورت وجود هرگونه ناهنجاری آن را به گره سرخوشه به جهت بررسی‌های بیشتر ارجاع می‌دهند. این خصوصیات بر اساس تحلیل صورت گرفته در بخش تحلیل رفتار حملات و نحوه عملکرد آن‌ها در بخش ۲-۲-۳ ارائه‌شده است.

در سطح دوم گره‌های سرخوشه هشدارهای رسیده از گره‌های مختلف را بررسی می‌کند و درصورتی‌که این هشدارها از حد آستانه بگذرند، به‌عنوان یک حمله شناخته‌شده و لیست مربوط به گره‌های مهاجم توسط سرخوشه به‌روزرسانی شده و به همه گره‌های خوشه ارسال می‌گردد.

در ادامه نیز با اصلاح عملیات سرخوشه‌ها از طریق یک سیستم مبتنی بر اعتماد که در بخش ۴-۴-۱-۳ تشریح می‌شود، سعی می‌کنیم عملکرد سیستم تشخیص نفوذ پیشنهادی را بهبود بدهیم.

۴-۴-۱-۱- قوانین تشخیص مبتنی بر خصوصیات حملات

در این بخش بر اساس تحلیل رفتار حملات مختلف و خصوصیات استخراج‌شده از آن‌ها به تشریح قوانین تشخیص مربوط به آن‌ها خواهیم پرداخت.

تشخیص حمله رد سرویس:

در این حمله مهاجم با توجه به‌سرعت بالا در ارسال بسته‌ها به سایر گره‌ها قصد دارد تا بارکاری آن‌ها را به حدی برساند که امکان سرویس‌دهی معمول خود را از دست بدهند. بنابراین با بررسی فاصله زمانی بین بسته‌های دریافتی[1] (IRP) می‌توان این مهاجم را شناسایی نمود. علاوه بر این، در اغلب موارد مهاجم با توان بالایی ارسال بسته‌ها را انجام می‌دهد که از روی قدرت سیگنال دریافتی[2] (RSSI) نیز می‌توان آن را شناسایی کرد. شبه کد تشخیص حمله رد سرویس در شکل ۴-۵ نشان داده‌شده است:

[1] Interval of Received Packets (IRP)
[2] Received Signal Strength Indicator (RSSI)

```
If (IRP < Threshold_IRP && RSSI > Threshold_RSSI) {
    Create (alert);
    Send (alert, node-ID, malicious-ID);
    //send to cluster-head
}
```

شکل (۴-۵): شبه کد تشخیص حمله رد سرویس

تحلیل پارامتر: پارامتر مهم در این روال حد آستانه $Threshold_{RSSI}$است. برای تعیین آن، به شیوه زیر عمل می‌کنیم. فرض کنید یک گره مفروض با قدرت P_0 سیگنالی را ارسال کند. در این حالت قدرت سیگنال دریافتی (RSSI) در گره i که با نماد R_i مشخص می‌شود به‌صورت زیر خواهد بود [۸۱]:

$$R_i = P_0 . K / {d_i}^{\alpha} \quad (۱-۴)$$

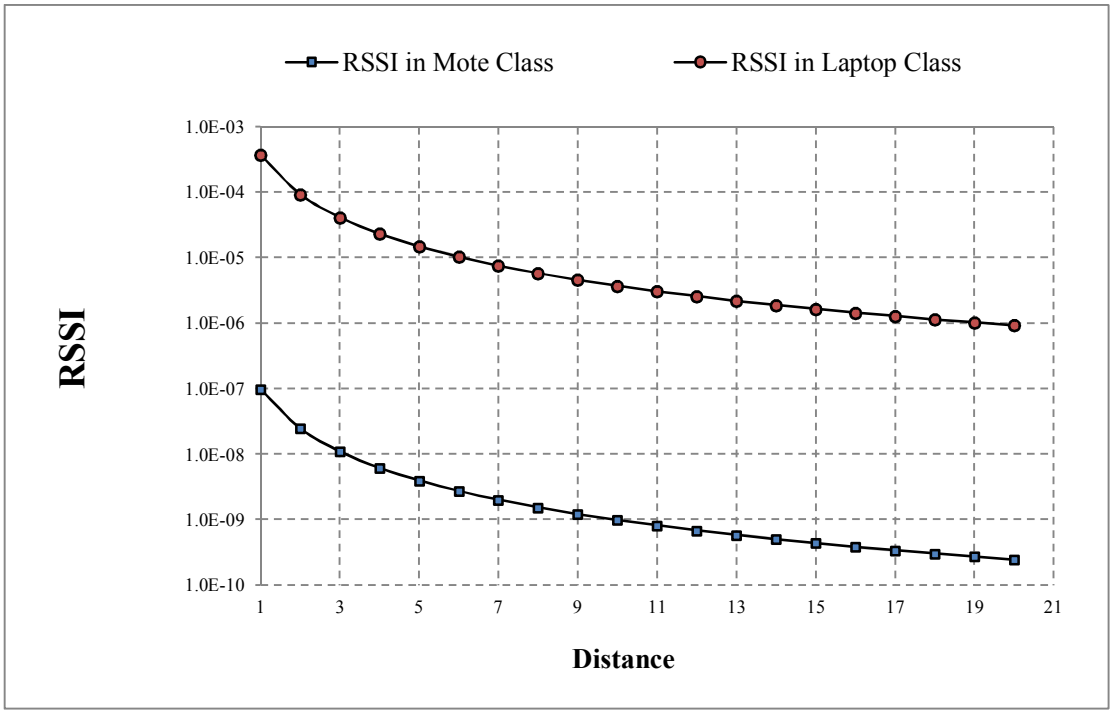
که در آن d_i فاصله اقلیدسی گره مفروض تا گره i، α فاکتور تضعیف سیگنال (که معمولاً برابر ۲ است) و K نیز یک ثابت است که از رابطه (۴-۲) بدست می‌آید:

$$K = Gt . Gr . (\frac{\lambda}{4\pi})^2 \quad (۲-۴)$$

$$R_i = P_0 . Gt . Gr . (\frac{\lambda}{4\pi})^2 / {d_i}^2 \quad (۳-۴)$$

در رابطه (۴-۳)، Gt ضریب تقویت آنتن در ارسال‌کننده، Gr ضریب تقویت آنتن در دریافت‌کننده و λ نیز طول‌موج را مشخص می‌کنند که بر اساس استاندارد IEEE 802.11 که برای شبکه‌های حسگر بی-سیم ارائه‌شده است، مقادیر آن‌ها $Gt=1.0$، $Gr=1.0$ و $\lambda=0.125$ می‌باشد. با توجه به این‌که P_0 در گره-های شبکه یکسان است، مقدار RSSI توسط رابطه (۴-۳) تعیین می‌گردد.

در نمودار شکل ۴-۶ تغییرات مقدار RSSI دریافتی برحسب تغییرات فاصله بین گره‌های شبکه (بر اساس چگالی پخش گره‌ها (ρ))، برای دو کلاس گره‌های معمولی (کلاس ذره) و گره‌های قدرتمند (کلاس لپ‌تاپ) ارائه‌شده است. همان‌طور که مشاهده می‌شود تفاوت فاحشی در RSSI دریافتی بین این دو کلاس از گره‌ها وجود دارد و بنابراین به‌راحتی می‌توان مقدار حد آستانه را برای RSSI دریافتی در گره‌های معمولی شبکه تعیین کرد (7.2E-07) که این مقدار بر اساس پارامترهای شبکه شبیه‌سازی‌شده در جدول ۵-۴ نیز ارائه‌شده است.



شکل (۴-۶): مقدار RSSI دریافتی برحسب تغییرات فاصله بین گره‌های شبکه

برای تعیین حد آستانه فاصله زمانی بین بسته‌ها $Threshold_{IRP}$ نیز با توجه به اینکه در حمله رد سرویس مهاجم باید با سرعت بسیار بالایی بسته‌ها را به سمت گره‌های هدف ارسال کند تا آن‌ها را از سرویس‌دهی در شبکه حذف نماید، بنابراین فاصله فاحشی بین فاصله زمانی بین بسته‌ها در حالت عادی شبکه و حمله رد سرویس وجود دارد. البته وابسته به نوع شبکه و این‌که میانگین فاصله زمانی بین بسته‌ها در آن‌ها متفاوت است (بین چند دهم ثانیه تا چند دقیقه)، باید در هر کاربردی این پارامتر در ابتدای کار شبکه تنظیم گردد. برای این کار در ابتدای کار شبکه و در حالت عادی آن، میانگین فاصله زمانی معمول بین بسته‌ها محاسبه‌شده و بر اساس آن $Threshold_{IRP}$ تعیین می‌گردد. این مقدار نیز بر اساس پارامترهای شبکه شبیه‌سازی‌شده در جدول ۵-۴ ارائه‌شده است.

به جهت بررسی فاصله زمانی بین بسته‌های دریافتی نیز می‌توان از کد AWK شکل ۴-۷ بر روی فایل trace خروجی از شبیه‌سازی انجام‌شده در NS2 استفاده کرد. در حقیقت این کد نحوه تشخیص و بررسی قانون فاصله زمانی بین بسته‌های دریافتی (IRP) را که در شبه کد ۴-۵ آمده، تعیین می‌کند.

```
for ( node-id in Node ){
    for ( packet in Packets_received [node-id] ){
        src = packet.source;
        time = packet.time;
        prev [src] = current [src];
        current [src] = time;
        interval = current [src] – prev [src];
        if ( interval < threshold ) {
            Create (alert); // src is malicious node
            Send (alert, node-id, src);
           //send alert to cluster-head
        }
    }
}
```

شکل (۴-۷): شبه کد AWK برای بررسی فاصله بین پیام‌ها

تشخیص حمله سیل ارسال سلام:

با توجه به این‌که در حمله سیل ارسال سلام، در اغلب موارد مهاجم یک گره خارجی با قدرت ارسال بالا می‌باشد، می‌توانیم از طریق قدرت سیگنال دریافتی (RSSI) آن را شناسایی نماییم. شبه کد تشخیص حمله سیل ارسال سلام در شکل ۵-۸ نشان داده‌شده است. همچنین با توجه به این‌که عملکرد این حمله موجب افزایش سربار مسیریابی می‌گردد، می‌توانیم با اعمال قانون فاصله بین پیام‌های مسیریابی[1] (RMI) نیز آن را شناسایی نماییم.

تحلیل پارامتر: به جهت تعیین حد بالای RMI نیز با توجه به تفاوت فاحش بین سربار مسیریابی در این حمله با سایر حملات موجود، با سازوکاری مشابه تعیین $Threshold_{IRP}$، مقدار $Threshold_{RMI}$ را تعیین می‌نماییم که بر اساس پارامترهای شبکه شبیه‌سازی‌شده در جدول ۵-۴ ارائه‌شده است.

```
If (RSSI > Threshold_RSSI && RMI < Threshold_RMI)
{
   Create (alert);
   Send (alert, node-ID, malicious-ID);
   //send to cluster-head
}
```

شکل (۴-۸): شبه کد تشخیص حمله سیل ارسال سلام

[1] Routing Messages Interval (RMI)

تشخیص حمله حفره‌چاهک:

مهم‌ترین پارامتر در شناسایی حمله حفره چاهک بالا رفتن نرخ حذف بسته‌هاست که گره‌های معمولی از طریق عملیات شنود[1] می‌توانند آن را تشخیص دهند. بدین ترتیب اگر نرخ حذف بسته‌ها از نرخ معمول بیشتر شود هشداری ایجاد و به سرخوشه ارسال می‌گردد. رابطه (۴-۴) نحوه محاسبه نرخ حذف بسته‌ها را از طریق شنود نشان می‌دهد.

$$PacketDrop\ Rate = 1 - \frac{packets\ actualy\ forwarded}{packets\ to\ be\ forwarded} \quad (۴-۴)$$

با مقایسه نرخ حذف بسته‌ها PDR با حد آستانه می‌توان حمله‌های مبتنی بر حذف بسته‌ها، بالأخص حمله حفره چاهک را شناسایی نمود. بازه رابطه (۴-۵) محدوده تغییرات PDR را نشان می‌دهد. هرچه این عدد به یک نزدیک‌تر شود، حمله محتمل‌تر خواهد بود.

$$0 < Threshold_{PDR} < PDR < 1 \quad (۵-۴)$$

در این نوع حمله نیز می‌توان علاوه بر معیار فوق مهاجم را با توجه به سیگنال دریافتی نیز شناسایی کرد. شکل ۴-۹ شبه کد مربوط به تشخیص این حمله را به کمک روابط بالا نشان می‌دهد.

```
If (PDR > Threshold_PDR && RSSI > Threshold_RSSI)
{
    Create (alert);
    Send (alert, node-ID, malicious-ID);
    //send to cluster-head
}
```

شکل (۴-۹): شبه کد تشخیص حمله حفره چاهک

تشخیص حمله ارسال انتخابی:

با توجه به این‌که اساس کار این حملات نیز مبتنی بر حذف بسته‌ها است، می‌توان مانند حمله حفره چاهک از عملیات شنود استفاده کرد و با محاسبه نرخ حذف بسته‌ها، مهاجم را شناسایی نمود. البته نرخ حذف بسته‌ها در این حملات با توجه به نوع عملکرد متفاوت بوده و در کل پایین‌تر از حمله حفره

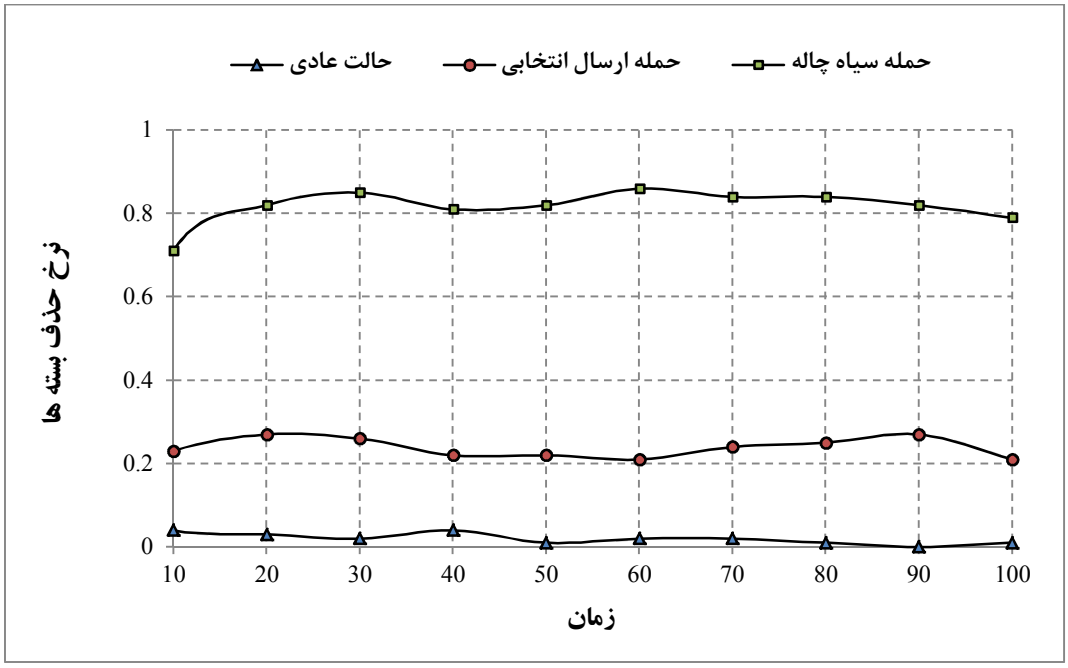
[1] Overhearing

چاهک است. بنابراین باید حد آستانه مربوط به حذف بسته‌ها در این حملات کمتر در نظر گرفته شود. شکل ۴-۱۰ شبه کد مربوط به تشخیص این حملات را نشان می‌دهد.

```
If (PDR > Threshold_PDR)
{
 Create (alert);
 Send (alert, node-ID, malicious-ID);
//send to cluster-head
}
```

شکل (۴-۱۰): شبه کد تشخیص حمله ارسال انتخابی

تحلیل پارامتر: به جهت تعیین حدود آستانه $Threshold_{PDR}$ مربوط به نرخ حذف بسته‌ها در حملات سیاه‌چاله و ارسال انتخابی، نمودار نرخ حذف بسته‌ها در سه حالت مختلف در شکل ۴-۱۱ ترسیم‌شده است. همان‌طور که مشاهده می‌شود نرخ حذف در حمله سیاه‌چاله بسیار بالا بوده و طور میانگین حدود ۰/۸۴ است و در حمله ارسال انتخابی حدود ۰/۲۶ است، درصورتی‌که در حالت عادی شبکه این نرخ زیر ۰/۰۲ است. بنابراین بر اساس شکل ۴-۱۱ به‌راحتی می‌توان حدود آستانه نرخ حذف بسته‌ها را برای حملات سیاه‌چاله و ارسال انتخابی مشخص کرد که این مقادیر در جدول ۵-۴ ارائه‌شده‌اند.



شکل (۴-۱۱): نرخ حذف بسته‌ها در حالات مختلف شبکه

تشخیص حمله سایبیل:

همان‌طور که در بخش ۲-۲-۳ بررسی کردیم یک حمله سایبیل با شیوه‌های مختلفی شبکه حسگر بی‌سیم را موردتهاجم قرار می‌دهد. بنابراین به جهت تشخیص حمله سایبیل باید خصوصیتی از آن را در نظر بگیریم که در شیوه‌های مختلف اجرائی آن قابلیت تفکیک گره‌های مهاجم را به‌خوبی دارا باشد. با این رویکرد، مهم‌ترین خصوصیتی که بتوان بر اساس آن سیستم تشخیص نفوذ را ارائه کرد این است که همه گره‌های سایبیل با شناسه‌های مختلف در یک مکان از شبکه قرار دارند چراکه همه آن‌ها تحت کنترل یک گره مهاجم با یک سخت‌افزار یکتا هستند. بنابراین از این خصوصیت به‌عنوان ایده اصلی در الگوریتم تشخیص نفوذ پیشنهادی بهره می‌بریم. به‌منظور عملی کردن این ایده می-بایست در ابتدا مکان گره‌های موجود در شبکه حسگر را مشخص نماییم.

روش پیشنهادی به‌گونه‌ای طراحی‌شده است که مشکلات باقی‌مانده در روش مقایسه نسبت قدرت سیگنال دریافتی (RSSI) [۸۱] که باعث افزایش هزینه و اتلاف انرژی می‌گردد را به حداقل می‌رساند. ایده اصلی در روش پیشنهادی برای تشخیص حمله سایبیل بر این اصل استوار است که تا حد امکان بررسی‌ها به‌صورت محلی و در داخل یک گره و بدون انجام ارتباطات انجام گردد و در صورت مشکوک شدن یک گره به حمله سایبیل با ارسال یک پیام به سرخوشه، تصمیم‌گیری نهایی را به آن واگذار نماید. به جهت میسر شدن چنین امری ابتدا می‌بایست محاسبات به‌گونه‌ای باشند که امکان عملیات محلی را به گره‌ها بدهند. بنابراین با توجه به رابطه ۴-۱ داریم:

$$d_i{}^{\alpha} = P_0.K \,/\, R_i \qquad (۶-۴)$$

حالا اگر ۲ گره S_1 با توان ارسال P_1 و S_2 با توان ارسال P_2 دارای فاصله یکسان از گره i باشند و نماد d_i^k فاصله اقلیدسی گره k از گره i باشد آنگاه داریم:

$$d_i^{S_1} = d_i^{S_2} \qquad (۷-۴)$$

حالا با توجه به رابطه (۴-۶) و جایگذاری آن در رابطه (۴-۷) داریم:

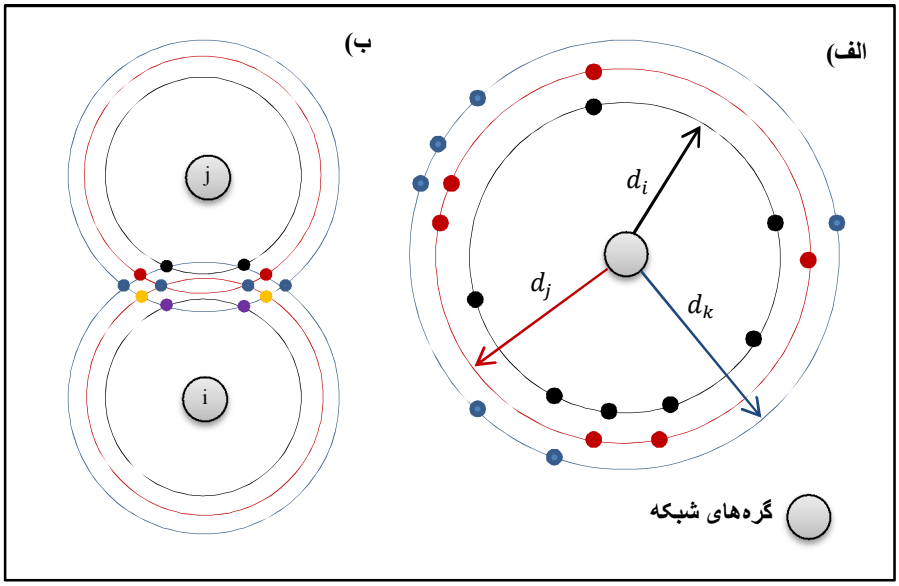
$$P_1.K \,/R_i^{S_1} = P_2.K \,/R_i^{S_2} \qquad (۸-۴)$$

$$P_1 / R_i^{S_1} = P_2 / R_i^{S_2} \quad (۹-۴)$$

$$R_i^{S_1} / R_i^{S_2} = P_1 / P_2 \quad (۱۰-۴)$$

رابطه (۴-۱۰) نشان می‌دهد که اگر دو گره S_1 و S_2 با توان‌های ارسال P_1 و P_2 که در فاصله یکسانی از گره i هستند، پیام‌هایی را به آن ارسال کنند در این صورت نسبت RSSI دریافتی از آن‌ها در گره i با نسبت توان‌های ارسالی از آن‌ها برابر خواهد بود.

با توجه به این‌که مهاجم می‌تواند با توان‌های ارسال متفاوتی پیام‌ها را از گره‌های سایبیل ارسال نماید بنابراین ما برای دو گره سایبیل S_1 و S_2 توان‌های ارسال P_1 و P_2 را در نظر گرفتیم. حالا به جهت این‌که تعیین کنیم دو گره S_1 و S_2 در یک مکان از شبکه حسگر قرار دارند با فرض این‌که در یک فضای دوبعدی (یک صفحه) هستیم حالات مختلف زیر را بررسی می‌کنیم.



شکل (۴-۱۲): نقاط با فاصله یکسان از گره‌های شبکه

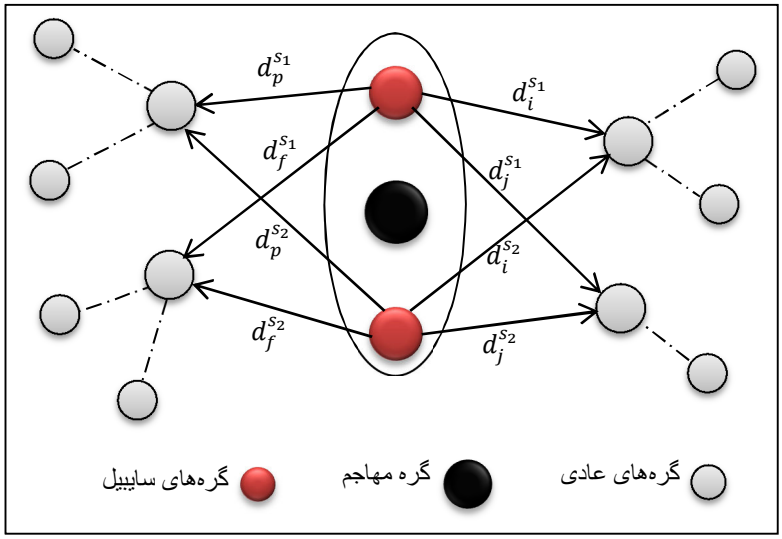
الف) اگر فقط یک گره مانند i را به‌عنوان گره ناظر در نظر بگیریم، همان‌طور که در شکل ۴-۱۲ الف مشاهده می‌گردد بی‌نهایت نقطه با فاصله یکسان و مکان‌های متفاوت وجود دارند. بنابراین احتمال یکسان بودن مکان گره‌هایی با فاصله یکسان بسیار پایین خواهد بود.

ب) اگر دو گره i و j را به‌عنوان ناظر در نظر بگیریم، در این صورت زوج نقاط همرنگ در شکل ۴-۱۲ب در فاصله یکسانی از هر دو ناظر هستند اما در مکان‌های متفاوتی قرار دارند. بنابراین بازهم نمی‌توان از روی فاصله یکسان به‌طور قطعی نتیجه گرفت مکان آن‌ها یکسان است.

ج) اگر سه گره i، j و f را به‌عنوان ناظر در نظر بگیریم، با فرض این‌که آن‌ها بر روی یک خط راست قرار نداشته باشند، در این صورت هیچ زوج نقاطی را نمی‌توان پیدا کرد که نسبت به هر سه ناظر فاصله یکسانی را داشته باشند. بنابراین به‌صورت قطعی می‌توان گفت که اگر سه گره ناظر مختلف برای دو گره S_1 و S_2 فاصله یکسانی را گزارش نمایند به‌طور قطعی آن‌ها در یک مکان از شبکه هستند.

با توجه به این‌که حالات فوق برای فضای دوبعدی بررسی شدند، بنابراین در فضای سه‌بعدی باید حداقل چهار گره ناظر برای تعیین یکسان بودن مکان دو گره S_1 و S_2، فاصله یکسانی را گزارش نمایند. یعنی باید بر طبق شکل ۴-۱۳ داشته باشیم:

$$\left(d_i^{S_1} = d_i^{S_2}\right) And \left(d_j^{S_1} = d_j^{S_2}\right) And \ \left(d_f^{S_1} = d_f^{S_2}\right) And \left(d_p^{S_1} = d_p^{S_2}\right) \quad (۱۱-۴)$$



شکل (۴-۱۳): فاصله گره‌های سایبیل از گره‌های شبکه

درنهایت با توجه به روابط ۴-۱۰ و ۴-۱۱ می‌توانیم بگوییم:

$$\left(\frac{R_i^{S_1}}{R_i^{S_2}} = \frac{P_1}{P_2}\right) And \left(\frac{R_j^{S_1}}{R_j^{S_2}} = \frac{P_1}{P_2}\right) And \left(\frac{R_f^{S_1}}{R_f^{S_2}} = \frac{P_1}{P_2}\right) And \left(\frac{R_p^{S_1}}{R_p^{S_2}} = \frac{P_1}{P_2}\right) \quad (۱۲-۴)$$

همچنین با توجه به این‌که عبارت سمت راست همه تساوی‌ها یک‌چیز است می‌توان نوشت:

$$\frac{R_i^{S_1}}{R_i^{S_2}} = \frac{R_j^{S_1}}{R_j^{S_2}} = \frac{R_f^{S_1}}{R_f^{S_2}} = \frac{R_p^{S_1}}{R_p^{S_2}} \quad (۱۳-۴)$$

حالا به‌راحتی می‌توانیم اجزاء عبارت ۴-۱۳ را به‌صورت محلی در هر گره انجام داده و سپس هر مقدار را به جهت بررسی نهایی به گره سرخوشه ارسال کنیم. برای مثال عبارت کسری سمت چپ تساوی در رابطه ۴-۱۳ که مربوط به نسبت قدرت سیگنال دریافتی در گره i از گره‌های S_1 و S_2 است به‌راحتی و بدون هیچ ارتباط اضافه‌ای با گره‌های دیگر قابل‌محاسبه است. بنابراین در شکل ۴-۱۴، عبارات کسری رابطه ۴-۱۳ به ترتیب به‌صورت محلی در گره‌های i، j، f و p قابل‌محاسبه هستند.

در ادامه هرکدام از این گره‌ها مقادیر نسبت قدرت سیگنال دریافتی خود را از گره‌های S_1 و S_2 به گره سرخوشه ارسال می‌نمایند.

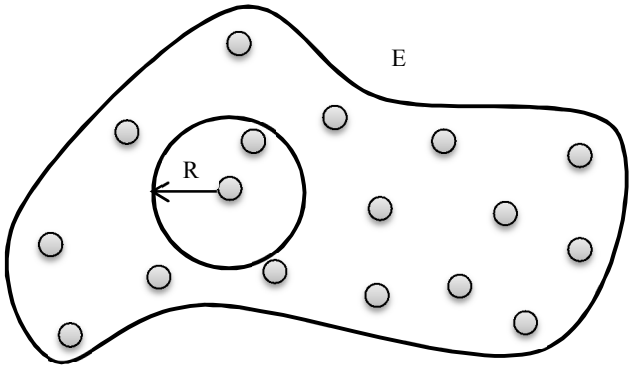
```
Receive (Packet, Si);
If (Si is new node || old_RSSISi <> new_RSSISi)
  {
    old_RSSISi= new_RSSISi;
    For all Sj is Candidate for Sybil attack
       {
         Ratio_RSSIij = RSSISi / RSSISj;
         Create (alert);
         Send (alert, node-Id, Si, Sj, Ratio_RSSIij);
         //send to cluster-head
       }
  }
```

شکل (۴-۱۴): شبه‌کد تشخیص حمله سایبیل

در سرخوشه نیز برای تشخیص حمله سایبیل بر اساس رابطه ۴-۱۳ کافی است شمارنده‌ای برای آن ایجاد شود که به ازای هر پیام دریافتی از گره‌ای مبنی بر مشکوک بودن به گره‌های S_1 و S_2، درصورتی‌که مقدار ارسالی از آن با مقدار ارسالی قبلی برابر باشد یک واحد به شمارنده اضافه نماید.

درنهایت با توجه به رابطه ۴-۱۳ که باید چهار گره دارای نسبت مقادیر برابری برای گره‌های S_1 و S_2 باشند، اگر شمارنده بیش از ۳ هشدار دریافت کند آن‌ها را به‌عنوان حمله سایبیل شناخته و لیست مهاجمین را بروز کرده و به همه گره‌های خوشه ارسال می‌کند.

با توجه به روال کاری تشریح شده می‌توان ادعا کرد که الگوریتم پیشنهادی برای تشخیص حمله سایبیل، با توجه به محاسبه ساده محلی و بدون هیچ ارتباط اضافی با سایر گره‌ها، حداقل انرژی مصرفی را در بین الگوریتم‌های مطرح خواهد داشت. همچنین الگوریتم پیشنهادی بدون نیاز به گره-های ناظر در شبکه و صرفاً بر اساس گره‌های عادی شبکه عملیات تشخیص خود را انجام می‌دهد و بنابراین دارای هزینه بسیار پایین‌تر نسبت به الگوریتم‌های موجود است.



شکل (۴-۱۵): میدان شبکه حسگر بی‌سیم

به جهت فرموله کردن نرخ تشخیص، ابتدا باید احتمال هندسی حضور یک گره در محدوده ارتباطی (همسایگی) گره n_i تعیین گردد.

با توجه به شکل ۴-۱۵، احتمال هندسی حضور یک گره در همسایگی گره i با شعاع ارتباطی R برابر است با:

$$\alpha = \frac{Area\ of\ favorable\ region}{Area\ of\ total\ region} = \frac{\pi R^2}{E}, \qquad \pi R^2 \le E \tag{۱۴-۴}$$

به کمک رابطه ۴-۱۴ می‌توان احتمال اینکه گره i دقیقاً x عدد همسایه داشته باشد را به شکل رابطه ۴-۱۵ نوشت.

$$P^i(x) = Pr(X = x) = \binom{N-1}{x} \alpha^x \, (1-\alpha)^{N-x-1} \quad (۱۵-۴)$$

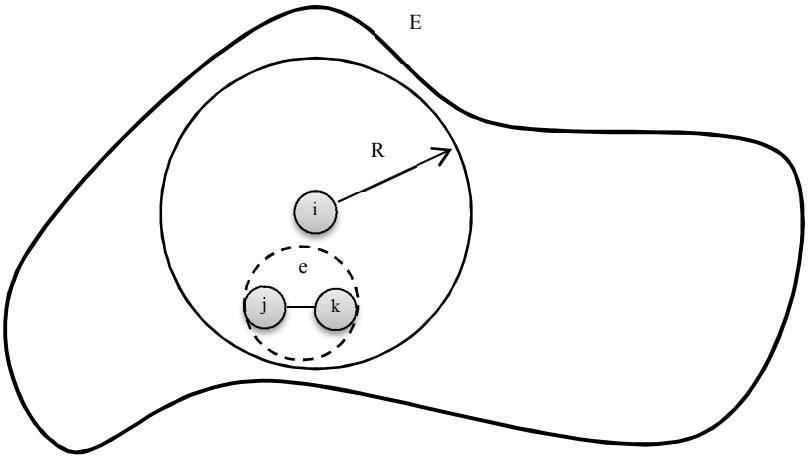
همان‌طور که در الگوریتم پیشنهادی بیان شد، به جهت تشخیص حمله سایبیل باید حداقل ۳ گره در همسایگی آن هشداری مبنی‌بر تهاجم را تولید نمایند؛ بنابراین به جهت تشخیص در گره i، باید این گره حداقل سه همسایه داشته باشد که احتمال آن در رابطه ۴-۱۶ ارائه‌شده است.

$$P^i = \sum_{x=3}^{N-1} P^i(x) \quad (۱۶-۴)$$

رابطه ۴-۱۶ در حقیقت احتمال تشخیص حمله سایبیل در یک گره از شبکه را مشخص می‌کند. بنابراین برای محاسبه احتمال تشخیص حمله سایبیل در کل شبکه حسگر بی‌سیم با N گره توزیع‌شده در محوطه E، از رابطه ۴-۱۷ استفاده می‌شود.

$$P_{Detection} = (P^i)^N \quad (۱۷-۴)$$

در ادامه به جهت صورت‌بندی رابطه نرخ هشدار نادرست، باید حالاتی را در نظر بگیریم که روش تشخیص نفوذ پیشنهادی به‌اشتباه حالت عادی گره‌ها را به‌عنوان حمله سایبیل می‌شناسد.



شکل (۴-۱۶): وضعیت فاصله گره‌ها در شبکه حسگر

بر طبق شکل ۴-۱۶، این امر زمانی رخ خواهد داد که به‌طور طبیعی دو گره یا بیشتر در یک مکان از شبکه قرار داشته باشند. البته با توجه به این‌که الگوریتم پیشنهادی بر اساس نسبت RSSI دریافتی،

مکان گره‌های سایبیل را تخمین می‌زند و مقدار آن تحت تأثیر دما، رطوبت، شرایط محیطی و عوامل دیگر تغییر می‌کند، باید یک مقداری خطا را نیز در نظر بگیریم.

$$if \begin{cases} d_{jk} < e, & then\ raise\ an\ alarm \\ d_{jk} \geq e, & else\ continue\ normal\ operation \end{cases} \quad (۱۸-۴)$$

بر طبق رابطه ۴-۱۸ فرض می‌کنیم اگر فاصله دو گره j و k یعنی d_{jk}، کمتر از e باشد، گره i به‌عنوان گره ناظر، بر اساس الگوریتم پیشنهادی، آن‌ها را در یک مکان تشخیص داده و به‌اشتباه آن‌ها را به‌عنوان حمله سایبیل خواهد شناخت. پارامتر e در اینجا مقدار خطای تخمین فاصله برآورد شده توسط یک گره حسگر است.

به جهت برآورد نرخ هشدار نادرست در کل شبکه حسگر بی‌سیم باید احتمال اینکه دو گره یا بیشتر در فاصله‌ای کمتر از e از هم قرار بگیرند را محاسبه نماییم. به‌عبارت‌دیگر احتمال قرار گرفتن دو گره در دایره‌ای به شعاع $e/2$ باید محاسبه گردد.

$$\beta = \frac{Area\ of\ favorable\ region}{Area\ of\ total\ region} = \frac{\pi(e/2)^2}{E} \quad (۱۹-۴)$$

به کمک رابطه ۴-۱۹، احتمال اینکه گره i دقیقاً x گره در فاصله e از خودش داشته باشد طبق رابطه ۴-۲۰ خواهد بود.

$$P^i(x) = Pr(X = x) = \binom{N-1}{x} \beta^x\ (1-\beta)^{N-x-1} \quad (۲۰-۴)$$

حالا با توجه به رابطه ۴-۲۰، کافی است احتمال اینکه هر گره مانند i در شبکه حسگر حداقل یک گره در فاصله کمتر مساوی e از خودش داشته باشد را محاسبه می‌کنیم.

$$P^i = \sum_{x=1}^{N-1} P^i(x) \quad (۲۱-۴)$$

در حقیقت رابطه ۴-۲۱ احتمال تولید هشدار نادرست در گره i را نشان می‌دهد. در ادامه به جهت محاسبه احتمال هشدار نادرست در کل شبکه حسگر بی‌سیم با N گره توزیع‌شده در محوطه E، کافی است رابطه ۴-۲۲ را محاسبه نماییم:

$$P_{FalseAlarm} = 1 - (1 - P^i)^N \quad (۲۲-۴)$$

در رابطه ۴-۲۲، مقدار $(1 - P^i)$ احتمال تولید هشدار درست در گره i خواهد بود و بنابراین برای این‌که در کل شبکه حسگر با N گره کلیه گره‌ها هشدار درست صادر نمایند باید مقدار $(1 - P^i)^N$ محاسبه گردد. درنهایت نیز مقدار رابطه ۴-۲۲ احتمال اینکه حداقل یک گره در شبکه هشدار نادرستی را تولید کند به ما می‌دهد که همان احتمال هشدار نادرست در کل شبکه حسگر است.

عملیات سرخوشه و تصمیم‌گیری نهایی:

هر وقت پیامی مبنی بر هشدار وجود مهاجم از گره‌های دیگر به سرخوشه ارسال می‌گردد، سرخوشه با بروز رسانی وضعیت هشدار صادرشده و مقایسه آن با حد آستانه، تصمیم‌گیری نهایی را انجام می‌دهد. همان‌طور که در شکل ۴-۱۷ مشاهده می‌شود، در صورت تجاوز هشدارها از حد آستانه، گره مفروض به‌عنوان مهاجم شناسایی‌شده و را در لیست مهاجمان قرار می‌گیرد و از طریق ارسال پیام به سایر گره‌های موجود در خوشه، لیست آن‌ها را نیز به‌روزرسانی می‌نماید.

```
Receive (alert);
If (Looking (alert, intrusion alert))
  {
    Attacker_Count [Node-ID] ++;
    If (Attacker_Count [Node-ID] > Threshold_Alarm)
      {
        Insert (Blacklist, Node-ID);
        Propagate (Blacklist);
      }
  }
```

شکل (۴-۱۷): شبه کد عملیات سرخوشه

۴-۴-۱-۲- کاهش هزینه عملیات شنود

همان‌طور که در تشخیص حملات حفره چاهک، کرم‌چاله، ارسال انتخابی و سایبیل اشاره کردیم، هر گره به جهت تشخیص حذف بسته‌ها در گره‌های همسایه خود از عملیات شنود استفاده می‌کند و به‌تبع آن گره‌هایی با درصد حذف نامتعارف را به‌عنوان مهاجم شناسایی می‌نماید.

مهم‌ترین مشکل در عملیات شنود مصرف انرژی در گره‌های شنود کننده است که باعث کاهش عمر شبکه می‌گردد. بنابراین باید به دنبال راهی باشیم تا این هزینه مصرف انرژی تا حد امکان کاهش یابد. در زیر دو راه‌حل برای این امر پیشنهاد می‌گردد:

انتخاب یک زیرمجموعه پوشا از گره‌ها برای شنود: در این روش به‌جای این‌که همه گره‌ها عملیات شنود را انجام دهند، با استفاده از یک الگوریتم انتخاب گره‌ها، تنها گره‌هایی را برای عملیات شنود و نظارت انتخاب می‌نماییم که با کمک آن‌ها بتوانیم کل عملیات ارسال در شبکه را پوشش داده و مورد شنود قرار دهیم. به‌عبارت‌دیگر با انتخاب یک زیرمجموعه از گره‌ها بتوانیم کل شبکه را برای عملیات شنود پوشش دهیم. این روش به ما این امکان را می‌دهد که جلوی انجام شنودهای اضافی و سربار در گره‌های دیگر را بگیریم و بنابراین هزینه مصرف انرژی عملیات شنود صرفاً بین گره‌های منتخب پخش خواهد شد و با حذف عملیات شنود از سایر گره‌ها مصرف انرژی در آن‌ها را کاهش دهیم.

در شکل (۴-۱۸) یک الگوریتم مناسب به جهت انتخاب زیرمجموعه پوششی از گره‌ها ارائه‌شده است که به‌صورت بهینه زیرمجموعه‌ای با حداقل تعداد گره‌های پوششی انتخاب می‌نماید. این الگوریتم در ابتدای کار شبکه حسگر بی‌سیم و توسط گره ایستگاه پایه اجرا می‌گردد. البته می‌توان آن را بر روی هر گره سرخوشه نیز اجرا نمود تا در هر خوشه به‌صورت مستقل یک زیرمجموعه پوششی برای شنود ایجاد نمود.

در الگوریتم شکل (۴-۱۸)، Neighbors(i) همسایه‌های مستقیم گره i را مشخص می‌نماید که این عملیات نیز می‌تواند در ابتدای کار شبکه توسط ارسال پیام‌های hello توسط گره‌ها انجام گردد و هر گره پس از تعیین همسایه‌های خودش، لیست مربوطه را به گره سرخوشه ارسال نماید.

```
Assign S = {List of all nodes in networks};
do  {
     Foreach (node i in S)
          Find Max Neighbors(i) in S;
     Insert i in spanning-Subset;
     S = S – Neighbors(i);
    }
while (S == null);
Send Overhearing request to nodes in spanning-subset;
```

شکل (۴-۱۸) : شبه کد انتخاب زیرمجموعه پوششی گره‌ها در شبکه

مشکلات این روش عبارتند از:

- افزایش سربار انرژی بر روی گره‌های منتخب: یک مشکل این روش عدم توازن مصرف انرژی بر روی گره‌های شبکه است که باعث می‌گردد گره‌های منتخب جهت شنود، که سربار انرژی بالاتری به آن‌ها تحمیل می‌گردد، زودتر انرژی خود را ازدست‌داده و شبکه را دچار مشکل نمایند. برای مقابله با این مشکل می‌توان از یک الگوریتم پویا به جهت انتخاب گره‌های پوششی استفاده کرد که بتواند بعد از مدت‌زمان مشخصی که انرژی گره‌های منتخب از حد معینی کمتر شد، مجدداً اقدام به انتخاب یک زیرمجموعه پوششی جدید نماید. که البته خود این الگوریتم و استفاده مجدد آن در حین کار شبکه مستلزم زمان و صرف انرژی است.
- وجود الگوریتم اولیه برای تعیین زیرمجموعه پوششی از گره‌ها برای عملیات شنود بر روی گره چاهک و نیاز به ارتباطات بین گره‌ها

عملیات شنود محدود: در این روش به‌جای این‌که هر گره همه پیام‌های محدوده تحت پوشش خود را شنود نماید، صرفاً به شنود پیام‌های ارسالی خود اکتفا نماید. به‌عبارت‌دیگر با این کار هر گره صرفاً به ارسال روبه‌جلوی پیام‌های خود از گره‌های همسایه مستقیمش (یک گام روبه‌جلو) نظارت خواهد کرد.

با انجام این عملیات، هزینه مصرف انرژی به جهت شنود محدود در هر گره پایین آمده و به حداقل خود می‌رسد و همه گره‌ها نیز به‌صورت متوازن و هماهنگ انرژی مصرف خواهند کرد و به‌تبع آن طول عمر شبکه نیز افزایش خواهد یافت.

مزیت عملیات شنود محدود نسبت به روش انتخاب زیرمجموعه شنود پوششی در این است که اولاً نیازمند الگوریتم اضافی به جهت انتخاب گره‌ها و تکرار مجدد آن ندارد و ثانیاً هزینه انرژی عملیات شنود به‌صورت متوازن بین همه گره‌ها پخش خواهد شد و نیازمند سازمان‌دهی مجدد زیرمجموعه پوششی جدید نیز نخواهد بود. بنابراین ما در شبیه‌سازی‌های خود از روش عملیات شنود محدود به جهت آشکارسازی حذف پیام‌ها در گره‌های شبکه و به‌تبع آن تشخیص حملات مربوطه استفاده خواهیم کرد.

در بخش تحلیل انرژی، میزان مصرف انرژی عملیات شنود محدود در مقایسه با عملیات ارسال و دریافت پیام‌ها مورد ارزیابی قرارگرفته است که نتایج حاصله نشان از مصرف انرژی حداقلی آن است.

۴-۴-۱-۳- بهبود دقت تشخیص به کمک اعتبار سنجی هشدارها

یکی از مشکلات سیستم‌های تشخیص نفوذ مبتنی بر همکاری گره‌ها، عدم ارزشیابی پیام‌های هشدار صادرشده از گره‌های مختلف در شبکه است که این امر موجب کاهش دقت تشخیص می‌گردد. به جهت غلبه بر این مشکل ما از یک روش مبتنی بر اعتماد سبک بهره خواهیم برد به‌گونه‌ای که بتواند بر اساس سطح اعتماد گره‌ها، پیام‌های هشدار تولیدشده توسط آن‌ها را ارزشیابی نماید. این ارزشیابی می‌تواند گره سرخوشه را در جهت تصمیم‌گیری نهایی خود در تشخیص گره‌های مهاجم و حملات یاری نماید و دقت تشخیص‌های آن را نیز ارتقاء دهد.

عملیات مبتنی بر اعتماد: سطح اطمینان یک گره به‌عنوان خصوصیت اعتماد تعریف می‌گردد.Tv_{XY} مقدار اعتماد گره Y است که توسط گره X محاسبه‌شده است. هر گره X برداری به جهت ارزیابی اعتماد گره‌های همسایه‌اش دارد که بردار اعتماد نامیده می‌شود و آن را با Tv_X نشان می‌دهیم:

$$Tv_X = \left(Tv_{X,1},\ Tv_{X,2}, \dots, Tv_{X,N}\right) \quad (۲۳-۴)$$

در رابطه (۴-۲۳)، $Tv_{X,i}$ مقدار اعتماد i امین همسایه گره X را نشان می‌دهد. به جهت محاسبه و به‌روزرسانی بردارهای اعتماد موجود در گره‌های شبکه از تابع توزیع بتا استفاده می‌کنیم:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\ \Gamma(\beta)}\ p^{\alpha-1}(1-p)^{\beta-1} \quad (۲۴-۴)$$

در رابطه (۴-۲۴)، Γ تابع گاما و $0 \le p \le 1$ و $\alpha > 0\ ,\ \beta > 0$ هستند. درواقع با استفاده از تابع توزیع بتا که به‌وسیله دو پارامتر α و β مشخص می‌گردد، می‌توانیم احتمالات پسین[1] را برای وقایع دودویی ارائه کنیم. امید ریاضی احتمال توزیع بتا نیز به‌صورت زیر ارائه می‌شود:

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad (۲۵-۴)$$

به جهت انطباق تابع بتا با عملیات محاسبه اعتماد گره‌ها در شبکه حسگر بی‌سیم، متغیر تصادفی p را به‌عنوان احتمال موفقیت تحویل بسته‌ها و تابع $f(p|\alpha,\beta)$ را نیز به‌عنوان احتمال این‌که p یک مقدار خاص دارد در نظر می‌گیریم. بنابراین امید ریاضی احتمال توزیع بتا یعنی$E(p)$ به‌صورت محتمل‌ترین مقدار p تفسیر می‌گردد که در شبکه حسگر به‌عنوان مقدار اعتماد گره‌ها در نظر گرفته می‌شود و پارامتر α به تعداد موفقیت‌آمیز تحویل بسته‌ها $(SPDs)$ و β نیز به تعداد ناموفق تحویل بسته‌ها $(UPDs)$ اشاره دارند. بنابراین با توجه به رابطه (۴-۲۵) و استفاده از آن برای پیش‌بینی اعتماد در آینده داریم:

$$Tv_{X,i} = \frac{SPDs+1}{SPDs+UPDs+2},\ \ where\quad SPDs, UPDs \ge 0 \quad (۲۶-۴)$$

[1] Posteriori Probabilities

با توجه به این‌که رابطه (۴-۲۶) برای محاسبه اعتماد گره‌های شبکه وابسته به عملیات شنود در گره‌ها است؛ بنابراین به‌طور کامل منطبق بر واحد تشخیص نفوذ مبتنی بر خصوصیات در سطح اول است و درنتیجه ازلحاظ مصرف انرژی بسیار سبک است.

هر گره حسگر X، میانگین اعتماد گره‌های همسایه‌اش را توسط رابطه (۴-۲۷) محاسبه می‌نماید:

$$E(X) = \frac{\sum_{i=1}^{N} Tv_{X,i}}{N} \qquad (۴-۲۷)$$

همچنین مقادیر اعتماد گره‌ها توسط تابع نگاشت رابطه (۴-۲۸) سطح‌بندی می‌شوند:

$$Mp(Tv_{node}) = \begin{cases} high & 0.8 \leq Tv_{node} \leq 1 \\ medium & 0.5 \leq Tv_{node} \leq 0.8 \\ uncertain & 0.3 \leq Tv_{node} \leq 0.5 \\ low & 0 \leq Tv_{node} \leq 0.3 \end{cases} \qquad (۴-۲۸)$$

پس از محاسبه میانگین اعتماد، این میزان توسط رابطه ۴-۲۸ به یک سطح مشخص از اعتماد نگاشت می‌یابد. هر پیام انتقالی در شبکه نیز باید در سرآیند خود حاوی سطح اعتماد گره ارسال‌کننده باشد. درنهایت پیام‌های هشدار رسیده از گره‌های مختلف به گره سرخوشه، بر اساس سطح اعتماد گره‌های ارسال‌کننده آن‌ها ارزیابی می‌شوند تا در عملیات تشخیص نفوذ تصمیم دقیق‌تری اتخاذ گردد.

در الگوریتم شکل ۴-۱۹، Node(alert) گره‌ای است که پیام هشدار را به سرخوشه ارسال کرده و Node-ID نیز گره‌ای است که مشکوک به حمله در شبکه است و پیام هشدار مربوط به آن است.

همان‌طور که در الگوریتم اصلاح‌شده در شکل ۴-۱۹ مشاهده می‌شود، هرگاه یک پیام هشدار درباره نفوذ در گره‌ای به سرخوشه ارسال گردد، بر اساس سطح اعتماد گره هشداردهنده مقادیر مختلفی به شمارنده نفوذ آن افزوده خواهد شد. به‌عبارت‌دیگر هرچه سطح اعتماد گره هشداردهنده بالاتر باشد این پیام هشدار دارای اهمیت بالاتری بوده و به‌تبع آن مقدار بیشتری نیز به شمارنده تشخیص نفوذ افزوده می‌شود.

```
Receive (alert);
If  (Looking (alert, intrusion alert )) {
    Switch Trust_Level (Node(alert)) {
        case 'high': Attacker_Count [Node-ID] += λ;
        case 'medium': Attacker_Count [Node-ID] += β;
        case 'uncertain': Attacker_Count [Node-ID] += δ;
    }
    If (Attacker_Count [Node-ID] > Treshold_Alarm)  {
        Insert(Blacklist, Node-ID);
        Propagate (Blacklist);
    }
}
```

شکل (۴-۱۹): شبه کد عملیات سرخوشه مبتنی بر اعتماد

ما چهار پارامتر $(\varphi, \delta, \beta, \lambda)$ را برای چهار سطح مختلف اعتماد در گره‌ها ارائه کردیم که رابطه (۴-۲۹) ارزش آن‌ها را بر اساس سطح اعتماد نشان می‌دهد. برای مثال گره‌ای با سطح اعتماد بالا در صورت ارسال پیام هشدار به سرخوشه بالاترین اهمیت را دارد و به شمارنده نفوذ مقدار $\lambda=1$ را اضافه می‌کند و گره‌ای با سطح اعتماد پایین، کمترین اهمیت را دارد و معمولاً مقدار ارزش آن $\varphi=0$ است.

$$\begin{aligned}&\text{Parameters: } 0 \le \varphi < \delta < \beta < \lambda \le 1\\&\text{Trust Levels: } \quad \text{low} \quad \text{uncertain} \quad \text{medium} \quad \text{high}\end{aligned} \tag{۴-۲۹}$$

رابطه (۴-۳۰) نحوه محاسبه شمارنده هشدار نفوذ برای یک گره مشکوک به حمله را بر اساس مقادیر رابطه (۴-۲۶) نشان می‌دهد:

$$\underset{Count}{Attacker}(Node) = \sum_{i=1}^{n1} \lambda + \sum_{j=1}^{n2} \beta + \sum_{k=1}^{n3} \delta + \sum_{p=1}^{n4} \varphi \tag{۴-۳۰}$$

در رابطه فوق مقادیر n_i به ترتیب تعداد هشدارهای رسیده از گره‌هایی با سطوح اعتماد مختلف بر اساس دسته‌بندی رابطه (۴-۲۸) است. با این الگوریتم مبتنی بر اعتماد و با توجه به این‌که در گره سرخوشه متناسب با سطح اعتماد گره‌ها به پیام‌های هشدار آن‌ها اهمیت می‌دهد، وضعیت دقت تشخیص بهبود خواهد یافت.

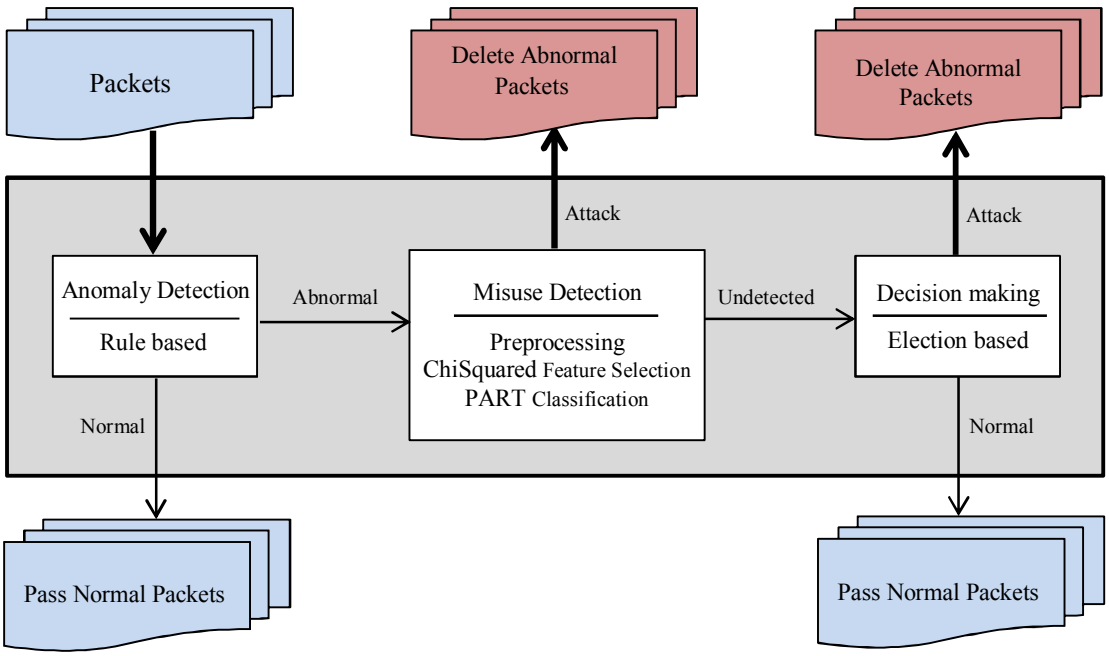
۴-۴-۲- تشخیص نفوذ سطح میانی (در سطح سرخوشه ها)

مواردی که در تشخیص نفوذ سطح پایین قابل‌تشخیص نبوده و نیازمند بررسی‌های بیشتری هستند، به‌وسیله ارتباطات به سرخوشه ها ارسال می‌شوند تا در سیستم تشخیص نفوذ سطح میانی که بر روی گره‌های سرخوشه اجرا می‌گردد، مورد بررسی قرار گیرند. در این مرحله همچنین ترافیک عادی ارسالی به خود سرخوشه نیز به جهت وجود ناهنجاری و تشخیص حملات بررسی می‌گردند. در این سطح سربار محاسبات و ارتباطات از فاز قبل بیشتر خواهد بود که با در نظر گرفتن منابع بیشتر در سرخوشه ها اجرای آن منطقی و معقول خواهد بود.

با توجه به این‌که گره‌های سرخوشه دارای اهمیت بالایی در شبکه‌های حسگر بی‌سیم هستند و عملیات مدیریت خوشه، تجمیع داده‌ها و انتقال اطلاعات را به ایستگاه پایه انجام می‌دهند، بسیار بیشتر از گره‌های عادی موردتوجه مهاجمان و هجوم حملات قرار می‌گیرند. همچنین کاملاً واضح است که نفوذ و کنترل یک سرخوشه توسط یک مهاجم، موجب اختلال در عملیات کل خوشه و بعضاً کل شبکه حسگر خواهد شد. بنابراین در یک شبکه حسگر حفظ امنیت گره‌های سرخوشه و به‌گونه‌ای تضمین آن بسیار حائز اهمیت است. با توجه به معایب روش‌های تشخیص نفوذ مبتنی بر ناهنجاری و تشخیص نفوذ مبتنی بر رفتار سوء، هیچ‌کدام به‌تنهایی قابلیت تأمین امنیت گره‌های سرخوشه را ندارند.

از طرفی با توجه به این‌که در شبکه‌های حسگر بی‌سیم، انرژی به‌عنوان یک پارامتر حیاتی مطرح است و عملاً طول عمر شبکه به آن وابسته است، باید از یک روش سبک‌وزن برای تشخیص نفوذ در آن‌ها استفاده گردد. البته در اغلب موارد گره‌های سرخوشه با توجه به عملیات مربوطه، دارای قابلیت‌های بالاتری نسبت به گره‌های عادی شبکه هستند. بنابراین می‌توانیم به جهت تأمین امنیت سرخوشه‌ها الگوریتم‌های تشخیص نفوذ کاراتری را با توجه به حساسیت امنیتی بالای آن‌ها، بکار ببریم.

ما در این بخش یک الگوریتم تشخیص نفوذ ترکیبی را به جهت تأمین امنیت سرخوشه‌ها ارائه می-کنیم که هم به جهت نرخ تشخیص و نرخ هشدارهای نادرست و هم به جهت مصرف انرژی، از کارائی مناسبی برخوردار است.



شکل (۴-۲۰): سیستم تشخیص نفوذ سطح میانی برای گره‌های سرخوشه

همان‌طور که در شکل ۴-۲۰ مشاهده می‌گردد روال سیستم تشخیص نفوذ پیشنهادی به این صورت است که در ابتدا بسته‌های داده رسیده از گره‌های دیگر توسط مدل تشخیص نفوذ مبتنی بر ناهنجاری موردبررسی قرار می‌گیرند. تشخیص نفوذ مبتنی بر ناهنجاری که در بخش ۴-۴-۲-۱ ارائه‌شده است می‌تواند به‌سرعت تعداد زیادی از بسته‌های عادی را فیلتر نماید و سپس بسته‌های غیرعادی را به مدل تشخیص رفتار سوء تحویل دهد (که در بخش ۴-۴-۲-۲ تشریح شده است) تا در آنجا حملات و نوع آن‌ها شناسایی شوند. درنهایت بسته‌هایی که توسط مدل تشخیص مبتنی بر رفتار سوء تشخیص داده نشوند نیز در مرحله تصمیم‌گیری تعیین وضعیت خواهند شد. در ادامه به تشریح جزئیات هریک از مراحل سیستم تشخیص نفوذ پیشنهادی می‌پردازیم.

۴-۴-۲-۱- تشخیص نفوذ مبتنی بر ناهنجاری پیشنهادی

مدل تشخیص ناهنجاری به‌عنوان خط اول دفاعی در سیستم تشخیص نفوذ پیشنهادی استفاده می‌گردد. با توجه به این‌که از تعداد بسیار زیاد بسته‌های موجود، درواقع تنها تعداد کمی از آن‌ها مربوط به حملات بوده و اغلب آن‌ها نیز مربوط به حالت عادی شبکه هستند، بنابراین با به‌کارگیری یک مدل تشخیص ناهنجاری که شبیه به یک فیلتر عمل می‌کند، به‌سرعت بسته‌های حالت عادی عبور داده‌شده و بسته‌های مربوط به حالت ناهنجاری فیلتر شده و برای تشخیص و بررسی بیشتر و دقیق‌تر به مدل تشخیص رفتار سوء تحویل داده می‌شوند.

در یک سیستم تشخیص ناهنجاری از یک مدل تعریف‌شده از رفتار عادی شبکه استفاده می‌گردد، بنابراین یک بسته درصورتی توسط سیستم غیرعادی تشخیص داده می‌شود که رفتار جاری در مقایسه با رفتار عادی تعریف‌شده انحراف داشته باشد.

یکی از مشکلات روش تشخیص ناهنجاری این است که اگر الگوهای رفتار جاری و رفتار عادی در شبکه تغییر کنند، در این صورت سیستم معمولاً ارتباطات عادی را به‌عنوان ارتباطات غیرعادی تشخیص می‌دهد و مشکل کلاس‌بندی اشتباه را ایجاد می‌کند. بااین‌وجود به‌ندرت ارتباطات غیرعادی را به‌عنوان ارتباطات عادی تشخیص می‌دهد.

برای رفع مشکل کلاس‌بندی اشتباه در مدل تشخیص ناهنجاری، در خط دفاعی دوم از یک سیستم تشخیص رفتار سوءاستفاده می‌کنیم تا بسته‌های غیرعادی تشخیص داده‌شده از مدل تشخیص ناهنجاری را تحویل گرفته و با بررسی‌های بیشتر و دقیق‌تر وضعیت نهایی آن‌ها را مشخص نماید. به‌عبارت‌دیگر مدل تشخیص ناهنجاری با دریافت تعداد بسیار زیادی از بسته‌ها، موارد نسبتاً کم غیرعادی را همچون یک فیلتر از موارد زیاد عادی جدا کرده و پس از عبور دادن بسته‌های عادی با دقت بسیار بالا، موارد غیرعادی را به جهت بررسی‌های دقیق‌تر به مدل تشخیص رفتار سوء تحویل می‌دهد.

همان‌طور که گفته شد برای ایجاد مدل تشخیص ناهنجاری برای نظارت بر وضعیت بسته‌های اطلاعاتی، باید یک الگوی رفتار عادی در شبکه ایجاد گردد که در این تحقیق به جهت نیاز به کارائی بالا از یک متد تحلیل مبتنی بر قانون استفاده‌شده است. برای ایجاد مدل تشخیص ناهنجاری، قوانین زیر برای متد مبتنی بر قانون در نظر گرفته‌شده‌اند [۳۲] و [۶] که در جدول ۴-۱ به‌طور خلاصه آورده شده‌اند.

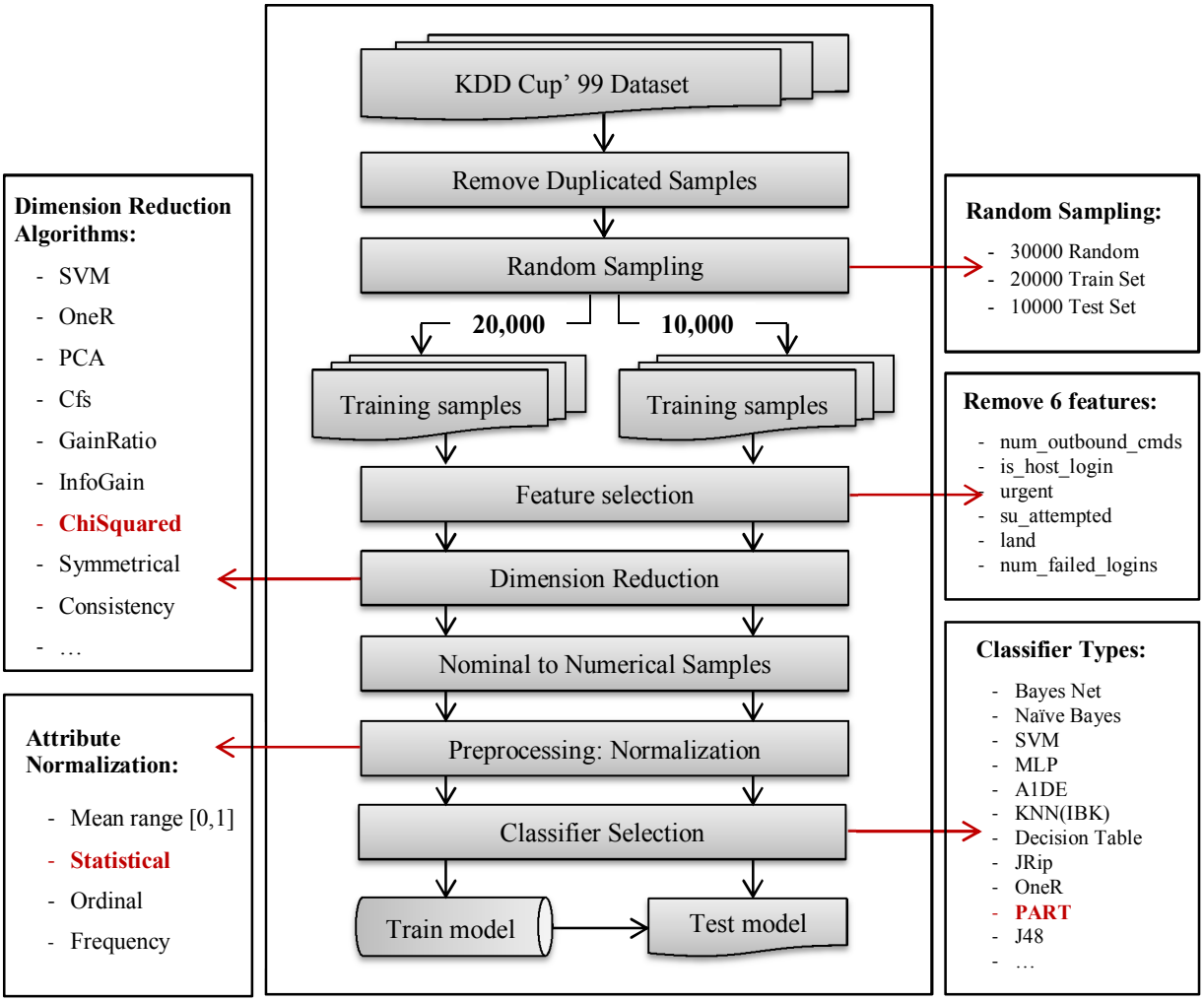
جدول (۴-۱): قوانین مدل تشخیص ناهنجاری

نام قانون	توصیف قانون	حملات قابل‌شناسایی
قانون فاصله	زمان بین دو پیام دریافتی پشت سر هم نباید از یک حد پایین و بالا تجاوز کند.	حملات رد سرویس و سیل ارسال پیام
قانون ارسال روبه‌جلو	یک پیام ارسالی باید توسط گره‌های میانی به سمت جلو هدایت گردد.	حملات سیاه‌چاله و ارسال انتخابی
قانون اصالت	پیام ارسالی توسط فرستنده نباید هنگامی‌که به گیرنده می‌رسد دچار تغییرات شده باشد.	حمله تغییر محتوا
قانون تأخیر	ارسال مجدد یک پیام باید بعد از یک‌زمان انتظار مشخصی انجام گردد.	حمله رد سرویس
قانون تکرار	یک پیام خاص تنها می‌تواند به تعداد دفعات معینی توسط یک گره یکسان تکرار و ارسال گردد.	حمله رد سرویس
قانون رنج رادیویی	یک پیام تنها باید از گره‌های همسایه دریافت گردد که رنج توان رادیویی دریافتی آن مشخص است.	حملات سایبیل و کرم چاله و سیل ارسال پیام
قانون پارازیت	تعداد برخوردها برای ارسال یک بسته باید کمتر از حد آستانه باشد.	حمله برخورد

۴-۴-۲-۲- مدل پیشنهادی برای تشخیص نفوذ مبتنی بر رفتار سوء

واحد تشخیص رفتار سوء، مدل‌های مختلفی از رفتار حملات شناخته‌شده را بکار می‌برد، بنابراین باید یک مدل پایه منطبق با این رفتارها ایجاد نماییم. ازآنجاکه عملکرد و کارائی در اغلب روش‌های تشخیص نفوذ از طریق داده‌های آموزشی تضمین می‌گردد، متدهای یادگیری ماشین با این روش منطبق است.

ما در این مرحله به جهت افزایش کارائی سیستم تشخیص نفوذ و همچنین کاهش انرژی مصرفی، یک مدل پیش‌پردازش داده را ارائه می‌کنیم و درنهایت برای بدست آوردن بهترین نرخ تشخیص، الگوریتم-های مختلف یادگیری ماشین را به جهت دسته‌بندی بررسی می‌کنیم. شکل ۴-۲۱ نمودار مراحل مدل پیشنهادی را برای اصلاحات در مجموعه داده‌ها نشان می‌دهد.



شکل (۴-۲۱): چارت مدل پیش‌پردازش پیشنهادی

یکی از عوامل مؤثر در افزایش پیچیدگی محاسباتی و مصرف حافظه در استفاده از روش‌های داده‌کاوی، تعداد نمونه‌های آموزشی برای ایجاد مدل است. بنابراین با توجه به تعداد بسیار زیاد نمونه-های موجود در مجموعه‌داده، عملاً امکان به‌کارگیری آن را در شبکه‌های حسگر بی‌سیم غیرممکن می‌نماید. بنابراین ما در ابتدا در مراحل اول و دوم مدل پیشنهادی، با استفاده از شیوه‌های مناسب پیش‌پردازش سعی می‌کنیم تعداد نمونه‌های موجود را به حد مناسبی برسانیم تا قابلیت استفاده در شبکه‌های حسگر بی‌سیم را داشته باشد.

۱. حذف نمونه‌های تکراری: همان‌طور که در شکل (۴-۲۱) مشاهده می‌شود با توجه به افزونگی داده‌های موجود در مجموعه‌دادگان، در ابتدا عملیات حذف نمونه‌های تکراری را از آن انجام می‌دهیم.

همان‌طور که در جدول ۴-۲ مشاهده می‌شود با انجام عملیات حذف نمونه‌های تکراری، حجم مجموعه دادگان به‌شدت کاهش پیدا می‌کند (کاهش ۷۰/۵۳٪)، که علاوه بر کاهش پیچیدگی محاسباتی و نیز کاهش انرژی مصرفی، به افزایش دقت تشخیص و کاهش مصرف حافظه نیز کمک می‌کند.

۲. نمونه‌برداری تصادفی داده‌ها: در ادامه از کل رکوردهای مجموعه‌دادگان KDD cup 99 بعد از حذف افزونگی، با استفاده از نمونه‌برداری تصادفی تعداد ۲۰۰۰۰ رکورد نمونه به‌عنوان داده‌های آموزشی و ۱۰۰۰۰ رکورد نیز به‌عنوان داده‌های آزمون انتخاب می‌شوند. با توجه به این‌که مجموعه نمونه‌های حملات Probe، U2R و R2L خیلی کم هستند بنابراین در عملیات نمونه‌گیری همه رکوردهای مربوط به آن‌ها را در نظر گرفته و همچنین دوسوم این رکوردها را به‌عنوان داده‌های آموزشی و یک‌سوم آن‌ها را نیز به‌عنوان داده‌های آزمون انتخاب می‌کنیم. اما همه مجموعه نمونه‌های دیگر مطابق با نرخ آن‌ها از مجموعه‌داده kddcup.data_10_percent.gz انتخاب می‌شوند که در جدول (۴-۲) آمار دقیق آن‌ها ارائه‌شده است.

جدول (۴-۲): تعداد داده‌ها و نرخ توزیع آن در مجموعه‌دادگان KDDCup'99

Category	Total data		No Duplicated data		Training data		Testing data	
	samples	Ratio(%)	samples	Ratio(%)	samples	Ratio(%)	samples	Ratio(%)
Normal	97278	19.69%	87832	60.33%	11079	55.40%	5549	55.49%
Dos	391458	79.24%	54572	37.48%	6798	33.99%	3393	33.93%
Probe	4107	0.83%	2130	1.46%	1421	7.11%	709	7.09%
R2L	1126	0.23%	999	0.69%	667	3.33%	332	3.32%
U2R	52	0.01%	52	0.04%	35	0.17%	17	0.17%
TOTAL	**494021**	**100%**	**145585**	**100%**	**20000**	**100%**	**10000**	**100%**

با توجه به این‌که تعداد زیاد ویژگی‌ها نیز یکی از مهم‌ترین عوامل در افزایش پیچیدگی محاسباتی و اتلاف انرژی بوده و همچنین باعث افزایش چشمگیر حافظه مصرفی خواهد بود، عملاً استفاده از روش‌های داده‌کاوی را در شبکه‌های حسگر بی‌سیم با توجه به محدودیت‌های محاسباتی و حافظه

گره‌های آن، غیرممکن می‌نماید. بنابراین به جهت غلبه بر این مشکل و کاهش پیچیدگی محاسباتی و اتلاف انرژی و همچنین حافظه مصرفی باید روش‌هایی را برای کاهش تعداد ویژگی‌ها به تعداد مناسب استفاده کنیم که این امر نیز در مراحل ۳ و ۴ در مدل پیشنهادی انجام‌شده است.

۳. انتخاب ویژگی‌ها (حذف ویژگی‌های بی‌اثر): به جهت بهینه‌سازی مجموعه دادگان در مرحله اول با یک مشاهده سطحی به‌راحتی می‌توان چند ویژگی را به دلیل عدم تمایز در مجموعه دادگان انتخاب کرده و آن‌ها را از مجموعه دادگان حذف کرد. همان‌طور که در شکل ۴-۲۱ مشاهده می‌شود، این مرحله تحت عنوان انتخاب ویژگی ارائه‌شده است که در آن شش ویژگی با کمترین اهمیت و عدم تمایز از مجموعه دادگان حذف‌شده‌اند. برای مثال دو ویژگی is_host_login و num_outbound_cmds در کل رکوردهای مجموعه دادگان دارای مقدار صفر هستند و بنابراین هیچ‌گونه تمایزی را در مجموعه دادگان ایجاد نخواهند کرد. این ویژگی‌ها در جدول ۴-۳ ارائه‌شده‌اند.

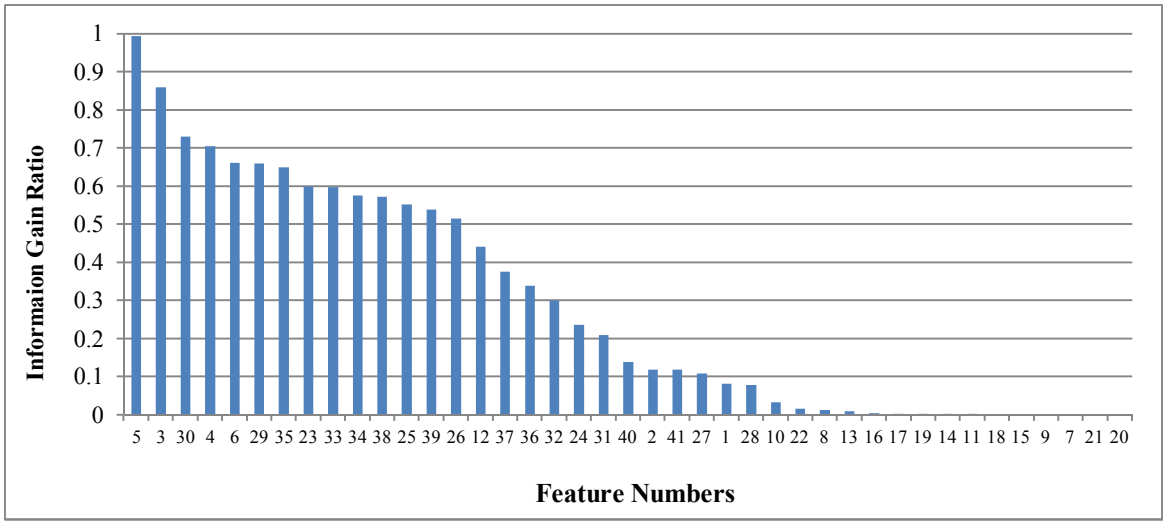
جدول (۴-۳): ویژگی‌های با کمترین اهمیت و عدم تمایز در مجموعه‌دادگان KDDCup'99

is_host_login	num_outbound_cmds	urgent	su_attempted	land	num_failed_logins

۴. کاهش ابعاد و انتخاب ویژگی‌های مؤثر: در ادامه به جهت کاهش بیشتر در پیچیدگی محاسباتی و جلوگیری از اتلاف انرژی در گره‌های شبکه حسگر بی‌سیم از یک الگوریتم انتخاب ویژگی به جهت کاهش ابعاد در مجموعه داده‌ها استفاده می‌کنیم.

در بین ویژگی‌های موجود در مجموعه داده‌ها، همه آن‌ها تأثیر قطعی روی خروجی ندارند و حتی برخی از آن‌ها باعث بالا رفتن خطا در طبقه‌بندی می‌شوند. در شکل (۴-۲۲)، رتبه‌بندی ۴۱ ویژگی موجود در مجموعه دادگان KDDCup'99 بر اساس نسبت بهره اطلاعات ارائه‌شده است. همان‌طور که در شکل ۴-۲۲ می‌گردد اغلب ویژگی‌ها دارای یک نسبت بهره اطلاعات (IGR) کمتر از میانگین مجموعه‌داده (IGR میانگین ۰/۲۹) هستند. درواقع فقط ۲۰ ویژگی بالای میانگین هستند که این امر نشان می‌دهد که مجموعه داده‌ها در یک گروه کوچکی از مقادیر متمرکز هستند. ویژگی‌هایی که

منجر به همگرایی دسته‌های ارتباطی شبکه به یک گروه کوچکی از مقادیر می‌گردند دارای اطلاعات خیلی کمی برای توصیف رفتار یک گره در شبکه هستند. این امر نشان‌دهنده این است که مجموعه داده‌ها شامل یک سری داده‌های نامربوط برای تشخیص نفوذ بوده و نیازمند بهینه‌سازی است.



شکل (۴-۲۲): رتبه‌بندی ویژگی‌های مجموعه‌دادگان KDDCup'99 بر اساس نسبت بهره اطلاعات

بنابراین انتخاب ویژگی یک بخش مهم در بهینه‌سازی مجموعه‌داده است که می‌تواند تأثیر مطلوبی بر کارائی سیستم تشخیص نفوذ بگذارد. ما به جهت انتخاب یک مجموعه مؤثر از ویژگی‌ها، مهم‌ترین روش‌های انتخاب ویژگی را موردبررسی قراردادیم که در جدول ۴-۴ نتایج حاصل از آن‌ها را بر اساس نرخ تشخیص بر روی الگوریتم‌های مختلف دسته‌بندی ارائه کردیم.

همان‌طور که در جدول ۴-۴ مشاهده می‌شود، بیشترین کاهش ویژگی‌ها مربوط به روش ChiSquared با ۴ ویژگی است که درعین‌حال نیز با نرخ تشخیص بالای ۹۹.۵۹٪ شرایط بسیار مطلوبی برای استفاده در شبکه‌های حسگر را دارد. همچنین روش InfoGain نیز با تعداد ویژگی ۱۱ و نرخ تشخیص ۹۹.۷۲، قابلیت استفاده در شبکه‌های حسگر را دارد، اما به جهت حدود ۳ برابری تعداد ویژگی‌های انتخاب‌شده به نسبت روش ChiSquared، سربار محاسباتی و درنتیجه مصرف انرژی بالاتری را به سیستم تحمیل می‌نماید. بنابراین ما به جهت کاهش ابعاد از متد انتخاب ویژگی ChiSquared استفاده می‌کنیم. چهار ویژگی انتخاب‌شده به جهت افزایش کارائی در سیستم تشخیص نفوذ در جدول (۴-۵) ارائه‌شده‌اند.

جدول (۴-۴): مقایسه نرخ تشخیص روش‌های انتخاب ویژگی موجود در مجموعه‌دادگان KDDCup'99

		Detection Rate of Various Classifiers								
Feature Selection Approaches	Selected Features	Random Tree	J48	Bayes Net	PART	JRip	Random Forest	A1DE	Decision Table	Naïve Bayes
Full Features	41	99.42	99.53	96.54	99.64	99.69	**99.80**	99.80	99.17	86.01
Remove ineffective Features	35	99.38	99.48	96.44	99.57	99.62	**99.80**	99.78	99.08	87.18
Chi Squared	4	99.40	99.32	97.97	**99.59**	99.45	99.44	99.49	98.34	89.57
One R	7	99.43	99.42	97.41	99.51	**99.57**	99.54	99.53	98.41	91.11
Consistency Subset + BFS	8	99.45	99.6	97.62	99.58	99.59	99.55	**99.61**	99.06	82.62
Info Gain	11	99.45	99.52	96.54	99.58	99.60	**99.72**	99.71	99.06	88.69
CFS Subset + BFS	13	99.39	99.48	97.01	99.48	99.56	99.63	**99.69**	98.97	91.99
Symmetrical Uncert	15	99.39	99.55	96.37	99.55	99.64	**99.76**	99.67	99.10	86.75
Correlation	15	98.79	98.91	93.62	99.01	98.96	**99.24**	98.36	96.52	81.61
ReliefF	15	98.54	98.72	93.91	98.78	98.66	**99.01**	98.62	96.75	89.97
Gain Ratio	16	99.43	**99.66**	97.30	99.61	99.59	99.60	99.56	98.83	88.45
SVM	22	99.56	99.56	96.42	99.64	99.70	**99.78**	99.75	99.05	84.94

جدول (۴-۵): ویژگی‌های انتخاب‌شده با الگوریتم انتخاب ویژگی ChiSquared

Feature #	Feature Name	Description
3	service	service on the destination, e.g., http, telnet,etc.
5	src_bytes	Number of data bytes from source to destination
30	diff_srv_rate	% of connections to different services
35	dst_host_diff_srv_rate	Dif_srv_rate for destination host

۵. هنجارسازی داده‌ها: در مرحله آخر ما به هنجارسازی مجموعه دادگان می‌پردازیم. مرحله هنجار-سازی ویژگی‌ها به‌عنوان یک گام اساسی در پیش‌پردازش داده‌ها به جهت افزایش کارائی تشخیص در سیستم‌های تشخیص نفوذ، مطرح است. چهار طرح مختلف برای هنجارسازی ویژگی‌ها در مرحله پیش‌پردازش داده‌ها در سیستم‌های تشخیص نفوذ وجود دارند که بر اساس اطلاعات ارائه شده در بخش کارهای پیشین (بخش ۳-۸)، مدل هنجارسازی آماری به‌عنوان بهترین انتخاب برای مجموعه داده‌های بزرگ معرفی‌شده است. بنابراین ما نیز از هنجارسازی آماری بر روی مجموعه دادگان استفاده کرده‌ایم. هدف از هنجارسازی آماری تبدیل داده‌های مشتق شده از هر توزیع نرمال به توزیع نرمال استاندارد با میانگین صفر و واریانس یک است. هنجارسازی آماری به‌صورت رابطه (۴-۳۱) تعریف می-شود:

$$x_i = \frac{v_i - \mu}{\sigma} \qquad (۴-۳۱)$$

که در آن مقدار μ، میانگین و σ نیز انحراف معیار مقادیر ویژگی داده‌شده است:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} v_i \quad , \quad \sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(v_i - \mu)^2} \qquad (۴-۳۲)$$

۶. انتخاب الگوریتم دسته‌بندی مناسب: در مرحله آخر نیز به جهت انتخاب بهترین الگوریتم دسته‌بندی داده‌ها در مدل پیشنهادی، به ارزیابی کارائی انواع رده‌بندهای موجود بر روی مجموعه دادگان KDDCup'99 پرداخته‌ایم که نتایج آن در جدول ۵-۱۰ در بخش نتایج ارائه‌شده است.

ما همچنین روش پیشنهادی خود را بر روی دادگان NSL نیز بررسی کردیم و به جهت انتخاب یک مجموعه مؤثر از ویژگی‌ها، مهم‌ترین روش‌های انتخاب ویژگی را موردبررسی قراردادیم که در جدول ۴-۶ نتایج حاصل از آن‌ها را بر اساس نرخ تشخیص بر روی الگوریتم‌های مختلف دسته‌بندی ارائه کردیم.

جدول (۴-۶): مقایسه نرخ تشخیص روش‌های انتخاب ویژگی موجود در مجموعه‌دادگان NSL

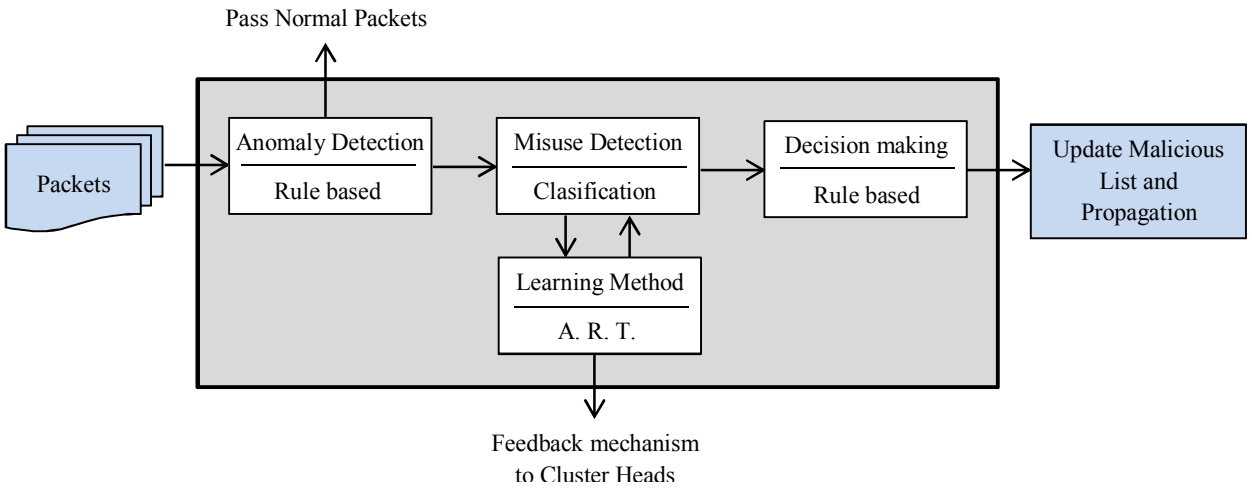
		Detection Rate of Various Classifiers							
Feature Selection Approaches	Selected Features	J48	Bayes Net	PART	JRip	Random Forest	A1DE	Decision Table	Naïve Bayes
Full Features	41	85.26	79.14	81.71	85.05	84.93	83.62	78.23	78.29
Symmetrical Uncert	8	86.49	79.97	**88.93**	87.27	85.91	83.33	78.26	59.79
Chi Squared	**9**	**89.71**	78.28	**89.83**	86.02	86.66	85.63	77.75	74.00
CFS Subset + BFS	9	86.05	80.85	**89.29**	86.85	86.89	85.22	78.19	67.06
Base Features in [2]	9	78.54	75.90	74.85	75.84	77.45	74.54	72.81	51.92
Info Gain	10	89.69	77.98	85.56	81.98	84.40	82.35	77.75	75.96
Consistency Subset + BFS	12	87.94	79.15	**88.73**	86.92	80.90	83.08	78.06	69.27
Gain Ratio	20	86.81	78.55	84.07	88.77	87.47	83.99	78.14	78.55
Features in [1]	22	88.68	78.84	83.58	81.09	83.44	82.11	77.69	69.89
SVM	24	89.50	79.41	85.40	86.29	84.48	85.19	78.23	73.84
Features in [16]	33	86.28	78.65	**87.38**	80.99	84.09	83.34	78.20	77.49

همانطور که در جدول ۴-۶ مشاهده می‌گردد در اینجا نیز روش ChiSquared با ۹ ویژگی با نرخ تشخیص بالای ۸۹.۸۳٪ دارای بهترین نرخ تشخیص در بین روش‌های مختلف انتخاب ویژگی بوده و شرایط مطلوبی برای استفاده در شبکه‌های حسگر را دارد.

۴-۴-۳- تشخیص نفوذ سطح بالا[1] (در سطح ایستگاه پایه)

درنهایت در تشخیص نفوذ سطح بالا که در ایستگاه پایه اجرا می‌گردد، تمامی ترافیک‌های ارسالی به آن، همراه با مواردی که در سطوح قبلی قابلیت تشخیص نداشته‌اند مورد بررسی‌های دقیق‌تر قرار می-گیرند. به‌عبارت‌دیگر در این سطح با توجه به منابع بالای ایستگاه پایه و همچنین اهمیت بالای امنیت سرخوشه‌ها، الگوریتم‌های تشخیص نفوذ قدرتمندتری به کار گرفته می‌شود، به‌گونه‌ای که عملاً امنیت سرخوشه‌ها تضمین گردد. طرحواره معماری پیشنهادی برای سیستم تشخیص نفوذ ایستگاه پایه در شکل ۴-۲۳ نشان داده‌شده است.

در این سطح نیز مانند سطح سرخوشه ها پیشنهاد می‌کنیم که از ترکیبی از روش‌های مبتنی بر ناهنجاری و مبتنی بر قانون استفاده گردد. همچنین با به‌کارگیری الگوریتم‌های یادگیری در این سطح امکان تشخیص حملات ناشناخته و جدید نیز فراهم گردیده است. به‌عبارت‌دیگر در تشخیص نفوذ سطح بالا که در ایستگاه پایه اجرا می‌گردد کاملاً مشابه تشخیص نفوذ میانی در سطح گره‌های سرخوشه رفتار می‌گردد و با توجه به اینکه در ایستگاه پایه ما محدودیت انرژی را نداریم می‌توانیم با به‌کارگیری الگوریتم‌های یادگیری امکان تشخیص حملات ناشناخته و جدید را فراهم کنیم. بنابراین تنها تفاوت تشخیص نفوذ سطح بالا با سطح میانی در به‌کارگیری الگوریتم‌های یادگیری در آن است.



شکل (۴-۲۳): سیستم تشخیص نفوذ سطح بالا برای ایستگاه پایه

[2] High Level Intrusion Detection

۴-۵- جمع‌بندی

در این بخش بر پایه روش‌های موجود برای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم که در بخش ۳ معرفی شدند و با توجه به مشکلات و چالش‌های مربوطه، معماری تشخیص نفوذ پیشنهادی را ارائه کردیم. منطق معماری پیشنهادی بر پایه سطوح مختلف حساسیت گره‌ها ازلحاظ تأمین امنیت و منابع مربوطه استوار است. ما با در نظر گرفتن این منطق یک معماری سه سطحی را طراحی کردیم و تمهیدات مختلفی را برای هر سطح در نظر گرفتیم. در سطح اول که مربوط به گره‌های عادی شبکه است و تحت عنوان تشخیص نفوذ سطح پایین از آن یادکردیم با ارائه یک روش تشخیص نفوذ مبتنی بر خصوصیات، یک شیوه سبک و مؤثر را برای امنیت گره‌های عادی ایجاد کردیم. در سطح دوم معماری پیشنهادی نیز با ارائه یک روش تشخیص ترکیبی مبتنی بر داده‌کاوی همراه با یک مدل پیش‌پردازش داده‌ها و الگوریتم کاهش ویژگی Shisquare، امنیت گره‌های سرخوشه را تأمین کردیم. در سطح آخر معماری پیشنهادی نیز با توجه به عدم محدودیت منابع و انرژی در گره چاهک از یک روش ترکیبی قوی به همراه الگوریتم‌های یادگیری ماشین به جهت شناسایی حملات جدید و بروز رسانی بانک حملات موجود استفاده کردیم. در فصل آتی نیز مراحل مختلف شبیه‌سازی و ارائه نتایج معماری تشخیص نفوذ پیشنهادی و مقایسه با کارهای موجود، تشریح می‌شود.

۵– شبیه‌سازی روش پیشنهادی و ارائه نتایج

در این بخش ما به شبیه‌سازی روش تشخیص نفوذ پیشنهادی و ارائه نتایج حاصل از ارزیابی خواهیم پرداخت. در ابتدا ما شبیه‌ساز NS2 را به جهت شبیه‌سازی شبکه‌های حسگر بی‌سیم معرفی می‌کنیم. در ادامه به شبیه‌سازی شبکه حسگر بی‌سیم همراه با معرفی انواع پارامترهای مهم آن خواهیم پرداخت.

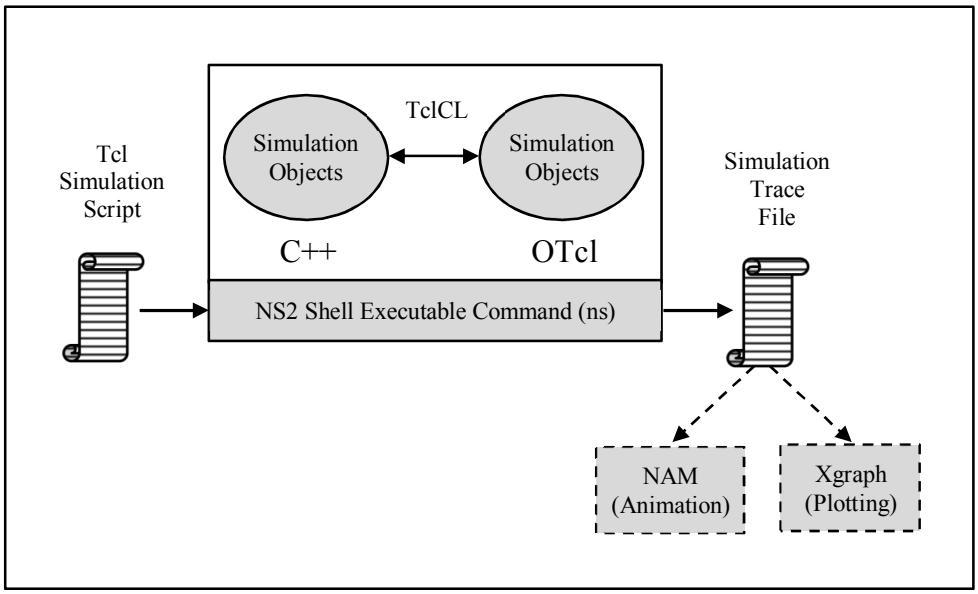
۵-۱- معرفی شبیه‌ساز NS2

ما به جهت شبیه‌سازی‌های خود از شبیه‌ساز NS2 استفاده کرده‌ایم. شبیه‌ساز NS2 به‌طور ساده یک ابزار شبیه‌سازی مبتنی بر رخداد است که برای مطالعه و بررسی ماهیت پویای شبکه‌های ارتباطی مطرح‌شده است. این شبیه‌ساز همانند شبکه‌های سیمی، عملیات و پروتکل‌های شبکه‌های بی‌سیم را نیز به‌خوبی می‌تواند پشتیبانی نماید. در این شبیه‌ساز از پروتکل‌های مسیریابی (مانند AODV، DSR، ...) گرفته تا پروتکل‌های لایه انتقال (مانند UDP و TCP) و همچنین پروتکل‌های لایه کاربردی (مانند CBR و FTP) به جهت تعریف ترافیک کاری در شبکه، همگی می‌توانند به‌خوبی مورداستفاده قرار گیرند تا کاربران بتوانند به‌خوبی عملکرد و رفتار موردنظرشان را در شبیه‌سازی ارائه نمایند [۲۱].

شکل ۵-۱ معماری پایه‌ای NS2 را نشان می‌دهد. در این شبیه‌ساز کاربران با فرامین اجرایی TCL که به‌عنوان آرگومان ورودی دستورات اجرایی ns می‌باشد، امکان تعریف سناریوی شبیه‌سازی شبکه موردنظر خود را دارند. در اغلب موارد به‌عنوان خروجی شبیه‌سازی، یک فایل اطلاعات شبیه‌سازی ایجاد می‌گردد که از آن به‌منظور ترسیم نمودارهای گرافیکی و همچنین ایجاد انیمیشن شبکه طراحی‌شده استفاده می‌شود. مراحل مختلف ایجاد خروجی در شکل ۵-۲ نشان داده‌شده است.

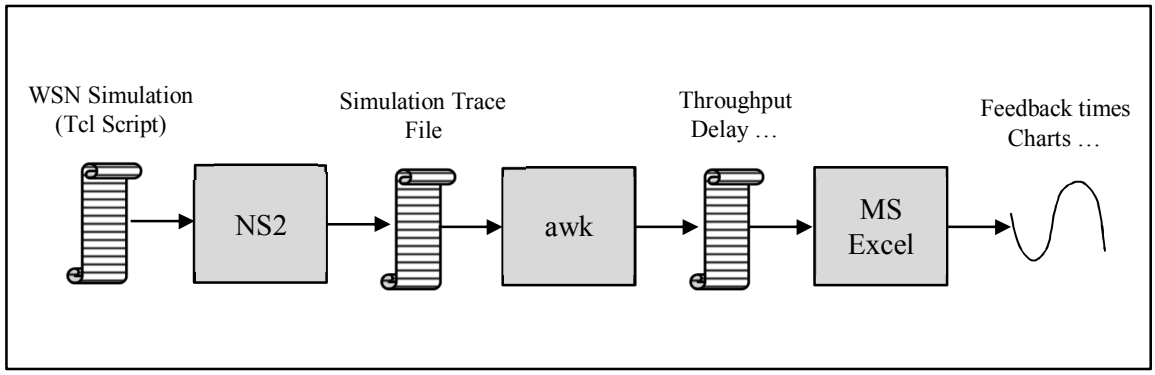
ابزار Nam (ابزار نمایش و متحرک‌سازی شبکه) یک بخش جدا است که همراه با ns برای ایجاد یک تفسیر بصری از توپولوژی شبکه و نمایش متحرک آن در زمان اجرای شبیه‌سازی مورداستفاده قرار می‌گیرد. شبیه‌ساز ns به‌صورت خودکار یک فایل Nam ایجاد می‌نماید که شامل اطلاعات توپولوژی

شبکه مانند وضعیت گره‌ها و پیکره‌بندی‌های آن‌ها همراه با داده‌های پیگیری وضعیت اجرایی شبکه است.



شکل (۵-۱): معماری پایه در شبیه‌ساز NS2 [۹۶]

awk زبانی است که برای تولید گزارش‌ها و استخراج بخشی از داده‌ها برای پردازش‌های بعدی، بکار می‌رود. در حقیقت awk به جهت تحلیل فایل‌های پیگیری خروجی از ns و ترسیم نمودارهای لازم مانند میزان گذردهی و معیارهای ارزیابی دیگر در شبکه شبیه‌سازی‌شده بکار می‌رود.



شکل (۵-۲): استفاده از فایل‌های خروجی در شبیه‌ساز NS2 برای نمایش رفتار شبکه و رسم نمودارها

۵-۲- مجموعه دادگان[1]

ما به جهت ارزشیابی مناسب سیستم تشخیص نفوذ پیشنهادی خود از مجموعه دادگان KDDCup'99 استفاده کردیم. به جهت عدم وجود یک نمونه واقعی از مجموعه‌داده در شبکه‌های حسگر بی‌سیم برای تشخیص نفوذ، مجموعه‌دادگان KDDCup'99 به‌عنوان نمونه‌ای برای ارزیابی کارائی سیستم‌های‌تشخیص‌نفوذ در این شبکه‌ها استفاده می‌گردد. مجموعه‌دادگان KDDCup'99، توسط دانشگاه کلمبیا و از طریق شبیه‌سازی نفوذها و حملات در یک محیط شبکه نظامی در سازمان DARPA و در سال ۹۸ تنظیم گردید [۹۷]. این کار در آزمایشگاه لینکلن ام‌آی‌تی انجام شد و سپس در سال ۹۹ در بایگانی UCI KDDCup قرار گرفت.

هر نمونه از این مجموعه‌دادگان یک اتصال بین دو میزبان در شبکه را منطبق با پروتکل‌های شبکه ارائه می‌نماید و از طریق ۴۱ ویژگی توصیف می‌گردد که شامل ۳۴ نوع ویژگی عددی[2] و ۷ نوع ویژگی سمبولیک[3] است و مطابق با خصوصیات مختلف حملات در نظر گرفته‌شده است. کلیه این ویژگی‌ها می‌توانند در ۴ دسته مختلف طبقه‌بندی شوند که در زیر تشریح شده‌اند [۶۲]:

- **ویژگی‌های پایه**[4]: این ویژگی‌ها مربوط به خصوصیات اتصال‌های TCP هستند.
- **ویژگی‌های محتوا**[5]: این ویژگی‌ها مربوط به خصوصیات درون ارتباطی است که به‌وسیله دانش دامنه پیشنهادشده‌اند.
- **ویژگی‌های ترافیکی**[6]: این ویژگی‌ها مربوط به خصوصیات استخراج‌شده از طریق یک پنجره زمانی دو ثانیه‌ای هستند.
- **ویژگی‌های میزبان**[1]: این ویژگی‌ها مربوط به خصوصیات طراحی‌شده برای تشخیص حملاتی هستند که بیش از دو ثانیه دوام‌دارند.

[1] Data Sets
[2] Numerical Features
[3] Symbolic Features
[4] Basic Features
[5] Content Features
[6] Traffic Features

در جدول ۵-۱ ویژگی‌های مجموعه دادگان KDD همراه با طبقه‌بندی فوق تشریح شده‌اند.

جدول (۵-۱): تشریح ویژگی‌های مجموعه دادگان KDD همراه با طبقه‌بندی آن‌ها

Type	#	Feature name	#	Feature name
Basic	1	Duration: Length (number of seconds) of the connection	6	dst_bytes: Number of data bytes from destination to source
	2	protocol_type: Type of the protocol, e.g., tcp, udp, etc.	7	Land: 1 if connection is from/to the same host/port; 0 else
	3	Service: service on the destination, e.g., http, telnet,etc.	8	wrong_fragme: Number of "wrong" fragments
	4	Flag: Normal or error status of the connection	9	Urgent: Number of urgent packets
	5	src_bytes: Number of data bytes from source to destination		
Content	10	Hot: Number of "hot" indicators	17	num_file_creations: Number of file creation operations
	11	num_failed_logins: Number of failed login attempts	18	num_shells: Number of shell prompts
	12	logged_in: 1 if successfully logged in; 0 otherwise	19	num_access_files: Number of operations on access control files
	13	num_compromised: Number of "compromised" conditions	20	num_outbond_cmds: No. of outbond comands in an ftp session
	14	root_shell: 1 if root shell is obtained; 0 otherwise	21	is_host_login: 1 if the login belongs to the "hot" list; 0 else
	15	su_attempted: 1 if "su root" command attempted; 0 else	22	is_guest_login: 1 if the login is a "guest" login; 0 else
	16	num_root: Number of "root" accesses		
Traffic	23	Count: Number of connections to the same host as the current connection in the past two seconds		
	24	Srv_count: Number of connections to the same service as the current connection in the past two seconds		
	25	Serror_rate: % of connections that have "SYN" errors	29	Same_srv_rate: % of connections to the same service
	26	Srv_serror_rate: % of connections that have "SYN" errors	30	Diff_srv_rate: % of connections to different services
	27	Rerror_rate: % of connections that have "REJ" errors	31	Srv_diff_host_rate: % of connections to different hosts
	28	Srv_rerror_rate: % of connections that have "REJ" errors		
Host	32	Dst_host_count: Count for destination host	37	Dst_host_srv_diff_host_rate: Diff_host_rate for dest. host
	33	Dst_host_srv_count: Srv_count for destination host	38	Dst_host_serror_rate: Serror_rate for destination host
	34	Dst_host_same_srv_rate: Same_sr... for destination host	39	Dst_host_srv_serror_rate: Srv_serror_rate for destination host
	35	Dst_host_diff_srv_rate: Dif_srv_rate for destination host	40	Dst_host_rerror_rate: Rerror_rate for destination host
	36	Dst_host_same_srv_port_rate: Same_src_p... for dest host	41	Dst_host_srv_rerror_rate: Srv_serror_rate for dest. host

هر نمونه در مجموعه‌دادگان KDDCup'99، دارای برچسبی است که حالت عادی یا یک حمله خاص را نشان می‌دهد. این مجموعه دادگان شامل ۲۳ برچسب است که یکی مربوط به حالت عادی و ۲۲ حالت دیگر مربوط به حملات مختلف هستند که در ۴ گروه Probe، DoS، U2R و R2L

[1] Host Features

طبقه‌بندی‌شده‌اند. بنابراین این پنج نوع رفتار در آزمایش‌های مربوط به طبقه‌بندی در سیستم‌های تشخیص نفوذ بکار می‌روند.

حملات جعل، تغییر و بازپخش اطلاعات مسیریابی، حفره چاهک، سایبیل، کرم‌چاله و جعل کردن تصدیق دریافت بسته‌ها، قبل از اینکه حمله را شروع کنند نیازمند ایجاد یک مرحله Probe هستند، بنابراین همه آن‌ها به‌عنوان حملات Probe طبقه‌بندی می‌شوند. حمله ارسال انتخابی که داده‌های نادرست را برای ایجاد یک حمله بکار می‌برد، به‌عنوان حمله DoS شناخته می‌شود. حملات حفره چاهک، کرم‌چاله و سیل ارسال پیام، ناشی از حملات داخلی هستند و بنابراین به‌عنوان حملات U2R طبقه‌بندی می‌شوند. حملات جعل، تغییر و بازپخش اطلاعات مسیریابی، حفره چاهک، سایبیل، کرم‌چاله، سیل ارسال پیام و جعل کردن تصدیق دریافت بسته‌ها، نقطه‌ضعف موجود در سیستم را برای ایجاد یک حمله استفاده می‌کنند و بنابراین آن‌ها به‌عنوان R2L طبقه‌بندی می‌شوند. در جدول ۵-۲ این چهار گروه همراه با توصیفشان و انواع حملات مربوطه ارائه‌شده‌اند [۶۳] [۹۷].

جدول (۵-۲): توصیف گروه‌های مجموعه دادگان KDD همراه با انواع حملات مربوطه

#	Class Type	Description	Attack Type
1	DOS	In DoS, an attacker tries to prevent legitimate users accessing or consume a service. Select Forward, which uses illegitimate data forwarding to make an attack, is known as a DoS attack.	Smurf, Back, Neptune, Teardrop, Land, Pod.
2	Probe	In Probe attack, an attacker tries to gain information about the victim machine. The intention is to check vulnerability on the victim machine. e.g. Port scanning. The attacks of Spoofed, Altered, or Replayed Routing Information, Sinkhole, Sybil, Wormholes, and Acknowledgment Spoofing need to make a probe step before they begin to attack, so they would be classified as Probe attacks.	Portsweep, Satan, Ipsweep, Nmap.
3	R2L	The attacker tries to gain access to the victim system by compromising the security via password guessing or breaking. Spoofed, Altered,or Replayed Routing Information, Sinkhole, Sybil, Wormholes, Hello Floods, and Acknowledgment Spoofing use the weakness in the system to make an attack, so they would be classified as R2L.	Buffer_Overflow, Guess_passwd, Warezclient, Spy, Warezmaster, Phf, Multihop, Imap.
4	U2R	In U2R, an attacker has local access privilege to the victim machine and tries to access super users (administrators) privileges via “Buffer overflow” attack. Sinkhole, Wormholes, and Hello Floods are caused by inner attacks, and are therefore classified as U2R.	Loadmodule, Perl, Ftp_write, Rootkit.

در این رساله مجموعه‌دادگان kddcup.data_10_percent.gz را در مرحله نمونه‌برداری در ایجاد مجموعه داده‌های آموزشی و آزمون استفاده کرده‌ایم. این مجموعه‌داده شامل ۱۰ درصد از داده‌های موجود در KDDCup'99 است که در آن تعداد کل رکوردهای ارتباطی ۴۹۴،۰۲۱ تا است. آمار کامل این مجموعه‌داده در جدول (۵-۳) ارائه‌شده است.

جدول (۵-۳): تعداد داده‌ها و نرخ توزیع آن در مجموعه‌دادگان KDDCup'99

Category	Total data		No Duplicated data		Training data		Testing data	
	samples	Ratio (%)	samples	Ratio (%)	samples	Ratio (%)	samples	Ratio (%)
Normal	97278	19.69%	87832	60.33%	11079	55.40%	5549	55.49%
Dos	391458	79.24%	54572	37.48%	6798	33.99%	3393	33.93%
Probe	4107	0.83%	2130	1.46%	1421	7.11%	709	7.09%
R2L	1126	0.23%	999	0.69%	667	3.33%	332	3.32%
U2R	52	0.01%	52	0.04%	35	0.17%	17	0.17%
TOTAL	**494021**	**100%**	**145585**	**100%**	**20000**	**100%**	**10000**	**100%**

۵-۳- معرفی معیارهای ارزیابی

به‌منظور بررسی نتایج شبیه‌سازی‌های انجام‌شده، در گام اول باید معیارهای مناسبی را برای ارزیابی کارائی و عملکرد شبکه حسگر بی‌سیم و سیستم تشخیص نفوذ پیشنهادی در نظر بگیریم. سپس این معیارها را بر روی خروجی شبیه‌سازی‌ها اعمال نموده و نتایج حاصله را در قالب نمودار ارائه می‌نماییم.

- **نرخ تشخیص:** نرخ تشخیص یا دقت تشخیص درصد حملات تشخیص داده‌شده را نسبت به کل حملات مشخص می‌نماید:

$$Detection\ Rate\ = \frac{No.of\ Detected\ Attacks}{No.of\ Attacks} * 100\% \qquad (۱-۵)$$

- **نرخ هشدار نادرست:** این معیار نرخ هشدار نادرست را در تشخیص حملات نشان می‌دهد. به‌عبارت‌دیگر مشخص می‌کند که چه درصدی از حملات تشخیص داده‌شده حمله نبوده‌اند و سیستم تشخیص نفوذ به‌اشتباه آن‌ها را حمله تشخیص داده است.

$$False\ Positive\ Rate = \frac{No.of\ misdetected\ Attacks}{No.of\ Normal\ connections} * 100\% \quad (۲-۵)$$

- **میانگین مصرف انرژی و طول عمر شبکه:** این معیار که در شبکه‌های حسگر بی‌سیم بسیار بااهمیت است میانگین مصرف انرژی گره‌های حسگر را در واحد زمان نشان می‌دهد و طول عمر شبکه از طریق آن مشخص می‌گردد. به‌عبارت‌دیگر این معیار میانگین انرژی مصرف‌شده در گره‌های شبکه را توسط سیستم تشخیص نفوذ پیشنهادی نشان می‌دهد:

$$Average\ Energy\ Consumption = \frac{\sum_{i=1}^{nodes} Initial\ Energy_i - Residal\ Energy_i}{No.of\ \ nodes} \quad (۳-۵)$$

- **معیار تأخیر انتها به انتها در ارسال:** این معیار زمان صرف شده برای ارسال یک بسته در طول شبکه از مبدأ به مقصد است.
- **معیار نرخ ارسال ترافیک:** به جهت بررسی دقیق‌تر پایداری شبکه در کنار تأخیر ارسال بهتر است از معیار نرخ ارسال ترافیک هم استفاده گردد که رابطه مربوط به آن به شکل زیر است:

$$Traffic\ Rate = \sum_{f=1}^{Max\ Flow} \frac{No.of\ sent\ packets * Packet\ size * 8}{flow\ time} \quad (۴-۵)$$

- **معیار گذردهی شبکه:** این معیار میزان داده‌های دریافت شده در کل شبکه را در واحد زمان بیان می‌کند:

$$Network\ Throughput = \sum_{f=1}^{Max\ Flow} \frac{No.of\ received\ packets * Packet\ size * 8}{flow\ time} \quad (۵-۵)$$

- **نرخ تحویل بسته‌ها:** این معیار میزان داده‌های دریافت شده را به نسبت داده‌های ارسال‌شده در کل شبکه مشخص می‌نماید و از تقسیم گذردهی شبکه بر نرخ ارسال ترافیک حاصل می‌شود:

$$Packet\ Delivery\ Ratio = \frac{No.of\ received\ packets}{No.of\ sent\ packets} * 100 \quad (۶-۵)$$

- **سربار مسیریابی:** این معیار میزان سربار ناشی از مسیریابی داده‌ها بین گره‌های شبکه حسگر را بیان می‌کند:

$$Normalized\ Routing\ Load\ (NRL) = \frac{No.of\ Routing\ packets}{No.of\ Received\ packets} \quad (۷-۵)$$

- **نرخ حذف بسته‌ها:** این معیار درصد بسته‌های حذف‌شده را نسبت به کل بسته‌های ارسال‌شده تعیین می‌نماید:

$$Packet\ Drop\ Ratio\ (PDR) = \frac{Packet\ Loss}{No.of\ sent\ packets} * 100 \quad (۸-۵)$$

- **مدت‌زمان آموزشی:** مدت‌زمانی که مدل بر اساس نمونه داده‌های آموزشی ساخته می‌شود.
- **مدت‌زمان آزمون:** مدت‌زمانی که مدل ساخته‌شده در مرحله آموزش بر اساس داده‌های آزمون مورد ارزیابی قرار می‌گیرد.
- **پیچیدگی محاسباتی:** این معیار حجم محاسبات مدل پیشنهادی را نشان می‌دهد که به تعداد ویژگی‌های انتخاب‌شده، تعداد نمونه‌های آموزشی و الگوریتم طبقه‌بندی استفاده‌شده وابسته است. این معیار رابطه مستقیم با زمان آزمون مدل ایجادشده دارد.

همچنین به جهت مقایسه مناسب روش پیشنهادی با کارهای موجود، از بستر یکسانی برای شبیه‌سازی همه روش‌ها استفاده کردیم که پارامترهای آن در جداول ۵-۴ و ۵-۶ ارائه‌شده است.

۵-۴- مراحل شبیه‌سازی‌ها

ما برای شبیه‌سازی و ارائه نتایج روش پیشنهادی از شبیه‌ساز قدرتمند NS2 استفاده می‌نماییم که یکی از مطرح‌ترین شبیه‌سازها در حوزه مطالعات شبکه است. برای انجام شبیه‌سازی ما باید در سه مرحله زیر کار شبیه‌سازی خود را انجام دهیم:

- مرحله اول شبیه‌سازی شبکه حسگر بی‌سیم که به‌عنوان محیط اصلی و پایه برای آزمون روش تشخیص نفوذ پیشنهادی ما استفاده می‌گردد. ما در این مرحله یک شبکه حسگر بی‌سیم همراه با تمامی پارامترهای لازم ایجاد خواهیم کرد.

- مرحله دوم شبیه‌سازی انواع حملات مفروض برای آزمون روش تشخیص نفوذ پیشنهادی است. در حقیقت ما برای شبیه‌سازی‌ها و ارائه نتایج روش پیشنهادی، نیازمند مجموعه‌ای از حملات به‌عنوان مجموعه دادگان هستیم که قبلاً در بخش‌های قبلی آن‌ها را تشریح نمودیم. مهم‌ترین حملاتی که در این مورد نیازمند آن‌ها هستیم حملات لایه شبکه و مسیریابی خواهند بود که بیشترین استفاده را در حملات و مهاجمان به خود اختصاص می‌دهند و همه مراجع نیز در طرح‌های پیشنهادی خود بر روی آن‌ها متمرکزشده‌اند.

- مرحله سوم شبیه‌سازی خود سیستم تشخیص نفوذ پیشنهادی است که باید بر روی گره‌های شبکه حسگر بی‌سیم نصب‌شده و سیستم را در مقابل حملات مفروض محافظت نماید. همان‌گونه که در فصل ۳ بحث شد، روش‌های مختلفی برای سیستم‌های تشخیص نفوذ در مراجع مختلف پیشنهادشده‌اند. ما نیز در این مرحله معماری پیشنهادی تشخیص نفوذ خود را با تمامی پارامترهای مربوطه و جزئیات دقیق آن بر روی شبکه حسگر بی‌سیم شبیه‌سازی‌شده در مرحله اول، نصب خواهیم کرد و نتایج اجرایی آن را در قالب نمودارهای آماری ترسیم خواهیم کرد. در انتها نیز روش پیشنهادی خود را در هر دو فاکتور درصد تشخیص حملات و میزان مصرف انرژی با روش‌های موجود مقایسه خواهیم نمود.

۵-۵- شبیه‌سازی شبکه‌های حسگر بی‌سیم

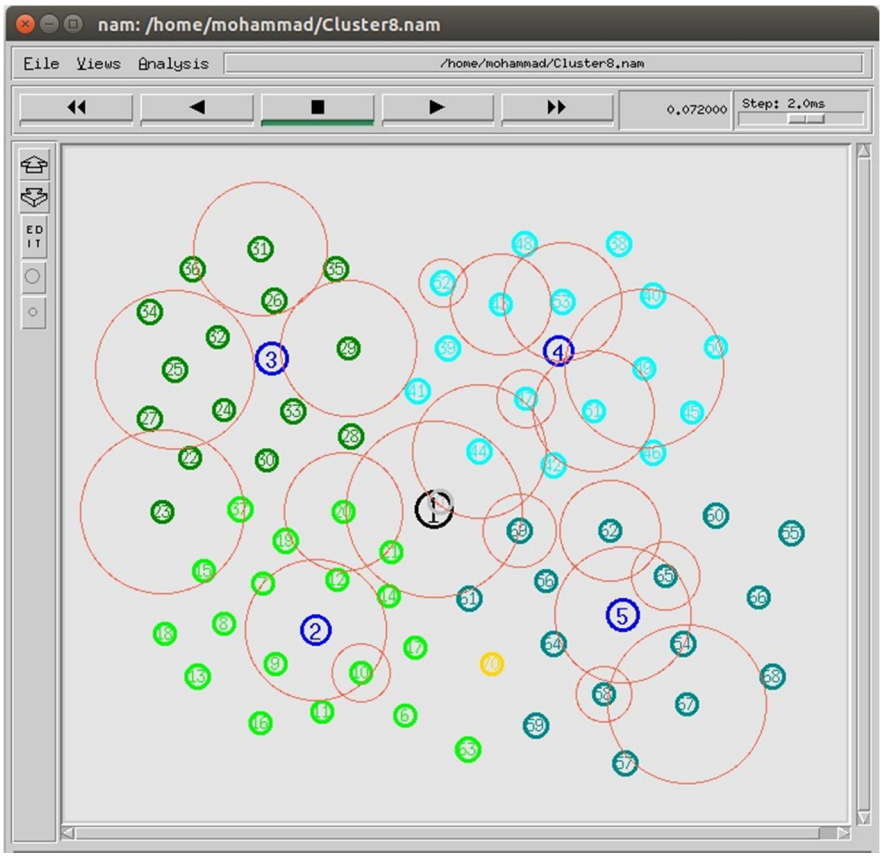
با توجه به توضیحات داده‌شده در بخش ۲-۱-۷ برای شبیه‌سازی شبکه‌های حسگر بی‌سیم و مدل ارائه‌شده، شبکه حسگر بی‌سیم خود را در شبیه‌ساز NS2 ایجاد کردیم. در این شبیه‌سازی، پارامترهای شبکه پایه خود را با توجه به ماهیت شبکه‌های حسگر بی‌سیم و نیازمندی‌های موجود و بررسی کاربردهای معمول در این شبکه‌ها تعیین کردیم [۳۶] [۹۸] [۹۹]. در این سناریو ما شبکه‌ای متشکل از ۲۰ تا ۱۰۰ گره در ۲ تا ۵ خوشه با وسعت $100 * 100\ m^2$، ارائه کرده‌ایم که با ترافیک CBR و

اندازه بسته‌های 70 byte در مدت‌زمان شبیه‌سازی 100 ثانیه تغذیه می‌گردد. در جدول (۵-۴) لیست پارامترها به‌صورت کامل همراه با مقادیر مربوطه ارائه‌شده است:

جدول (۵-۴): پارامترهای شبیه‌سازی شبکه حسگر بی‌سیم

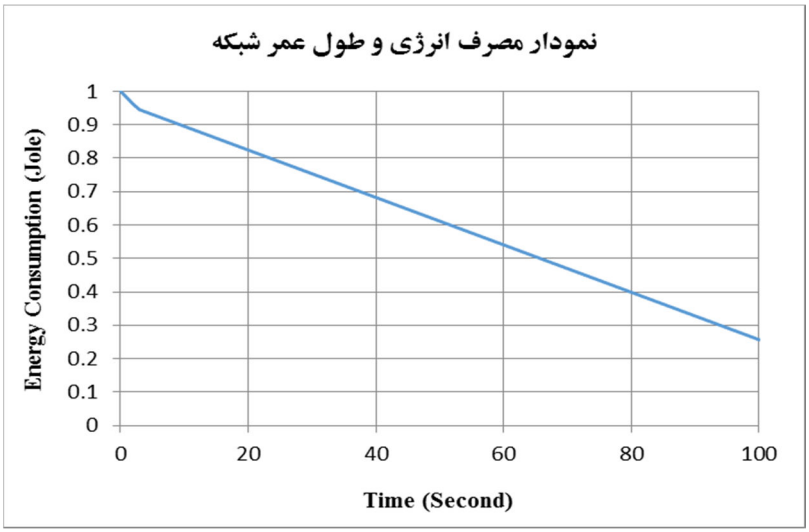
No	Parameters	Values
1	Number of nodes	20/40/60/80/100
2	Size of network	100 * 100 m^2
3	Routing protocol	AODV
4	MAC protocol	802.11
5	Link Layer protocol	LL
6	Type of traffic	CBR
7	Packet size	70 byte
8	Clustering method	Static / Dynamic (LEACH)
9	Number of Cluster	2 / 3 / 4 / 5
10	Antenna Model	Omni Antenna
11	Interface Queue Type	Drop Tail
12	Queue Length	50
13	Simulation Time	100 sec
14	Type of nodes	Mica2
15	Sensing Power	0.015 w
16	Processing Power	0.024 w
17	Sleep Power	0.0001 w
18	RX Power	0.024 w
19	TX Power	0.036 w
20	Energy Model	Battery
21	Initial Energy of nodes	1 Joule
22	Channel Type	Wireless Channel
23	Radio Propagation Model	Two Ray Ground
24	Antenna Model	Omni Antenna

شکل ۵-۳ که از نرم‌افزار NAM گرفته‌شده است، مربوط به شبیه‌سازی شبکه حسگر با پارامترهای جدول ۵-۴ است که در آن گره‌های آبی پررنگ نشان‌دهنده سرخوشه‌ها، گره مشکی‌رنگ معرف ایستگاه پایه هستند. همچنین به جهت نشان دادن گره‌های معمولی مربوط به هر خوشه از رنگ یکسان استفاده‌شده است.



شکل (۵-۳): نمای گرافیکی شبکه حسگر بی‌سیم تولیدشده با NAM

در شکل ۵-۴ و جدول ۵-۵ نتایج مصرف انرژی، میزان گذردهی، تأخیر ارسال، نرخ حذف بسته‌ها و نرخ ارسال ترافیک در شبکه منتج شده از شبیه‌سازی فوق و بدون در نظر گرفتن هیچ حمله‌ای ارائه‌شده است.



شکل (۵-۴): نمودار مصرف انرژی و طول عمر شبکه حسگر بی‌سیم

جدول (۵-۵): نتایج شبیه‌سازی شبکه حسگر بی‌سیم

Throughput (kbps)	Transfer Rate (Packet Delivery)	end to end delay (ms)	Normalized Routing Load	Traffic Rate (kbps)	Packet Drop Rate (PDR)
41.2878	99.66	26.16	0.365	41.427	25

۵-۶- شبیه‌سازی حملات لایه شبکه و مسیریابی

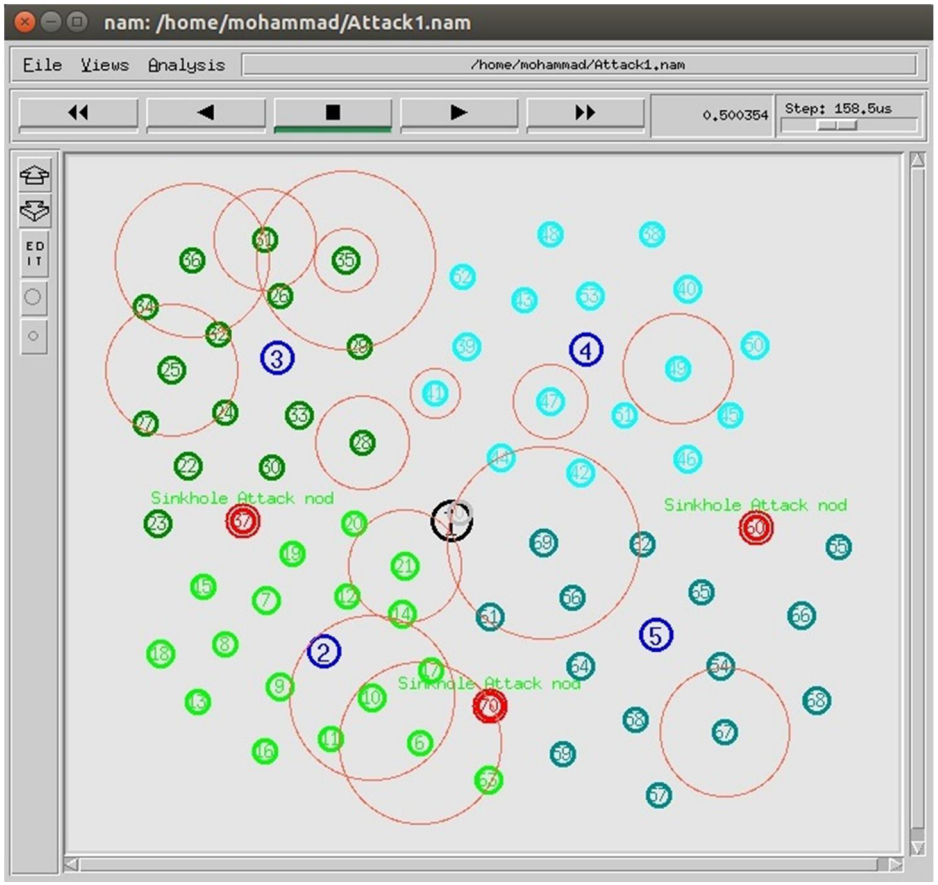
بعدازاین که ما در بخش قبل شبکه حسگر بی‌سیم مطلوب خود را همراه با پارامترهای کاملی طراحی کردیم، نوبت به شبیه‌سازی حملات مختلف رسیده است. این کار با توجه به توضیحات ارائه‌شده در بخش ۲-۲-۴ در مورد شبیه‌سازی حملات لایه شبکه و مسیریابی انجام‌شده است. به جهت شبیه‌سازی حملات در NS2 و اعمال رفتار و عملکرد آن‌ها در شبکه حسگر بی‌سیم مفروض، با ایجاد تغییراتی در پروتکل مسیریابی گره‌های مهاجم که در فایل‌های AODV.h و AODV.cc قرار دارند، عملکرد مربوط به آن‌ها را شبیه‌سازی نمودیم.

همان‌طور که در بخش‌های قبلی نیز بیان کردیم ما در شبیه‌سازی‌های خود فقط حملات لایه شبکه و فرایند مسیریابی را بررسی کردیم، چراکه مستعدترین حملات در شبکه‌های حسگر بی‌سیم هستند و این شبکه‌ها را دچار چالش می‌نمایند. جدول ۵-۶ پارامترهای مربوط به شبیه‌سازی حملات مفروض بر روی شبکه ایجادشده در بخش قبلی را ارائه می‌نماید:

جدول (۵-۶): پارامترهای شبیه‌سازی حملات لایه شبکه و مسیریابی

No	Parameters	Values
1	Type of attacker	Sinkhole/ flooding/ DOS/ select forwarding/ Sybil
2	Simulation Time	100 sec
3	Type of attacker nodes	Mica2
4	Initial Energy of Attackers	10
5	Number of Attacker	1 / 2 / 3
6	Attacker location	Random / manual
7	Transfer rate of packets	Between 0.01 to 0.1 sec

درنهایت در آزمایش‌های خود درصدی از گره‌های موجود در شبکه حسگر را به‌صورت تصادفی، به‌عنوان گره مهاجم در نظر گرفته‌ایم و عملکرد و کارایی شبکه حسگر را در حضور آن‌ها بررسی نموده‌ایم. بنابراین این مهاجمین که از انواع مختلف حملات می‌توانند باشند به طور همزمان نیز می‌توانند در شبکه فعالیت نمایند. شکل ۵-۵ که از نرم‌افزار NAM گرفته‌شده است، مربوط به شبیه‌سازی شبکه حسگر با پارامترهای جدول ۵-۴ در حضور گره‌های مهاجم در حمله حفره چاهک است که در آن گره‌های آبی‌رنگ نشان‌دهنده سرخوشه‌ها، گره مشکی‌رنگ معرف ایستگاه پایه و گره‌های قرمزرنگ نشان‌دهنده مهاجمین می‌باشند. همچنین به جهت نشان دادن گره‌های معمولی در هر خوشه از رنگ‌های یکسان استفاده‌شده است. ما در شبیه‌سازی‌ها برای توزیع گره‌های شبکه حسگر در محیط، هر دو روش توزیع تصادفی و توزیع دستی را ارائه و ارزیابی کردیم که شکل ۵-۵ نمونه‌ای از توزیع دستی است که به نسبت توزیع تصادفی دارای چگالی توزیع یکنواخت‌تری در محیط است.



شکل (۵-۵): نمای گرافیکی شبکه حسگر بی‌سیم تولیدشده با NAM در حضور حملات

۵–۶–۱– نتایج شبیه‌سازی‌ها و ارزیابی حملات

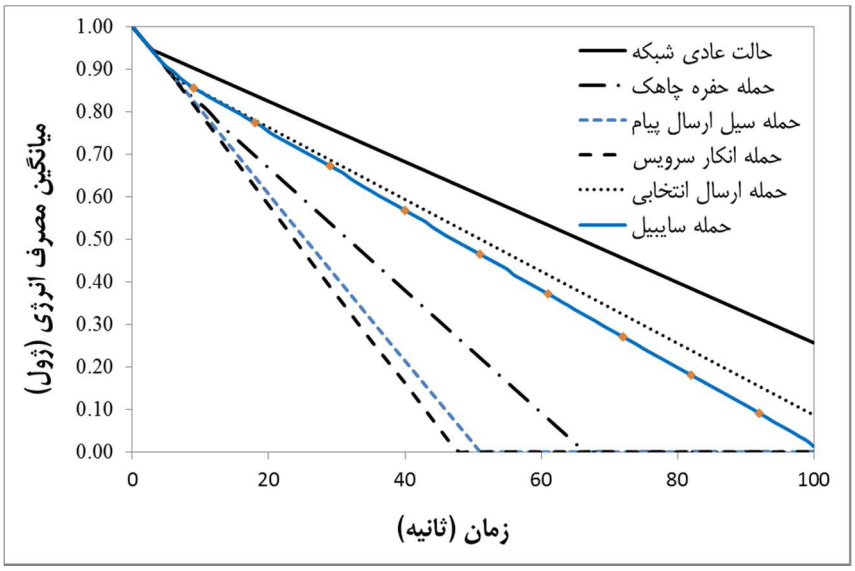
ما معیارهای ارزیابی بخش ۵-۳ را از طریق زبان AWK پیاده‌سازی کردیم و آن‌ها را بر روی فایل trace خروجی شبیه‌سازی اعمال نمودیم و بر اساس آن نتایج حاصله را ترسیم کرده‌ایم. جدول ۵-۷ و نمودارهای ۵-۶ تا ۵-۱۲ نتایج این شبیه‌سازی‌ها را نشان می‌دهند.

همان‌طور که در جدول ۵-۷ مشاهده می‌گردد، در حمله حفره چاهک، گره مخرب خود را به‌عنوان گلوگاه در برقراری ارتباط معرفی می‌کند و سپس اقدام به حذف بسته‌های شبکه کرده، که باعث کاهش چشمگیر گذردهی شبکه و نرخ تحویل بسته‌ها می‌گردد. در حمله سیل ارسال پیام، مهاجم با ارسال سیل‌آسای پیام‌ها در شبکه و ایجاد سربار بالایی در مسیریابی علاوه بر مختل کردن کار شبکه و کاهش چشمگیر گذردهی شبکه، به‌سرعت نیز باعث تحلیل انرژی گره‌ها در شبکه می‌گردد. به جهت بررسی دقیق‌تر نمودارهای مربوط به هر معیار ارزیابی در ادامه ارائه‌شده‌اند.

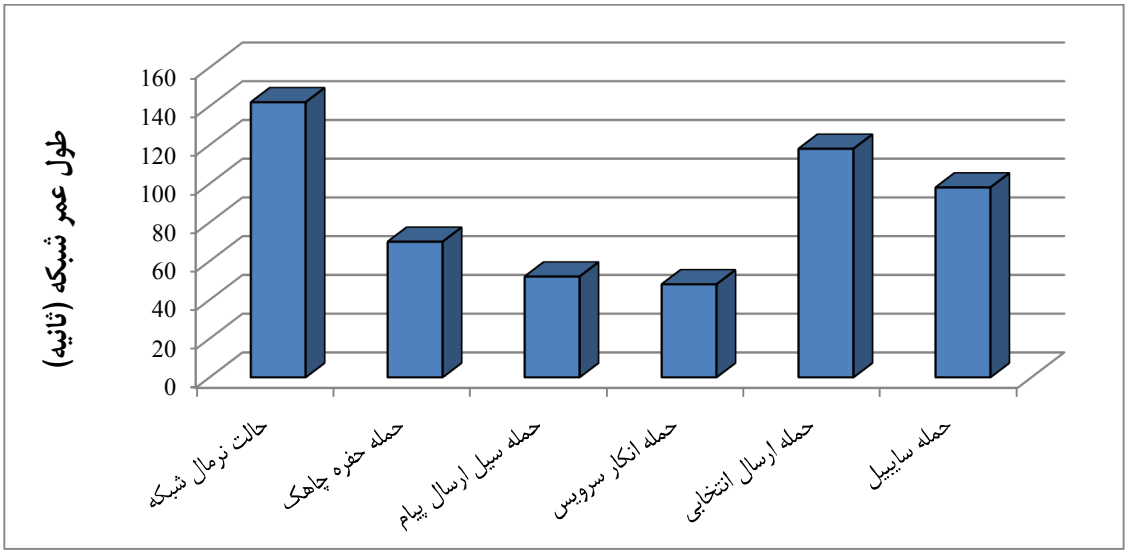
جدول (۵-۷): نتایج شبیه‌سازی شبکه حسگر بی‌سیم در حضور حملات مختلف

Attack type	Life Time	Flows	Packets Sent	Packets Received	Packets Dropped	End to End Delay (ms)			Packet Delivery		Throughput (Kbps)		Traffic Rate (Kbps)		Routing Load	Energy Consume	
						avg	min	max	total	flow	total	flow	total	flow		node	CH
Normal	150	69	7396	7371	25	0.026	0.002	3.268	99.66	99.64	41287	604	41427	606	0.365	0.756	9.789
Select Forwarding Attack	112	69	7396	6471	925	0.052	0.002	6.050	87.49	86.59	36249	530	41431	606	0.634	0.913	11.71
Sybil Attack	101	69	7395	7103	252	0.089	0.002	10.048	96.05	95.78	39806	582	41442	606	0.95	1.023	12.70
Sinkhole Attack	67	69	5236	2646	5078	0.137	0.002	5.962	50.53	48.65	14829	302	29343	609	1.578	1.438	13.01
Hello Flooding Attack	50	69	4292	1898	1152	2.143	0.002	28.193	44.22	32.58	10654	226	24091	611	36.285	1.936	14.47
DOS Attack	47	70	104108	7195	96725	4.503	0.002	35.689	6.91	76.3	40330	782	583560	8601	1.546	2.087	13.80

با توجه به نمودارهای ارائه‌شده در شکل‌های ۵-۶ و ۵-۷ به‌خوبی مشاهده می‌گردد که حملات مفروض شبکه را تحت تأثیر خود قرار داده و طول عمر شبکه را به‌شدت کاهش می‌دهند. همانطور که در شکل ۵-۷ مشاهده می‌گردد، در حمله رد سرویس مهاجم با ارسال پیام‌های فراوان به گره‌های شبکه عملا امکان سرویس‌دهی را از آن‌ها گرفته و به سرعت منابع و انرژی گره‌ها را مصرف می‌کند.



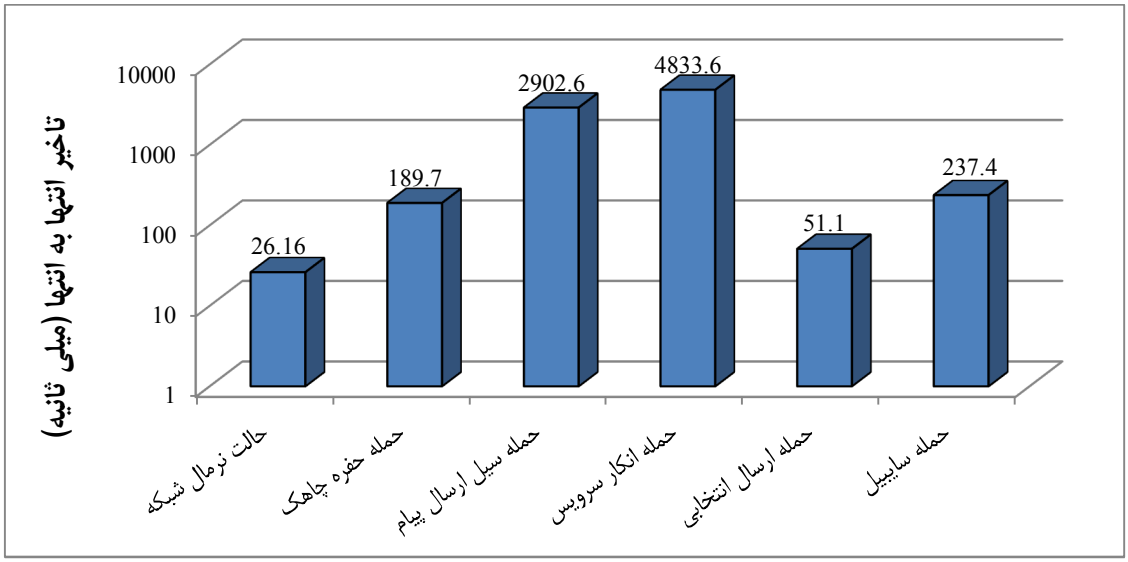
شکل (۵-۶): نمودار میانگین مصرف انرژی گره‌ها در شبکه حسگر بی‌سیم در حضور حملات مختلف



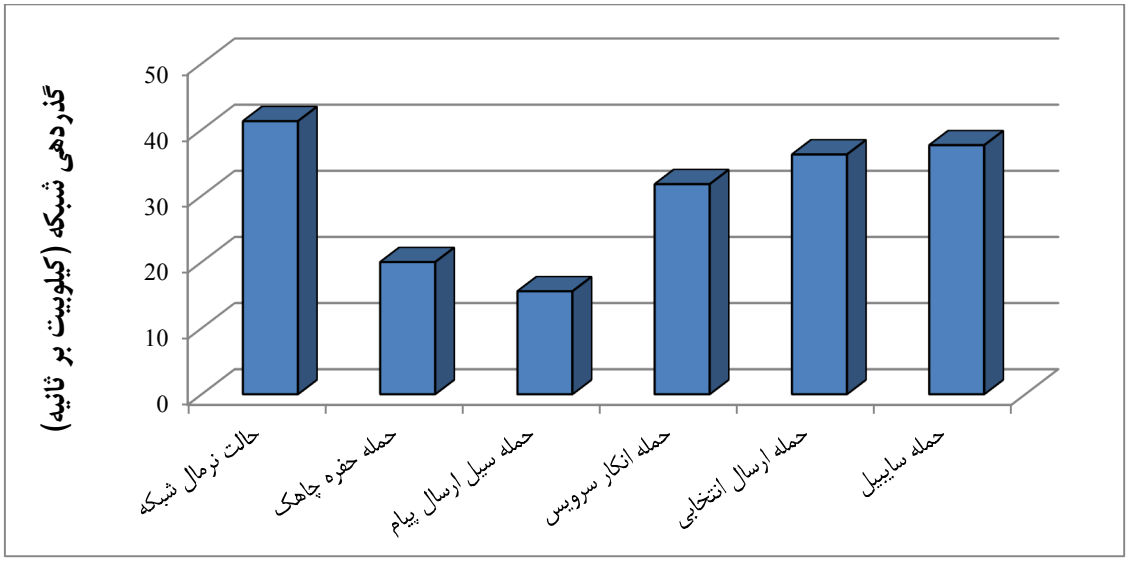
شکل (۵-۷): نمودار طول عمر شبکه

همان‌طور که در شکل ۵-۸ دیده می‌شود، یکی از اثرات مخرب حملات رد سرویس و سیل ارسال پیام، ایجاد تأخیر بسیار بالا در ارسال داده‌هاست که باعث کاهش چشمگیر کارائی شبکه می‌گردد.

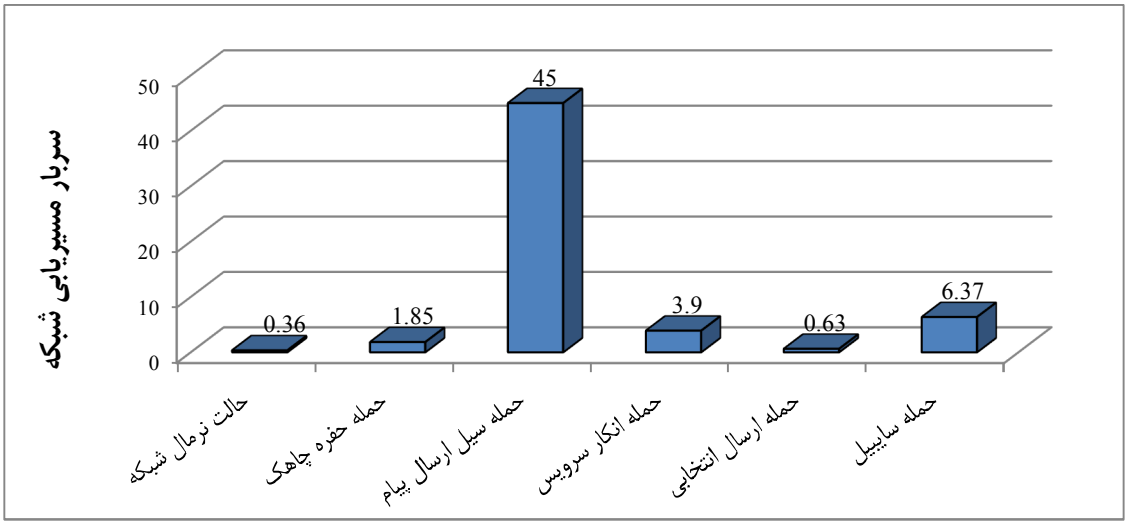
اثر حملات مختلف در میزان گذردهی نیز در شکل ۵-۹ دیده می‌شود، حمله سیل ارسال با افزایش شدید سربار مسیریابی باعث می‌گردد ارسال داده‌ها در گره‌ها به تعویق بیفتد و به همین دلیل کاهش چشمگیری در گذردهی شبکه رخ می‌دهد. در حمله حفره‌چاهک نیز با توجه به این‌که حجم بالای ترافیک ارسال‌شده از سوی گره‌ها به گره مهاجم بدون گذر از آن حذف می‌شوند بنابراین میزان گذردهی در شبکه به‌شدت افت پیدا می‌نماید.



شکل (۵-۸): نمودار تأخیر ارسال انتها به انتها



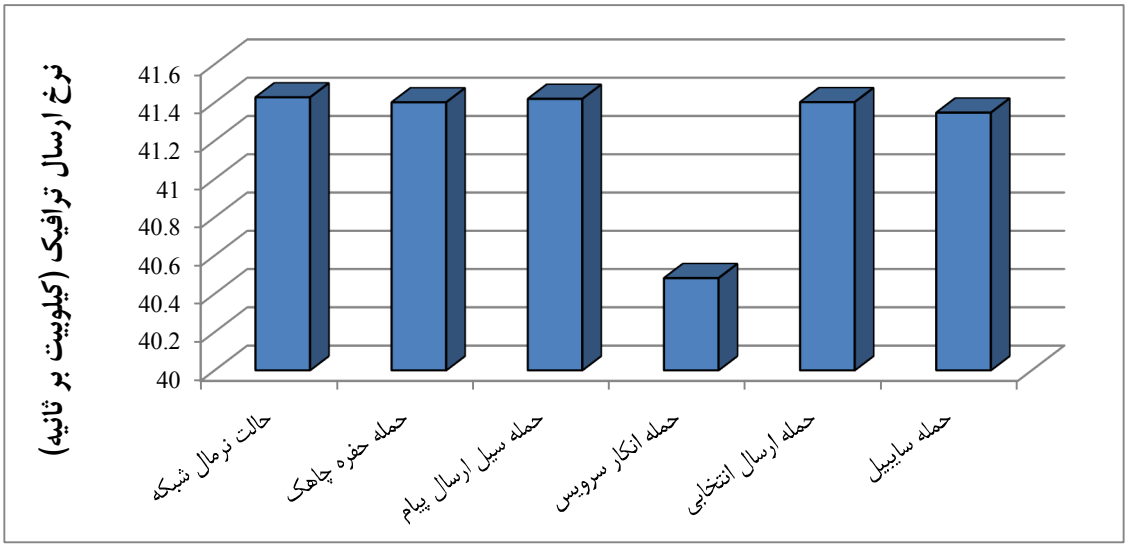
شکل (۵-۹): نمودار میزان گذردهی شبکه



شکل (۵-۱۰): نمودار میزان سربار مسیریابی

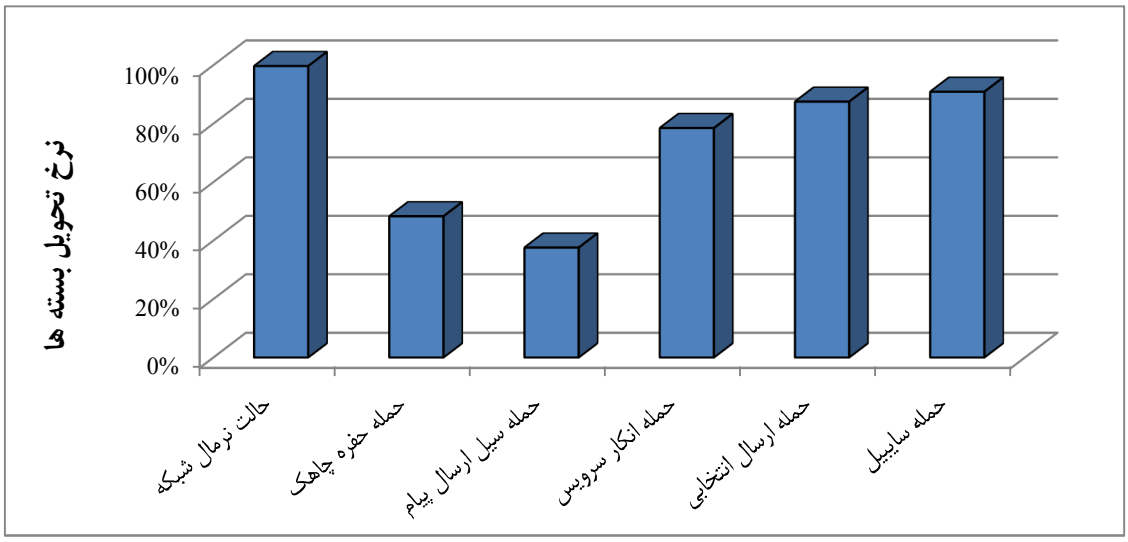
یکی از اثرات مخرب حمله سیل ارسال در مقایسه با سایر حملات ایجاد پیام‌های فراوان ارتباطی به گره‌های دیگر است که باعث می‌گردد به‌شدت سربار مسیریابی در شبکه افزایش یابد که این امر در شکل ۵-۱۰ دیده می‌شود. این امر باعث کاهش چشمگیر کارائی در شبکه می‌گردد.

در شکل ۵-۱۱ نرخ ترافیک به نمایش درآمده است که در آن نرخ ترافیک حمله رد سرویس با اختلاف کمی نسبت به سایر حملات دیده می‌شود. دلیل این امر نیز این است که حمله رد سرویس با تزریق تعداد بسیار زیادی بسته‌های داده عملاً نرخ ارسال بسته‌های داده واقعی شبکه را با مشکل مواجهه کرده و نرخ ترافیک را کاهش می‌دهد.



شکل (۵-۱۱): نمودار نرخ ترافیک

حمله سیل ارسال پیام با افزایش شدید سربار مسیریابی باعث می‌گردد ارسال داده‌ها در گره‌ها به تعویق بیفتد و همچنین حمله حفره‌چاهک نیز با حذف گسترده بسته‌های داده در بین مسیر عملاً باعث کاهش چشمگیر نرخ تحویل بسته‌ها می‌شود که این امر در شکل ۵-۱۲ مشاهده می‌شود.



شکل (۵-۱۲): نمودار نرخ تحویل بسته‌ها

۵-۷- شبیه‌سازی سیستم تشخیص نفوذ پیشنهادی

بعد از شبیه‌سازی شبکه حسگر بی‌سیم در بخش ۵-۵ و همچنین شبیه‌سازی حملات لایه شبکه و مسیریابی روی آن در بخش ۵-۶، در این مرحله نوبت به شبیه‌سازی سیستم تشخیص نفوذ پیشنهادی می‌رسد. با توجه به توضیحات گفته‌شده در بخش ۲-۳-۵ در مورد شبیه‌سازی سیستم‌های تشخیص نفوذ ما در ادامه شبیه‌سازی سیستم تشخیص نفوذ پیشنهادی را با پارامترهای جدول ۵-۸ انجام دادیم و نتایج حاصل از آن را در سطوح مختلف در بخش‌های بعدی ارائه می‌نماییم.

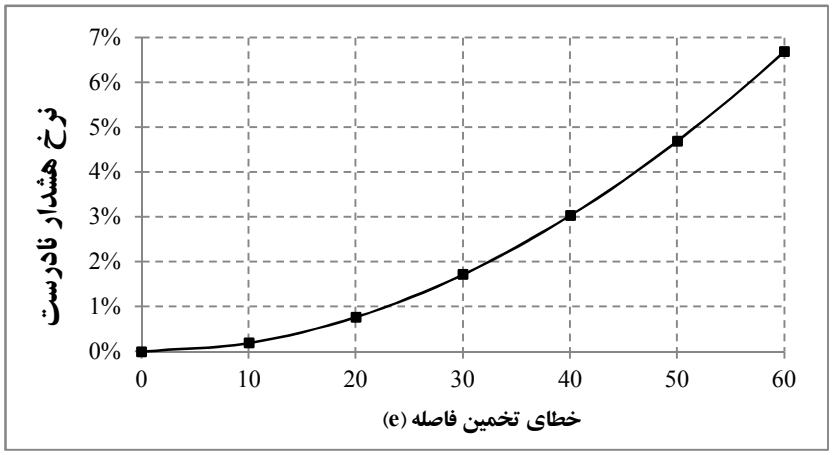
جدول (۵-۸): حدود آستانه مربوط به تشخیص حملات مختلف

No	Parameters	Values
1	$Treshold_{RSSI}$ of All attacker	7.2E-07
2	$Treshold_{IRP}$ of DoS attack	0.15
3	$Treshold_{PDR}$ of Sinkhole attack	0.5
4	$Treshold_{PDR}$ of Selectforward attack	0.12
5	$Treshold_{RMI}$ of HelloFlood attack	0.15

۵–۷–۱– نتایج تشخیص نفوذ پیشنهادی سطح پایین (گره‌های عادی)

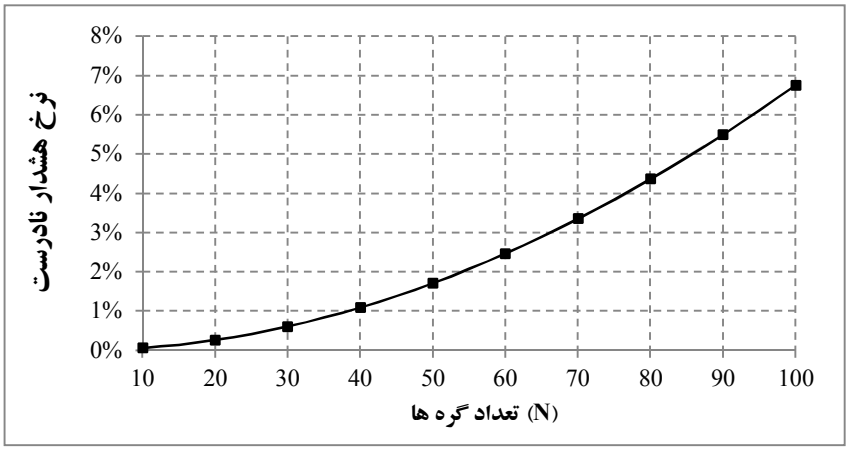
در ابتدا ما برای هر حمله به‌صورت جداگانه یک سیستم تشخیص نفوذ ارائه کرده و شبیه‌سازی را انجام داده و نتایج را استخراج کردیم. سپس یک سیستم تشخیص نفوذ یکپارچه برای همه حملات مفروض ارائه نمودیم. برای نمونه ما در زیر تشریح نتایج مربوط به حملات سایبیل را ارائه کردیم.

- شبیه‌سازی و تشریح نتایج سیستم تشخیص نفوذ حملات سایبیل: شکل ۵-۱۳، نرخ هشدار نادرست را به‌صورت تابعی از خطای تخمین فاصله گره‌ها نشان داده است. در این سناریو مساحت شبکه $E=10km^2$ و تعداد گره‌های شبکه N=50 در نظر گرفته‌شده است.



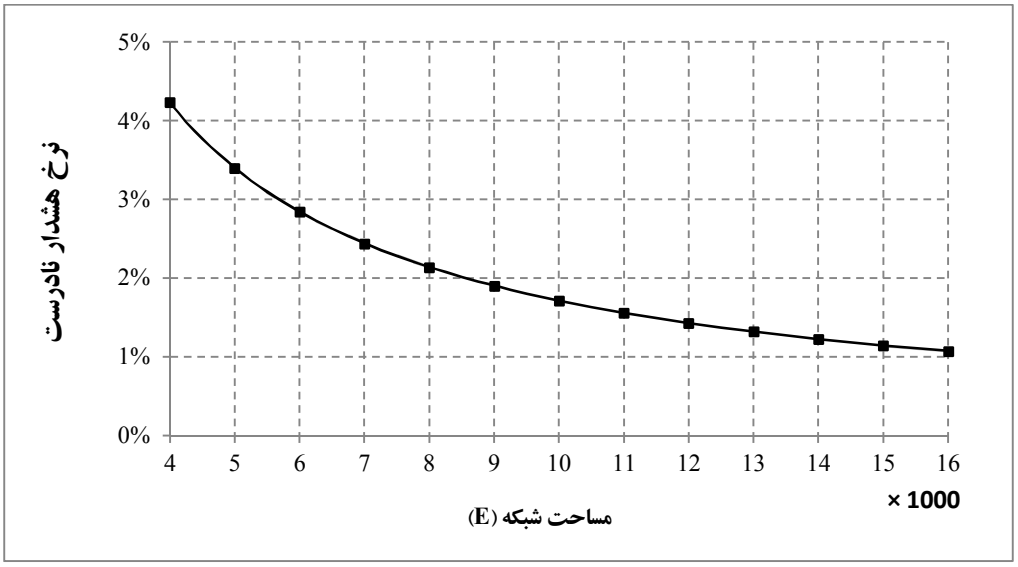
شکل (۵-۱۳): نرخ هشدار نادرست بر اساس تابعی از خطای تخمین فاصله

شکل ۵-۱۴، نرخ هشدار نادرست را به‌صورت تابعی از تعداد گره‌ها نشان می‌دهد. در این سناریو مساحت شبکه برابر با $E=10km^2$ و میانگین خطای تخمین فاصله e=30 cm در نظر گرفته‌شده است.



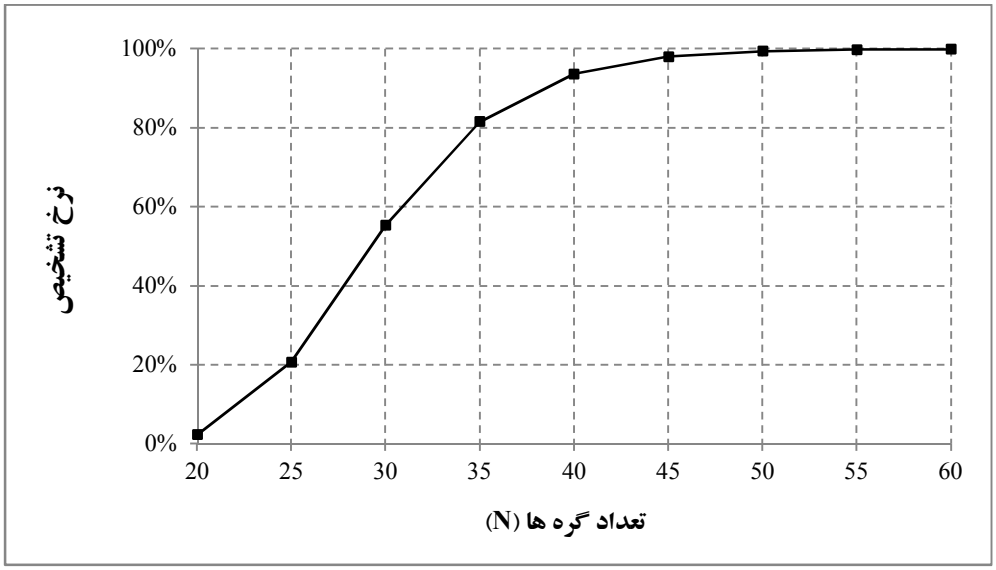
شکل (۵-۱۴): نرخ هشدار نادرست به‌صورت تابعی از تعداد گره‌ها

شکل ۵-۱۵، نرخ هشدار نادرست را به‌صورت تابعی از مساحت شبکه حسگر نشان می‌دهد. در این سناریو تعداد گره‌های شبکه N=50 و میانگین خطای تخمین فاصله e=30 cm در نظر گرفته‌شده است.



شکل (۵-۱۵): نرخ هشدار نادرست بر اساس تابعی از مساحت شبکه

همچنین در شکل ۵-۱۶، نرخ تشخیص را به‌صورت تابعی از تعداد گره‌ها نشان می‌دهد که مهم‌ترین پارامتر در تشخیص حمله سایبیل است. در این سناریو مساحت شبکه برابر با $E=10km^2$ و میانگین خطای تخمین فاصله e=30 cm در نظر گرفته‌شده است.



شکل (۵-۱۶): نرخ تشخیص به‌صورت تابعی از تعداد گره‌ها

به جهت ارزیابی و مقایسه سیستم تشخیص نفوذ پیشنهادی پارامترهای آن را به‌صورت زیر در نظر گرفتیم که با توجه به نتایج شکل‌های ۵-۱۳ تا ۵-۱۶ بهترین تنظیم برای سیستم پیشنهادی است.

- مساحت شبکه برابر با $E=10\ km^2$
- میانگین خطای تخمین فاصله $e=30\ cm$
- تعداد گره‌های شبکه $N=50$

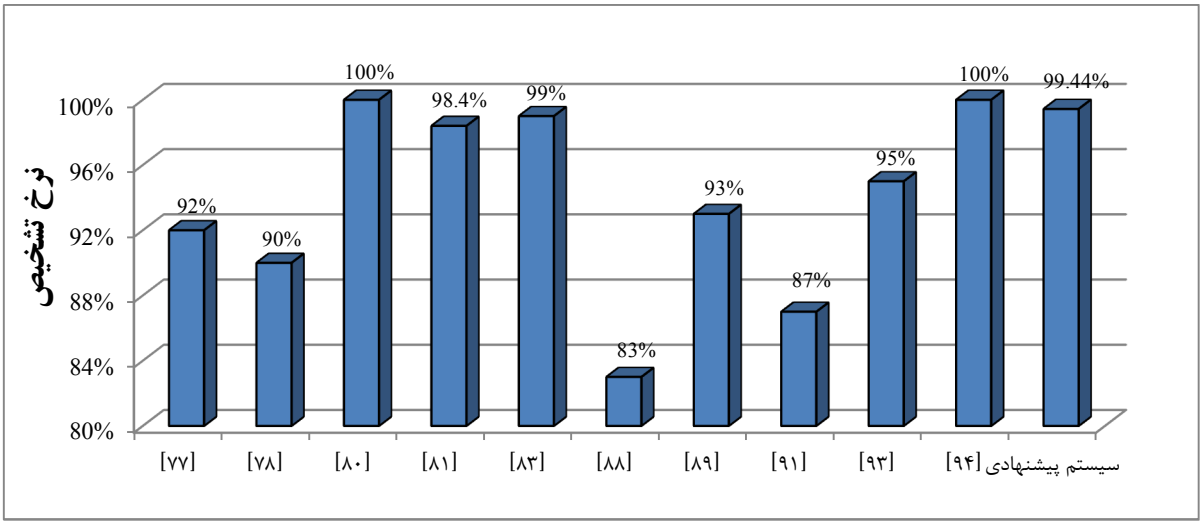
همچنین به جهت مقایسه مناسب روش پیشنهادی با کارهای موجود، از بستر یکسانی برای شبیه‌سازی همه روش‌ها استفاده کردیم که پارامترهای آن در جداول ۵-۴، ۵-۶ و ۵-۸ ارائه‌شده است.

با توجه به نتایج ارائه‌شده در شکل‌های ۵-۱۷ تا ۵-۱۹، سیستم پیشنهادی با نرخ تشخیص بالای ۹۹/۴۴٪ و نرخ هشدار نادرست پایین ۱/۷٪ و همچنین میانگین مصرف انرژی کم ۰/۷۴۱ ژول، به‌عنوان یک روش مؤثر و سبک، مطرح است.

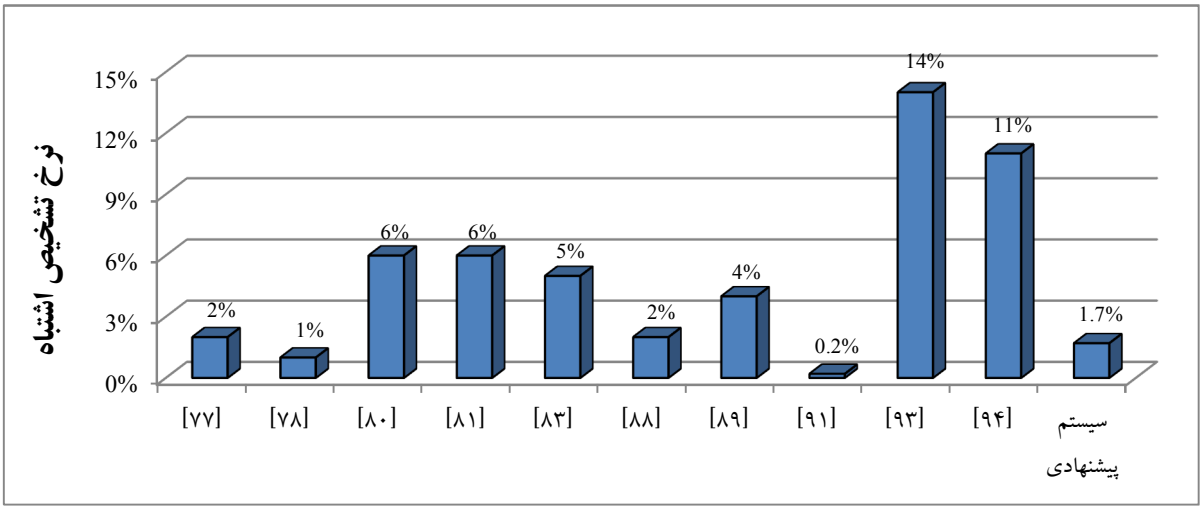
همان‌طور که در شکل ۵-۱۷ مشاهده می‌شود روش‌های مراجع [۸۰] و [۹۴] با نرخ تشخیص ۱۰۰٪ با اختلاف ناچیز، بهتر از روش پیشنهادی هستند، اما با توجه به نرخ هشدار نادرست ۶٪ روش [۸۰] و انرژی مصرفی بالای آن و همچنین نرخ هشدار نادرست بالای ۱۱٪ روش [۹۴]، سیستم پیشنهادی شرایط مطلوب‌تری را ارائه می‌نماید.

با توجه به شکل ۵-۱۸، نرخ هشدار نادرست در روش‌های [۹۱] و [۷۸] کمی بهتر از روش پیشنهادی هستند، اما به جهت نرخ تشخیص پایین ۸۷٪ و ۹۰٪ در آن‌ها، سیستم پیشنهادی مناسب‌تر از آن‌ها می‌باشد.

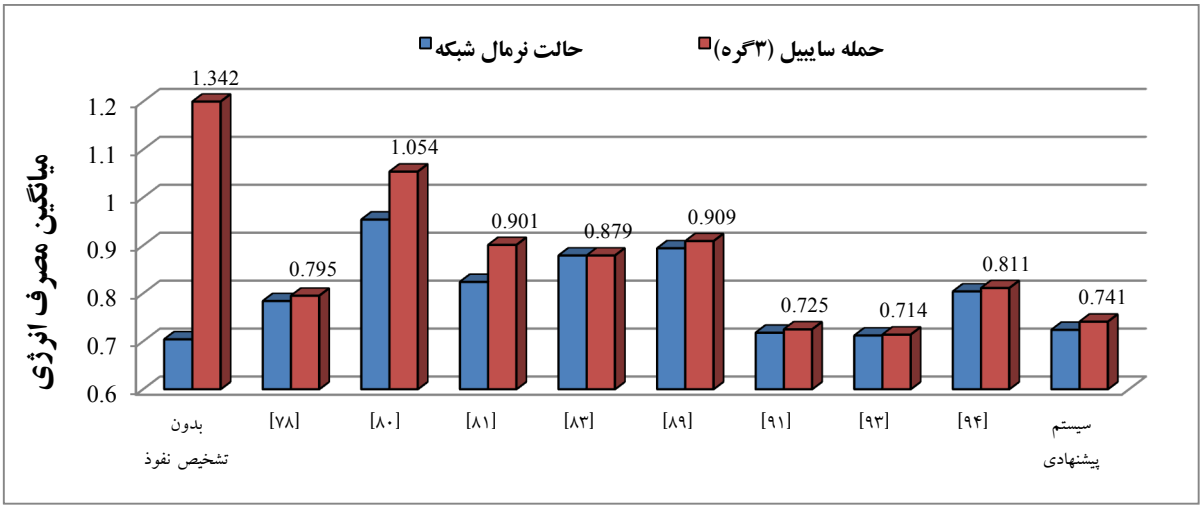
ازلحاظ مصرف انرژی نیز با توجه به شکل ۵-۱۹، روش‌های مراجع [۹۱] و [۹۳]، از روش پیشنهادی سبک‌وزن‌تر هستند اما به جهت نرخ تشخیص پایین ۸۷٪ روش [۹۱] و همچنین نرخ تشخیص ۹۵٪ و نرخ بسیار بالای هشدار نادرست ۱۴٪ در روش [۹۳]، سیستم پیشنهادی شرایط مطلوب‌تری را ارائه می‌نماید.



شکل (۵-۱۷): نرخ تشخیص سیستم پیشنهادی در مقایسه با مراجع دیگر



شکل (۵-۱۸): نرخ تشخیص نادرست سیستم پیشنهادی در مقایسه با مراجع دیگر

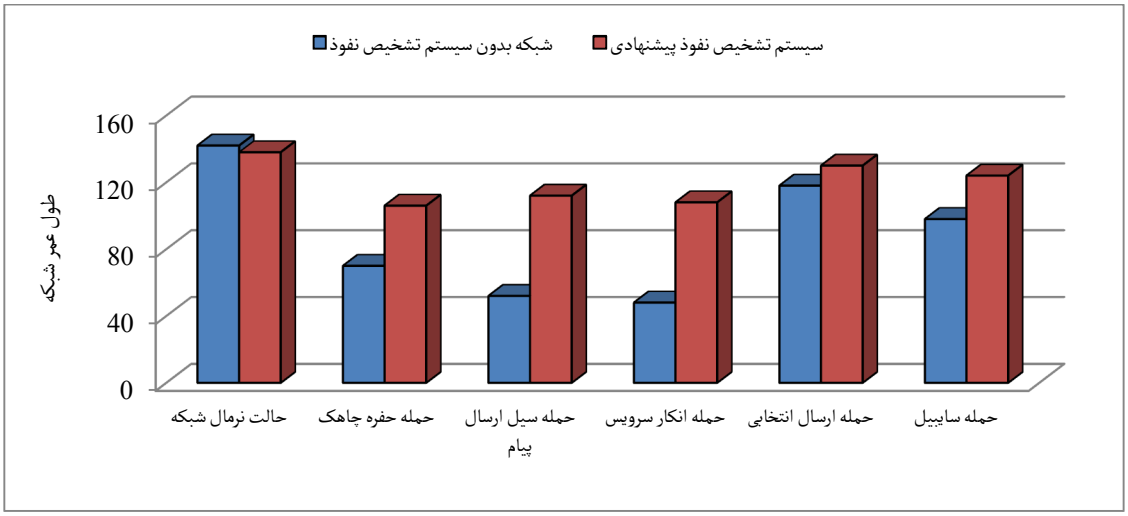


شکل (۵-۱۹): میانگین مصرفی انرژی سیستم پیشنهادی در مقایسه با مراجع دیگر

- **شبیه‌سازی و تشریح نتایج سیستم تشخیص نفوذ یکپارچه برای همه حملات**

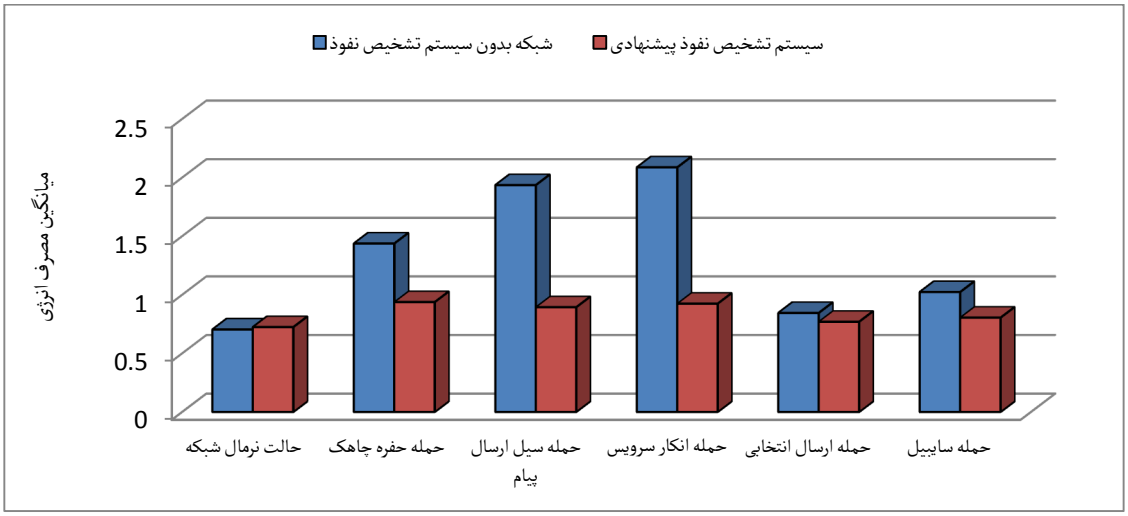
در شکل‌های ۵-۲۰ تا ۵-۲۷ سیستم تشخیص پیشنهادی بر اساس معیارهای مختلف کارائی (ارائه‌شده در بخش ۵-۳) در شبکه‌های حسگر، به تفکیک حملات مورد ارزیابی قرارگرفته است.

ارزیابی طول عمر شبکه	حالت عادی شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله سایبیل
شبکه بدون سیستم تشخیص نفوذ	142	70	52	48	118	98
سیستم تشخیص نفوذ پیشنهادی	138	106	112	108	130	124



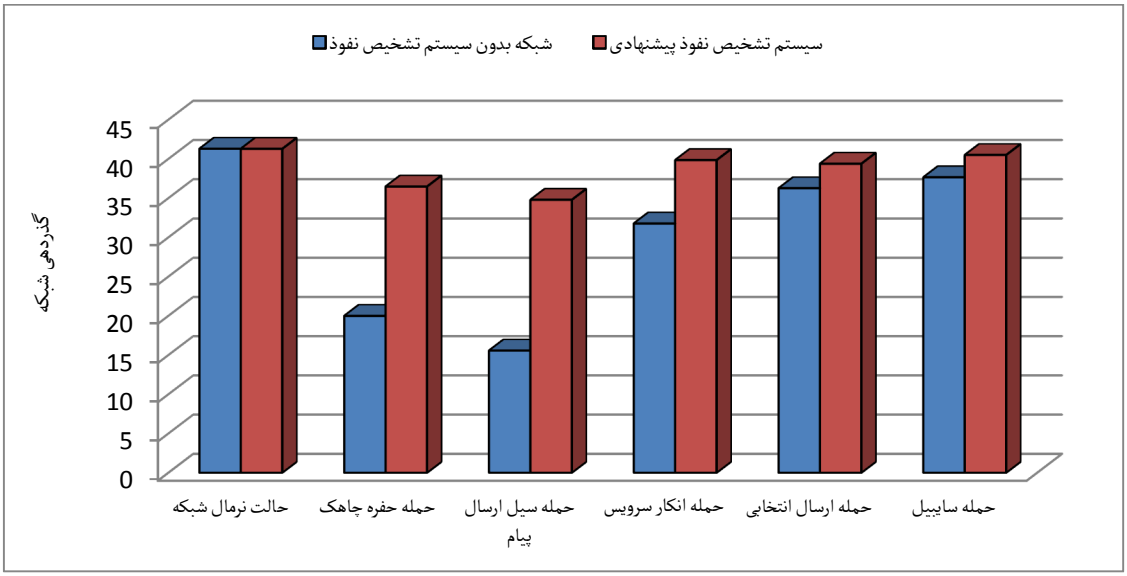
شکل (۵-۲۰): طول عمر شبکه در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی میانگین مصرف انرژی	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله سایبیل
شبکه بدون سیستم تشخیص نفوذ	0.7042	1.4377	1.9358	2.0871	0.8451	1.0234
سیستم تشخیص نفوذ پیشنهادی	0.7242	0.9377	0.8936	0.9242	0.7698	0.8049



شکل (۵-۲۱): میانگین مصرف انرژی در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی گذردهی شبکه	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله ساییبل
شبکه بدون سیستم تشخیص نفوذ	41.287	19.9844	15.5641	31.76	36.25	37.65
سیستم تشخیص نفوذ پیشنهادی	41.272	36.47	34.78	39.84	39.38	40.49

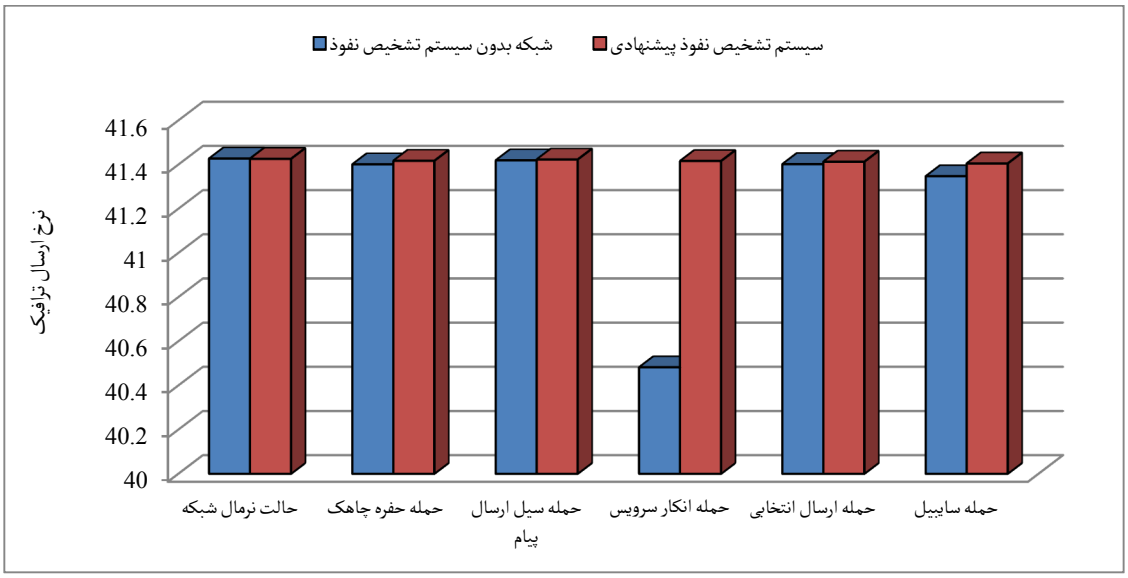


شکل (۵-۲۲): گذردهی شبکه در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی نرخ تحویل بسته‌ها	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله ساییبل
شبکه بدون سیستم تشخیص نفوذ	99.66%	48.28%	37.58%	78.46%	87.49%	90.89%
سیستم تشخیص نفوذ پیشنهادی	99.54%	88.11%	83.98%	96.84%	95.04%	97.64%

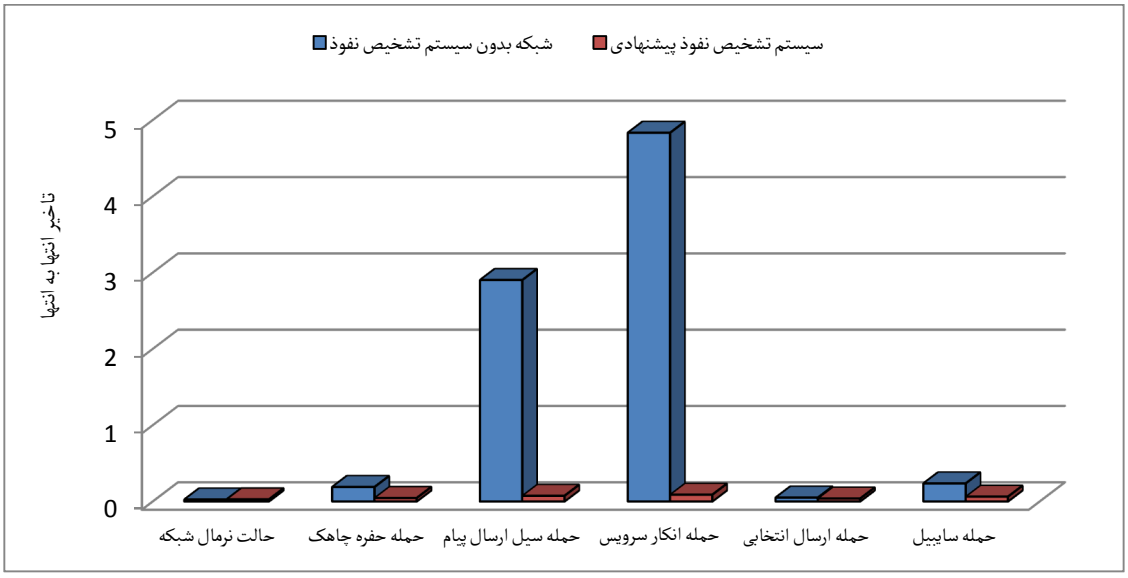
شکل (۵-۲۳): نرخ تحویل بسته‌ها در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی نرخ ارسال ترافیک	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله ساییبل
شبکه بدون سیستم تشخیص نفوذ	41.427	41.401	41.419	40.482	41.402	41.347
سیستم تشخیص نفوذ پیشنهادی	41.426	41.417	41.423	41.416	41.413	41.405



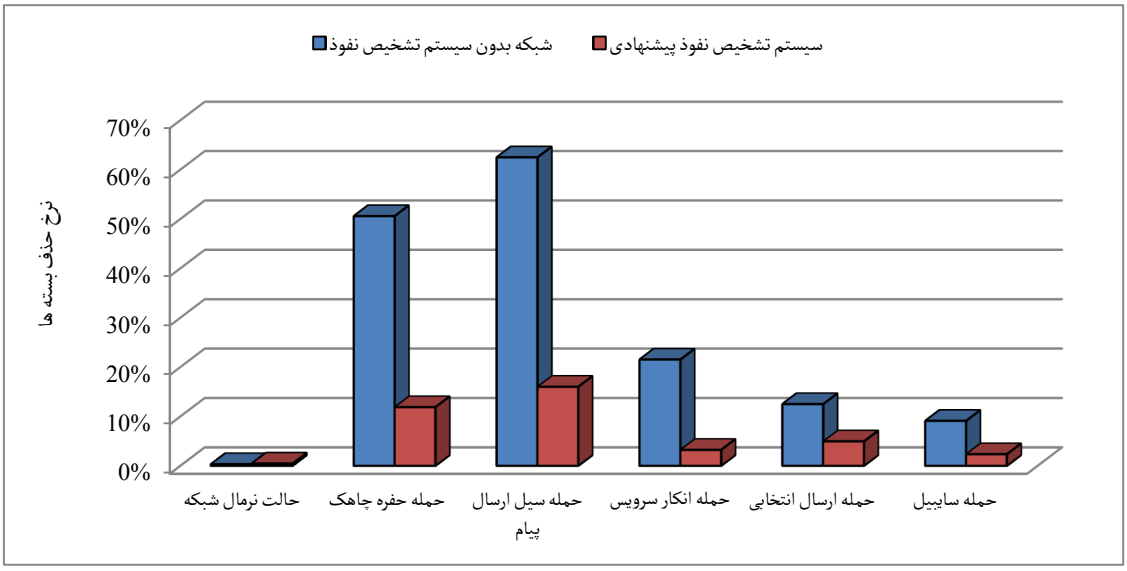
شکل (۵-۲۴): نرخ ارسال ترافیک در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی تأخیر انتها به انتها	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله ساییبل
شبکه بدون سیستم تشخیص نفوذ	0.0261	0.1897	2.9026	4.833	0.0511	0.237
سیستم تشخیص نفوذ پیشنهادی	0.0273	0.0459	0.0745	0.0892	0.0382	0.063



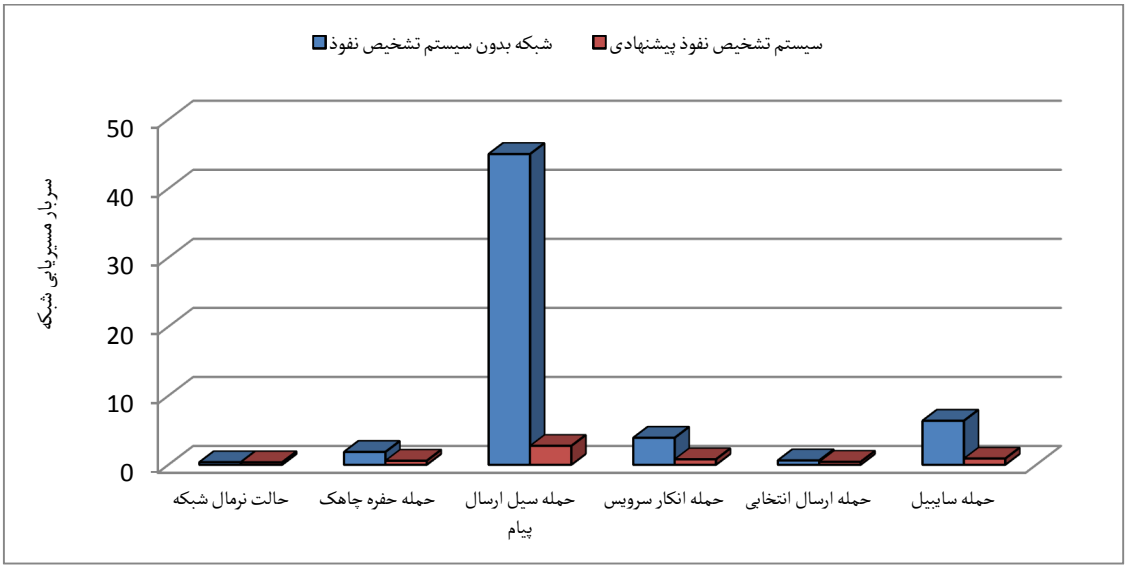
شکل (۵-۲۵): تأخیر انتها به انتها در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی نرخ حذف بسته‌ها	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله سایبیل
شبکه بدون سیستم تشخیص نفوذ	0.34%	50.59%	62.49%	21.53%	12.51%	9.11%
سیستم تشخیص نفوذ پیشنهادی	0.46%	11.89%	16.02%	3.24%	4.96%	2.36%



شکل (۵-۲۶): نرخ حذف بسته‌ها در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

ارزیابی سربار مسیریابی شبکه	حالت نرمال شبکه	حمله حفره چاهک	حمله سیل ارسال پیام	حمله رد سرویس	حمله ارسال انتخابی	حمله سایبیل
شبکه بدون سیستم تشخیص نفوذ	0.36	1.85	45	3.9	0.63	6.37
سیستم تشخیص نفوذ پیشنهادی	0.35	0.58	2.73	0.79	0.42	0.89

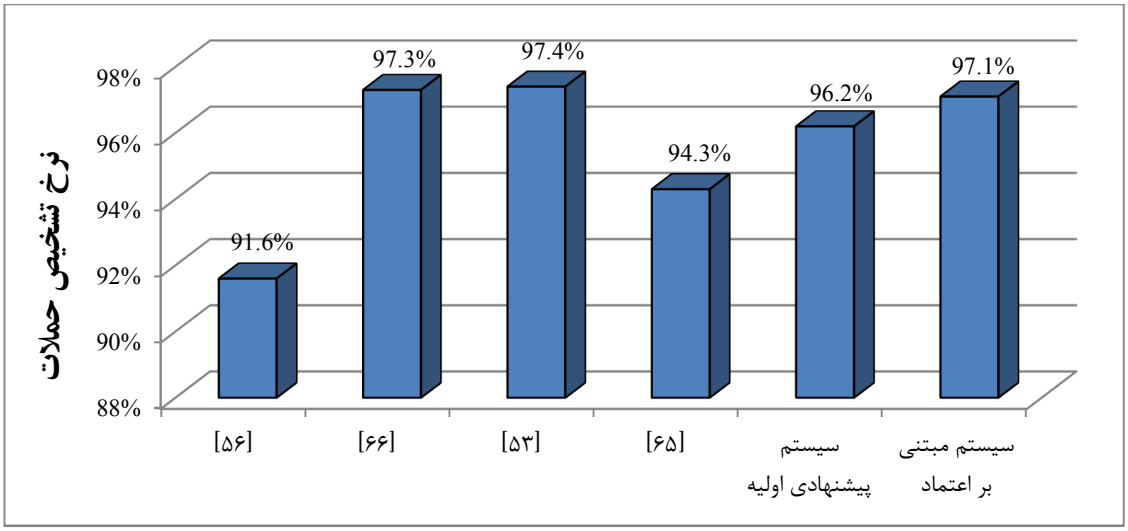


شکل (۵-۲۷): سربار مسیریابی شبکه در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه

با توجه به شکل‌ها و با مقایسه حالات شبکه در حضور و عدم حضور سیستم تشخیص نفوذ پیشنهادی، مشاهده می‌گردد که حملات مختلف کارایی شبکه را به‌شدت تنزل می‌دهند و با به‌کارگیری تشخیص نفوذ پیشنهادی به‌خوبی می‌توان کارائی و عملکرد شبکه را در حد مطلوب حفظ کرد.

جدول ۵-۹ نیز نرخ تشخیص و همچنین نرخ هشدار نادرست را در سیستم تشخیص نفوذ پیشنهادی اولیه و تشخیص نفوذ اصلاح‌شده بر اساس سطح اعتماد را در مقایسه با کارهای موجود، به تفکیک حملات مختلف نشان می‌دهد.

تحلیل نرخ تشخیص: همان‌طور که در شکل ۵-۲۸ و ۵-۲۹ مشاهده می‌شود، نرخ تشخیص و نرخ هشدار نادرست در سیستم پیشنهادی با اصلاح انجام‌شده بر اساس سطح اعتماد بهبودیافته است.

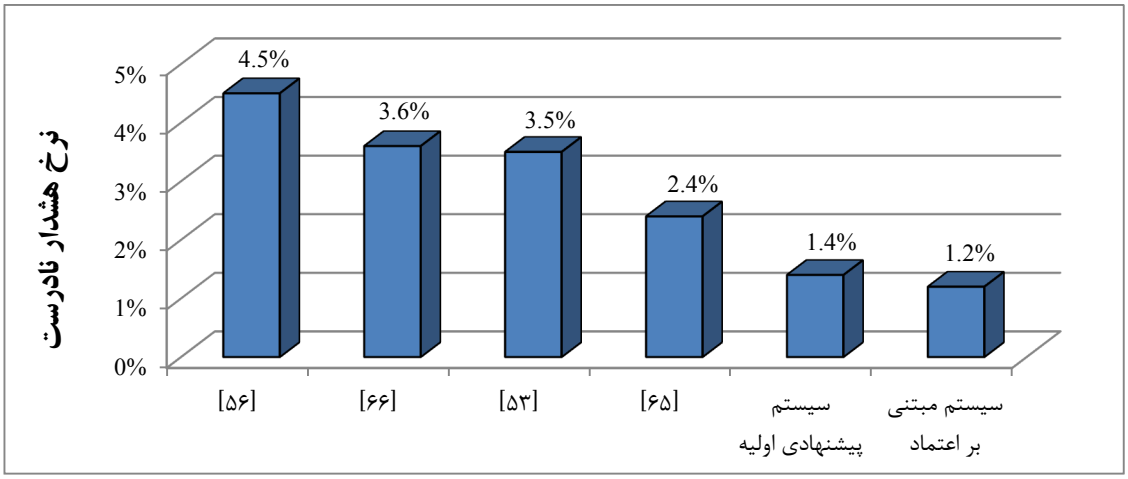


شکل (۵-۲۸): نمودار نرخ تشخیص حملات

همان‌طور که در شکل ۵-۲۸ مشاهده می‌گردد، نرخ تشخیص سیستم پیشنهادی با میانگین ۹۷/۱٪ با اختلاف کمی بعد از [۵۳] و [۶۶] قرار دارد. اما با توجه به نرخ هشدار نادرست خیلی پایین ۱/۲٪ روش پیشنهادی به نسبت مراجع دیگر که در شکل ۵-۲۹ ارائه‌شده و همچنین میانگین مصرف انرژی کمتر نسبت به کارهای موجود در شکل ۵-۳۱، سیستم پیشنهادی شرایط مطلوب‌تری را ارائه می‌کند.

جدول (۵-۹): مقایسه سیستم تشخیص نفوذ پیشنهادی با کارهای موجود به تفکیک حملات مختلف

نوع حمله	سیستم پیشنهادی اولیه		سیستم مبتنی بر اعتماد		OWIDS [56]		GHIDS [66]		KBIDS [53]		ECOC [65]	
	نرخ تشخیص	هشدار نادرست	نرخ تشخیص	هشدار نادرست	نرخ تشخیص	هشدار نادرست	نرخ تشخیص	هشدار نادرست	نرخ تشخیص	هشدار نادرست	نرخ تشخیص	هشدار نادرست
حمله رد سرویس	٪۹۵/۶	٪۱/۲	٪۹۶/۱	٪۰/۹۴	---	---	---	---	٪۹۶/۲	٪۳/۷	٪۹۵/۲	٪۱/۴
حمله سیل ارسال پیام	٪۹۷/۵	٪۰/۹	٪۹۸/۲	٪۰/۸۶	٪۹۲/۷	٪۳/۴	٪۹۷/۲	٪۲/۲	٪۹۸/۴	٪۴/۳	٪۹۶/۲	٪۱/۷
حمله حفره چاهک	٪۹۴/۷	٪۱/۱	٪۹۵/۸	٪۱/۰۳	٪۹۳/۴	٪۴/۷	٪۹۶/۳	٪۳/۵	٪۹۷/۶	٪۲/۶	٪۹۶/۱	٪۱/۲
حمله ارسال انتخابی	٪۹۳/۸	٪۲/۳	٪۹۵/۷	٪۱/۸	٪۸۸/۹	٪۵/۶	٪۹۸/۴	٪۵/۱	---	---	٪۹۱/۱	٪۳/۴
حمله سایبیل	٪۹۹/۴	٪۱/۷	٪۹۹/۶	٪۱/۵	٪۹۱/۳	٪۴/۳	---	---	---	---	٪۹۲/۷	٪۴/۳
میانگین کل	**٪۹۶/۲**	**٪۱/۴**	**٪۹۷/۱**	**٪۱/۲**	**٪۹۱/۶**	**٪۴/۵**	**٪۹۷/۳**	**٪۳/۶**	**٪۹۷/۴**	**٪۳/۵**	**٪۹۴/۳**	**٪۲/۴**



شکل (۵-۲۹): نمودار نرخ هشدار نادرست

تحلیل مصرف انرژی: در بحث تحلیل انرژی ابتدا باید بخش‌های مختلفی که در مصرف انرژی سیستم تشخیص نفوذ پیشنهادی دخیل هستند مشخص شوند. مشخصاً یک سیستم تشخیص نفوذ در دو بخش پردازش و انتقال پیام‌ها انرژی مصرف می‌کند. در بخش پردازش الگوریتم تشخیص نفوذ با توجه به سبک بودن الگوریتم ارائه‌شده به دلیل استفاده از یک روش مبتنی بر قانون ساده، مصرف انرژی بسیار ناچیز و قابل‌چشم‌پوشی است. در بخش انتقال پیام‌ها که مهم‌ترین بخش در مصرف انرژی است، سه عملیات ارسال، دریافت و شنود پیام‌ها هستند که دو عملیات اول آن یعنی ارسال و دریافت پیام‌ها مربوط به عملکرد عادی شبکه حسگر بی‌سیم بوده و تنها عملیات شنود پیام‌ها مربوط به عملکرد سیستم تشخیص نفوذ می‌باشد. با توجه به این‌که عملیات شنود نیز در هر گره صرفاً به بررسی اطلاعات ابتدایی سرآیند بسته‌های دریافتی می‌پردازد تا مشخص کند که گره‌های همسایه‌اش پیام‌های ارسالی آن را انتقال می‌دهند، بنابراین حداقل انرژی در این عملیات مصرف خواهد شد. رابطه محاسبه انرژی برای انتقال پیام‌ها در زیر ارائه‌شده است:

$$\underset{Consump.}{Energy}(Q) = \frac{Power * Elec.Current * Packet\ Size}{Bandwidth} \qquad (۹-۵)$$

با توجه به این‌که طول پیام‌ها در شبکه حسگر ۷۰ بایت است که ۲ بایت اول سرآیند پیام، مربوط به گره بلافصل بعدی (گام بعدی) است و با جایگذاری مقادیر مربوطه با پارامترهای رابطه (۵-۹) با مقادیر موجود در جدول ۵-۴ میزان مصرف انرژی برای ارسال، دریافت و شنود مشخص خواهد شد:

- Q_{Tran} $= 0.6999552\ mJ\ /\ message$
- $Q_{Reception} = 0.4666368\ mJ\ /\ message$
- $Q_{Listening} = 0.01333247\ mJ\ /\ message$

همان‌طور که از نتایج معلوم است، میزان مصرف انرژی در عملیات شنود نسبت به عملیات ارسال و دریافت پیام‌ها بسیار ناچیز است و بنابراین نشان‌دهنده مصرف انرژی بسیار پایین سیستم تشخیص نفوذ پیشنهادی و سبک بودن آن خواهد بود. در ادامه به جهت ارزیابی دقیق انرژی مصرفی سیستم تشخیص نفوذ پیشنهادی و ارائه نمودارهای مربوطه، دو سناریوی مختلف را ارائه کرده‌ایم:

الف) سناریوی اول: بررسی حالت عادی شبکه

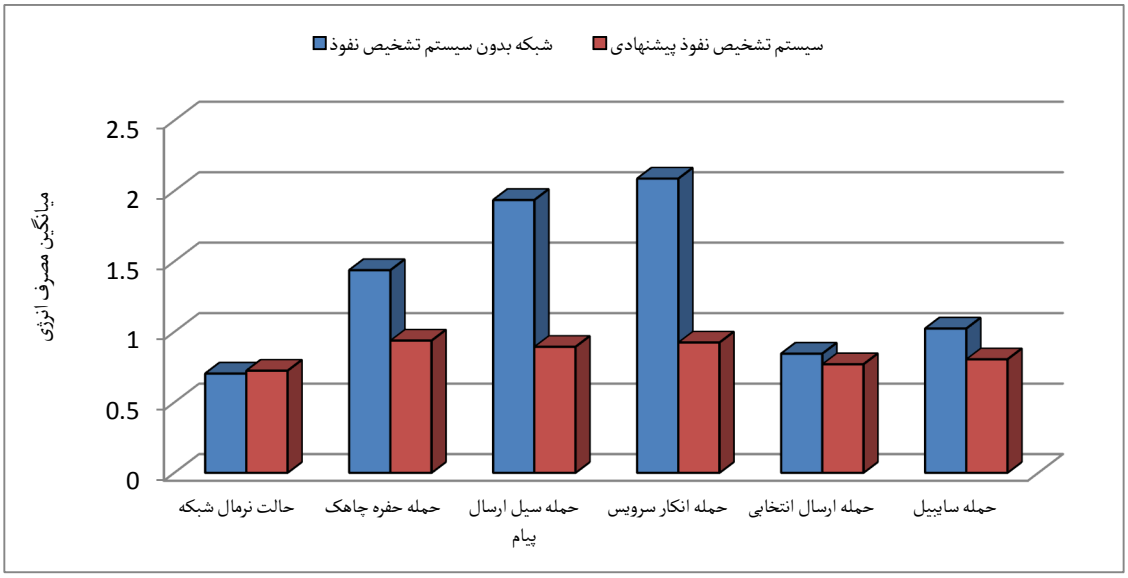
- شبکه بدون سیستم تشخیص نفوذ و بدون حضور حملات
- شبکه همراه با تشخیص نفوذ پیشنهادی و بدون حضور حملات

از مقایسه دو حالت فوق میزان مصرف انرژی سیستم تشخیص نفوذ پیشنهادی مشخص می‌گردد. همان‌طور که در شکل (۵-۳۱) مشاهده می‌شود تفاوت کمی بین این دو حالت وجود دارد که نشان‌دهنده سبک‌وزن بودن سیستم تشخیص نفوذ پیشنهادی است. به‌عبارت‌دیگر سیستم تشخیص نفوذ پیشنهادی ما سربار ناچیزی را به سیستم تحمیل می‌نماید که قابل‌چشم‌پوشی است.

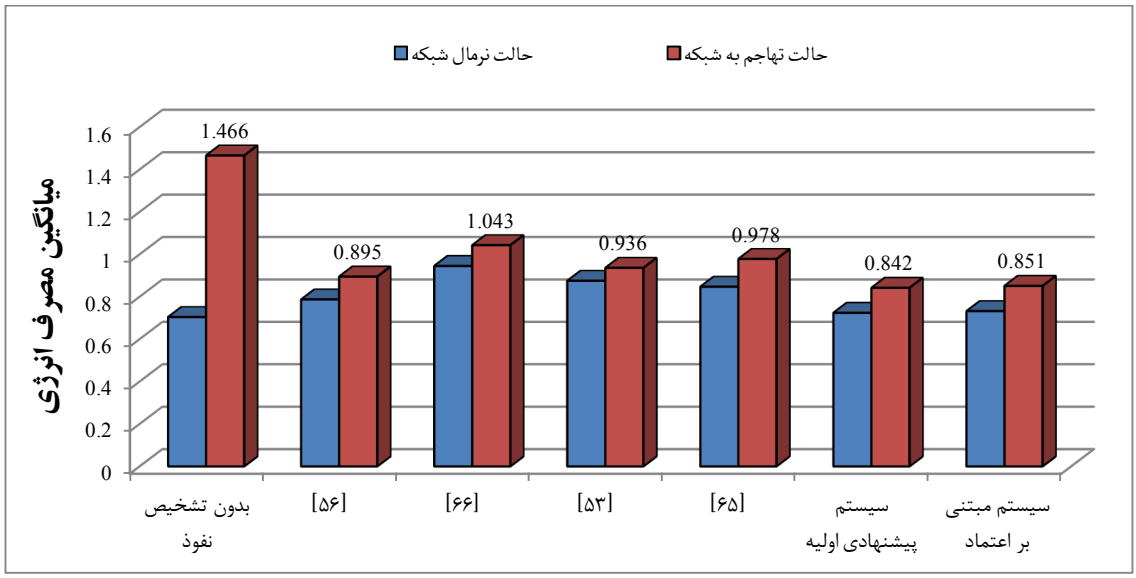
ب) سناریوی دوم: بررسی شبکه در حالت تهاجم حملات مختلف

- شبکه در حضور حملات و بدون سیستم تشخیص نفوذ
- شبکه در حضور حملات و همراه با تشخیص نفوذ پیشنهادی

از مقایسه دو حالت فوق نیز میزان کارایی سیستم تشخیص نفوذ پیشنهادی در مقابل حملات مختلف مشخص می‌شود. همان‌طور که در شکل (۵-۳۰) مشهود است سیستم تشخیص نفوذ پیشنهادی عملکرد بسیار خوبی را از خود نشان می‌دهد به‌گونه‌ای که میزان مصرف انرژی شبکه را با تشخیص‌های مناسب خود به‌شدت کاهش می‌دهد.



شکل (۵-۳۰): میانگین مصرف انرژی در سیستم پیشنهادی در برابر حملات مختلف و حالت عادی شبکه



شکل (۵-۳۱): میانگین مصرف انرژی سیستم تشخیص نفوذ پیشنهادی و کارهای موجود

۵-۷- ۲- نتایج تشخیص نفوذ پیشنهادی سطح میانی (سرخوشه‌ها)

در ادامه نتایج حاصل از شبیه‌سازی مدل پیشنهادی برای تشخیص نفوذ سطح میانی (سرخوشه‌ها) بر روی مجموعه‌دادگان KDDCup'99 و همچنین ارزیابی الگوریتم‌های طبقه‌بندی مختلف در جدول (۵-۱۰) ارائه‌شده‌اند.

همان‌طور که در جدول (۵-۱۰) مشاهده می‌گردد، بهترین نرخ تشخیص و نرخ هشدار اشتباه به ترتیب با ٪۹۹/۵۹ و ٪۰/۲۴ مربوط به الگوریتم طبقه‌بندی PART[1] است درعین‌حال نیز زمان آموزش (۰/۷۶ ثانیه) و آزمون (۰/۰۲۵ ثانیه) بسیار پایینی دارد که کاملاً آن را برای استفاده در شبکه‌های حسگر بی‌سیم مناسب می‌نماید. بنابراین ما به جهت طبقه‌بندی از الگوریتم طبقه‌بندی PART برای آموزش و آزمون نهایی سیستم تشخیص نفوذ پیشنهادی استفاده می‌نماییم.

PART الگوریتمی برای استنتاج قوانین به‌وسیله تولید تکراری درختان تصمیم جزئی[2] است که توسط فرانک و ویتن ارائه شده است [۱۰۰]. این الگوریتم از دو الگوریتم C4.5 و PIPPER مشتق شده است که هر دوی آن‌ها از درختان تصمیم برای تولید مجموعه قوانین استفاده می‌کنند. برخلاف این دو روش، الگوریتم PART نیازی به اجرای بهینه‌سازی سراسری ندارد. در بهینه‌سازی سراسری ابتدا درخت تصمیم تولید می‌گردد و سپس به یک مجموعه قوانین تبدیل شده و در نهایت آن قوانین را ساده‌سازی می‌کند. برای دادگان عظیم، بهینه‌سازی سراسری نیازمند زمان بسیار بالایی برای تولید قوانین است. بنابراین الگوریتم PART به جهت تولید قوانین با ادغام دو الگوی تولید قوانین از درختان تصمیم و شیوه تقسم و غلبه، مشکل فوق را مرتفع می‌نماید و بنابراین از لحاظ پیچیدگی محاسباتی سبک است. در این روش یک قانون در یک زمان تولید شده و سپس نمونه‌های پوششی توسط آن قانون حذف می‌گردد و برای نمونه‌های باقی‌مانده نیز با همین الگو به‌طور تکراری قوانین بعدی استخراج شده تا زمانی که هیچ نمونه‌ای باقی نماند. در یک دادگان چند کلاسه، این کار به‌طور خودکار منجر به تولید یک لیست مرتب از قوانین می‌شود که در واقع نوعی از طبقه‌بند است و به آن لیست تصمیم اطلاق می‌گردد.

[1] Partial Decision Tree
[2] repeatedly producing partial decision trees

جدول (۵-۱۰): ارزیابی کارائی انواع طبقه‌بندهای موجود بر روی مجموعه‌دادگان KDDCup'99 بر اساس مدل پیشنهادی

Classifiers Algorithms		TP Rate	FP Rate	Precision	F-Measure	ROC Area	Kappa Statistic	Training Time	Testing Time
Bayes	A1DE	99.49	0.35	99.48	99.48	99.99	99.1	0.14	0.054
	Bayes Net	97.97	1.7	98.08	98.01	99.88	96.44	0.18	0.054
	Naïve Bayes	89.57	7.51	89.66	88.94	96.04	81.52	0.04	0.111
	HMM	55.43	55.43	30.72	39.53	50.00	0.00	0.12	0.032
Functions	MLP	96.81	2.37	96.78	96.77	98.76	0.9441	1048.2	0.542
	SVM	98.11	1.46	97.98	98	98.32	0.9667	21.25	8.764
	SMO	93.87	4.8	93.48	93.54	95.71	0.8913	45.97	0.098
	Logistic	94.96	3.26	94.94	94.90	97.74	0.9118	53.55	0.089
Rules	Decision Table	98.34	1.39	98.17	98.25	99.75	0.9708	0.94	0.035
	FURIA	99.51	0.36	99.5	99.5	99.73	0.9915	70.19	0.086
	JRip	99.45	0.42	99.44	99.44	99.63	0.9904	7	0.031
	PART	**99.59**	**0.24**	**99.59**	**99.58**	99.89	**0.9923**	0.76	**0.025**
Trees	J48	99.32	0.42	99.31	99.31	99.63	0.9881	0.55	0.021
	Random Forest	99.44	0.33	99.43	99.43	99.97	0.9901	6.88	0.433
	Random Tree	99.4	0.32	99.39	99.39	99.57	0.9894	0.12	0.016
	REP Tree	99.09	0.56	99.07	99.06	99.7	0.984	0.22	0.017

در ادامه نیز نتایج مقایسه بین سیستم تشخیص نفوذ پیشنهادی برای سرخوشه‌ها با سیستم‌های موجود ازلحاظ نرخ تشخیص و نرخ هشدار نادرست و همچنین مدت‌زمان آموزش و آزمون و میزان پیچیدگی محاسباتی ارائه‌شده است. همه نتایج ارائه‌شده در جدول ۵-۱۱، میانگین محاسبه‌شده از ۱۰ بار اجرای عملیات شبیه‌سازی هستند. همچنین برای انجام یک مقایسه مناسب بین روش پیشنهادی با کارهای موجود، از دادگان یکسانی (KDDcup'99) برای شبیه‌سازی همه روش‌ها استفاده‌شده است که جزئیات آن در جدول ۵-۴ ارائه‌شده است.

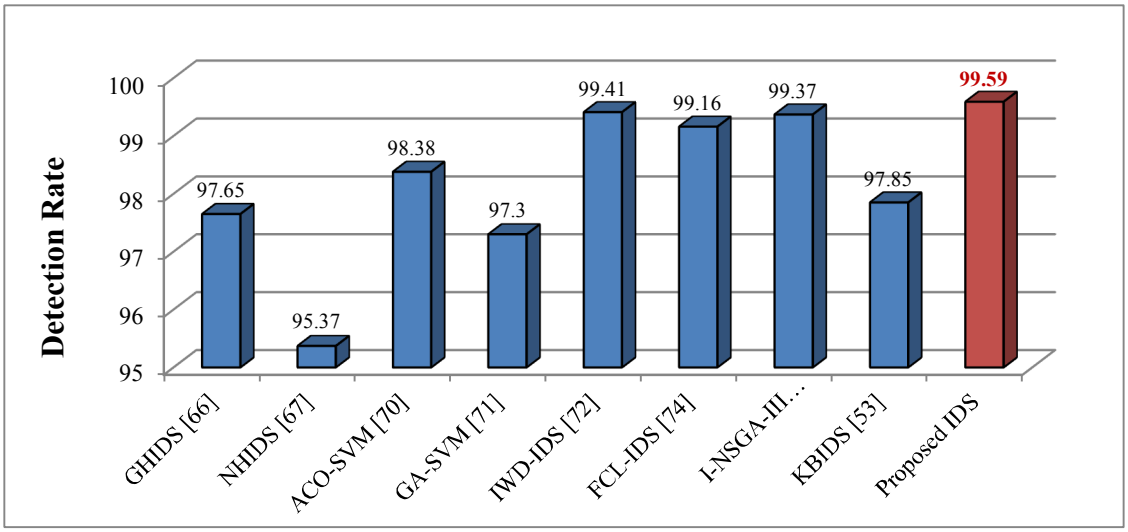
جدول (۵-۱۱): مقایسه کارائی سیستم تشخیص نفوذ پیشنهادی برای سرخوشه ها با سیستم‌های موجود

#	IDS Method	Feature selected	Detection Rate	False Alarm Rate	Computational	Training Time	Testing Time
1	IIDS [69]	24	90.96	2.06	low	135.37	0.29
2	GHIDS [66]	41	97.65	3.85	Very high	1229	73.45
3	NHIDS [67]	4	95.37	2.24	low	0.09	0.01
4	ACO-SVM [70]	25	98.38	0.004	medium	28.01	1.44
5	GA-SVM [71]	10	97.3	0.02	high	68.84	11.69
6	IWD-IDS [72]	9	99.41	1.41	medium	69.21	2.76
7	MCFA [73]	19	94.74	2.52	medium	0.84	1.74
8	FCL-IDS [74]	25	99.16	0.74	low	58.55	0.08
9	I-NSGA-III [75]	20	99.37	0.06	medium	30.2	1.06
10	KBIDS [53]	13	97.85	1.87	medium	84.3	3.83
11	**Proposed IDS**	**4**	**99.59**	**0.24**	**low**	**0.76**	**0.025**

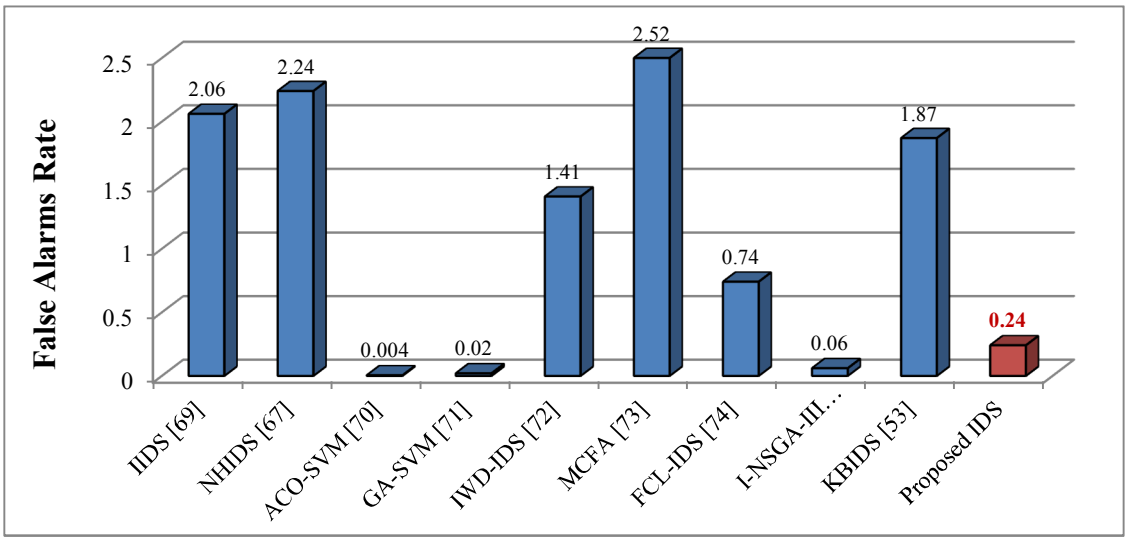
همان‌طور که در جدول ۵-۱۱ مشاهده می‌گردد روش پیشنهادی با نرخ تشخیص ٪۹۹.۵۹ دارای بهترین نرخ تشخیص به نسبت کارهای موجود است. ازلحاظ نرخ هشدارهای نادرست نیز سیستم تشخیص نفوذ پیشنهادی با نرخ ٪۰/۲۴ بعد از I-NSGA-III و GA-SVM و ACO-FS-SVM قرار دارد

که به جهت پیچیدگی محاسباتی آن‌ها و همچنین مدت‌زمان بالاتر آموزش و آزمون، در شرایط مطلوب‌تری نسبت به آن‌ها قرار دارد.

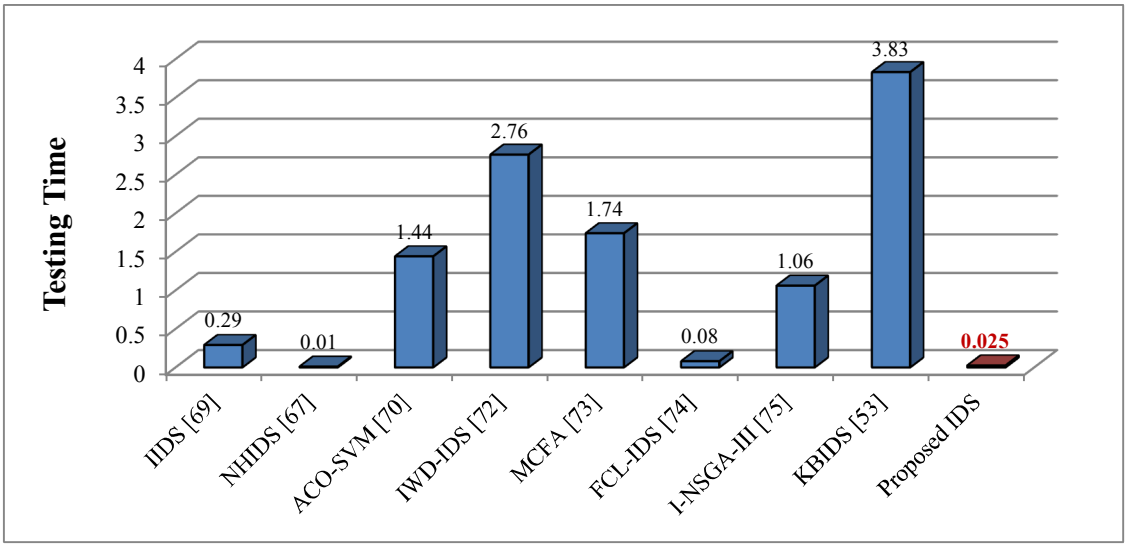
بنابراین با توجه به نتایج ارائه‌شده در جدول ۵-۱۱ و شکل‌های ۵-۳۲ تا ۵-۳۴، سیستم پیشنهادی با نرخ تشخیص بالای ۹۹/۵۹٪ و نرخ هشدار نادرست پایین ۰/۲۴٪ و همچنین زمان پایین اجرای مدل یعنی ۰/۰۲۵ ثانیه (که نشان‌دهنده پیچیدگی محاسباتی پایین آن است)، به‌عنوان یک روش مؤثر و سبک برای تأمین امنیت سرخوشه‌ها در شبکه‌های حسگر بی‌سیم مطرح است و با به‌کارگیری آن در شبکه‌های حسگر بی‌سیم، به‌خوبی می‌توان کارائی و عملکرد شبکه را در حد مطلوب حفظ نمود.



شکل (۵-۳۲): نمودار نرخ تشخیص سیستم پیشنهادی در مقایسه با کارهای موجود



شکل (۵-۳۳): نمودار نرخ هشدارهای نادرست سیستم پیشنهادی در مقایسه با کارهای موجود



شکل (۵-۳۴): نمودار زمان آزمون مدل اجرایی سیستم پیشنهادی در مقایسه با کارهای موجود

همان‌طور که در شکل ۵-۳۲ مشاهده می‌گردد، نرخ تشخیص سیستم تشخیص نفوذ پیشنهادی ۹۹/۵۹٪ است که بالاترین نرخ را در بین سیستم‌های موجود دارد. همچنین با نرخ بسیار پایین ۰/۲۴٪ هشدارهای نادرست که در شکل ۵-۳۳ ارائه‌شده است، سیستم پیشنهادی با اختلاف ناچیزی بعد از روش‌های مراجع [۷۰]، [۷۱] و [۷۵] قرار دارد، اما به دلیل پیچیدگی محاسباتی بالای آن‌ها الگوریتم پیشنهادی شرایط مطلوب‌تری را دارد. علاوه بر این، سیستم تشخیص نفوذ پیشنهادی با زمان آزمون بسیار پایین ۰/۰۲۵٪ ثانیه‌ای که در شکل ۵-۳۴ ارائه‌شده است، با یک اختلاف ناچیز بعد از روش [۶۷] قرار دارد، اما به جهت نرخ پایین تشخیص و نرخ بالای هشدارهای نادرست در [۶۷]، الگوریتم پیشنهادی دارای شرایط مطلوب‌تری است.

۵-۸- نتیجه‌گیری و کارهای آینده

در این بخش جمع‌بندی کارهای انجام‌شده و تحلیل نتایج به‌دست‌آمده در رساله ارائه می‌شود. در ادامه نیز کارهای آتی در بهبود سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم و مسائل مشابه (مانند امنیت و تشخیص نفوذ در اینترنت اشیاء)، پیشنهاد می‌شود.

شبکه‌های حسگر بی‌سیم یکی از فناوری‌های کاربردی و جذاب است که در سال‌های اخیر بسیار موردتوجه محققان قرارگرفته است. با توجه به این‌که این شبکه‌ها معمولاً در مکان‌های دور و فاقد

حفاظت و یا اغلب در شرایط عملیاتی خصمانه به کار گرفته می‌شوند، برای تهاجم و حملات امنیتی بسیار مستعد هستند. بنابراین تأمین امنیت آن‌ها با توجه به محدودیت منابع موجود در آن‌ها یک چالش اساسی محسوب می‌گردد. در همین راستا ما در این تحقیق، در ابتدا با شبیه‌سازی یک نمونه کامل از شبکه‌های حسگر بی‌سیم به‌صورت پارامتری و همچنین شبیه‌سازی حملات لایه شبکه و فرایند مسیریابی بر روی آن، به تحلیل دقیق رفتار آن‌ها در شبکه و استخراج خصوصیات آن‌ها پرداختیم. سپس به جهت تأمین امنیت شبکه‌های حسگر بی‌سیم، یک معماری تشخیص نفوذ کارآ در سه سطح مختلف ارائه کردیم، به‌گونه‌ای که بر اساس سطح امکانات و حساسیت گره‌های موجود در شبکه‌های حسگر، الگوریتم‌های متفاوتی را به جهت تشخیص حملات لایه شبکه و فرایند مسیریابی طراحی کرده و ارائه نمودیم.

در سطح گره‌های عادی (تشخیص نفوذ سطح پایین)، با توجه به محدودیت منابع شدید و سطح انرژی پایین موجود در آن‌ها، یک سیستم تشخیص نفوذ سبک مبتنی بر خصوصیات ارائه کردیم که بر اساس ویژگی‌های استخراج‌شده از حملات مختلف پایه‌گذاری شده است. در ادامه با اصلاح عملیات فوق از طریق یک سیستم مبتنی بر اعتماد، عملکرد سیستم تشخیص نفوذ پیشنهادی را بهبود دادیم. سیستم تشخیص نفوذ پیشنهادی با نرخ تشخیص بالای ۹۷/۱٪ و نرخ هشدار نادرست خیلی پایین ۱/۲٪ و همچنین میانگین مصرف انرژی کم ۰/۰۲ ژول، در مقایسه با کارهای موجود به‌عنوان یک روش مؤثر و سبک برای تشخیص نفوذ در سطح گره‌های عادی در شبکه‌های حسگر بی‌سیم مطرح است و با به‌کارگیری آن در شبکه‌های حسگر بی‌سیم، به‌خوبی می‌توان کارائی و عملکرد شبکه را در حد مطلوب حفظ نمود.

در سطح گره‌های سرخوشه (تشخیص نفوذ سطح میانی)، با توجه به این‌که بسیار بیشتر از گره‌های عادی موردتوجه مهاجمان و هجوم حملات قرار می‌گیرند (به دلیل عملیات حیاتی آن‌ها در شبکه مانند عملیات مدیریت خوشه، تجمیع داده‌ها و انتقال اطلاعات کل خوشه به ایستگاه پایه)، یک سیستم تشخیص نفوذ ترکیبی مبتنی بر الگوریتم‌های داده‌کاوی را به جهت تأمین امنیت سرخوشه‌ها

ارائه کردیم که با به‌کارگیری یک مدل پیش‌پردازش داده‌ها، پیچیدگی محاسباتی و حافظه مصرفی را در سیستم تشخیص نفوذ به‌طور چشمگیری کاهش داده و امکان استفاده از الگوریتم‌های طبقه‌بندی داده‌کاوی را در تشخیص نفوذ و تأمین امنیت سرخوشه‌ها در شبکه‌های حسگر بی‌سیم فراهم می‌نماید. نتایج حاصل از شبیه‌سازی‌ها نشان می‌دهند که سیستم پیشنهادی در مقایسه با کارهای موجود که اغلب پیچیدگی محاسباتی و حافظه بالایی دارند، علاوه بر پیچیدگی محاسباتی پایین، با نرخ تشخیص بالای ۹۹/۵۹٪، نرخ هشدار نادرست پایین ۰/۲۴٪ و همچنین زمان پایین اجرای مدل یعنی ۰/۰۲۵ ثانیه که تداعی‌گر مصرف انرژی حداقلی آن است، به‌عنوان یک سیستم تشخیص نفوذ مؤثر و سبک برای تأمین امنیت سرخوشه‌ها در شبکه‌های حسگر بی‌سیم مطرح است.

نوآوری‌های ارائه‌شده در این رساله:

۱۱. در معماری پیشنهادی خود از ایده ابتکاری یک روش مبتنی بر سطح اهمیت گره‌ها بهره بردیم که هر چه درجه اهمیت گره افزایش می‌یابد (مثلاً گره سرخوشه) ما نیز حساسیت سیستم تشخیص نفوذ را افزایش داده تا قدرت تشخیص بیشتری ایجاد نماییم و به‌این‌ترتیب تضمین بیشتری برای حفظ امنیت ایجاد نماییم.

۱۲. ارائه الگوریتم‌های ابتکاری مناسب در بخش‌های مختلف معماری پیشنهادی به جهت بهبود کارایی آن

۱۳. استخراج ویژگی‌های جدید به جهت استفاده در سیستم تشخیص نفوذ پیشنهادی که از طریق شبیه‌سازی یک نمونه کامل از شبکه‌های حسگر بی‌سیم به‌صورت پارامتری و همچنین شبیه‌سازی حملات لایه شبکه و فرایند مسیریابی بر روی آن و تحلیل دقیق رفتار آن‌ها در شبکه انجام گردید.

۱۴. بهبود میزان تفکیک‌پذیری ویژگی‌های استخراج‌شده و موجود برای بهبود دقت تشخیص شناسایی حملات در سیستم تشخیص نفوذ پیشنهادی از طریق تحلیل دقیق رفتار حملات تعیین مناسب‌تر حدود آستانه مربوط به ویژگی‌ها

۱۵. بهبود دقت تشخیص حملات مختلف با ارائه یک روش مبتنی بر اعتماد به جهت ارزشیابی هشدارهای صادرشده برای تشخیص حملات و ترکیب آن با سیستم تشخیص نفوذ مبتنی بر خصوصیات پیشنهادی اولیه

۱۶. ارائه یک روش پیش‌پردازش داده‌ها بر روی دادگان به جهت بهبود دقت تشخیص و مصرف انرژی در سیستم تشخیص نفوذ ترکیبی پیشنهادی برای تأمین امنیت سرخوشه‌ها

۱۷. بررسی و تحلیل خصوصیات مربوط به طبقه‌بندهای مختلف و انتخاب یک روش مناسب به جهت طبقه‌بندی دادگان

۱۸. بررسی و تحلیل خصوصیات مربوط به الگوریتم‌های مختلف کاهش ویژگی‌ها و انتخاب یک روش مناسب کاهش ابعاد دادگان به جهت بهبود دقت تشخیص و مصرف انرژی معماری پیشنهادی

۱۹. استفاده از امکانات گره چاهک به جهت بهبود امنیت و کارایی سیستم تشخیص نفوذ پیشنهادی و همچنین استفاده از یک روش یادگیری ماشین بر روی آن به جهت شناسایی الگوی حملات جدید

۲۰. پوشش تمامی حملات لایه شبکه و فرایند مسیریابی توسط سیستم پیشنهادی با ادغام ویژگی‌های موجود و استخراج‌شده

۲۱. ارزشیابی سیستم پیشنهادی با همه معیارهای کارائی مربوط به شبکه‌های حسگر بی‌سیم

در این پژوهش راهکاری نوین برای تأمین امنیت در شبکه‌های حسگر بی‌سیم از طریق ارائه یک معماری تشخیص نفوذ کارآ ارائه‌شده است. در راهکار ارائه‌شده تمرکز زیادی بر روی سطوح مختلف حساسیت گره‌ها ازلحاظ تأمین امنیت و محدودیت منابع مربوطه شده است. ما با در نظر گرفتن این منطق یک معماری سه سطحی را طراحی کردیم و تمهیدات مختلفی را برای هر سطح در نظر گرفتیم. در این بخش، پیشنهادهایی برای کارهای آینده آورده می‌شود.

۱. به جهت بهبود معماری پیشنهادی با ارائه یک سیستم تشخیص نفوذ سطح بالا، از پتانسیل-های ایستگاه پایه (عدم وجود محدودیت منابع و انرژی و وجود قابلیت‌های سخت‌افزاری بالا)، برای ارتقاء سطح امنیت سرخوشه‌ها استفاده کنیم.

۲. با به‌کارگیری الگوریتم‌های یادگیری در کنار معماری پیشنهادی امکان تشخیص حملات ناشناخته و جدید را نیز فراهم نماییم و از این طریق دقت تشخیص آن را بهبود دهیم.

۳. ارائه یک الگوریتم کاهش ابعاد منطبق بر خصوصیات سیستم‌های تشخیص نفوذ و شبکه‌های حسگر بی‌سیم به جهت انتخاب مجموعه ویژگی‌های مناسب‌تر و به‌تبع آن بهبود دقت تشخیص معماری پیشنهادی

۴. استخراج ویژگی‌های جدید با ترکیب ویژگی‌های موجود و همچنین ایجاد ویژگی‌های آماری (از طریق تحلیل الگوهای آماری ویژگی‌های موجود) و استفاده از آن‌ها به جهت بهبود دقت تشخیص معماری پیشنهادی

۵. استفاده از سیستم تشخیص نفوذ پیشنهادی با اعمال تغییرات مناسب و منطبق بر خصوصیات اینترنت اشیاء به جهت تأمین امنیت کاربردهای وابسته به اینترنت اشیاء که در حال حاضر به‌عنوان یکی از موضوعات بسیار مهم تحقیقاتی است.

۶- منابع و مراجع

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks,” in IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] E. Cayirci and C. Rong, “Security in Wireless Ad Hoc and Sensor Networks”, book published by Wiley, 2009.

[3] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” in IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[4] E. Egea-Lopez, J. Vales-Alonso, A. S. Martinez-Sala, P. Pavon-Marino, J. Garcia-Haro, "Simulation Tools for Wireless Sensor Networks", in Procedia Summer Simulation Multiconference - SPECTS, 2005.

[5] I. T. Downard, "Simulating Sensor Networks in NS-2," in Technical Report NRL/FR/5522-04-10073, Naval Research Lab, Washington DC, U.S.A., May 2004.

[6] H. Al-hamadi, I. Chen, and V. Tech, “Integrated Intrusion Detection and Tolerance in Homogeneous Clustered Sensor Networks”, in ACM Transaction on Sensor Networks (TOSN), vol. 11, no. 47, pp. 1–25, 2015.

[7] R. Deshmukh, R. Deshmukh, M. Sharma, “Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network”, in International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, no. 6, pp. 200 – 208, 2013.

[8] C.C. Su, K.M. Chang, Y.H. Kuo and M.F. Horng, “The new intrusion prevention and detection approaches for clustering-based sensor networks”, in IEEE Wireless Communications and Networking Conference, vol. 4, pp. 1927-1932, May 2005.

[9] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” in IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 1–23, Second Quarter 2006.

[10] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor Network Security: A Survey”, in IEEE Communications Surveys & Tutorials, vol. 11, no. 2, pp. 52-73, 2009.

[11] K. Khan, W. Goodridge, and D. Ragbir, “Security in Wireless Sensor Networks,” in Global Journal of Computer Science and Technology, vol. 12, no. 16, pp. 42-49, 2012.

[12] J. R. Douceur, “The Sybil attack”, in First International Workshop on Peer-to-Peer Systems (IPTPS ’02), 2002.

[13] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, in First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127, 2003.

[14] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, “TAG: a tiny aggregation service for ad hoc sensor networks”, in Symposium on Operating Systems Design and Implementation, 2002.

[15] A. Nadeem, M. Howarth, "Adaptive intrusion detection & prevention of denial of service attacks in MANETs", in Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the world wirelessly, pp. 926-930. ACM, 2009.

[16] S. Ghildiyal, A. K. Mishra, A. Gupta, N. Garg, "Analysis Of Denial Of Service (Dos) Attacks In Wireless Sensor Networks", in International Journal of Research in Engineering and Technology (IJRET), vol. 3, Jun. 2014.

[17] A. Agah, K. Basu, and S. K. Das, "Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling", in IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 1-8 , 2005.

[18] A. Agah and S.K. Das, “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach”, in International Journal of Network Security, vol. 5, no. 2, 145-153, 2007.

[19] J. Deng, R. Han, and S. Mishra, “Countermeasures against traffic analysis in wireless sensor networks”, in Technical Report CU-CS987-04, University of Colorado, 2004.

[20] G. Dini and M. Tiloca, “ASF: An attack simulation framework for wireless sensor networks,” in 8th IEEE International Conference on Wireless Mobile Computer Network Communications, pp. 203–210, 2012.

[21] K. K. Waraich and B. Singh, “Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks”, in International Journal of Advanced Science and Technology, vol. 82, pp. 63-70, 2015.

[22] H. Ehsan, F. A. Khan, “Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs”, in IEEE, 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1181-1187, 2012.

[23] J. Sen, “A Survey on Wireless Sensor Network Security”, in International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, pp. 55-78, 2009.

[24] A. Fuchsberger, “Intrusion detection systems and intrusion prevention systems”, in Elsevier Journal of Information Security Technical Report, vol. 10, no. 3, pp. 134-139, Dec. 2005.

[25] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks”, in Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.

[26] A. Agah, K. Basu, S.K. Das, “Preventing DoS attack in sensor networks: A game theoretic approach”, in Proceedings of IEEE International Conference on Communications, Seoul, South Korea, 2005.

[27] M. Mohi, A. Movaghar, and P. M. Zadeh, "A Bayesian game approach for preventing DoS attacks in wireless sensor networks", in International Conference on Communications and Mobile Computing, CMC'09, pp. 507-511, 2009.

[28] I. Butun, S. D. Morgera, and R. Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks”, in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp 266-282, 2013.

[29] Y. Zhang, W. Lee, and Y.A. Huang, “Intrusion detection techniques for mobile wireless networks”, in Journal of Wireless Networks, vol. 9, no. 5, pp. 545-556, 2003.

[30] N. A. Alrajeh, S. Khan and B. Shams, “Intrusion Detection Systems in Wireless Sensor Networks: A Review”, in International Journal of Distributed Sensor Networks, vol. 2013, Article ID 167575, pp. 1-7, 2013.

[31] T.S. Sobh, “Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art”, in Elsevier Journal of Computer Standards and Interfaces, vol. 28, no 6, pp. 670-694, Sep. 2006.

[32] S. Rajasegarar, C. Leckie, AND M. Palaniswami, “Anomaly detection in wireless sensor networks”, in IEEE Wireless Communications, vol. 15, no. 4, pp. 34-40, Aug. 2008.

[33] S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, “An experimental study of hierarchical intrusion detection for wireless industrial sensor networks”, in IEEE Transactions on Industrial Informatics, vol. 6, no. 4, pp. 744-757, Nov. 2010.

[34] E. Ngai, J. Liu and M. Lyu, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks”, in IEEE International Conference on Communications (ICC), vol. 8, pp. 3383–3389, 2006.

[35] F. Bao, R. Chen, M.J. Chang and J.H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trustbased routing and intrusion detection”, in IEEE Transactions on Network Service Management, vol. 9, no. 2, pp. 169–183, 2012.

[36] A. Diaz, P. Sanchez, J. Sancho, and J. Rico, "Wireless sensor network simulation for security and performance analysis," in Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 432-435, May 2013.

[37] G.H. Lai and C.M. Chen, "Detecting Denial of Service Attacks in Sensor Networks", in Journal of Computers, vol.18, no.4, Jan. 2008.

[38] M. Guechari, L. Mokdad, and S. Tan, "Dynamic solution for detecting denial of service attacks in wireless sensor networks", in IEEE International Conference on Communications (ICC), pp. 173-177, 2012.

[39] R.C. Chen, C.F. Hsieh, Y.F. Huang, “A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks”, in Proceeding of ACM ICUIMC, pp. 238-245, 2009.

[40] A.A. Strikos, “A full approach for intrusion detection in wireless sensor networks”, in School of Information and Communication Technology, 2007.

[41] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, “Distributed Anomaly Detection in Wireless Sensor Networks”, in IEEE International Conference on Communications, pp. 3864-3869, 2007.

[42] I. Krontiris, T. Dimitriou and F.C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”, in Proceeding of 13th Europe Wireless Conference, pp 1-10, 2007.

[43] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling and T. Dimitriou, “Cooperative intrusion detection in wireless sensor networks”, in Springer Journal of Wireless Sensor Networks, pp. 263-278, 2009.

[44] A.P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz and H.C. Wong, “Decentralized Intrusion Detection in Wireless Sensor Networks,” in 1st ACM International Workshop on Quality of service & security in wireless and mobile networks, pp. 16–23, Oct. 2005.

[45] S.S. Doumit and D.P. Agrawal, “Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks”, in IEEE Military Communications Conference (MILCOM), pp. 609-614, 2003.

[46] I. Onat and A. Miri, “A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks”, in IEEE System Communications, pp 422-427, 2005.

[47] A. Agah, S.K. Das, K. Basu and M. Asadi, “Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach,” in Proceeding of 3rd IEEE International Symposium on Network Computing and Appllications (NCA), pp. 343-346, Nov. 2004.

[48] A. Agah and S.K. Das, “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach”, in International Journal of Network Security, vol. 5, no. 2, pp. 145-153, 2007.

[49] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, “Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks”, in IEEE International Communications Conference (ICC), pp. 3864-3869, 2007.

[50] Y. ZHANG, X. LI, and Y. LIU, "The detection and defence of DoS attack for wireless sensor network", in Journal of China Universities of Posts and Telecommunications, vol. 19, pp. 52-56, 2012.

[51] V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” in Journal of High Speed Networks, vol. 15, no. 1, pp. 33-51, 2006.

[52] I. Onat and A. Miri, “An Intrusion Detection System for Wireless Sensor Networks”, in IEEE International Conference on Wireless Mobile Computing and Network Communications (WiMob), vol. 3, pp. 253-259, 2005.

[53] H. Qu, Z. Qiu, X. Tang, M. Xiang, P. Wang, “An Adaptive Intrusion Detection Method for Wireless Sensor Networks”, in International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 11, 2017.

[54] R. Roman, J. Zhou, and J. Lopez, “Applying intrusion detection systems to wireless sensor networks,” in 3rd IEEE Consumer Communications and Networking Conference, pp. 640-644, 2006.

[55] Z. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks", in Computer Communications, vol. 34, pp. 468-484, 2011.

[56] C. F. Hsieh, R. C. Chen, and Y. F. Huang, “Applying an Ontology to a Patrol Intrusion Detection System for Wireless Sensor Networks”, in International Journal of Distributed Sensor Networks, vol 2014, pp. 1-14, 2014.

[57] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, “Catching Packet Droppers and Modifiers in Wireless Sensor Networks”, in IEEE Transactions Parallel and Distributed Systems, vol. 23, no. 5, pp. 835–843, May 2012.

[58] Xu X. , “ Adaptive Intrusion Detection Based on Machine Learning: Feature Extraction, Classifier Construction and equential Pattern Prediction”, in International Journal of Web Services Practices vol.2, no.1-2, pp:49–58, 2006.

[۵۹] س. صفیر، "بهبود کارایی سیستم‌های تشخیص نفوذ برای شبکه‌های بی‌سیم" پایان نامه کارشناسی ارشد، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف تهران، سال ۱۳۹۱.

[۶۰] ه. باغچه‌بند، "امنیت شبکه‌های بی‌سیم حسگر با استفاده از الگوریتم چندعاملی رمزنگاری و سیستم تشخیص نفوذ با بکارگیری الگوریتم‌های هوشمند" پایان نامه کارشناسی ارشد، دانشکده مهندسی برق و الکترونیک، دانشگاه صنعتی و فناوری پیشرفته کرمان، سال ۱۳۹۰.

[61] M. E. Elhamahmy, H. N. Elmahdy, I. A. Saroit, “A New Approach for Evaluating Intrusion Detection System”, in International Journal of Artificial Intelligent Systems and Machine Learning, vol 2, no 11, Nov. 2010.

[62] P. Aggarwal, S. K. Sharma, “Analysis of KDD Dataset Attributes - Class wise For Intrusion Detection”, in 3rd International Conference on Recent Trends in Computing, pp. 842 – 851, 2015.

[63] S. K. Sahu, S. Sarangi, S. K. Jena, “A Detail Analysis on Intrusion Detection Datasets”, in IEEE International Advance Computing Conference (IACC), pp. 1348-1353, 2014.

[64] W. Wang, S. J. Knapskog, S. Gombault, “Attribute Normalization in Network Intrusion Detection”, in 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009.

[65] H. Zhou, Q. Liu, C. Cui, “Research on Intrusion Detection Algorithm Based on Multi-Class SVM in Wireless Sensor Networks”, in Communications and Network, vol. 5, no. 3, pp. 524-528, Sep. 2013.

[66] Y. Maleh, A. Ezzati, Y. Qasmaoui, M. Mbida, “A Global Hybrid Intrusion Detection System for Wireless Sensor Networks,” in Procedia Computer Science, vol. 52, pp. 1047-1052, 2015.

[67] H. Sedjelmaci, M. Feham, “Novel hybrid intrusion detection system for clustered wireless sensor network”, in International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 4, pp. 1-14, Aug. 2011.

[68] M. M. Ozcelik, E. Irmak, S. Ozdemir, “A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks”, in International Symposium on Networks, Computers and Communications (ISNCC), 2017.

[69] S. S. Wang, K. Q. Yan, S. C. Wang, C. W. Liu, “An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks”, in Expert Systems with Applications, vol. 38, no. 12, pp. 15234-15243, Dec. 2011.

[70] W. Xingzhu, “ACO and SVM Selection Feature Weighting of Network ntrusion Detection Method”, in International Journal of Security and Its Applications, vol. 9, no. 4, pp. 129-270, Apr. 2015.

[71] M. Aslahi-Shahri, R. Rahmani, M. Chizari, et al. “A hybrid method consisting of GA and SVM for intrusion detection system”, in Neural computing and applications, vol. 27, no. 6, pp. 1669–1676, Aug. 2016.

[72] N. Acharya, S. Singh, “An IWD-based feature selection method for intrusion detection system”, in Soft Computing, vol. 22, no. 13, pp. 4407-4416, Jul. 2018.

[73] R. Kaur, M. Sachdeva and G. Kumar, “Nature Inspired Feature Selection Approach for Effective Intrusion Detection”, in Indian Journal of Science and Technology, vol. 9, no. 42, pp. 1-9, Nov. 2016.

[74] Ramakrishnan, S. Devaraju, “Attack's feature selection-based network intrusion detection using fuzzy control language”, in International journal of fuzzy systems, vol. 19, no. 2, pp. 316–328, Apr. 2017.

[75] Y. Zhu, J. Liang, J. Chen, Z. Ming, “An improved NSGA-III algorithm for feature selection used in intrusion detection”, in Knowledge-Based Systems, vol. 116, pp. 74-85, Jan. 2017.

[76] J. Newsome , E. Shi, D. Song, A. Perrig, “The Sybil attack in sensor networks: analysis and defenses”, in Proceeding of the International Symposium on Information Processing in Sensor Networks, pp. 259–268, 2004.

[77] S. Chen, G. Yang and S. Chen “A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks”, in Proceeding of the International Conference on Communications and Mobile Computing, China, pp. 142-146, 2010.

[78] A. Jangra, S. Priyanka, “Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)”, in Proceeding of the International Conferences on Advances in ICT for Emerging Regions, 2011.

[79] Vasudeva1 A. and Sood M., “Sybil Attack on Lowest ID Clustering Algorithm in The Mobile Ad-hoc Network”, in Proceeding of the International Journal of Network Security & Its Applications (IJNSA), vol.4, no.5, 2012.

[80] S. Zhong, Y. G. Liu, Y. R. Yong, "Privacy-preserving location based services for mobile users in Wireless Networks", In Proceeding of the Technical Report, Yale Computer Science, 2004.

[81] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks", In Proceeding of the IEEE Computer Society International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 570–574, 2006.

[82] M. Wen, H. Li, Y-F. Zheng and K-F. Chen, “TDOA-Based Sybil Attack Detection Scheme for Wireless Sensor Networks”, in Journal of Shanghai University (English Edition), vol.12, no. 1, pp. 66-70, 2008.

[83] K. F. Ssu, W. T. Wang and W. C. Chang, “Detecting Sybil attacks in wireless Sensor Networks using neighboring information”, in Computer Networks, vol. 53, no. 18, pp. 3042–3056, Dec. 2009.

[84] C. Piro, C. Shields, B. N. Levine, “Detecting the Sybil Attack in Mobile Ad-hoc Networks”, Securecomm and Workshops, pp 1-11, 2006.

[85] R. Muraleedharan, X. Ye, L. A. Osadciw, “prediction of Sybil attack on WSN using Bayesian network and Swarm intelligence", in Proceedings of Wireless Sensing and Processing, 2008.

[86] Y. Zhang, W. Liu, W. Lou, Y. Fang, “Location-based compromisetolerant security mechanisms for wireless sensor networks”, in IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247–260, 2006.

[87] Q. Zhang, P. Wang, D. S. Reeves, P. Ning, “Defending against Sybil attacks in sensor networks”, in Proceedings of IEEE International Conference on Distributed Computing Systems Workshops, pp. 185–191, 2005.

[88] R. Amuthavalli and R. S. Bhuvaneswaran, “Detection and prevention of sybil attack in wireless sensor network employing random password comparison method,” in Journal of Theoretical and Applied Information Technology, vol. 67, no. 1, pp. 236–246, 2013.

[89] U. Suriya, R. Vayanaperumal, “Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method,” in The Scientific World Journal, vol. 2015, pp. 1-7, 2015.

[90] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, A. K. Pathan, “A novel energy-efficient sybil node detection algorithm for intrusion detection system in wireless sensor networks,” in 3rd International Conference on Eco-friendly Computing and Communication Systems, Dec. 2014.

[91] A .Andalib, M. Jamshidi, F. Andalib, D. Momeni, “A Lightweight Algorithm for Detecting Sybil Attack in Mobile Wireless Sensor Networks using Sink Nodes”, in International Journal of Computer Applications Technology and Research, vol. 5, no. 7, pp. 433-438, 2016.

[92] K. Butler, S. Ryu, P. Traynor, P. D. McDaniel, “Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems”, in IEEE Transaction on Parallel and Distributed Systems, vol. 20, no. 12, pp. 1803-1815, 2009.

[93] W. Shi, S. Liu and Z. Zhang, “A Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network”, in KSII Transactions of Internet and Information Systems, vol. 9, no. 9, pp. 3738-3750, sep. 2015.

[94] P. Sarigiannidis, E. Karapistoli, A. A. Economides, “Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information”, in Elsevier, Expert Systems with Applications, vol. 42, no. 21, pp. 7560-7572, 2015.

[95] R. Singh, J. Singh, R. Singh, “TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks”, in IJCSNS, International Journal of Computer Science and Network Security, vol. 16, no. 11, pp. 90-99, 2016.

[96] G. Gautam, B. Sen, “Design and Simulation of Wireless Sensor Network in NS2”, in International Journal of Computer Application, vol. 113, no. 16, pp. 14-16. Mar. 2015.

[97] C. Elkan, “Results of the KDD’99 classifier learning”, in ACM SIGKDD Explorations Newsletter, vol. 1, no. 2, pp. 63-64, Jan. 2000.

[98] K. Khan, W. Goodridge, “Fault Tolerant Multi-Criteria Multi-Path Routing in Wireless Sensor Networks”, in International Journal of Intelligent Systems and Applications, vol. 7, no. 6, pp. 55-63, May. 2015.

[99] C. A. Jayakody, R. Samarasinghe, S. R. Kodituwakku, “SecAODV: Lightweight Authenticat on for AODV Protocol”, in International Journal of Computer Applications, vol. 137, no. 13, pp. 33-38, Mar. 2016.

[100] E. Frank, I. H. Witten, “Generating Accurate Rule Sets Without Global Optimization”, in Fifteenth International Conference on Machine Learning, San Francisco, pp. 144-151, 1998.

Abstract

Wireless sensor networks are one of the applied and attractive technologies that have attracted the attention of researchers in recent years. These networks because of their inherent advantages such as lower cost and easier deployment on the environment, to play a role in a wide range of applications. However, resource constrains, such as limited processing power, memory and energy are main challenge in WSN design and application. Given that WSNs are often used in remote and unprotected locations or even hostile operating conditions, they are highly susceptible to intrusions and security attacks, which, given their limited resources, reduces their performance considerably. Therefore, security in WSNs has become an important issue, and actually security is considered as one of the essential parameters in quality of service (QOS), especially if these networks are involved in critical processes. Many security solutions are designed for WSNs to specific attacks. These security mechanisms are able to guarantee security at some levels; however, they cannot be completely prevented from most of the security attacks. The intrusion detection system (IDS) is one of defense method against attacks, which is actually the second line of defense against invaders after intrusion prevention systems (IPS), and its task is detecting and reporting attacks and invaders. One of the benefits of IDSs against other security methods is to cover a wide range of attacks on WSNs. Researchers have provided various IDSs for WSNs, but due to the limitations in WSNs, designing an effective and efficient IDS that be usable in them is still a major challenge. We plan to propose an efficient architecture for IDSs on WSNs by examining existing methods. Our meaning of efficient architecture is improvements in energy consumption and waste as the main parameter in sensor nodes as well as improving the detection accuracy of attacks. The main idea of our proposed architecture is to pay attention to the importance level of the nodes and their sensitivity in the network and, on this basis, we will use effective detection algorithms at different levels. Our goal in this architecture is to cover network layer attacks and routing, which are the most common attacks in sensor networks. In order to proper and desirable validation, by performing simulations of the proposed architecture, all performance criteria have been evaluated on that. The results obtained from simulations show that the proposed architecture is well-known as an effective and lightweight method for the WSNs, and by applying it in WSNs, the performance of the network can be kept in the optimum level.

Key Words: Wireless Sensor Networks (WSNs), Intrusion Detection Systems (IDSs), Network Layer Attacks and Routing, Security Mechanisms, Performance Criteria.

Shahrood University of Technology

Faculty of Computer Engineering

Ph.D. Thesis in Artificial Intelligence Engineering

An Efficient Architecture for Intrusion Detection Systems in Wireless Sensor Networks

By:

Mahdi Sadeghizadeh

Supervisor:

Dr. Omidreza Marouzi

Advisor:

Dr. Ali Akbar Pouyan

January 2019