یک سامانهٔ تشخیص نفوذ برای شبکه‌های حس‌گر بی‌سیم بدن

پیام محمودی نصر*[1]، علیرضا رحمانی[2]

[1]دانشکده مهندسی و فناوری- دانشگاه مازندران – مازندران – ایران

[2]مؤسسه آموزش عالی صنعتی مازندران – مازندران – ایران

چکیده

شبکه‌های حس‌گر بی‌سیم به دلیل کاربردهای متنوعی که دارند همواره مورد به آن توجه شده است. در تقسیم‌بندی شبکه‌های حسگر بی‌سیم، این شبکه‌ها به‌دلیل کاربردهای حساس پزشکی از اهمیت ویژه‌ای برخوردارند. هرگونه حمله به شبکه‌های حسگر بی‌سیم بدن می‌تواند خسارت‌های جانی جبران‌ناپذیری برای بیمار به همراه داشته باشد. یکی از روش‌های تأمین امنیّت استفاده از سامانه‌های تشخیص نفوذ به‌عنوان یک دفاع خط دوم است. در این مقاله یک سامانهٔ تشخیص نفوذ مبتنی بر ناهنجاری با استفاده از روش‌های ترکیبی ارائه‌شده است. در سامانه تشخیص نفوذ پیشنهادی، نخست با استفاده از الگوریتم ژنتیک، ویژگی‌هایی از داده‌های جمع‌آوری‌شده انتخاب می‌شوند که موجب به دست آمدن بالاترین نرخ تشخیص شوند. سپس، با استفاده از روش‌های ماشین بردار پشتیبان و k نزدیک‌ترین همسایهٔ طبقه‌بندی داده‌ها به‌منظور کشف ترافیک ناهنجار از ترافیک داده‌های طبیعی انجام می‌شود. نتایج شبیه‌سازی برای حملهٔ جلوگیری از سرویس نشان می‌دهد که استفاده از سامانه پیشنهادی با استفاده از روش طبقه‌بندی k نزدیک‌ترین همسایه می‌تواند بازده‌ای معادل ۹۰٪ داشته باشد.

واژه‌های کلیدی: **شبکه حسگر بی‌سیم بدن، تشخیص نفوذ، حمله جلوگیری از سرویس، الگوریتم ژنتیک چندهدفه.**

An Intrusion Detection System for Wireless Body Area Networks

Payam Mahmoudi Nasr*[1] and Alireza Rahmani

[1]Engineering and Technology Dep., University of Mazandaran, Mazandaran, Iran
Mazandaran Institute of Technology, Mazandaran, Iran

Abstract:

Wireless Body Area Network (WBAN) is a pioneer trend in healthcare technology. A WBAN consists of small sensors that may be worn or implanted on the patient's body or around them. These sensors are responsible for sending wireless, real-time physiological signs of the patient's body (such as blood pressure, heart rate, blood sugar, temperature, breathing, etc.) to an intermediate device. An intermediate device (such as a mobile phone) collects and prepares data to send and display to the doctor. In the WBAN, since data is sent through all broadcasts, any cyber attack such as eavesdropping and data modification/ sabotage can be done. Any cyber-attack on a WBAN could jeopardize the patient's health; therefore, securing the WBAN plays a crucial role in healthcare applications. Due to the limitation of energy, memory, and processing power of sensors in WBAN, it is not possible to use traditional security methods, such as encryption and security protocols. For this reason, one of the methods to provid security in the WBAN is the use of intrusion detection systems. An intrusion detection system (IDS), as a second-line defense, is one of the security methods in computer networks. Intrusion detection is the intelligent monitoring of network or computer systems to find any security breach. These systems are divided into two groups, signature-based and anomaly-based. One of the advantages

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۱/۸/۱۷ • تاریخ پذیرش: ۱۴۰۱/۱۲/۳ • تاریخ انتشار: ۱۴۰۲/۵/۲۰ • نوع مطالعه: پژوهشی

of anomaly-based systems is the detection of zero-day attacks. Statistical, knowledge-based, data mining and machine learning methods can be used to implement anomaly-based intrusion detection systems. In this paper, a new IDS has been presented which is able to detect denial of service (DoS) attacks in a WBAN. The proposed IDS is a hybrid anomaly-based system using machine learning and feature engineering methods. In the proposed IDS, a genetic algorithm is used to select features of collected data, in a way that increases the performance of the IDS, and as a result the WBAN (increasing detection rate and reducing energy consumption in the node). Then, using support vector machine and k nearest neighbor algorithms, the data classification is performed to detect DoS traffic from regular data traffic. Simulation results indicate that the proposed IDS has effective performance with a 90% detection rate.

Keywords: Anomaly detection, cyber security, DoS attack, Genetic algorithm, WBAN.

۱- مقدمه

در حال حاضر شبکه‌های حسگر بی‌سیم بدن[1] به‌عنوان یکی از فن‌آوری‌های پیشرو و کلیدی به‌منظور حمایت از برنامه‌های کاربردی حوزهٔ سلامت بر روی تلفن همراه است[1]. یک شبکه حسگر بی‌سیم بدن از تعدادی حسگر کوچک تشکیل‌شده که ممکن است به‌صورت پوشیدنی و یا کاشته‌شده بر روی بدن بیمار و یا اطراف وی قرار گرفته باشند. این حسگرها وظیفه ارسال بی‌سیم و بی‌درنگ[2] علائم فیزیولوژی بدن بیمار (مانند فشارخون، ضربان قلب، قند خون، دما، تنفس و ...) به یک دستگاه میانی را به عهده دارند. این دستگاه میانی (مانند تلفن همراه) وظیفهٔ جمع‌آوری و آماده‌سازی داده‌ها را برای ارسال و نمایش به پزشک به عهده دارد [2]. هرگونه حملهٔ سایبری به شبکه حسگر بی‌سیم بدن که باعث جلوگیری و یا تغییر در داده‌های مربوط به‌سلامتی بیمار شود، می‌تواند خسارت‌های غیرقابل بازگشتی برای سلامتی بیمار به همراه داشته باشد. هدف این مقاله ارائهٔ یک سامانه تشخیص نفوذ هوشمند به‌منظور افزایش امنیّت سایبری شبکهٔ حسگر بی‌سیم بدن است.

ازآنجاکه در شبکه حسگر بی‌سیم بدن ارسال داده از طریق همه‌پخشی انجام می‌شود، هرگونه حملهٔ سایبری مانند استراق سمع، تغییر داده، جلوگیری از سرویس[3] و ... قابل انجام است. این‌گونه حملات علاوه‌برآن‌که موجب نقض حریم خصوصی بیمار می‌شود، می‌تواند منجر به تشخیص و درمان اشتباه شود[3, 4]. به‌دلیل محدودیت انرژی، حافظه و قدرت پردازشی گره‌ها در شبکه حسگر بی‌سیم بدن امکان استفاده از روش‌های سنتیِ تأمین امنیّت، مانند رمزنگاری و پروتکل‌های امن، وجود ندارد. به همین دلیل یکی از روش‌های تأمین امنیّت در شبکه حسگر بی‌سیم بدن استفاده از سامانه‌های تشخیص نفوذ است [5]. در سامانه‌های تشخیص نفوذ وظیفه هرگونه فعالیت گره‌های حسگر در شبکه نظارت می‌شوند.

تشخیص نفوذ یک پایش هوشمندانه در شبکه بر روی تمامی سامانه‌های کامپیوتری برای یافتن هرگونه تخطّی امنیّتی است. این سامانه‌ها به دو گروه مبتنی بر امضا و ناهنجاری تقسیم می‌شوند. یکی از مزیت‌های سامانه‌های مبتنی بر ناهنجاری تشخیص حملات روز صفر[4] است. برای پیاده‌سازی سامانه‌های تشخیص نفوذ مبتنی بر ناهنجاری می‌توان از روش‌های آماری، مبتنی بر دانش، داده‌کاوی، و یادگیری ماشین استفاده کرد[6].

این مقاله یک سامانه تشخیص نفوذ ترکیبی مبتنی بر ناهنجاری با استفاده از روش‌های یادگیری ماشین و داده‌کاوی پیشنهاد می‌دهد. سامانه تشخیص نفوذ پیشنهادی با هدف شناسایی حملات جلوگیری از سرویس پیشنهاد شده است. در این سامانه به‌منظور افزایش نرخ تشخیص، نخست داده‌های جمع‌آوری‌شده از شبکه تحلیل می‌شوند و در جریان آماده‌سازی قرار می‌گیرند. بدین ترتیب که با استفاده از الگوریتم ژنتیک، ویژگی‌هایی از ترافیک شبکه استخراج می‌شوند که ضمن توجه به مصرف انرژی گره‌ها موجب بالاترین نرخ تشخیص نفوذ می‌شوند. در مرحلهٔ دوم، از روش‌های طبقه‌بندی با نظارت (ماشین بردار پشتیبان[5] و k نزدیک‌ترین همسایه[6]) برای جداسازی بین ترافیک طبیعی شبکه و داده‌های گره مهاجم استفاده می‌شود. روش‌های بانظارت به علت دخالت انسان در مرحله یادگیری نسبت به روش‌های بدون نظارت از دقت بالاتری برخوردار هستند. خلاصهٔ نوآوری‌های این مقاله عبارت‌اند از:

۱- ارائهٔ یک روش مبتنی بر الگوریتم ژنتیک برای انتخاب بهترین ویژگی‌ها از میان داده‌های جمع‌آوری‌شده، به‌منظور بالا بردن نرخ تشخیص نفوذ در ترافیک شبکهٔ حسگر بی‌سیم بدن

[1] Wireless body area network (WBAN)
[2] Real time
[3] Denial of service attack (DoS)
[4] Zero day attack
[5] Support vector machine (SVM)
[6] K nearest neighbor

۲- ارائهٔ یک سامانه تشخیص نفوذ مبتنی بر ناهنجاری با استفاده از ترکیب الگوریتم ژنتیک و روش‌های طبقه‌بندی داده

این مقاله به‌صورت زیر ادامه داده می‌شود. بخش دوم مقاله به‌مرور پژوهش‌های پیشین می‌پردازد. در بخش سوم، مفاهیم پایه شامل معماری شبکه‌های حسگر بی‌سیم بدن، انواع حمله در آنها، و سامانه‌های تشخیص نفوذ بررسی شده‌اند. الگوی پیشنهادی برای تشخیص نفوذ در بخش چهارم ارائه می‌شود. بخش پنجم نحوهٔ ارزیابی و نتایج شبیه‌سازی را نشان می‌دهد. در بخش ششم نتایج حاصل از این مقاله آورده شده است.

۲- پژوهش‌های پیشین

مصطفی صباح و همکاران [7] بازبینی مناسبی بر روی شبکهٔ حسگر بی‌سیم بدن انجام داده‌اند. در این بازبینی، کاربردها، مشخصات، تعداد گره، انواع گره، توپولوژی، امنیّت، حریم خصوصی و انواع تهدیدهای شبکهٔ حسگر بی‌سیم بدن بررسی شده است. در همین راستا، دودانگه و همکاران [8] نیز جنبه‌های امنیّتی شبکه‌های حسگر بی‌سیم بدن و اولویت آن‌ها را بررسی کرده‌اند.

راه‌حل‌های ارتباطی که در یک شبکه حسگر بی‌سیم بدن استفاده می‌شوند، شامل(ZigBee) IEEE 802.15.4، بلوتوث با انرژی کم، و IEEE 802.15.6 هستند [9]. پروتکل ZigBee برای ارتباط‌های بی‌سیم کوتاه‌برد، شبکه‌های با نرخ بیت پایین، و انرژی کم پیشنهاد می‌شود. بلوتوث با انرژی کم (BT LE) با هدف استفاده از بلوتوث و انرژی کمتر در سال ۲۰۱۰ طراحی و پیشنهاد شد. پروتکل IEEE 802.15.6 نیز در سال ۲۰۱۲ برای ارتباط‌های بی‌سیم در مجاورت و درون بدن طراحی و پیشنهاد شده است. محمد عثمان و همکاران [10] نیز شبکه‌های حسگر بی‌سیم بدنی را از زاویهٔ انتقال داده بررسی کرده‌اند. ایشان انتقال داده را در این شبکه به چهار بخش (۱) جمع‌آوری داده توسط حسگر، (۲) انتقال به گره سینک یا چاهک، (۳) انتقال به دروازهٔ اینترنت، و (۴) انتقال به پزشک، تقسیم کرده‌اند و سپس به بررسی تهدیدهای امنیّتی هر بخش پرداخته‌اند.

ازآنجاکه حسگرهای قرارگرفته بر روی بدن بیمار ممکن است از دقّت کافی در اندازه‌گیری برخوردار نباشند، ضروری است تا مقادیر اندازه‌گیری‌شده توسط حسگرها بررسی شوند. هرگونه مقدار اندازه‌گیری‌شدهٔ اشتباه می‌تواند منجر به ایجاد یک هشدار اشتباه برای بیمار و پزشک شود. عثمان سالم و همکاران [11] به‌منظور جداسازی بین مقادیر اندازه‌گیری‌شده درست و اشتباه از فیلتر کالمن استفاده کرده‌اند. ایشان از فیلتر کالمن برای پیش‌بینی مقدار اندازه‌گیری توسط حسگر استفاده می‌کنند. با محاسبهٔ مقدار همگرایی بین این دو مقدار و پایش دیگر جنبه‌های سلامتی بیمار، می‌توانند مقادیر اندازه‌گیری‌شدهٔ اشتباه را شناسایی کنند. آلراجه و همکاران [12] یک سامانه تشخیص نفوذ طراحی کرده‌اند که در این سامانه از داده‌های ویژه‌ای به نام WSN_DS استفاده شده است. WSN-DS نام داده‌هایی است که نویسندگان با شبیه‌سازی شبکه WSN آن‌ها را برای چهار نوع حمله جلوگیری از سرویس به دست آورده‌اند. در این شبیه‌سازی از پروتکل LEACH که یکی از پرطرفدارترین پروتکل‌های شبکه حسگر بی‌سیم است، استفاده شده است. مهم‌ترین هدف این مقاله ایجاد یک مجموعه-دادهٔ[1] ویژه برای سامانه تشخیص نفوذ در شبکه‌های حسگر بی‌سیم است. نویسندگان معتقدند که مجموعه-داده‌هایی که تاکنون استفاده‌شده، مانند KDDCUP یک مجموعه-دادهٔ عمومی هستند و برای شبکه‌های حسگر بی‌سیم نباید از آن‌ها استفاده کرد. لطیف و همکاران [13] یک سامانه تشخیص نفوذ مبتنی بر الگوریتم درخت تصمیم ارائه کرده‌اند. در این مقاله فرض شده که شبکهٔ حسگر بی‌سیم بدن مبتنی بر ابر[2] بوده و برای مراقبت‌های بهداشتی استفاده می‌شود. به همین دلیل نویسندگان از حملهٔ جلوگیری از سرویس توزیع‌شده برای شبیه‌سازی حمله استفاده کرده‌اند و سامانه تشخیص نفوذ خود را برای آن طراحی کرده‌اند. جی‌ها [14] با افزودن یک دستگاه خارجی به شبکهٔ حسگر بی‌سیم بدن، به نام MEDMON امنیّت آن را تأمین کرده‌اند. این دستگاه برای هر دو مرحله دادهٔ آزمایشی و دادهٔ واقعی در نزدیک محل شبکهٔ حسگر بی‌سیم قرارگرفته و برای بیمارهای مختلف آموزش می‌بینند. بدین ترتیب می‌تواند میان ویژگی‌های رفتاری شبکه‌های حسگر بی‌سیم بدن اولویت‌بندی کرده و رفتار عادی و ناهنجار را طبقه‌بندی کند. MEDMON برای تشخیص ناهنجاری، سیگنال‌های موجود در شبکهٔ حسگر بی‌سیم، بدن را نظارت کرده و بعد از تحلیل آن‌ها تشخیص می‌دهد که ترافیک موجود، مربوط به یک ترافیک عادی است یا به یک ترافیک ناهنجار تعلق دارد. تامیلاراسو و همکاران [15] یک معماری تشخیص نفوذ توزیع‌شده را برای امنیّت شبکه‌های حسگر بی‌سیم ارائه

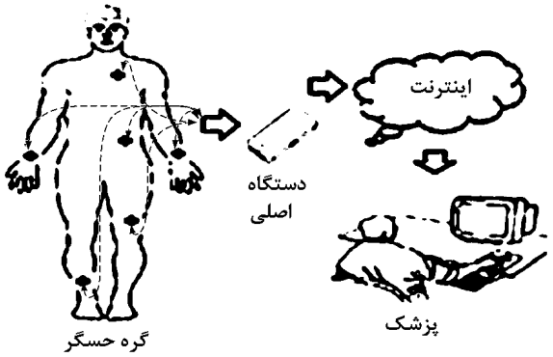
[1] Dataset
[2] Cloud

داده‌اند. معماری ارائه‌شده بر این اساس است که گره‌های محلی بتوانند به‌صورت خودمختار حملات محلی خود را تشخیص دهند. این در حالی است که گره دروازه یا چاهک می‌تواند حملات کلی را در نظر بگیرد. عملکرد این سامانه در مقایسه‌های انجام‌شده نشان داده است که بین ۶ تا ۹ درصد امنیّت شبکه حسگر بی‌سیم بدن را افزایش داده است. یاتینگ و همکاران [16] یک تابع مسیریابی با بیشینه‌کردن مقدار تابع هزینه به منظور انتخاب گره بعدی را به‌صورت پویا پیشنهاد کرده‌اند. روش پیشنهادی علاوه‌بر افزایش قابلیت اطمینان انتقال داده مصرف انرژی گره را کاهش و طول عمر شبکه را افزایش می‌دهد. نبوی و همکاران [17] یک مسیریابی مبتنی بر دمای حسگر بی‌سیم و خوشه‌بندی با استفاده از الگوریتم کلونی مورچه‌ها ارائه داده‌اند. نویسندگان برای یافتن سرخوشهٔ مناسب، از انرژی باقیمانده در گره و دمای گره حسگر به عنوان شاخصه‌های تابع هزینه استفاده می‌کنند. بیلندی و همکاران [18] یک پروتکل مسیریابی با استفاده از الگوریتم بهینه‌سازی ازدحام ذرات ارائه کرده‌اند. در این روش انتخاب گره فرستنده بر اساس فاصله و انرژی باقی‌ماندهٔ گره‌ها محاسبه می‌شود. نویسندگان نشان داده‌اند که روش پیشنهادی تعادلی بین تعداد حداقلی گره‌های فرستنده و افزایش بازده انرژی و طول عمر شبکه برقرار کرده‌اند. جدول (۱) خلاصه‌ای از سامانه‌های تشخیص نفوذ ارائه‌شده برای شبکه‌های حسگر بی‌سیم بدن را نشان می‌دهد.

(جدول- ۱): سامانه‌های تشخیص نفوذ شبکه‌های حسگر بی‌سیم بدن

(Table 1): Intrusion Detection System for WBAN.

منبع	سال	طبقه‌بندی‌کننده	مجموعه داده/ شبیه ساز	نوع حمله	نرخ تشخیص/
[24]	2016	Naive Bayes	NSLKDD	U2R, R2L, Probe, DoS	98.00
[25]	2016	SVM	NSLKDD	U2R, R2L, Probe, DoS	97.03
[26]	2017	Deep Learning	NSLKDD	U2R, R2L, Probe, DoS	84.86
[27]	2017	DT, SVM, RF, NBC, KNN	Castalia	Data Falsif-ication, DoS, Listening	97.21
[28]	2018	RNN	NSLKDD	U2R, R2L, Probe, DoS	85.43
[29]	2019	NN	NSLKDD	U2R, R2L, Probe, DoS	98.02
[30]	2020	SVM, KNN, DT, RF	N/A	MITM, replay false data injection , DoS	98.4
[31]	2020	RF, KNN, ANN, SVM	N/A	MITM attacks	N/A
[32]	2021	Deep Learning	NSL-KDD, CSE-CIC-IDS2018	U2R, R2L, Probe, DoS	98.81
[33]	2022	RF & robust scaling	NSL-KDD	U2R, R2L, Probe, DoS	94.23



(شکل-۱): معماری شبکه حسگر بی‌سیم بدن

(Figure 1): WBAN architecture.

۳- مفاهیم پایه

۳-۱- معماری شبکه‌های حسگر بی‌سیم بدن

شکل (۱) معماری شبکه‌های حسگر بی‌سیم بدن را نشان می‌دهد. در این معماری، حسگرهای بی‌سیم (از نوع پوشیدنی یا کاشته‌شده روی بدن انسان) اطلاعات سلامتی و حیاتی بدن انسان را پایش، جمع‌آوری، و آن‌ها را به یک دستگاه اصلی (گره میانی) ارسال می‌کنند تا در نهایت در اختیار پزشک قرار گیرند[19, 20].

اگرچه ممکن است به نظر آید که معماری شبکه‌های حسگر بی‌سیم بدن شبیه به شبکه‌های حسگر است، اما تفاوت‌های مختلفی بین آن‌ها وجود دارد. جدول (۲) تفاوت‌های این دو شبکه را نشان می‌دهد. همین اختلاف‌ها منجر می‌شود تا امنیّت در شبکه‌های حسگر بی‌سیم بدن نسبت به شبکه‌های حسگر متمایز شود [21].

(جدول- ۲): تفاوت شبکه‌های حسگر بی‌سیم و حسگر بی‌سیم بدن

(Table 2): Difference of WANs and WBANs.

نوع اختلاف	شبکه‌های حسگر بی‌سیم بدن	شبکه‌های حسگر بی‌سیم
تعداد گره	تعداد گره‌ها محدود است	تعدادگره‌ها زیاد و بصورت متراکم هستند
دقت در نتیجه	از بین رفتن یک گره خطرناک است	از بین رفتن چند گره تاثیر چندانی ندارد
خصوصیت گره‌ها	ناهمگن	همگن
کیفیت خدمات	تحمل از بین رفتن بسته‌ها را ندارد	از بین رفتن بسته‌ها قابل جبران است
مقیاس حمله	کم است	زیاد است

۳-۲- حمله در شبکه‌های حسگر بی‌سیم بدن

حملات متفاوتی در شبکه‌های حسگر بی‌سیم بدن قابل‌اجرا است که در ادامه به برخی از آن‌ها به‌اختصار اشاره می‌شود[22]:

حملهٔ ارسال انتخابی[1]: این حمله شامل گره مهاجمی است که از رسیدن بسته‌ها به دستگاه اصلی جلوگیری می‌کند.

حمله تزریق دادهٔ کاذب[2]: در این نوع حمله گره مخرب، داده‌هایی برخلاف داده‌های حس‌شده توسط حسگر را به دستگاه اصلی ارسال می‌کند.

حملهٔ سیبل[3]: در این حمله گره مهاجم تغییر قیافه داده و به‌عنوان یکی از مجموعه گره‌های متعدد شبکه معرفی می‌شود.

حملهٔ حفره[4]: در این حمله گره ناهنجار، خود را به‌عنوان یک گره با منابع زیاد معرفی می‌کند تا حسگرهای دیگر بسته‌های خود را از طریق مسیر گره ناهنجار عبور دهند.

حملهٔ استراق سمع[5]: در این حمله گره مهاجم، با استفاده از یک آنتن قوی، می‌تواند به داده‌های ارسالی از دیگر گره‌های حسگر بی‌سیم بدن گوش‌داده و بدین ترتیب، تمامی داده‌ها را سرقت کند.

حملهٔ زمان‌بندی[6]: این حمله هنگام تنظیم زمان‌بندی پروتکل ارتباطی انجام می‌شود. برای مثال، در پروتکل تقسیم زمانی[7] گره مخرب، زمان ارسال بسته را برای تمامی گره‌ها یکسان قرار می‌دهد. بدین ترتیب بسته‌های ارسالی به‌علت تصادم از بین خواهند رفت.

حملهٔ جلوگیری از سرویس[8]: حملهٔ جلوگیری از سرویس عبارت از انواع تلاش‌هایی است که یک گره مهاجم انجام می‌دهد تا یک گره دیگر نتواند خدماتی را به سایر گره‌ها ارائه دهد. روش‌های ایجاد حملهٔ جلوگیری از سرویس می‌تواند متفاوت باشد. برای مثال، یک مهاجم می‌تواند با استفاده از مصرف بیش‌ازحد منابع یک گره (مانند پردازشگر یا حافظه) به آن گره آسیب برساند. همین‌طور گره مهاجم می‌تواند با در دست گرفتن کنترل شبکه، ترافیک زیادی را بر روی شبکه بارگذاری کند تا بدین ترتیب از رسیدن بسته‌های دیگر (بسته‌هایی که مربوط به علائم حیاتی بیمار هستند)، به مقصد جلوگیری کرده و موجب از دست رفتن آن‌ها شود.

[1] Selective forwarding attack
[2] False data injection attack
[3] Sybil attack
[4] Hole attack
[5] Eavesdropping attack
[6] Scheduling attack
[7] Time division modulation (TDM)
[8] Denial of service attack

در شبکه‌های حسگر بی‌سیم بدن از سه نوع حملهٔ معروف جلوگیری از سرویس به شرح زیر می‌توان استفاده کرد:

حملهٔ حفره سیاه[9]: در حملهٔ حفره سیاه گره مهاجم از آغاز خود را به‌عنوان گره چاهک معرفی می‌کند. بدین ترتیب گره مهاجم می‌تواند تمامی بسته‌های دریافتی را از بین ببرد.

حملهٔ حفره خاکستری[10]: در این حمله گره مهاجم مانند حمله حفرهٔ سیاه خود را به‌عنوان گره چاهک معرفی کرده، با این تفاوت که بسته‌های دریافتی را به‌صورت انتخابی و یا تصادفی از بین می‌برد.

حملهٔ سیل‌آسا[11]: در این حمله گره مهاجم بسته‌های اطلاعاتی را به‌صورت سیل‌آسا به‌سمت گره قربانی ارسال می‌کند. دریافت و پردازش بسته‌های سیل‌آسا به‌وسیلهٔ گره قربانی علاوه‌بر آنکه مصرف انرژی گره را افزایش می‌دهد، موجب پر شدن بافر ورودی گره شده و امکان دریافت بسته‌های جدید را از بین خواهد برد.

۳-۳- سامانه تشخیص نفوذ

سامانه تشخیص نفوذ یکی از پاسخ‌های امنیّتی به حملات سایبری در شبکه‌های رایانه‌ای‌ست. یک سامانه تشخیص نفوذ شامل مجموعه‌ای از ابزارها، روش‌ها، و منابعی است که هرگونه فعالیت غیرمجاز یا تأییدنشده را به‌عنوان نفوذ به شبکه اعلام کرده و ممکن است برای آن یک هشدار تولید کند. از یک سامانه تشخیص نفوذ به‌عنوان خط دوم دفاع از حمله در شبکه‌های حسگر بی‌سیم بدن استفاده می‌شود، این بدان علت است که روش‌های پیش‌گیری از حمله (مانند رمزگذاری، احراز هویت، کنترل دسترسی و ...) به‌عنوان نخستین خط دفاع در برابر حملات، هیچ‌گاه نمی‌توانند به‌طور صددرصد از حملات جلوگیری کنند؛ بنابراین سامانه‌های تشخیص نفوذ این اطمینان را ایجاد می‌کنند که اگر در شبکه گره مهاجمی وجود داشته باشد، آن را شناسایی و به مدیر شبکه اعلام کند.

یک سامانه تشخیص نفوذ از بخش‌های زیر تشکیل‌شده است [23]:

[9] Blackhole attack
[10] Grayhole attack
[11] Flooding attack

۱) واحد پایش[1]: این واحد وظیفهٔ پایش فعالیت‌های داخلی، الگوی ترافیکی، و بهره‌وری منابع سامانه را به عهده دارد.

۲) واحد تحلیل: این واحد وظیفه تحلیل رفتار عادی و غیرعادی تمامی گره‌ها را به عهده دارد.

۳) واحد تشخیص: این واحد به‌عنوان مهم‌ترین واحد شناخته شده و وظیفه اصلی آن تصمیم‌گیری در مورد شناسایی رفتارهای مخرب است.

سه واحد دیگر نیز، به‌عنوان واحدهای اختیاری و مکمل، ممکن است در سامانه‌های تشخیص نفوذ استفاده شوند.

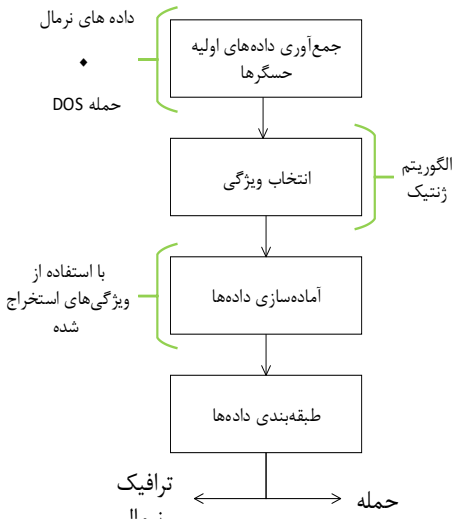
۴) واحد ثبت وقایع: این واحد وظیفه ثبت بسته‌های مخرب را، به‌منظور تحلیل بیشتر به عهده دارد.

۵) واحد هشدار: این واحد هنگام شناسایی یک رفتار مخرب، با ایجاد هشدار مدیر سامانه را مطلع می‌کند.

۶) واحد جلوگیری: در سامانه‌های تشخیص نفوذ پیشرفته پس از شناسایی یک رفتار مخرب، این واحد وظیفهٔ جلوگیری از حمله شناخته‌شده را دارد. برای مثال، این کار می‌تواند با خروج گره مخرب از شبکه انجام شود.

۴- الگوی پیشنهادی سامانهٔ تشخیص نفوذ

شکل (۲) معماری سامانه تشخیص نفوذ پیشنهادی را نشان می‌دهد. همان‌طورکه مشاهده می‌شود (۱)، پس از جمع‌آوری داده‌های اولیه (شامل ترافیک طبیعی و ترافیک حمله جلوگیری از سرویس) (۲) داده ها تحلیل شده تا ویژگی‌های موردنیاز جهت افزایش کارایی[2] سامانه تشخیص نفوذ استخراج شوند. این ویژگی‌ها باید به‌نحوی تعیین شوند که شامل بیشترین اطلاعات جهت پایش و تحلیل نفوذ در شبکه باشند. ویژگی‌های تکراری و کم‌ارزش موجب افزایش سربار محاسباتی و پیچیدگی سامانه می‌شوند. به همین دلیل، انتخاب ویژگی یکی از مهم‌ترین عملیات در یک سامانه تشخیص نفوذ است. با توجه به ویژگی‌های خاص شبکه‌های بی‌سیم بدن، ویژگی‌های موردنیاز سامانه تشخیص نفوذ باید به‌نحوی انتخاب شوند که ضمن افزایش نرخ تشخیص درست[3]، موجب کاهش نرخ هشدار اشتباه[4]، و مصرف انرژی در گره‌ها شود. از آنجا که الگوریتم ژنتیک یکی از بهترین روش‌های یادگیری آسان و کارآمد برای انتخاب ویژگی است، در الگو پیشنهادی با استفاده از الگوریتم ژنتیک و تابع برازش تعریف‌شده، ویژگی‌های مورد نظر از بین داده‌ها استخراج می‌شوند. (۳) در مرحلهٔ سوم با توجه به ویژگی‌های استخراج‌شده، داده‌ها آماده می‌شوند تا در مرحلهٔ آخر (۴) با استفاده از یکی از روش‌های طبقه‌بندی داده‌ها، ترافیک طبیعی از ترافیک حمله تشخیص داده شود. در الگو پیشنهادی از حملهٔ سیل‌آسا برای ایجاد حمله جلوگیری از سرویس استفاده شده است. شکل (۳) الگوریتم پیاده‌سازی آن را نشان می‌دهد.



شکل (۲): معماری سامانه تشخیص نفوذ پیشنهادی

(Figure 2): The proposed IDS architecture.

```
NN: Normal Node
MN: Malicious Node
SN: Sink Node
SNB: Sink Node Buffer
RDA: Random Duration of the Attack
WHILE (RDA != 0)
    MN broadcasts many messages with
    high transmitting power
    RDA = RDA -1
ENDWHILE
IF (SNB = FULL)
    SN drops packets
ELSE IF
    SN receives packets
ENDIF
```

شکل (۳): الگوریتم پیاده‌سازی حملهٔ سیل‌آسا

(Figure 3): Flooding attack algorithm

۴-۱- تابع برازش چندهدفه

با توجه به ویژگی‌های شبکه حسگر بی‌سیم بدن، شاخصه‌های زیر برای افزایش کارایی سامانه تشخیص نفوذ پیشنهادی در نظر گرفته‌شده‌اند:

[1] Monitoring
[2] Performance
[3] Detection rate
[4] False alarm rate

الف) انرژی مصرفی: میزان مصرف انرژی همواره به‌عنوان یکی از شاخص‌های حیاتی در شبکه‌های حسگر بی‌سیم بدنی است. در شبکهٔ حسگر بی‌سیم بدن انرژی مصرفی هر گره عبارت است از انرژی محاسباتی یا پردازشی، به‌علاوهٔ انرژی موردنیاز جهت انتقال بسته‌های اطلاعاتی. بدین ترتیب روابط (۱) و (۲)، نحوهٔ محاسبهٔ انرژی مصرفی هر گره را نشان می‌دهند.

$$E_{Node}^{Total} = \alpha.E^{Comp} + \beta.E^{Comm} \quad (۱)$$

$$E^{Comm} = (E^{Trans} + E^{Rece} + E^{Idle}) \quad (۲)$$

در این رابطه E^{Comp} انرژی محاسباتی، E^{Comm} انرژی ارتباطی[1] که شامل انرژی انتقال E^{Trans}، انرژی دریافت E^{Rece}، و انرژی حالت بیکاری E^{Idle} است. α و β ضرایب ثابت هستند که برای هر گره می‌تواند مقدار متفاوتی داشته باشد.

ب) نرخ تشخیص درست: نرخ تشخیص یکی از شاخص‌های مهم برای ارزیابی یک سامانه تشخیص نفوذ است. به این منظور می‌توان از رابطه (۳) استفاده کرد:

$$DR = TP/(TP + FN) \quad (۳)$$

در این رابطه TP[2] تعداد حملاتی است که درست تشخیص داده‌شده و FN[3] تعداد حملاتی است که تشخیص داده نشده است.

ج) نرخ هشدار اشتباه: یکی دیگر از شاخص‌های مهم برای ارزیابی یک سامانه تشخیص نفوذ، نرخ هشدار اشتباه است. برای این منظور می‌توان از رابطه (۴) استفاده کرد:

$$FAR = FP/(FP + TN) \quad (۴)$$

در این رابطه FP[4] تعداد بسته‌های سالم است که به‌اشتباه حمله تشخیص داده‌شده و TN[5] تعداد بسته‌های سالم است که به‌درستی به‌عنوان بستهٔ سالم شناسایی‌شده‌اند.

بدین ترتیب با توجه به شاخص‌های تعریف‌شده و مجموعه ویژگی‌های ارائه‌شده، تابع برازش چندهدفهٔ نهایی با حداقل کردن مقادیر شاخص‌های روابط (۱) و (۴) و حداکثر کردن شاخص رابطهٔ (۳) به‌صورت زیر تعریف می‌شود:

$$F = \max(DR)/\min(E_{Node}^{Total}, FAR) \quad (۵)$$

به‌عبارت‌دیگر، تابع برازش چندهدفه را می‌توان به‌صورت حداکثری زیر نوشت:

$$F = \max(DR, -E_{Node}^{Total}, -FAR) \quad (۶)$$

۲-۴- انتخاب ویژگی با استفاده از الگوریتم ژنتیک

با توجه به تابع برازش چندهدفهٔ تعریف‌شده، در این بخش برای انتخاب ویژگی از الگوریتم NSGA-II به شرح زیر استفاده می‌شود:

الف) ایجاد جمعیت اولیه: جمعیت اولیه با استفاده از جمع‌آوری اطلاعات از تمامی گره‌های همسایه و نمایش کروموزوم‌ها به دست می‌آید. به‌منظور انتخاب ویژگی‌های مناسب در هر کروموزوم، هر بیت نشان‌دهندهٔ یک ویژگی است به‌نحوی‌که با یک کردن بیت مربوط، آن ویژگی انتخاب و با صفر شدن آن، ویژگی در نظر گرفته نخواهد شد. در آغاز سامانه تشخیص نفوذ، داده‌هایی مانند تعداد بیت‌های ارسالی، دریافتی، از بین رفته و ... مربوط به گره‌ها را در شبکهٔ جمع‌آوری و آن‌ها را در قالب یک کروموزوم نمایش می‌دهد. شکل (۴) ساختار یک کروموزوم ۳۲ بیتی را برای این منظور نشان می‌دهد.

ب) محاسبهٔ معیار برازندگی: این مرحله با استفاده از تابع برازش چندهدفه انجام می‌شود.

ج) مرتب‌سازی جمعیت: بر اساس الگوریتم ارائه‌شده، هر جواب x بر جواب y در صورتی غالب است که شرایط زیر برای آن برقرار باشد:

- جواب x بدتر از جواب y در هیچ‌یک از توابع هدف نباشد.
- جواب x حداقل در یکی از توابع هدف بهتر از y باشد.

د) محاسبهٔ فاصلهٔ ازدحامی و انتخاب: هر جواب x نسبت به y در صورتی پذیرفته می‌شود که:

- جواب x دارای رتبه نامغلوب (r_x) بهتری باشد. به‌عبارت‌دیگر $(r_x < r_y)$
- چنانچه دو جواب دارای رتبهٔ یکسانی باشند، جوابی انتخاب می‌شود که دارای فاصلهٔ ازدحام (d) بیشتری باشد.

فاصلهٔ ازدحام فاکتوری برای انتخاب جواب بهتر از نظر پراکندگی است $(r_x = r_y, d_x > d_y)$. برای محاسبهٔ فاصله ازدحام از روابط زیر استفاده می‌شود:

$$d_k^1 = (f_1(x_{k+1}) - f_1(x_{k-1}))/(f_1^{\max} - f_1^{\min}) \quad (۷)$$

$$d_k^2 = (f_2(x_{k+1}) - f_2(x_{k-1}))/(f_2^{\max} - f_2^{\min}) \quad (۸)$$

$$d_k^3 = (f_3(x_{k+1}) - f_3(x_{k-1}))/(f_3^{\max} - f_3^{\min}) \quad (۹)$$

$$d_k = d_k^1 + d_k^2 + d_k^3 \quad (۱۰)$$

[1] Communication
[2] True positive
[3] False negative
[4] False positive
[5] True negative

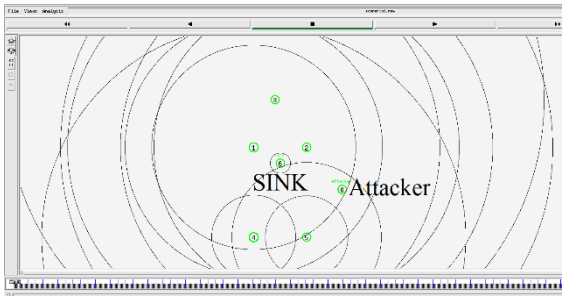
در این روابط x_k جواب k ام، d_k^1 فاصله ازدحام جواب k ام برای تابع هدف اول، d_k^2 فاصله ازدحام جواب k ام برای تابع هدف دوم، d_k^3 فاصله ازدحام جواب k ام برای تابع هدف سوم، و d_k فاصله ازدحام جواب k ام است.

ه) تقاطع: در این مرحله هر دو تقاطع تک‌نقطه‌ای و دو نقطه‌ای برای انتخاب کروموزوم‌ها از جمعیت قابل انجام است.

و) جهش: برای ایجاد فرزندان جدید

ز) تلفیق: تلفیق جمعیت به‌دست‌آمده با جمعیت قبلی

ح) جایگزینی: با توجه به ویژگی‌های ارائه‌شده، در این مرحله بهترین اعضای جمعیت به‌دست‌آمده با جمعیت والدین جایگزین می‌شوند. روش جایگزینی بدین‌صورت است که نخست، اعضای رتبه‌های پایین‌تر جایگزین والدهای قبلی می‌شوند و سپس بر اساس فاصلهٔ ازدحامی مرتب می‌شوند.



(شکل-۵): محیط شبیه‌سازی شده شبکهٔ حسگر بی‌سیم بدن

(Figure 5): Simulated environment of WBAN.

۵- راستی‌آزمایی و نتایج شبیه‌سازی

۵-۱- محیط شبیه‌سازی

به‌منظور شبیه‌سازی شبکه‌های حسگر بی‌سیم بدن از شبیه‌ساز *NS2_v2.35* بر روی سامانه‌عامل *Ubuntu Linux16.04 LTS* استفاده شده است. شبکهٔ شبیه‌سازی‌شده شامل هفت عدد گره حسگر بی‌سیم بدن است که از بین آن‌ها شش عدد در شبکهٔ اصلی قرارگرفته و یکی از آن‌ها به‌عنوان گره مهاجم در نظر گرفته‌شده‌است.

شکل (۵) محیط شبیه‌سازی‌شده و شکل (۶) شاخص‌های درنظرگرفته‌شده برای شبکهٔ حسگر بی‌سیم بدن را نشان می‌دهند. در این شکل گره شمارهٔ صفر گره مهاجم، گره شمارهٔ شش گره چاهک و باقی گره‌ها حسگرهای شبکه هستند. گره مهاجم با استفاده از حملهٔ سیل‌آسا وظیفهٔ ایجاد ناهنجاری در شبکه را به عهده دارد. جدول (۳) شاخص‌های در نظر گرفته‌شده برای محیط شبیه‌سازی را نشان می‌دهد. همان‌طورکه مشاهده می‌شود، از پروتکل *AODV* در لایهٔ شبکه و از پروتکل *Zigbee* در لایهٔ پیوند استفاده شده است. به‌منظور کاهش مصرف انرژی ماژول تشخیص نفوذ برای جمع‌آوری اطلاعات تنها در گره چاهک قرار داده شده است. ازآنجاکه هدف اصلی مقاله ارائهٔ یک سامانه تشخیص نفوذ است، فرض بر آن است که تمامی گره‌ها از انرژی کافی برخوردارند.

۵-۲- جمع‌آوری داده و انتخاب ویژگی

بعد از شبیه‌سازی گره‌های حسگر، گره چاهک، و گره مهاجم، نوبت به جمع‌آوری داده، شبیه‌سازی حمله، و انتخاب ویژگی با استفاده از الگوریتم پیشنهادی می‌رسد. همان‌طورکه پیش‌تر گفته شد، در این مقاله از حملهٔ سیل‌آسا برای شبیه‌سازی حملهٔ جلوگیری از سرویس استفاده شده است. برای این منظور لازم است تا برخی از فایل‌های شبیه‌ساز *NS2* مانند *AODV.cc* تغییر داده شوند. به‌منظور جمع‌آوری داده از برنامه‌نویسی به زبان *AWK*، که بر روی پردازش متن متمرکز است، و ویژهٔ خروجی گرفتن از شبیه‌ساز *NS2*، استفاده شده است. همچنین، نرم‌افزار متلب ۲۰۱۵ برای انتخاب ویژگی استفاده شده است. برای آسانی بیشتر ضرایب α, β برابر ۱ فرض شده‌اند. جدول (۴) بهترین ویژگی‌های انتخاب‌شده از میان ترافیک داده‌ها را نشان می‌دهد. پس از انتخاب ویژگی، نوبت به آماده‌سازی داده‌های جمع‌آوری‌شده با توجه به ویژگی‌های انتخابی می‌رسد. شکل (۷) نمونه‌ای از داده‌های آماده‌سازی‌شده برای ویژگی‌های انتخابی را نشان می‌دهد.

11	10	9	8	7	6	5	4	3	2	1	0
SE						DR					
	Send Packets						Drop Packets				
23	22	21	20	19	18	17	16	15	14	13	12
						RE					
Acknowledged Packets							Received Packets				
				31	30	29	28	27	26	25	24
				FR							AC
					Forwarded Packets						

(شکل- ۴): ساختار کروموزوم

(Figure 4): Chromosome structure.

```
# ======================================================================
# Define options
# ======================================================================
set val(chan)           Channel/WirelessChannel    ;# Channel Type
set val(prop)           Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)          Phy/WirelessPhy/802_15_4
set val(mac)            Mac/802_15_4
set val(ifq)            Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)             LL                         ;# link layer type
set val(ant)            Antenna/OmniAntenna        ;# antenna model
set val(ifqlen)         20                         ;# max packet in ifq
set val(nn)             7                         ;# number of mobilenodes
set val(rp)             AODV                       ;# routing protocol
set val(x)              200
set val(y)              200
```

(شکل- ۶): شاخص‌های تعریف‌شده برای شبکهٔ حسگر بی‌سیم بدن

(Figure -6): Defined parameters of the WBAN

time	send	recv	drop	enLN	AODV	cbr	packetsize	avgAB
2.00226	31	89	11	8899.41	95	18	5239	44.2524
3.0023	72	126	19	12596.3	73	92	6020	50.7131
4.00403	93	105	17	10493.7	38	177	6867	53.2925
5.00527	32	30	1	2997.49	0	63	1904	54.8209
6.00591	35	31	1	3097.03	0	67	2014	56.1825
7.00739	32	26	4	2597.2	0	62	1903	57.0982
8.00899	34	30	2	2996.43	0	66	2002	57.849
9.05194	34	33	0	3295.65	0	67	2025	58.3737
10.0526	33	25	4	2496.41	0	62	1919	58.7693
11.0538	33	32	1	3195.03	0	66	2000	59.1041
12.0544	47	68	9	6787.93	14	68	5714	58.7085
13.1	33	29	63	2894.58	0	95	33577	58.9946
14.1	33	27	63	2694.64	0	93	32539	59.2458
15.1	33	31	61	3093.49	0	95	32575	59.4682
16.1	33	29	62	2893.56	0	94	32557	59.6665
17.1023	34	27	56	2693.69	0	90	28489	59.8669
18.1038	33	32	1	3192.13	0	66	2000	60.026
19.1516	34	31	1	3091.99	0	66	2007	60.1982
20.1519	34	29	3	2892.16	0	66	2025	60.3204
21.1539	32	30	1	2991.51	0	63	1918	60.4216
22.1542	33	31	1	3090.86	0	65	1975	60.5318
23.1569	34	29	2	2891.11	0	65	1989	60.6497
24.1602	33	33	0	3289.48	0	66	1993	60.7429
25.2013	34	32	1	3189.39	0	67	2039	60.7945
26.2013	33	31	1	3089.34	0	65	1968	60.9239
27.2027	33	30	2	2989.32	0	65	1996	60.9519
28.2032	33	29	2	2889.32	0	64	1943	61.0678
29.2066	34	27	3	2689.74	0	64	1976	61.1022
30.2507	34	32	1	3187.46	0	67	2039	61.1764
31.251	33	29	2	2888.28	0	64	1955	61.2342
32.2526	33	33	0	3286.26	0	66	1993	61.2888
33.2532	33	26	4	2588.87	0	63	1930	61.3787
34.3003	34	33	24	3285.47	0	91	8421	61.4626
35.3003	41	45	33	4479.16	18	80	16330	61.4006
36.3013	33	29	82	2886.42	0	104	35745	61.469
37.3016	33	31	81	3085.11	0	105	35761	61.5448
38.3026	33	31	81	3084.74	0	105	35757	61.6273
39.3026	34	26	84	2586.91	0	104	35766	61.6946
40.3045	33	25	52	2487.13	0	86	22187	61.7597
41.351	34	33	0	3282.61	0	67	2011	61.8305
42.3519	33	29	2	2884.37	0	64	1943	61.8897

(شکل- ۷): نمونه‌ای از داده‌های آماده‌شده با توجه به ویژگی‌ها

(Figure 7): Sample of data prepared according to

(جدول-۳): شاخص‌های شبیه‌سازی در NS2

(Table -3): Simulation parameters in NS2

شاخصه	مقدار
نوع کانال	بی‌سیم
الگو انتشار	TwoRayGround
پروتکل Mac	Zigbee, IEEE 802.15.4
نوع صف	اولویتی
اندازهٔ صف	۲۰
نوع لایهٔ پیوند	LL
تعداد گره‌ها	۷
اندازهٔ شبکه	۲۰۰*۲۰۰
پروتکل مسیریابی	AODV

(جدول-۴): ویژگی‌های انتخاب‌شده

(Table -4): Selected features

عنوان ویژگی	توضیح
SEND	تعداد بسته‌های فرستاده‌شده
RECV	تعداد بسته‌های دریافت‌شده
DROP	تعداد بسته‌های که در شبکه به دلایلی از بین رفته‌اند
ENLN	مقدار انرژی باقی‌مانده گره سینک (ژول)
AODV	تعداد بسته‌های مربوط به پروتکل مسیریابی
CBR	تعداد بسته‌های مربوط به نوع ترافیک استفاده‌شده
PACKETSIZE	اندازه بسته‌ها
AVGAB	میانگین فاصلهٔ فرستنده به گره سینک

(جدول-۵): نتایج طبقه‌بندی ماشین بردار پشتیبان با هستهٔ خطی

(Table 5): Classification by SVM with Linear Kernel

SVM (Linear)	*FP*	*FN*	*TP*	*TN*	D^{Rate}
Test Data	9	6	14	0	0.4828
Train Data	7	15	164	83	0.9182

(جدول-۶): نتایج طبقه‌بندی ماشین بردار پشتیبان با هستهٔ MLP

(Table -6): Classification by SVM with Polynomial Kernel

SVM (MLP)	*FP*	*FN*	*TP*	*TN*	D^{Rate}
Test Data	9	6	14	0	0.4828
Train Data	48	30	123	68	0.71

(جدول-۷): نتایج طبقه‌بندی ماشین بردار پشتیبان با هستهٔ چندجمله‌ای

(Table- 7): Classification by SVM with MLP Kernel

SVM (Polynomial)	Poly-Order	*FP*	*FN*	*TP*	*TN*	D^{Rate}
Test Data	1	9	6	14	0	0.4828
	2	4	6	19	0	0.6552
	3	6	5	17	1	0.6207
	4	6	5	17	1	0.6207
Train Data	1	7	15	164	83	0.9182
	2	4	13	167	85	0.9368
	3	1	12	170	86	0.9517
	4	0	10	171	88	0.9628

(جدول-۸): نتایج طبقه‌بندی ماشین بردار پشتیبان با هستهٔ RBF

(Table- 8): Classification by SVM with RBF Kernel

SVM (RBF)	Sigma	*FP*	*FN*	*TP*	*TN*	D^{Rate}
Test Data	0.1	0	6	23	0	0.7931
	0.2	2	6	21	0	0.7241
	0.3	3	6	20	0	0.6897
	0.4	10	6	13	0	0.4483
Train Data	0.1	1	0	170	98	0.9963
	0.2	2	5	169	93	0.974
	0.3	2	10	169	88	0.9554
	0.4	2	10	169	88	0.9554

۳-۵- طبقه‌بندی داده‌ها و نتایج ارزیابی

در سامانه تشخیص نفوذ پیشنهادی برای یافتن ترافیک حمله از ترافیک داده‌های طبیعی، از روش‌های متفاوتی برای طبقه‌بندی می‌توان استفاده کرد. در این مقاله از دو روش طبقه‌بندی ماشین بردار پشتیبان با هسته‌ها و ضرایب متفاوت و k نزدیک‌ترین همسایه با مقادیر k متفاوت به‌منظور مقایسه و یافتن نتایج دقیق‌تر، و برای طبقه‌بندی داده‌ها از نرم‌افزار متلب ۲۰۱۵ استفاده شده است. از رابطهٔ عمومی (۱۱) که ترکیبی از روابط (۳) و (۴) هستند نیز، برای ارزیابی دقت هر یک از روش‌های طبقه‌بندی استفاده‌شده است.

$$D^{Rate} = (TP+TN)/(FP+FN+TN+TP) \quad (11)$$

جداول (۵) الی (۸) نتایج طبقه‌بندی ماشین بردار پشتیبان با هسته‌های متفاوت و جدول (۹) نتیجه طبقه‌بندی k نزدیک‌ترین همسایه با مقادیر مختلف k را نشان می‌دهد. نتایج به‌دست‌آمده با توجه به تقسیم داده‌های جمع‌آوری‌شده به سه گروه آموزش، ارزیابی و آزمون به نسبت ۸۰٪، ۱۰٪ و ۱۰٪ به دست آمده است. همان‌طورکه مشاهده می‌شود، نتیجهٔ روش k نزدیک‌ترین همسایه با مقدار k=3 معادل ۰.۹ است که بهترین نتیجه را نسبت به روش ماشین بردار پشتیبان با هسته‌های متفاوت به دست آورده است. جدول (۱۰) مقایسهٔ نتایج مربوط به دو روش طبقه‌بندی را نشان می‌دهد. همان‌طورکه مشاهده می‌شود، اگرچه بهترین تشخیص مربوط به روش KNN است، تعدادی هشدار اشتباه نیز در روش KNN دیده می‌شود. بنابراین، می‌توان بیان کرد که اگر شبکه در محیطی باشد که احتمال حمله به آن کم باشد، می‌توان از روش SVM نیز بهره برد؛ ولی چنان‌چه احتمال حمله زیاد باشد، می‌توان هشدارهای اشتباه را نادیده گرفت و از روش KNN استفاده کرد.

۶- نتیجه‌گیری

در این مقاله یک سامانه تشخیص نفوذ ترکیبی برای شبکه‌های حسگر بی‌سیم بدن ارائه شد. در سامانه پیشنهادی، نخست، با استفاده از الگوریتم ژنتیک ترافیک شبکه مورد پالایش قرار می‌گیرد. بدین ترتیب که تنها ویژگی‌هایی از داده‌های جمع‌آوری‌شده انتخاب می‌شوند که موجب افزایش دقت سامانه تشخیص نفوذ می‌شود. پس از آماده‌سازی داده‌ها، مرحلهٔ شناسایی و جداسازی ترافیک طبیعی شبکه از ترافیک گره مهاجم می‌رسد. در این مرحله مشاهده شد که با استفاده از روش k نزدیک‌ترین همسایه دقت سامانه پیشنهادی به ۹۰٪ می‌رسد. همچنین، در سامانه پیشنهادی نشان داده‌شد، چنان‌چه داده‌های در حالِ پردازش، نخست، پالایش شوند،

روش‌های طبقه‌بندی با درصد بالایی قادر به شناسایی ترافیک داده‌های مخرب هستند. به‌عنوان ادامهٔ کار می‌توان الگوریتم‌های بدون نظارت را نیز ارزیابی کرد.

6-Refrence ۶-مراجع

[1] M. Ghamari, B. Janko, R. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors*, vol. 16, no. 6, p. 831, 2016.

[2] M. Contaldo, B. Banerjee, D. Ruffieux, J. Chabloz, E. Le Roux, and C. C. Enz, "A 2.4-GHz BAW-based transceiver for wireless body area networks," *IEEE transactions on biomedical circuits and systems*, vol. 4, no. 6, pp. 391-399, 2010.

[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658-1686, 2014.

[4] S. Ullah *et al.*, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol. 36, no. 3, pp. 1065-1094, 2012.

[5] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113-122, 2017.

[۶] محمودی نصر پیام، یزدیان ورجانی علی. "یک سامانه مدیریت دسترسی برای کاهش تهدیدهای عملیاتی در سامانه اسکادا" پردازش علائم و داده‌ها. ۱۳۹۶; ۱۴ (۴) :۳-۱۸

[6] Mahmoudi-Nasr P, Yazdian Varjani A. "An Access Management System to Mitigate Operational Threats in SCADA System", *JSDP* 2018; 14 (4) :3-18.

[7] M. S. Taha, M. S. M. Rahim, M. M. Hashim, and F. A. Johi, "Wireless body area network revisited," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 3494-3504, 2018.

[8] P. Dodangeh and A. H. Jahangir, "A biometric security scheme for wireless body area networks," *Journal of Information Security and Applications*, vol. 41, pp. 62-74, 2018.

[9] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1635-1657, 2014.

[10] M. Usman, M. R. Asghar, I. S. Ansari, and M. Qaraqe, "Security in Wireless Body Area Networks: From In-Body to Off-Body Communications," *IEEE Access*, vol. 6, pp. 58064-58074, 2018.

[11] O. Salem, A. Serhrouchni, A. Mehaoua, and R. Boutaba, "Event Detection in Wireless Body Area Networks using Kalman Filter and Power Divergence," *IEEE Transactions on Network and Service Management*, 2018.

[12] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 167575, 2013.

[13] R. Latif, H. Abbas, S. Latif, and A. Masood, "EVFDT: an enhanced very fast decision tree algorithm for detecting distributed denial of service attack in cloud-assisted wireless body area network," *Mobile Information Systems*, vol. 2015, 2015.

[14] N. K. Jha, A. Raghunathan, and M. Zhang, "Securing medical devices through wireless monitoring and anomaly detection," ed: Google Patents, 2018.

[15] G. Thamilarasu and Z. Ma, "Autonomous mobile agent based intrusion detection framework in wireless body area networks," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*, 2015: IEEE, pp. 1-3.

[16] Y. Qu, G. Zheng, H. Wu, B. Ji, and H. Ma, "An energy-efficient routing protocol for reliable data transmission in wireless body area networks," *Sensors*, vol. 19, no. 19, p. 4238, 2019.

[17] S. R. Nabavi, N. Osati Eraghi, and J. Akbari Torkestani, "Temperature-Aware Routing in Wireless Body Area Network Based on Meta-Heuristic Clustering Method," *Journal of Communication Engineering*, 2021.

[18] N. Bilandi, H. K. Verma, and R. Dhir, "PSOBAN: a novel particle swarm optimization based protocol for wireless body area networks," *SN Applied Sciences*, vol. 1, no. 11, pp. 1-14, 2019.

[19] B. Vahedian and P. Mahmoudi-Nasr12, "Toward Energy-efficient Communication Protocol in Wireless Body Area Network: A Dynamic Scheduling Policy Approach."

[20] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers & Security*, p. 102211, 2021.

[۲۱] ربیع پورمحمدجواد، قسوری حسین. خنشان امیرحسین, "بررسی تحلیلی شبکه‌های حسگر بی‌سیم بدنی و مقایسه تکنولوژی‌های گوناگون جهت ارتباطات در شبکه",سومین کنفرانس ملی مهندسی برق و کامپیوتر سامانههای توزیع شده و شبکه های هوشمند, تهران, ۱۳۹۵.

[21] M. rabiepour, H. ghasvari and A. khanshan, " Analytical investigation of the capabilities and limitations of using various routing algorithms for use in wireless body area networks ", *3th National Conference on Electrical and Computer Engineering Distributed Systems and Smart Grids*, 2016.

[22] S. Karchowdhury and M. Sen, "Survey on attacks on wireless body area network,"

International Journal of Computational Intelligence & IoT, Forthcoming, 2019.
[23] S. M. Othman, N. T. Alsohybe, F. M. Ba-Alwi, and A. T. Zahary, "Survey on intrusion detection system types," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 4, pp. 444-463, 2018.
[24] M. Dhuha I., and Sarab M. Hameed. "A feature selection model based on genetic algorithm for intrusion detection." *Iraqi Journal of Science*, pp. 168-175, 2016.
[25] Bamakan, Seyed Mojtaba Hosseini, et al. "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization." *Neurocomputing*, Vol. 199,pp. 90-102, 2016.
[26] P. Hamed Haddad, GholamHossein Dastghaibyfard, and Sattar Hashemi. "Two-tier network anomaly detection model: a machine learning approach." *Journal of Intelligent Information Systems*, Vol. 48, no.1, pp. 61-74, 2017.
[27] Odesile, Adedayo, and Geethapriya Thamilarasu. "Distributed intrusion detection using mobile agents in wireless body area networks." *2017 Seventh International Conference on Emerging Security Technologies (EST)*. IEEE, 2017.
[28] Shone, Nathan, et al. "A deep learning approach to network intrusion detection." *IEEE transactions on emerging topics in computational intelligence*, Vol. 2, no.1, pp. 41-50. 2018.
[29] Woo, Ju-ho, Joo-Yeop Song, and Young-June Choi. "Performance enhancement of deep neural network using feature selection and preprocessing for intrusion detection." *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2019.
[30] Newaz, AKM Iqtidar, et al. "Heka: A novel intrusion detection system for attacks to personal medical devices." *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2020.
[31] Hady, Anar A., et al. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." *IEEE Access*, Vol. 8, pp. 106576-106584, 2020.
[32] Iwendi, Celestine, et al. "Security of things intrusion detection system for smart healthcare." *Electronics* Vol. 10, no.12, pp. 1375, 2021.
[33] Gupta, Karan, et al. "A tree classifier based network intrusion detection model for Internet of Medical Things." *Computers and Electrical Engineering*, Vol. 102,pp. 108158, 2022.

پیام محمودی نصر تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر، به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۵ از دانشگاه صنعتی امیرکبیر و در مقطع دکترای مهندسی قدرت در سال ۱۳۹۵ در دانشگاه تربیت مدرس به پایان رسانده و هم‌اکنون استادیار دانشکدهٔ مهندسی و فناوری دانشگاه مازندران است. زمینه‌های پژوهشی موردعلاقهٔ ایشان عبارتند از: امنیت شبکه‌های صنعتی و کامپیوتری، امنیت داده‌ها و شبکه‌های کامپیوتری.
نشانی رایانامهٔ ایشان عبارت است از:
P.mahmoudi@umz.ac.ir

علیرضا رحمانی متولد ۱۳۶۹ تحصیلات خود را در مقطع کارشناسی فناوری اطلاعات در سال ۱۳۹۲ در دانشگاه غیردولتی هاتف زاهدان، و در مقطع کارشناسی ارشد فناوری اطلاعات گرایش شبکه‌های رایانه‌ای در سال ۱۳۹۷ در مؤسسهٔ غیردولتی صنعتی مازندران به پایان رسانده است. زمینه‌های موردعلاقهٔ ایشان شبکه‌های رایانه‌ای بی‌سیم است.
نشانی رایانامهٔ ایشان عبارت است از:
Alireza.rahmani9923@gmail.com