فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دوم، شماره ۱، بهار ۱۳۹۷

بررسی و ارزیابی رویکردهای تشخیص نفوذ بر مبنای سیستم ایمنی مصنوعی

حسین شیرازی[۱]، احسان فرزادنیا[۲] و علیرضا نوروزی[۳]

تاریخ دریافت: ۱۳۹۷/۰۱/۲۰ تاریخ پذیرش: ۱۳۹۷/۰۳/۱۲

چکیده:

در سالهای اخیر جهت گیری کارهای پژوهشی در زمینه ارائه سیستمهای تشخیص نفوذ به سمت الهام گرفتن از سیستم ایمنی زیستی به منظور حل مسائل پیچیده این حوزه بوده است. سیستم ایمنی مصنوعی و پتانسیلِ اعمالِ مصونیّت آن، با پیش زمینه دفاع زیستی آن در واقع راهکاری برای کنترل امنیّت و تشخیص ناهنجاری شبکه سازمان مطرح می باشد. در این پژوهش متدهای مختلف ایمنی مصنوعی در مقایسه با سایر متدهای یادگیری ماشین و الگوریتمهای فراابتکاری با هدف ارائه رویکردی نو برای حل مسئله تشخیص نفوذ بررسی و ارزیابی شده اند. ارزیابی ها در نرم افزار استاندارد Weka3.6 تحت دادگان نفوذ NSL-KDD انجام شده اند. نتایج آزمایشات حاکی از آنست که بعد از تعبیه فاز انتخاب ویژگی در متدهای ایمنی مصنوعی به ترتیب در Immunos99 , ARIS2Paralell و CSCA منجر به افزایش محسوسی در دقّت دسته بندی می گردند. در نتیجه رویکردِ Bat + ARIS2Paralell به ترتیب با ضریب همبستگی ۰,۹٤٦ ، نرخ تشخیص ۰,۹۷۳ صحّت ۰,۹۷۲۵ و خطای مثبت کاذب ۰,۰۲۸ دسته بندی مطلوب تری را در بین سایر رویکردها داشته و به نظر میرسد به دلیل نرخ همبستگی بالا قابلیت اطمینان در خصوص امکان بهره برداری در جهت توسعه سیستم های تشخیص نفوذ آینده را داشته باشد.

واژگان کلیدی: سیستم تشخیص نفوذ ، انتخاب ویژگی ، الگوریتمهای فراابتکاری ، سیستم ایمنی مصنوعی ، بهره اطلاعات

۱. نویسنده مسئول، دانشیار، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر، Shirazi@mut.ac.ir
۲. دانشجوی کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر، Ehsan_farzadnia@mut.ac.ir
۳. استادیار، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر، Nowroozi@mut.ac.ir

[Downloaded from ic4i-journal.ir on 2026-11-23]

۱. مقدمه

طبیعت ، همیشه الگویی مناسب برای حل مسائل پیچیده بوده است. با نگاهی عمیق به سیستم های دفاعی موجودات زنده در طبیعت می توان از الگوهای موفّق زیستی در فرایند تشخیص و پاسخ هوشمندانه به حملات و رفتارهای محرّک زیست محیطی به خوبی الهام گرفت و در علم امنیت شبکه و خصوصاً سیستم های تشخیص و جلوگیری از نفوذ[1] به بکار گرفت. کاری که دانشمندان همواره به دنبال کشف حقایق و رازهای طبیعت بوده اند تا نتایج حاصل از آنرا در حل مسائل و چالشهای علوم کامپیوتر مُدل سازی و به صورت سَفت افزاری[2] به کار ببندند. [۱۰] [۱۸] لذا هر مدل بیولوژیکی در موقعیتی خاص می تواند راهگشای مشکلی بزرگ در اِکو سیستم های ساخته بشر باشد. به عقیده نگارندگان ، یک IDS مبتنی بر ایمنی مصنوعی[3] در اصل دارای یک اِکو سیستم مصنوعی می باشد که با الهام از رفتار دفاعی سیستم ایمنی بدن انسان (HIS) در برابر نفوذ آنتی ژنها و میکروبها همواره در تلاش است تا از طریق برقراری ایمنی به کنترل امنیّت اطلاعات سازمان دست یابد.

ذکر این نکته نیز حائز اهمیت است که وجود برخی چالشها مانند تشخیص حملات ناشناخته [4] و نرخ های خطای منفی اشتباه [5] بالا در اکثر سامانه های تشخیص و جلوگیری از نفوذ باعث شده تا جهت گیری پژوهشها به سمت کاربرد رویکرد تشخیص رفتار ناهنجار به جای رویکرد مبتنی بر امضاء [6] سوق پیدا کند. در توسعه سیستم های تشخیص نفوذ شبکه مبتنی بر تشخیص رفتار ناهنجار ، عمدتاً تکنیکهای داده کاوی و روشهای هوش مصنوعی مبتنی بر یادگیری ماشین به منظور آنالیز و استخراج دانش الگو استفاده می شود تا سیستم پس از کسب تجربه لازم در خصوص الگوی نرمال ترافیک شبکه ، در نهایت ترافیک با رفتار ناهنجار را شناسایی کند. [۳۳-۳۶][۳۰] روشهای مختلف تشخیص ناهنجاری عبارتند از : انواع تکنیکهای یادگیری ماشین (متدهای یادگیری با نظارت[7] ، بدون نظارت [8] و یا نیمه نظارت شده) ، قواعد وابستگی[9] ، منطق فازی[10] و گاهاً روشهای ترکیبی[11].

سیستم ایمنی مصنوعی از سیستم ایمنی بیولوژیک بدن انسان [12] الهام گرفته شده و شاخه ای از هوش محاسباتی می باشد. [۱۰] تفاوت اصلی آن با سایر متدها در نحوه نگرش به مسئله کشف ناهنجاری و حل آن می باشد. در سیستم ایمنی مصنوعی دو رویکرد تشخیص خوب های شناخته شده [13] و بدهای شناخته شده [14] طوری با هم تلفیق شده اند که در نهایت منجر به شناسایی نفوذ و حتی حملات ناشناخته می گردند. در اصل سازوکار فعالیت

---

[1] Intrusion detection system (IDS)

[2] ترکیب نرم افزار و سخت افزار را سفت افزار گویند.

[3] Artificial immune based intrusion detection system(AIDS)

[4] Unknown attacks

[5] False negative errors

[6] همانگونه که می دانیم به طور کلی سیستم های تشخیص نفوذ با دو رویکرد توسعه داده شده اند : اولی رویکرد تشخیص مبتنی بر پایگاه داده امضاهای حملات یا سوء استفاده معروف بوده و روش دیگر مبتنی بر شناختن ترافیک سالم با ایجاد پروفایل های سیستم (ترافیک خودی) و یافتن ترافیک ناسالم از روی عدم تطابق با امضاهای پیشین که به روش مبتنی بر ناهنجاری معروف است و سعی دارد با تکنیکهای آماری و یادگیری ماشین الگوی رفتار نرمال را آموخته و در صورت عدم تطبیق نسبی الگوی جدید ، ناهنجاری را کشف نماید.

[7] Classification methods

[8] Clustering methods

[9] Association rules

[10] Fuzzy logic

[11] Such as Ensemble base or Hybrid based

[12] Human Immune System (HIS)

[13] Known good

[14] known bad

[Downloaded from ic4i-journal.ir on 2026-11-23]

عوامل خودی (تشخیص دهنده ها [1]) سیستم به منظور کسب تجربه در کنار یکدیگر و همینطور ترکیب آن با رویه بروز رسانی پایگاه امضاء های حملات (روش مبتنی بر سوء استفاده) [2] منجر به ایجاد مصونیّت سیستم در برابر عوامل آنتی ژنیک خارجی [3] می گردد. در مورد سامانه های تشخیص نفوذ شبکه ، هر ترافیک ورودی به سیستم با الگوی ناشناس که تحت آنالیز و بررسی سیستم قرار میگیرد به عنوان عامل غیر خودی، برای سیستم الگویی آنتی ژنیک محسوب می گردد. نکته ای که در اینجا وجود دارد اینست که کاربرد یک تکنیک انتخاب ویژگی [4] منجر به افزایش دقّت دسته بندی و کاهش زمان محاسباتی سیستم تشخیص (افزایش سرعت آن) می گردد (به دلیل گزینش برخی خصیصه های مهم و مرتبط با هرنوع حمله) [۱۹] [۳۱-۳۲]. در پژوهش جاری، تاثیرِ ترکیبِ برخی از موثرترین و بهترین رویکردهای انتخاب ویژگی الهام گرفته شده از هوش ازدحامی جانداران [5] با متدهای ایمنی مصنوعی مورد ارزیابی مقایسه ای قرار گرفته اند. به منظور درک مفاهیم زیستی این تحقیق و آشنایی کامل با سیستم ایمنی زیستی و مصنوعی ، مطالعه مرجع [۲۶] به عنوان پیش نیاز پیشنهاد میگردد.

ساختار مقاله شامل بخشهای زیر می باشد: بخش دوّم به کلیّات و طرح مسئله اختصاص دارد. اهمیت و ضرورت ارزیابی رویکردهای تشخیص نفوذ بهمراه خلاصه ای از پیشینه کارهای تحقیقاتی در زمینه کاربرد سیستم ایمنی مصنوعی و متدهای آن در جهت حل مسئله تشخیص نفوذ ارائه شده است. هچنین مبانی و ادبیات نظری تحقیق که شامل آشنایی با سیستم ایمنی مصنوعی و معرّفیِ مهمترین متد آن می باشد نیز از موارد مهم این بخش میباشد. در بخش سوّم ، مجموعه آزمایشاتِ مقایسه ای و آنالیز یافته های مهمّ تحقیق اختصاص دارد. بدین ترتیب که الگوریتمهای ایمنی مصنوعی با سایر متدها در دو فاز مجزّا مورد ارزیابی مقایسه ای قرار گرفته و تاثیر استفاده از الگوریتم های مختلف انتخاب ویژگی فراابتکاری[6] در ترکیب با رویکردهای مختلف تشخیص نفوذ بدقّت آنالیز شده اند. بحث ، نتیجه گیری و ارائه پیشنهاداتی برای کارهای آینده نیز موضوع بخش انتهایی این مقاله است.

۲. کلیات

۲-۱. اهمیّت و ضرورت موضوع تحقیق

حملات سایبری را می توان بُرداری در نظر گرفت که منشاء تمامی آنها به سوء استفاده از یک آسیب پذیری در شبکه قربانی و عمدتاً بواسطه حملات شناسایی و تحت شبکه صورت می پذیرد. بنابراین اهمیت کنترل امنیّت شبکه سازمان خصوصاً در سازمان های نظامی را به عنوان یک هدف می توان مطرح نمود که در تلفیق با سیاستهای فرماندهی همواره باید نظارت گردد. (مانیتورینگ) در پروسه نظارت ، عوامل انسانی متخصّص همواره نقش اساسی دارند که نظارت آنها ممکن است با خطا همراه باشد.

[1] به آنتی بادیها که جزو عوامل اصلی شناسایی حملات در سیستم ایمنی بیولوژیک هستند ، تشخیص دهنده می گویند. سیستم ایمنی همواره در تلاش است تا با تولید تشخیص دهنده های دارای الگوی مناسب ، بتواند حملات ناشناخته را شناسایی و کشف نماید.

[2] misuse detection
[3] non-Self
[4] Feature Selection
[5] Swarm intelligence
[6] Meta-heuristic optimization algorithms

[Downloaded from ic4i-journal.ir on 2026-11-23]

خطر حاصل از بُروزِ این خطا زمانی اهمیت فراوانی پیدا می کند که حمله ای سایبری از طریق شبکه در شُرُف وقوع باشد. در نتیجه استفاده از سامانه هوشمندی که بتواند به نحوی بر مبنای یادگیری قبلی خود ، این خطر بالقوّه را استنباط و به نحوی آنرا اطلاع دهد غیر قابل انکار خواهد بود. سیستم های تشخیص ناهنجاری شبکه مبتنی بر یادگیری ماشین و تکنیکهایی که در بخش قبل بدان ها اشاره شد دو فاز یادگیری و تست دارند. این سیستم ها به جهت اینکه یادگیری موفقی داشته باشند نیازمند پایگاه داده ای کافی و بِروز از پروفایلهای ترافیک نرمال شبکه هستند که بر مبنای آن بتوانند ترافیک مشکوک ورودی را کشف نمایند. از طرفی روش تشخیص در تکنیکهای مبتنی بر سوء استفاده بر خلاف سیستم های تشخیص ناهنجاری ، به میزان بِروز بودن پایگاه امضاءهای حملات آنها وابسته است. این سیستم های غیر هوشمند، امروزه چالشهای اساسی دارند و اغلب در برابر تهاجم ناتوانند امّا متاسفانه هنوز در سازمان ها و نهادهای اطلاعاتی مورد استفاده قرار میگیرند. هر یک از این دو رویکرد مزیّـت و چالشهای خود را دارند . مزیّت رویکرد تشخیص ناهنجاری آنست که نیازی به پایگاه داده حملات و امضای آنها نداشته و وابسته به میزان یادگیری از پروفایلهای رفتار نرمال (خودی) هستند. چالش آنها در زیاد بودن حجم داده های نرمال نسبت به داده های ناهنجار می باشد بطوریکه در شبکه هایی که نرخ وقوع حملات در آنها در بازه های زمانی در نظر گرفته شده نسبتاً بالاست خروجی مطلوبی ندارند.

طرفی مزیّت رویکرد دوّم (تشخیص مبتنی بر سوء استفاده) نیز آنست که سریعتر عمل نموده و فاز یادگیری هوشمندی ندارند. بنابراین صرفاً با تطبیق نمونه ورودی با پایگاه امضاء ، ناهنجاری را کشف می کنند. مهم ترین چالشِ این رویکرد بِروز نبودنِ این پایگاه و عدمِ کشفِ حملاتِ روزِ صفر می باشد. سیستم ایمنی مصنوعی هر دو رویکرد فوق را در خود دارد بطوریکه با پتانسیل تولید و تکثیر تشخیص دهنده ها (آنتی بادی ها) می تواند پروفایل سازی نموده و قبل از مواجهه با نمونه مشکوک (ترافیک شبکه ورودی) بواسطه روند بلوغ تشخیص دهنده های بالغ ، حد آستانه تحمّلِ سیستم را در برابر نفوذ بالا برده و با عوامل خودی بیاموزد. این پتانسیلِ خودی یادگیری [1] سیستم ایمنی دقیقاً مشابه مانُورهای نظامی می باشد.

۲-۲. پیشینه تحقیق

ویژگی مهم سیستم ایمنی مصنوعی وجود نوعی حیات مصنوعی در درون سیستم است. انتخاب منفی به عنوان مهمترین متدِ ایمنی مصنوعی یعنی انتخاب آن دسته از تشخیص دهنده هایی که به عنوان تشخیص دهنده های خودی با هیچ یک از الگوهای خودی دیگر تطبیق نخورده و با غیر خودیها بایند شوند. این دسته از تشخیص دهنده های بالغ به منظور تکثیر و طی نمودن فرایند بلوغ ، انتخاب میگردند. در دهه اخیر ، ایده های متعددی با استفاده از سیستم ایمنی مصنوعی در سیستم های تشخیص نفوذ استفاده شده اند [۱-٤] [۱۰] [۱۳-۱٤] [۲۱] از طرفی پتانسیل هر سیستم ایمنی زیستی می تواند نقطه عطفی در جهت الهام گرفتن ایده های برتر باشد. ایده هایی که شاید راهگشای مسائل بزرگ و سختی باشند که حل آنها نیازمند

[1] Self-training

[Downloaded from ic4i-journal.ir on 2026-11-23]

بررسی عمیق و موشکافانه ساختار دفاعی زیست جانداران در طبیعت دارد.

به عنوان نمونه ، در مقاله [۱] نویسنده از مکانیزمهای پاسخ در گیاهان الگوبرداری کرده و مدلی را با الهام از سیستم ایمنی گیاه ارائه نموده که می تواند عملکرد IDS را در پاسخ به حملات افزایش دهد. ضمناً وی به بیان چالشهایی در پاسخ به حملات پرداخته است : از جمله انتخاب تشخیص دهنده موثّر، انتقال سیگنال هشدار امن و سریع از گره آلوده به سایر گره ها در شبکه با پیاده سازی تئوری خطر در یک شبکه محلّی بوسیله الگوریتم سلولهای دندریت و تاثیر همکاری گره های همسایه در جهت بهبود نرخ تشخیص. در [۱۹] انواع الگوریتم های فراابتکاری الهام گرفته شده از طبیعت دسته بندی و بررسی شده و تعدادی از استراتژیهای جستجوی بهینه برای حل مسائل انتخاب ویژگی در تشخیص نفوذ ارائه شده است.

همچنین از رفتار حشرات و جانوران برای مقابله با حملات در مقاله [۱۲] ایده هایی مطرح شده که نشان می دهد ویژگی هوش ازدحامی جانداران می تواند کارائی سیستم های تشخیص نفوذ را افزایش دهد. مقاله [۳] از ترکیب شبکه عصبی مصنوعی و الگوریتم FCM استفاده کرده است. در مقاله [۸] از روش ترکیبی الگوریتمهای CFA برای انتخاب ویژگی بهینه ، الگوریتم C5 برای دسته بندی ترافیک و اعمال جریان داده آنومالی به ورودی SVM تک کلاسه استفاده شده است. در مقاله [۵] از الگوریتم IG (که رویکرد فیلتر دارد) برای انتخاب ویژگی ورودی و از الگوریتم خفّاش برای بهینه سازی پارامترهای ورودی به دسته بند SVM در تشخیص آنومالی استفاده شده است. تجاربِ حاصل از آزمون این تحقیق نشان می دهند که BAT فرایند انتخاب پارامترهای ورودی را برای تکنیک SVM بهبود می بخشد. مقالات دیگری همچون [۱۶] از الگوریتم BBA (الگوریتم BAT باینری) به عنوان نسخه بهبود یافته BAT در ترکیب با دسته بند SVM استفاده کرده اند. از جمله پژوهشهای اخیر در حوزه انتخاب (کاهش) ویژگی به شرح ذیل اند :

مقاله [۲] از روش کاهش ویژگی Chi-square مبتنی بر SVM چند کلاس استفاده کرده است. ایده اصلی چند کلاسه بودن SVM در اینست که بتوان ضمن کاهش زمان تشخیص ، دقت دسته بندی را نیز بالا برد. همچنین تحقیق [۱۱] نیز از الگوریتم زنبور بهمراه SVM به منظور انتخاب ویژگی در مسئله تشخیص آنومالی شبکه استفاده نموده و با سایر الگوریتم ها rough DPSO rough LGP MARS, SVDF, مقایسه و ارزیابی نموده است.

نتایج حاکی از آنست که رویکرد BA-SVM به دلیل پیاده سازی آسان و موثر عمل نمودن در پیاده کردن راه حلهای بهینه ، بهتر از بقیه الگوریتم ها میباشد. گرچه Rough set نیز دارای نرخ هشدار اشتباه در حد صفر بوده اما عملکردی به اندازه BA ندارد. بالاخره در [۱۹] ، شش الگوریتم انتخاب ویژگی (فیلتر و راپر) مورد بررسی و ارزیابی قرار گرفته اند که الگوریتم دسته بندی درخت تصمیم گیری C4.5 و چند مورد الگوریتم انتخاب ویژگی مبتنی بر اطلاعات متقابل نیز جزو آنهاست.

اصولاً کلّیه الگوریتمهای الهام گرفته شده از حیات و جانداران به سه دسته زیر تقسیم میشوند [۲۴]. از رابطه زیر به خوبی مشخص است که تمام الگوریتم های الهام گرفته شده از طبیعت بیولوژیک نبوده و ضمناً سیستم ایمنی مصنوعی به دلیل الهام از سیستم ایمنی بیولوژیک ، خود در دسته دوم جای میگیرد.

[Downloaded from ic4i-journal.ir on 2026-11-23]

Swarm intelligence ⊂ Bio-inspired ⊂ Nature-inspired

طبق بررسی های انجام شده ، الگوریتم های فراابتکاری و مبتنی بر هوش ازدحامی جانداران مانند BAT, Bee, GA, PSO, rough set , [7] CFA دارای پتانسیل بالقوّه ای برای حل دو مسئله دسته بندی و انتخاب ویژگی میباشند. بطوریکه در پژوهشها رویکردهایی که از این متدهای فراابتکاری استفاده کرده اند همواره نرخ های عملکرد دسته بندی آنها بهبود چشمگیری پیدا کرده است. این در مورد رویکردهایی که از متدهای ایمنی مصنوعی بهره برده اند نیز صدق می کند. [۲۱] چالش اصلی متدهای ایمنی مصنوعی در وجود پارامترهایی با اندازه بازه ی حقیقی و عدم تخصیص بهینه مقادیر ورودی در آنهاست، بگونه ای که حتّی با کوچکترین تغییر محسوسی در ابعاد مسئله، نرخ های خروجی به شدّت تغییر می یابند. از اینرو به نظر می رسد اگر الگوریتم انتخاب ویژگی مناسبی در ترکیب با متدهای دسته بندی ایمنی مصنوعی به کار رود ، تاثیر این کاربرد به عنوان فاز پیش پردازش در عملکرد خروجی بسیار مشهود خواهد بود.

ما در مجموعه آزمایشات خود در بخش های بعدی به این مسئله پرداخته و از الگوریتم های فرا ابتکاری پیشنهادی در ترکیب با متدهای ایمنی مصنوعی در جهت ارائه تصویری بهتر از نحوه عملکرد این متدها استفاده نموده ایم. ضمناً نتیجه این ترکیب را با سایر رویکردهای یادگیری ماشین ارزیابی مقایسه ای نموده –ایم. همچنین یک چالش دیگر، بحث مواجهه با داده حجیم می باشد که وجود پارامترهایی با بازه ای با مقادیر پیوسته باعث می شوند که پیکربندی آنها با مشکل مواجه گردد. چرا که همانگونه که گفته شد با تغییر محسوس ابعاد مسئله ، مقادیر پارامترها و به طور خاص مقادیر حدود آستانه تولید و تکثیر و حد آستانه وابستگی در این متدها ناگزیر باید بسته به شرایط ابعاد مسئله تغییر یابند. این تغییراتِ پیوسته، در مواردی به صورتی است که به نظر می رسد با کاربرد الگوریتم فراابتکاری موثّر در انتخاب بهینه ترین پارامترهای ورودی نیز بتوان با این مشکل مقابله نموده و نتیجه مطلوبی هم از نظر کارائی و هم از نظر بُعدِ زمان و پیچیدگیِ محاسباتی ارائه نمود.

۲-۳. پرسشِ تحقیق

امروزه کشف حملات سایبری تحت شبکه هنوز یک مشکل اساسی و یکی از مسائل سخت حوزه امنیت شبکه است. تحقیق حاضر سعی بر آن دارد با پرداختن به سیستم ایمنی مصنوعی ، نتیجه ترکیب آن با متدهای یادگیری ماشین را در بهبود عملکرد این سیستم در مسئله تشخیص نفوذ ارزیابی نموده و رویکردی نو در راستای طراحی و توسعه یک سیستم تشخیص ناهنجاری شبکه ارائه دهد.

۲-٤. روش شناسیِ تحقیق

در این تحقیق ، از نرم افزار Weka3.6 و دادگان نفوذ NSL-KDD (آخرین بروز رسانی ۲۰۱٦) استفاده شد. نسخه مذکور ٤ نسخه از الگوریتم های ایمنی مصنوعی را در خود دارد که عبارتند از :

- Immunos99
- ARIS2parallel
- CLONALG
- CSCA
- ARIS

این الگوریتم ها اوّلین بار طی گزارش فنّی [۲۷] در سال ۲۰۰۵ ارائه شده اند. در این تحقیق سعی بر آن شد که تا

[Downloaded from ic4i-journal.ir on 2026-11-23]

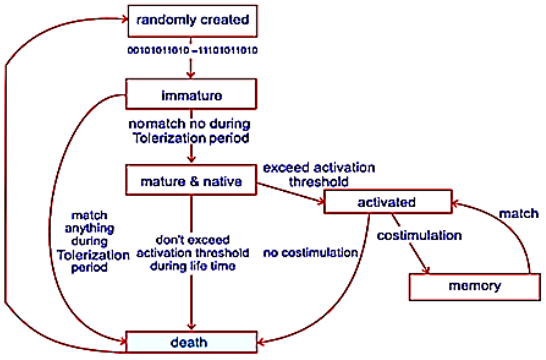
حد امکان از تمامی متدهای داده کاوی در این نرم افزار استفاده شود تا ارزیابی کاملی صورت گیرد.

۲-۵. مبانی نظری و ادبیات تحقیق

الگوریتم انتخاب منفی (NSA) به عنوان نخستین سیستمی که اوّلین بار توسط دانشمندی به نام فورِست و همکارانش در سال ۱۹۷٤ ارائه گردید [۲۸] که مکانیزم آن در شکل (۱) ارائه شده است. این الگوریتم سازوکار لنفوسیتهای B را در تولید و تکثیر تشخیص دهنده ها در (پروفایل سازی) در جهت مصون سازی هسته سیستم ایمنی در برابر نفوذ (کشف نمونه آنتی ژنیک و ناهنجار) نشان می دهد.

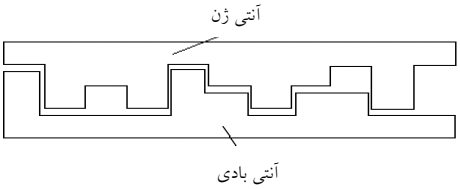
فورِست و همکارانش این الگوریتم را در مسئله تشخیص آنومالی به بردند. در سیستم آنها که در واقع یک نوع دسته بند باینری بود ، رشته های تصادفی به عنوان آنتی بادی های نابالغ تولید می شدند. مفهوم بلوغ این تشخیص دهنده ها بدین صورت ممکن بود که می بایست این رشته ها حداقل در r بیت متوالی که بر حسب تجربه تعیین می شد ، با رشته های مشکوک ترافیک شبکه که به معادل بیتی تبدیل شده بودند تطبیق می خوردند. حاصل این تطبیق رشته های تشخیص دهنده خودی (تشخیص دهنده های نابالغ) با رشته های غیر خودی (رشته بیتی نمونه مشکوک ترافیک شبکه) بالغ بود. با این رخداد، هر تشخیص دهنده خودی که بالغ می شد به مجموعه بالغ ها اضافه می شد و بدین ترتیب رشته های متوالی به صورت تصادفی پیوسته تولید می شدند.

شکل (۱): الگوریتم انتخاب منفی پیشنهاد شده از سوی فورست و همکاران ، برگرفته از [۲۸]



شرط لازم برای بالغ شدن رشته های تصادفی خودی این بود که اوّلا نباید با رشته های خودی بالغ موجود تطبیق بخوردند (بایند شوند) تا بالغ شوند که به آن حد تحمّل مصونیّت می گویند. در شکل زیر الگوی رشته آنتی بادی با الگوی رشته غیر خودی در ٤ بیت صورت گرفته است.

شکل (۲): تطبیقِ دو الگوی خودی و غیر خودی (r = 4)



ثانیاً برای هر رشته خودی تشخیص دهنده ، یک طول عمر تعریف شده بود که در طول عمر خود در صورتیکه با حداقل یک نمونه غیر خودی مشکوک تطبیق موفّق انجام نداده باشد حذف می شود. این پروسه مبنای بیولوژیکی دارد و به این نوع مرگ زود –رَس که مانع بلوغ رشته می شود اصطلاحاً "apoptosis" می گویند. حال تشخیص دهنده بالغ به ازاء هر تطبیق الگو در حداقل r بیت متوالی با عوامل آنتی ژنیک ناشناخته، تکثیر میشود. به این پدیده نیز بلوغ وابستگی گفته می شود. یعنی به تعداد تطبیق هر

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ۱، بهار ۱۳۹۷

[Downloaded from ic4i-journal.ir on 2026-11-23]

تشخیص دهنده[1] بالغ MD با نمونه مشکوک آنتی ژن AG، MD تکثیر می شود تا سیستم ایمنی در مواجهه با AG با همان الگوی بیتی که قبلاً شناسایی شده در آینده نیز سریع آنرا کشف نماید.

ثُباتِ مصونیّتِ سیستمِ ایمنی و بطور کلّی سیستم تشخیص نفوذ مبتنی بر ایمنی ، نیازمندِ گُذرِ زمان است. به عبارت دیگر سیستم ایمنی ، پتانسیلِ کشفِ حملات را با تولید رشته تشخیص دهنده های با الگوهای تصادفی ابتدا با خود می آموزد و در عین حال به مُرورِ زمان و با تکثیر رشته های بالغی که در تطبیق ، موثر بوده اند می تواند احتمالِ کشف عوامل نفوذ ناشناخته و شناخته شده را تا حد زیادی بالا ببرد و سیستم را مصون نگه دارد. جهت بررسی جزئیّات بیشتر در خصوص استراتژی های ذاتی دفاعیِ سیستم ایمنی زیستی و مصنوعی ، مطالعه دقیقِ مرجع [۲۶] توصیه می گردد.

۲-۶. ایمـــنی و امنیّت

به عقیده نگارندگان و از دیدگاه زیستی ، ایمنی "روش محافظت از سیستم " در برابر نفوذ عوامل میکروب و آنتی ژنها می باشد در حالیکه " امنیّت " به درجه ای از مقاومت یا محافظت از دارایی های با ارزش یک سیستم (در اینجا بافتهای سلولی سالم بدن موجود زنده) در برابر سوء استفاده از آسیب پذیریها (تخریب سلولی توسط آنتی ژنها و عوامل پاتوژنیک به بدن) گفته می شود که باید کنترل شود. همین مفهوم در دنیای امنیت شبکه نیز قابل اقتباس می باشد. در واقع ایمنی یا مصونیّت ، روش مقابله با نفوذ است که راهکارها و استراتژیهای متفاوتی برای آن وجود دارد. در صورتی که استراتژی صحیحی به کار برده شود ، امنیّت سیستم (امن بودن آن) کنترل خواهد شد. متدهای سیستم ایمنی مصنوعی که مدلی انتزاعی از سیستم ایمنی زیستی بدن انسان هستند راهکار مناسبی برای کنترل امنیت شبکه می باشند که خصوصاً در دهه های اخیر مورد توجه محققان بوده و از آنها در طراحی سامانه های تشخیص ناهنجاری در تحقیقات به کرّات استفاده شده است. [۲۱] [۱۸] [۱۳] [٤] [۱]

۳. روش پیشنهادی

۳-۱. شرایط انجام آزمایش

در این بخش، حاصل ترکیب الگوریتم های مختلف فراابتکاری و یادگیری ماشین را با متدهای ایمنی مصنوعی تحت شرایط آزمایش و دادگان یکسان، ارزیابی مقایسه ای نموده ایم. تمامی آزمایشات در ابزار دانش کاوی استاندارد Weka v3.6 [2] و تحتِ دادگانِ نفوذ NSL-KDD [3] انجام شده اند. اطلاعات ترافیکی ۲۲ نوع حمله از انواع مختلف در [۱۹] بیان شده اند. البته نمی توان تمام آنها را در انجام آزمایش ها به کار برد. بنابراین برای انجام آزمایشات از ده درصد این دادگان استفاده شد. مشخصات سیستمی که این آزمایش ها در آن انجام شده به شرح زیر است :

پردازنده چهار هسته ای با مشخّصـــــــــات زیر Intel ® Core™ i5-3230. With 2.6 GHz
حافظه ٤ گیگا بایت. (۳٫۸۷ قابل استفاده) – میزان حافظه اختصاص داده شده به نرم افزار وکا را با استفاده از دستور مربوطه [4] از حالت پیش فرض آن که ۵۱۲ مگابایت بود به

[1] Mature generated detector

[2] متعلق به دانشگاه Waikato نیوزیلند

[3] این دادگان اصلاح شده DARPA98 می باشد

[4] Command prompt:

[Downloaded from ic4i-journal.ir on 2026-11-23]

۳۰۷۲ مگابایت افزایش دادیم تا بتوان با داده های در حدود بیش از ۲۵۰۰۰ رکورد به راحتی کارکرد.

- نوع سیستم بورد : x64–based processor
- سیستم عامل : windows 8.1 pro
- دادگانِ نفوذ با فرمت Arff : به دلیل آنکه کار با داده حجیم با کامپیوتری با مشخصات فوق عملاً بسیار زمانبر بوده و حافظه و توان پردازشی بالایی برای انجام این کار نیاز هست ، ما در هر آزمایش زیر مجموعه هایی از این دادگانِ حجیم را به صورت تصادفی یکنواخت انتخاب نمودیم.

تمامی زیر مجموعه دادگان استفاده شده دارای برچسب هستند. همچنین در مجموعه آزمایشات علاوه بر معیارهای کارائی و عملکردیِ رایج ، از معیارِ ضریبِ همبستگی cc نیز در ارزیابی ها استفاده شده است.

۳-۲. ارزیابیِ مقایسه ای

رویکردهای مهمّ دسته بندی و شناساییِ الگو که بیشترِ پژوهشگران [۳۳-۳۷][۲۹-۳۰][۱۷-۱۵][۱۲-۱۱][۸][۶-۵][۳-۲] به توسعه و بهبود آنها پرداخته اند شامل موارد زیر هستند :

SVM ، Naïve bayse ، شبکه های عصبی ، درخت های تصمیم گیری C4.5 (J48 Consolidated) ، Random ،Decision Tree ، LAD Tree،RandomTree ، JRip ، RST ها مانند Rule ، NBTree ،Forest. BTree ، Part ، Decision Table و الگوریتمهای فراابتکاری و مبتنی بر هوش ازدحامی جانداران مانند PSO ،BAT ، Bee ، Ant ، Coucko، CFA و همچنین الگوریتمهای ایمنی مصنوعی مانند NSA , CSA و [1] DCA که جدیداً در سالهای اخیر مورد پژوهش قرار گرفته اند. البتّه در نسخه جدیدِ نرم افزارِ وِکا، تعدادی الگوریتم نیز بدان افزوده شده اند، مثل AutoWeka. مجموعه آزمایش های ما از دو فاز تشکیل شده اند.

۳-۲-۱. فازِ نُخُست

به عنوان فاز نخست آزمایش ، ما زیر مجموعه داده یادگیری KDDTrain_20.arff را که ۲۰ درصد تصادفی از کل دادگان یادگیری ما را تشکیل می دهد را در این نرم افزار به عنوان دادگانِ اوّلِ آزمایش بارگذاری نموده و تست ها ، بدون اعمال الگوریتم انتخاب ویژگی و با 10 fold- Cross validation به شکل زیر انجام شدند.

نرم افزارِ وِکا ، کلاً چهار روش تست را بر روی مجموعه داده ممکن می سازد. از جمله روش دیگر تست که می تواند به عنوان پارامتر ورودی به اختیارِ کاربر به شکل پویا تغییر کند Percentage split می باشد. در این روش می توان تعیین کرد که سیستم تشخیص از چه درصدی از کُل دادگان نفوذ آموزش ببیند و مابقی نیز به تست اختصاص می یابد.

C:\program files\weka – 3 – 8 **java – classpath weka. jar; wekaclassalgo. jar – Xmx3072m weka. gui. GUIChooser**

[1] Dendritic cell Algorithm

[Downloaded from ic4i-journal.ir on 2026-11-23]

جدول (۱): نتایج آزمایش فاز اول با پارامتردهی پیشفرض وِکا (بدون اعمال کاهش ویژگی) در دادگان به اندازه ۲۵۲۳۶ ، ارزیابی مقایسه ای عملکرد در یک بار اجرا

Type	Classifier Alg	TP Rate	FP Rate	Precision	Recall (DR)	F-Measure	MCC	ROC Area	PRC Area	Mean absolute error	Build Time	Root mean squared error	Accuracy	Correctly ٪ Classified Instances	Incorrectly ٪ Classified Instances
Tree	J48 Consolidated	۰,۹۹٦	۰,۰۰٤	۰,۹۹٦	۰,۹۹٦	۰,۹۹٦	۰,۹۹۱	۰,۹۹۸	۰,۹۹٦	۰,۰۰٦۳	٥,۷۳	۰,۰٦٥۱	۰,۹۹٦	۹۹,٥٥۱٤	**۰,٤٤۸٦**
	LADTree	۰,۹۷۷	۰,۰۲٤	۰,۹۷۷	۰,۹۷۷	۰,۹۷۷	۰,۹٥٤	۰,۹۹۷	۰,۹۹۷	۰,۰٤٤٤	٤۰,٥۲	۰,۱۳۱۹	۰,۹۷٦٥	۹۷,۷۰۹٦	**۲,۲۹۰٤**
	NBTree	۰,۹۹۷	۰,۰۰۳	۰,۹۹۷	۰,۹۹۷	۰,۹۹۷	۰,۹۹۳	۰,۹۹۹	۰,۹۹۹	۰,۰۰۳۳	٤٦,۱۱	۰,۰٥٥۳	۰,۹۹۷	۹۹,٦۷٤٥	**۰,۳۲٥٥**
	BFTree	۰,۹۹۷	۰,۰۰۳	۰,۹۹۷	۰,۹۹۷	۰,۹۹۷	۰,۹۹٤	۰,۹۹۸	۰,۹۹٦	۰,۰۰٤۷	۲٦,٤۲	۰,۰٥٥٥	۰,۹۹۷	۹۹,٦۸۲٤	**۰,۳۱۷٦**
	ADTree	۰,۹۸۱	۰,۰۲۰	۰,۹۸۲	۰,۹۸۱	۰,۹۸۱	۰,۹٦۳	۰,۹۹۸	۰,۹۹۸	۰,۰٦۲۷	۱۰,۱۱	۰,۱۳٥۱	۰,۹۸۰٥	۹۸,۱۳٤۳	**۱,۸٦٥۷**
	Random Forest	۰,۹۹۸	۰,۰۰۲	۰,۹۹۸	۰,۹۹۸	۰,۹۹۸	۰,۹۹٦	۱,۰۰۰	۱,۰۰۰	۰,۰۰٦٥	۸,۰۳	۰,۰٤۳۳	۰,۹۹۸	۹۹,۷۹۷٦	**۰,۲۰۲٤**
	Random Tree	۰,۹۹٥	۰,۰۰٥	۰,۹۹٥	۰,۹۹٥	۰,۹۹٥	۰,۹۹۰	۰,۹۹٥	۰,۹۹۳	۰,۰۰٤۹	۰,۱٦	۰,۰٦۹۷	۰,۹۹٥	۹۹,٥۰۷۸	**۰,٤۹۲۲**
	REPTree	۰,۹۹٥	۰,۰۰٥	۰,۹۹٥	۰,۹۹٥	۰,۹۹٥	۰,۹۹۱	۰,۹۹۸	۰,۹۹۷	۰,۰۰٦۸	۱,۰۲	۰,۰٦٥۳	۰,۹۹٥	۹۹,٥٤۳٥	**۰,٤٥٦٥**
Rule	JRip	۰,۹۹٦	۰,۰۰٤	۰,۹۹٦	۰,۹۹٦	۰,۹۹٦	۰,۹۹۲	۰,۹۹۷	۰,۹۹٥	۰,۰۰٥۹	۱۰,۹٤	۰,۰٦۳۲	۰,۹۹٦	۹۹,٥۸۳۲	**۰,٤۱٦۸**
	Decision Table	۰,۹۹۰	۰,۰۱۱	۰,۹۹۰	۰,۹۹۰	۰,۹۹۰	۰,۹۸۰	۰,۹۹۹	۰,۹۹۹	۰,۰۳٦٦	۱٤,۱٦	۰,۱۱۰۳	۰,۹۸۹٥	۹۹,۰۰۷٦	**۰,۹۹۲٤**
	PART	۰,۹۹٦	۰,۰۰٤	۰,۹۹٦	۰,۹۹٦	۰,۹۹٦	۰,۹۹۲	۰,۹۹۸	۰,۹۹۷	۰,۰۰٤۹	۳,۱۳	۰,۰٦۱۹	۰,۹۹٦	۹۹,٦۰۳	**۰,۳۹۷**
Function	(C-SVC) LibSVM	۰,۹۷٤	۰,۰۲۹	۰,۹۷٥	۰,۹۷٤	۰,۹۷٤	۰,۹٤۹	۰,۹۷۲	۰,۹٦۱	۰,۰۲٦	٤٤۸,۹۷	۰,۱٦۱۱	۰,۹۷۲٥	۹۷,٤۰۳۹	**۲,٥۹٦۱**
	LibLINEAR	۰,۹۳٥	۰,۰٦٤	۰,۹۳٦	۰,۹۳٥	۰,۹۳٥	۰,۸۷۱	۰,۹۳٦	۰,۹۰۸	۰,۰٦٤٥	٦,۱۹	۰,۲٥٤۱	۰,۹۳٥٥	۹۳,٥٤٥٦	**٦,٤٥٤٤**
	MLPClassifier	۰,۹۷۹	۰,۰۲۳	۰,۹۷۹	۰,۹۷۹	۰,۹۷۹	۰,۹٥۷	۰,۹۸۷	۰,۹۸٤	۰,۰۳۹۲	۱۰,۹۷	۰,۱۳٦۸	۰,۹۷۸	۹۷,۸٥۲٥	**۲,۱٤۷٥**
Immune	AIRS2	-	-	-	-	-	-	-	-	-	High	-	-	-	-
	AIRS2Parallel	-	-	-	-	-	-	-	-	-	High	-	-	-	-
	CLONALG	۰,٦۸٤	۰,۲۹۷	۰,۷۱۱	۰,٦۸٤	۰,٦۷۹	–	۰,٦۹۳	–	۰,۳۱٦۳	۹,۲۲	۰,٥٦۲٤	۰,٦۹۳٥	٦۸,۳٦٦۹	**۳۱,٦۳۳۱**
	CSCA	-	-	-	-	-	-	-	-	-	High	-	-	-	-
	Immunos2	۰,۸۸۹	۰,۱۲٤	۰,۹۰۲	۰,۸۸۹	۰,۸۸۸	–	۰,۸۸۳	–	۰,۱۱۰٦	۰,۱۷	۰,۳۳۲٦	۰,۸۸۲٥	۸۸,۹٤۰۹	**۱۱,۰٥۹۱**
	Immunos99	-	-	-	-	-	-	-	-	-	High	-	-	-	-

برخی از تکنیکهای به کار رفته در جدول ۱ مثل ARIS ، CSCA ، immunos99 دارای پیچیدگی زمانی بالایی در فاز یادگیری اوّلیه برای ایجاد مدل هستند. شکل (۳) تصویری از محیط نرم افزار وکا نُسخه ۳,٦ بوده که دسته بندهای ایمنی مصنوعی را نشان می دهد.

فاز یادگیریِ الگوریتم های ایمنی مصنوعی در اجرای اوّل بسیار طولانی تر است. این به علّت تولیدِ حافظه تشخیص دهنده های بالغ از طریق تولید و تکثیرِ آنها در حین فرایندِ تست و همچنین کسب تجربه لازم در برخورد با داده عظیم می باشد.

[Downloaded from ic4i-journal.ir on 2026-11-23]

کسب این تجربه وابستگی زیادی به پارامترها و حدود آستانه و نرخ های تکثیرِ انتخاب شده توسط کاربر دارد که چالش سیستم ایمنی مصنوعی میباشد. این الگوریتمها همگی پارامترهای مهم ورودی دارند که مقدار آن توسط کاربر تعیین می گردد. به عنوان نمونه برای متدهای انتخاب هایی که پس از شروع به کارِ این دو الگوریتمِ انتخابِ تکثیری تولید می شوند از رابطه زیر بدست می آید. [۱٤]

$$N_c = \sum_{i=1}^{n} \left\lfloor \frac{\beta.N}{i} + 0.5 \right\rfloor \qquad (۱)$$

استراتژی خود الگوریتم تعیین می شود . مطابق مطالب گفته شده در بخش پیشینه تحقیق، استراتژی الگوریتم انتخاب تکثیری توسط آنتی بادیها (تشخیص دهنده ها) بدست می آید. بطوریکه اگر آنتی بادی $\boldsymbol{i}$ اُم تعداد بیشتری تشخیص غیر خودی را در طولِ عُمر خود انجام داده باشد Affinity آن بالا می رود و بدین ترتیب آنتی بادیهایی که تشخیصی انجام نداده اند جهش می یابند و سیستم مجددا به به شکل تصادفی آنتی بادی جدید تولید می کند. Affinity در اصل به میزان مشابهتِ الگوی دو رشته آنتی بادی (خودی تولید شده) و غیر خودی (اتک) گفته می شود که هر چه این میزان بالا باشد بهتر بوده و تکثیرِ آن آنتی بادی بالا می رود. البته نرخ تکثیر در این آزمایش برابر $\boldsymbol{\beta = 0.2}$ پیشفرض در مرحله شروع به کار الگوریتم تعیین شد که در واقع نرخ مناسب و با هر بار تشخیص موفّق، برای آنتی بادی $\boldsymbol{i}$ متغیر است. جالب است بدانید معیار مورد استفاده برای Affinity در اکثر مقالات فاصله همینگ (Hamming distance) میباشد. سیستمِ ایمنی

در زیر مجموعه داده تصادفی انتخاب شده (با اندازه ۲۵۲۳٦) بسیار بالا بوده و چندین ساعت طول می کشد.

تکثیری CLONALG/CSCA اندازه جمعیت آنتی بادیها یا Antibody Pool، اندازه حافظه سلولهای حافظه B ، فاکتور تکثیر یا β، تعداد تکثیر (numClone) از جمله مهمترین پارامترهای ایمنی مصنوعی می باشند. مجموع تعداد تکثیر

که N اندازه استخر آنتی بادی که در این آزمایش برابر ۱۵۰ آنتی بادی تعیین گردید، $\mathbf{N_c}$ مجموع کل تعداد تکثیرهای مربوط به کل آنتی بادیها که تعداد شانN تا می باشد. $\boldsymbol{n}$ تعداد آنتی بادیهای انتخاب شده برای تکثیر که توسط

پس از اوّلین دوره یادگیری خود به مرورِ زمان نتایجِ مطلوبِ تجربه ی کسب شده را در حافظه خود memory B cells برای دفعاتِ بعد ثبت می کند در نتیجه در مواجهه با نمونه ای با الگوی ناشناخته ، پتانسیل تشخیص غیر خودی بالاتر رفته و سیستم تشخیص پویایی لازم را در دراز مدت از خود نشان می دهد. دسته بندهای ایمنی مصنوعیِ immunos99 و ARIS2parallel بر خلاف الگوریتمهای رایج دسته بندی ، با تکرارهای مکرّر و با تغییر پارامتردهی ورودی از سوی کاربر، نرخ دسته بندی و تشخیص غیر خودی (نفوذ) آنها به مراتب بهبود محسوسی می یابد. درصورتیکه ما این بهبود را در بیشتر تکنیکهای مبتنی بر داده کاوی و یادگیری ماشینِ رایج چندان مشاهده نمی نماییم. این خصوصیّتِ مهمّ، دست برنامه نویسان و مهندسان را در توسعه این الگوریتم های زیست مبنا باز تر می کند تا چالشهای اساسی آنها را برطرف نمایند. در طول انجامِ آزمایش نخست مشاهده گردید که زمان تست و یادگیری اوّلیه متدهای ایمنی مصنوعی immunos99 ARIS2parallel, CLONALG, CSCA, ARIS بنابراین ما موقّتاً تا زمان بهبودِ آنها از انجام برخی تست ها صرف نظر نمودیم و به جای آن ، این بار همین آزمایش را

[Downloaded from ic4i-journal.ir on 2026-11-23]

با دَه درصد تصادفیِ یکنواخت از این زیر مجموعه (اندازه ۲۵۲٤ رکورد) تست نموده و با عملکردِ سایر دسته بندهای موجود در جدول قبل مقایسه نمودیم. نتایج بر اساس پارامترهای پیشفرضِ وکا به شرح زیر می باشند.

جدول (۲): نتایج آزمایش فاز اول با پارامتردهی پیشفرض (بدون اعمال کاهش ویژگی) به اندازه ۲۵۲٤ ، ارزیابی مقایسه ای عملکرد با تکرار اجرا

Type	Classifier Alg	TP Rate	FP Rate	Precision	Recall (DR)	F-Measure	MCC	ROC Area	PRC Area	Mean absolute error	Build Time	Root mean squared error	Accuracy	Correctly ٪ Classified Instances	Incorrectly ٪ Classified Instances
Tree	J48 Consolidated	۰,۹۸٤	۰,۰۱٦	۰,۹۸٤	۰,۹۸٤	۰,۹۸٤	۰,۹٦۸	۰,۹۸۸	۰,۹۸۳	۰,۰۲۱٦	۰,۳۳	۰,۱۲۳۸	۰,۹۸٤	۹۸,٤۲٦۸	**۱,٥۷۳۲**
	LADTree	۰,۹۷۳	۰,۰۲۷	۰,۰۲۷	۰,۰۲۷	۰,۹۷۳	۰,۹٤۷	۰,۹۹٦	۰,۹۹٦	۰,۰٤۷۲	۲,۷۳	۰,۱۳۸۷	۰,۹۷۳	۹۷,۳۳۷٦	**۹۷,۳۳۷٦**
	NBTree	۰,۹۸۹	۰,۰۱۱	۰,۹۸۹	۰,۹۸۹	۰,۹۸۹	۰,۹۷۸	۰,۹۹٦	۰,۹۹٦	۰,۰۱۱۱	۷,۱۳	۰,۰۹۷	۰,۹۸۹	۹۸,۹۱۰۹	**۱,۰۸۹۱**
	BFTree	۰,۹۸٤	۰,۰۱٦	۰,۹۸٤	۰,۹۸٤	۰,۹۸٤	۰,۹٦۹	۰,۹۹۲	۰,۹۸۹	۰,۰۱۹۱	۳,٤٤	۰,۱۲۱۷	۰,۹۸٤	۹۸,٤۲٦۸	**۱,٥۷۳۲**
	ADTree	۰,۹۷۱	۰,۰۲۹	۰,۹۷۱	۰,۹۷۱	۰,۹۷۱	۰,۹٤۳	۰,۹۹۷	۰,۹۹۷	۰,۰٥٦٥	۰,٥۲	۰,۱٤۳۳	۰,۹۷۱	۹۷,۱۳٥۹	**۲,۸٦٤۱**
	Random Forest	۰,۹۹٤	۰,۰۰٦	۰,۹۹٤	۰,۹۹٤	۰,۹۹٤	۰,۹۸۷	۱,۰۰۰	۱,۰۰۰	۰,۰۲۰۸	۰,٤۸	۰,۰۷۷۸	۰,۹۹٤	۹۹,۳٥٤٦	**۰,٦٤٥٤**
	Random Tree	۰,۹۸۳	۰,۰۱۷	۰,۹۸۳	۰,۹۸۳	۰,۹۸۳	۰,۹٦٥	۰,۹۸٥	۰,۹۷۸	۰,۰۱۷	~۰	۰,۱۲٦۹	۰,۹۸۳	۹۸,۲٦٥٤	**۱,۷۳٤٦**
	REPTree	۰,۹۸۱	۰,۰۱۹	۰,۹۸۱	۰,۹۸۱	۰,۹۸۱	۰,۹٦۳	۰,۹۹۲	۰,۹۸۹	۰,۰۲۳۸	۰,۱٤	۰,۱۲۰۲	۰,۹۸۱	۹۸,۱٤٤٤	**۱,۸٥٥٦**
Rule	JRip	۰,۹۹۰	۰,۰۱۰	۰,۹۹۰	۰,۹۹۰	۰,۹۹۰	۰,۹۸۱	۰,۹۹۲	۰,۹۸۹	۰,۰۱٤۳	۰,۸٤	۰,۰۹۷۱	۰,۹۹۰	۹۹,۰۳۱۹	**۰,۹٦۸۱**
	Decision Table	۰,۹۷۹	۰,۰۲۲	۰,۹۷۹	۰,۹۷۹	۰,۹۷۹	۰,۹٥۷	۰,۹۹٤	۰,۹۹۲	۰,۰۷۱۸	۱,۱٤	۰,۱٥۷۳	۰,۹۷۸٥	۹۷,۸٦۲	**۲,۱۳۸**
	PART	۰,۹۸٥	۰,۰۱٥	۰,۹۸٥	۰,۹۸٥	۰,۹۸٥	۰,۹٦۹	۰,۹۹۰	۰,۹۸٦	۰,۰۱۹۲	۰,۱٤	۰,۱۱۸٥	۰,۹۸٥	۹۸,٤٦۷۱	**۱,٥۳۲۹**
Function	(C-SVC) LibSVM	۰,۹۲۱	۰,۰۸٥	۰,۹۳۱	۰,۹۲۱	۰,۹۲۰	۰,۸٥۱	۰,۹۱۸	۰,۸۹۰	۰,۰۷۹٥	۲,٤۸	۰,۲۸۱۹	۰,۹۱۸	۹۲,۰٥۳۲	**۷,۹٤٦۸**
	LibLINEAR	۰,۸۹۸	۰,۰۹۹	۰,۹۰۲	۰,۸۹۸	۰,۸۹۸	۰,۸۰۰	۰,۹۰۰	۰,۸٦۰	۰,۱۰۱۷	۰,٥٥	۰,۳۱۸۸	۰,۸۹۹٥	۸۹,۸۳٤٦	**۱۰,۱٦٥٤**
	MLPClassifier	۰,۹۷۹	۰,۰۲۱	۰,۹۷۹	۰,۹۷۹	۰,۹۷۹	۰,۹٥۸	۰,۹۹۳	۰,۹۹۲	۰,۰۳۹٦	۳,۳۸	۰,۱۳٥۲	۰,۹۷۹	۹۷,۹۰۲٤	**۲,۰۹۷٦**
Immune	AIRS2	۰,۹۷۱	۰,۰۲۹	۰,۹۷۱	۰,۹۷۱	۰,۹۷۱	–	۰,۹۷۱	–	۰,۰۲۸٦	۲۱۳۰,۸	۰,۱٦۹۲	۰,۹۷۱	۹۷,۱۳٥۹	**۲,۸٦٤۱**
	AIRS2Parallel	-	-	-	-	-	–	-	–	-	-	-	-	-	-
	CLONALG	۰,۸۷٦	۰,۱۲۲	۰,۸۷۸	۰,۸۷٦	۰,۸۷٦	-	۰,۸۷۷	-	۰,۱۲۳۸	۱,۳۹	۰,۳٥۱۹	۰,۸۷۷	۸۷,٦۱٦	**۱۲,۳۸٤**
	CSCA	۰,۹۳٤	۰,۰٦٦	۰,۹۳٤	۰,۹۳٤	۰,۹۳٤	-	۰,۹۳٤	-	۰,۰٦٦۲	٤۷,۲٥	۰,۰٦٦۲	۰,۹۳٤	۹۳,۳۸٤٤	**٦,٦۱٥٦**
	Immunos2	۰,۸۹۳	۰,۱۱۱	۰,۸۹٦	۰,۸۹۳	۰,۸۹۲	-	۰,۸۹۱	-	۰,۱۰۷۳	۰,۰۲	۰,۳۲۷٦	۰,۸۹۱	۸۹,۲٦۹۹	**۱۰,۷۳۰۱**
	Immunos99	۰,۹۰٤	۰,۰۹۷	۰,۹۰٥	۰,۹۰٤	۰,۹۰٤	–	۰,۹۰٤	–	۰,۰۹٥٦	٤۰٥,۲۲	۰,۳۰۹۲	۰,۹۰۳٥	۹۰,٤۳۹۷	**۹,٥٦۰۳**

با بررسی جدول (۲) مشاهده میگردد که در بین درخت های تصمیم گیری، R Forest نسبت به بقیّه دسته بندها از دقت بالاتری (۰,۹۹٤) برخوردار بوده و در بین متدهای ایمنی مصنوعی نیز به ترتیب CSCA و Immunos99 در مقایسه با سایرِ این متدها بهتر عمل نموده اند. این نتایج را می توان در منحنی RoC به خوبی استنباط نمود.

[Downloaded from ic4i-journal.ir on 2026-11-23]

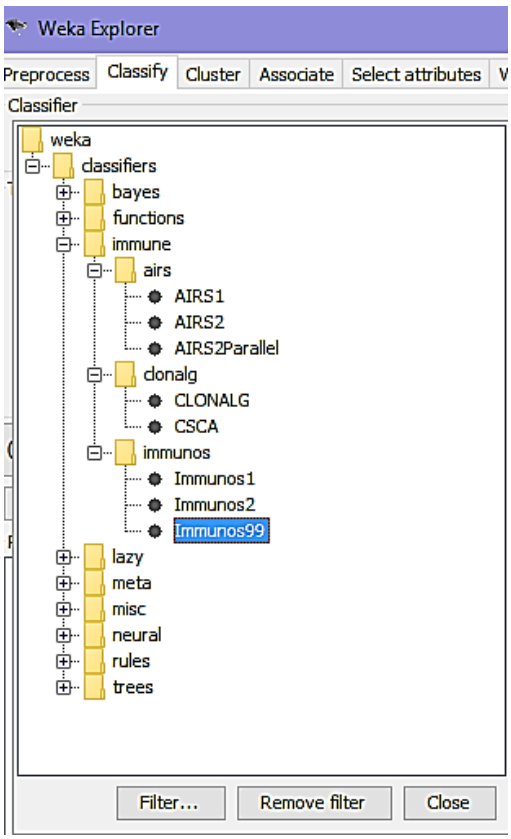
همچنین در بین متدهای Rule نیز DT و JRip و در بین توابع نیز MLP و سپس LibSVM بهتر عمل نموده اند. ولی در بین متدهای ایمنی مصنوعی نمی توان بررسی دقیقی داشت. به گونه ای که در ادامه آزمایشات (فاز دوّم) مشاهده می شود که عملکرد متدهای ایمنی مصنوعی با اعمال فرایند کاهش ویژگی و بروز رسانی، نرخ پارامترهای ورودی به شدّت تغییر یافته و کاربرد انتخاب ویژگی در مورد آنها بسیار مطلوبتر و ضروری به نظر می رسد.

الگوریتم immunos ترکیبی از دو الگوریتم AIRS و CNOLANG می باشد که هردوی آنها از متد انتخاب تکثیری و از تئوری ایمنی اکتسابی[1] الهام گرفته شده اند. این الگوریتم بواسطه گروه هایی از عوامل خودی (تشخیص دهنده های بالغ موثر)، B cell ها یا حافظه تشخیص دهنده های سیستم را آماده کند تا بتوانند نوعی از آنتی ژن با الگویی خاص را شناسایی و برچسب بزنند. [۱۰] [۱٤]

در نتیجه این الگوریتمها با تغییر پارامترها طی run هـــــــای مکرّر ، نرخ های خروجیِ تشخیص و کارائی آنها تغییر محسوسی پیدا می کنند. بطوریکه گاهی تفاوت زیادی بین نرخ های تشخیص برای دو نوع ترافیک نرمال و آنومالی نسبت به سیکلهای اجرای قبلِ در این الگوریتمها مشاهده می گردد و در نتیجه پایدار نیستند. بنابراین میانگینِ این معیارها به درستی نرخ های تشخیص و کارائی را نشان نمی دهند. چراکه سیستم ایمنی مصنوعی بسته به شرایطِ پارامتریک در نرخ های مختلف تکثیر ، نرخ حدود آستانه تعیین شده و حجم داده و نوع تست (n-fold یا ...) ، دسته بندی متفاوتی را در مواجهه با دو نوع ترافیک نرمال و آنومالی دارند. در نتیجه می توان گفت این سیستم ها بیشتر به پارامترهای ورودی کاربر حساسیت دارند و این حساسیت نسبت به سایر دسته بند های رایج بیشتر است.

سیستم ایمنی مصنوعی تلفیقی از دو رویکرد known good و known bad در تشخیص آنومالی از نرمال ارئه می دهد. محقّقان همواره سعی داشته اند این تلفیق را بهبود داده و سیستم AIS را پویاتر نمایند. تاکنون تحقیقی ارائه نشده که به شکل جامع بتواند با تلفیق این دو راهکار، چالشهای ایمنی مصنوعی را در تشخیص نفوذ رفع نماید.

شکل (۳): دسته بندهای ایمنی مصنوعی نرم افزار وکا نسخه ۳,٦



این چالشها عبارتند از : تولید تشخیص دهنده های بالغ ، یادگیری در حین تشخیص و بالعکس ، بلادرنگ

[1] Adaptive immunity theory

[Downloaded from ic4i-journal.ir on 2026-11-23]

بودن تشخیص و مقابله با حملات روز صفر[1]. آسیب پذیری روز صفر – حمله ای که در روز کشف آن توسط متخصّصانِ امنیت و قبل از شناسایی آن رخ دهد. البته پویایی پارامتریک سیستم ایمنی مصنوعی ، خود می تواند یک مزیّت نیز باشد زیرا سیستم همواره به شکلی پویا در حال پردازش و رُشدِ ایمنی بوده و در این حیات مصنوعی، همواره به دو فرایندِ تکثیر و بلوغ (بروز رسانی پایگاه داده های خود و اصلاح رشته ها، تشخیص دهنده ها) می پردازد که این ایعنی یادگیری در حین تشخیص و بالعکس. از جدول (۲) ملاحظه می شود که تقریباً تمامی دسته بند ها دارای خطا بوده و دقت آنها نسبتاً پایین است. این به دلیل درگیر شدن دسته بند با ویژگیهای اضافی و غیر مرتبط [2] می باشد.

به منظور افزایش دقت دسته بند ها و ارزیابی مقایسه ایِ کارائی هر کدام، موثّرترین تکنیکهای کاهش ویژگی بر روی دادگان مربوطه مورد آزمایش قرار گرفتند. در این تکنیکها استراتژیهای جستجوی مبتنی بر Swarm Intelligence (هوش ازدحامی جانداران) به کار رفته اند. همچنین از رویکرد "راپر" نیز علیرغم نقطه قوّت آن در افزایش دقّت تشخیص و کاهش خطا به دلیل زمان زیاد یادگیریِ آن استفاده نشد. همانگونه ای که از این جدول قابل مشاهده است هر یک از این الگوریتمهای کاهش ابعاد با استراتژی جستجوی متفاوت در ترکیب با یکدیگر رویکرد کاهش ابعاد را تشکیل می دهند و در هر بار تست با استراتژی های مختلف می توانند زیر مجموعه ویژگیهای متفاوتی را به عنوان زیر مجموعه بهینه از بین کُل ۴۱ ویژگی انتخاب نمایند. نتیجه مطلوبِ بررسی و ارزیابی مقایسه ایِ رویکردهای کاهش ویژگی در جدول (۳) به عنوان فاز دوّم آزمایش به کار رفته اند.

قبل از اینکه به ارزیابی این جدول بپردازیم نیاز است که معیاری کلی برای تعیین اینکه کدام یک از متدهای فوق می توانند با پارامترهای پیش فرض و در شرایط یکسان آزمایش، زیر مجموعه ویژگی بهتری را از بین ۴۱ ویژگی مرتبط و نا مرتبط انتخاب نمایند. بنابراین به کمک متد Information Gain که میزان اطلاعات بدست آمده از هر ویژگی را محاسبه و بدست می دهد می توان آمار دقیق ویژگیهای غیر مرتبط و اضافی را بدست آورد. [۲۱][۳۱]

البته این اطلاعات کلی بوده و تنها در شرایطی کاربرد دارد که هدف، صرفاً دسته بندی ما باینری، تفکیکِ غیر خودی (ترافیک آنومالی) از خودی (نرمال) باشد نه دسته بندی حملات به گروه چهارگانه. به عبارت دیگر در شرایطی که آزمایش به گونه ای باشد که دسته بندیِ نوع و جزئیّاتِ حمله مد نظر بوده و نه صرفاً تشخیص آنومالی از نرمال، این اطلاعات کمکی نمی کنند و حتّی ممکن است حذفِ یک ویژگیِ خاص که اطلاعات کمتری نسبت به بقیه می دهد اشتباه نیز بوده باشد. در [۲۱] ، پژوهشگر بهره اطلاعات[3] هر یک از ۴۱ ویژگی در دیتاست **NSL – KDD** را به کمک رابطه زیر بدست آورده است:

$$Gain(S.A) \equiv Entropy\ (s) - \sum_{v \in Values(A)}^{n} \left(\frac{|S_v|}{|S|}\ Entropy\ (S_v)\right) \quad (۲)$$

[1] Zero days Vulnerabilities
[2] Redundant & non-related
[3] Information Gain (IG)

[Downloaded from ic4i-journal.ir on 2026-11-23]

جدول (۳): نتیجه اعمال رویکردهای مختلف انتخاب/کاهش ویژگی بر روی دادگان

شماره ردیف	اولویت	الگوریتم انتخاب ویژگی (ارزیاب)	متد (استراتژی) جستجو	تعداد ویژگیهای انتخاب شده	نام ویژگیها
۱	۱۲	CfsSubsetEval	Best First	۵	۵،۶،۱۲،۳۰،۳۹
۲	۱۰		Ant Search	۶	۵،۶،۱۲،۲۳،۳۰،۳۹
۳			Bat Search	۵	۵،۶،۱۲،۲۹،۳۸
٤			Bee Search	۵	۵،۶،۱۲،۲۶،۳۰
۵	۸		CuckooSearch	۸	۳،۵،۶،۱۲،۲۲،۲۵،۲۹،۳۹
۶	۹		GeneticSearch	۱۰	۵،۶،۱۲،۱٤،۱۹،۲۳،۲۵،۳۰،۳٤،۳۹
۷			PSOSearch	۵	۵،۶،۱۲،۲۹،۳۸
۸	۱۵		HarmonySearch	٤	۵،۶،۱۲،۳۰
۹		ChiSquaredAttributeEval	Ranker	٤۱	همه
۱۰		Classifier subset evaluator	Ant Search	۱	۲
			...	۱	
۱۱	۶	ConsistencySubsetEval	Ant Search	۹	۱،۳،۵،۶،۲۹،۳۲،۳٤،۳۵،۳۹
۱۲	۲		BatSearch	۱۵	۱،۲،۳،٤،۵،۶،۷،۲۳،۲۷،۲۹،۳۱،۳۳،۳٤،۳۶،۳۹
۱۳	٤		BeeSearch	۹	۱،۳،۵،۱۹،۲۰،۲۳،۳۲،۳۳،۳۶
۱٤	۵		Best First	۷	۱،۳،۵،۲۳،۳۲،۳۳،۳۶
۱۵	۱		CuckooSearch	۱۲	۱،۲،۳،۵،۹،۲۲،۲٤،۲۷،۳۱،۳۳،۳۵،۳۶
۱۶	۳		PSOSearch	۱۱	۳،۵،۹،۱۳،۲۳،۳۲،۳۳،۳٤،۳۶،۳۹،٤۱
۱۷	۱۱	FilteredSubsetEval *	Ant Search	۶	۵،۶،۱۲،۲۳،۳۰،۳۹
۱۸			BatSearch	٤	۵،۱۲،۲۹،۳۸
۱۹	۱۳		BeeSearch	۵	۵،۶،۱۲،۲۶،۳۰
۲۰	۱٤		Best First	۵	۵،۶،۱۲،۳۰،۳۹
۲۱	۷		CuckooSearch	۸	۳،۵،۶،۱۲،۲۲،۲۵،۲۹،۳۹
۲۲			PSOSearch	۵	۵،۶،۱۲،۲۹،۳۸
۲۳		GainRatioAttributeEval	Ranker	٤۱	همه
۲٤		InfoGainAttributeEval	Ranker	٤۱	همه
۲۵		principal components analysis	Ranker	75 Eigenvectors	Ranked attributes *

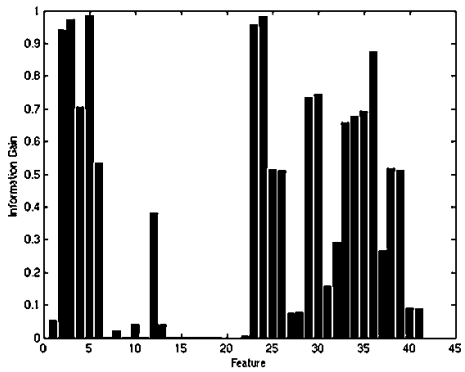
نحوه بدست آوردن بهره اطلاعات هر ویژگی به صورت زیر می باشد. [۲۳] اگر S دادگان یادگیری با $\mathbf{m}$ کلاس و نمونه های یادگیری شامل s_i نمونه از کلاس $\mathbf{I}$ و s کل تعداد نمونه ها در نمونه یادگیری باشند ، اطلاعات مورد انتظار که برای دسته بندی یک نمونه مورد نیاز است، با رابطه زیر محاسبه می گردد:

$$I(s_1.s_2 \ldots . s_m) = -\sum_{i=1}^{m} \frac{s_i}{s} \log(\frac{s_i}{s}) \quad (۳)$$

یک ویژگی F با مقادیر $\{f_1.f_2.\ldots.f_v\}$ می تواند دادگان یادگیری را به v زیر مجموعه $\{S_1.S_2.\ldots.S_v\}$ تقسیم کند که $\mathbf{S_j}$ زیر مجموعه ای است که مقدار f_j را برای ویژگی F دارد. بنابراین $\mathbf{S_j}$ شامل s_{ij} نمونه از کلاس i می باشد. آنتروپی ویژگی F به از رابطه زیر بدست می آید.

[Downloaded from ic4i-journal.ir on 2026-11-23]

$$E(F) = \sum_{j=1}^{v} \frac{s_{1j}+\cdots+s_{mj}}{s} \times \left(s_{1j}.s_{2j} \ldots . s_{mj}\right)$$



(٤)

در نتیجه ، بهره اطلاعات برای ویژگی $\boldsymbol{F}$ از رابطه زیر بدست آید:

$$Gain(F) = I(s_1.s_2 \ldots . s_m) - E(F) \qquad (٥)$$

تحقیق [۲۳] بَهره اطلاعات هر ویژگی را در دادگان نفوذ NSL-KDD را به صورت نمودار (۱) محاسبه نموده است. اطلاعات ویژگیها در این نمودار ، برای هر زیر مجموعه تصادفی انتخاب شده از دادگان نفوذ تقریباً در همین حدود می باشد. همانگونه که مشاهده می گردد ویژگیهای ۲،۳،۵،۲۳،۲٤،۳٦ بالاترین نرخ بهره اطلاعات را ارائه می دهند، توجه شود که ویژگیهای ۲،۳ از نوع غیر عددی می باشند. در ادامه آزمایشات ، ما از نرخ های بهره ویژگیها استفاده نموده و آنها را به ترتیب نزولی از چپ به راست بر اساس میزان بهره اطلاعات اولویت بندی نمودیم. سطرها نیز معرّف الگوریتم های فراابتکاری کاهش ابعاد می باشند که در جدول (٤) ارزیابی شده اند. در این جدول زیرمجموعه ویژگیهای انتخاب شده در هر یک از این رویکردها به ترتیب اولویت بهره اطلاعات به تفکیک مشخص شده اند.

نمودار (۱): میزان اطلاعات بدست آمده از هر ویژگی از دادگان نفوذ

از جمع بندی نتایج حاصل از ارزیابی جدول فوق و مقایسه نتایج آن با اطلاعات نمودار (۱) مشاهده می شود که به ترتیب از چپ به راست رویکردهای کاهش ویژگیِ ۱۵،۱۲،۱٦،۱۳،۱٤،۱۱،۲۱،۵،٦،۲،۱۷،۱،۱۹،۲۰،۸ در مجموع دارای پتانسیل بالقوّه و موثری برای کاربرد در ایجاد مدل تشخیص نفوذ هستند ، زیرا این ویژگیها در اکثر رویکردها انتخاب شده اند. بنابراین الگوریتمهای جستجوی کوکو ، Bat ، PSO ، Bee ، Ant ،Genetic نسبت به بقیه زیر مجموعه های موثرتری را نتیجه می دهند. بعلاوه این زیر مجموعه ها اطلاعات بیشتری را در اختیار دسته بند قرار میدهند. ما در بین این رویکردها مواردی که تعداد ویژگیهای انتخاب شده آنها کمتر یا خیلی بیشتر است را حذف نموده و مطلوب ندانستیم.

ذکر این نکته ضروری است که در ایجاد هر نوع حمله ای (از بین چهار نوع حمله ممکن) فقط برخی از این ویژگیها بر رخداد آن حمله موثراند. به عنوان مثال برای حملات از نوع U2R و R2L صرفاً با ویژگیهای "مُحتوایی" در دادگان، می توان این نوع حملات را کشف کرد و انواع دیگر ویژگیها تاثیر چندانی در کشف این حملات ندارند. [۲۰]

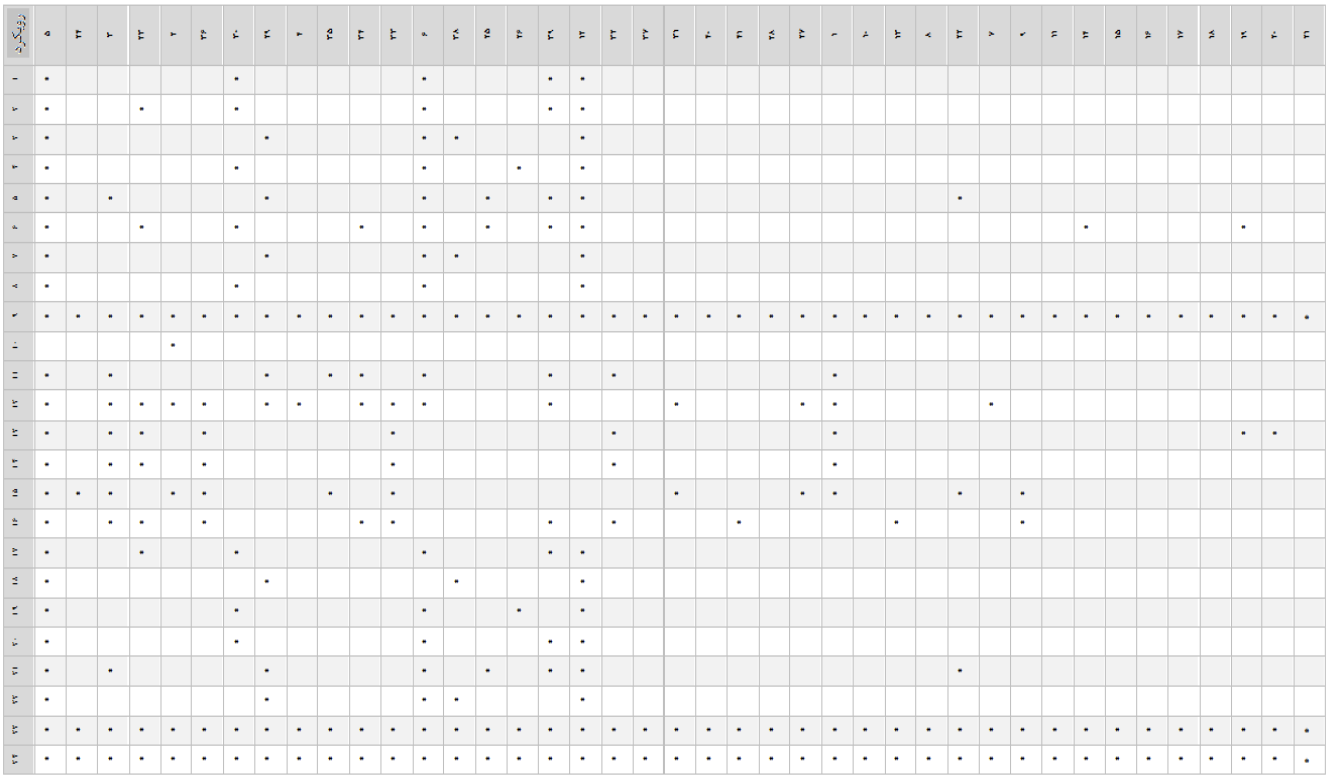
۳-۲-۲. فاز دوّم

از بین رویکرد های انتخاب ویژگی ارزیابی شده در فاز اوّل در جدول ۳ ، ما شش رویکرد را مطابق جدول ۵

[Downloaded from ic4i-journal.ir on 2026-11-23]

انتخاب نموده و بر روی پارامترهای آن بررسی هایی را به منظور انتخاب پارامترهای بهینه انجام دادیم تا زیر مجموعه های بهتری را نتیجه دهند.

جدول (٤): استخراج بهترین رویکرد کاهش ویژگی با تطبیق زیر مجموعه ویژگیهای آن با میزان اطلاعات هر ویژگی بر اساس اولویت



جدول (٥): رویکردهای انتخاب شده دارای موثرترین ویژگیها جهت اعمال بر ورودی دسته بند

نام رویکرد کاهش ویژگی (به ترتیب اولویت)	تعداد ویژگی	ویژگیها
CuckooSearch + ConsistencySubsetEval	١٢	١،٢،٣،٥،٩،٢٢،٢٤،٢٧،٣١،٣٣،٣٥،٣٦
Batsearch + ConsistencySubsetEval	١٥	١،٢،٣،٤،٥،٦،٧،٢٣،٢٧،٢٩،٣١،٣٣،٣٤،٣٦،٣٩
PSOSearch + ConsistencySubsetEval	١١	٣،٥،٩،١٣،٢٣،٣٢،٣٣،٣٤،٣٦،٣٩،٤١
BeeSearch + ConsistencySebsetEval	٩	١،٣،٥،١٩،٢٠،٢٣،٣٢،٣٣،٣٦
AntSearch + ConsistencySubsetEval	٩	١،٣،٥،٦،٢٩،٣٢،٣٤،٣٥،٣٩
GeneticSearch + CfsSubsetEval	١٠	٥،٦،١٢،١٤،١٩،٢٣،٢٥،٣٠،٣٤،٣٩

جدول (٦): رویکردهای کاهش ویژگی (بهبود یافته) دارای موثرترین ویژگیها جهت اعمال بر ورودی دسته بند

نام رویکرد کاهش ویژگی (به ترتیب اولویت)	تعداد ویژگی	ویژگیها
CuckooSearch + ConsistencySubsetEval	٧	٣،٥،٢٥،٣٢،٣٤،٣٥،٣٦
Batsearch + ConsistencySubsetEval	١٤	١،٣،٤،٥،٨،١٥،١٧،١٨،٢٣،٢٥،٣٢،٣٣،٣٦،٣٨
PSOSearch + ConsistencySubsetEval	٧	٣،٥،٣٢،٣٤،٣٥،٣٦،٣٩
BeeSearch + ConsistencySebsetEval	١٠	١،٣،٥،١٥،٣٤،٣٥،٣٦،٣٧،٣٩،٤١
AntSearch + ConsistencySubsetEval	١١	٣،٥،١٩،٢٦،٣٠،٣٢،٣٣،٣٤،٣٦،٣٧،٣٩
GeneticSearch + CfsSubsetEval	١٠	٤،٥،٦،٨،١٢،٢٩،٣٢،٣٣،٣٤،٣٨

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ١، بهار ١٣٩٧

[Downloaded from ic4i-journal.ir on 2026-11-23]

در جستجوی کوکو ، نرخ های accelerate type را از حالت نرمال خارج و Population Size، iteration را دو برابر نموده و مقدار سیگما را از مقدار پیش فرض آن به مقدار ۰,۸ افزایش دادیم. همچنین نرخ فرکانس گزارش دهی نیز ۸۰ ست شد. در جستجوی خفّاش نیز type accelerate را به سریع ست کرده ، فرکانس به ۰,۵ و iteration نیز دو برابر شد. همچنین پارامتر mutationProb (احتمال جهش) را افزایش داده و از مقدار پیشفرض آن یعنی ۰,۰۲ به ۰,۰۸ ارتقا دادیم. مقادیر پارامترهای جمعیت نیز دو برابر (٤٠) و مقدار پارامتـــــر نرخ گزارش دهی به ۵۰ تنظیم شد. در مورد الگوریتم استراتژی جستجو PSOSearch (ازدحام ذرّات) نیز بنا به استناد به مقاله [٦] مقادیر پارامترهای Population به ۱۵۰ و C1 و C2 نیز پیشفرض ۰,۳٤ انتخاب شد. برای الگوریتم جستجوی Bee search (زنبور) نیز مقادیر شتاب ، تکرار، جمعیت ، فرکانس را دو برابر و مقدار احتمال

جدول (۷): نتایج آزمایش فاز دوّم ، ارزیابی مقایسه ای (با اعمال بهترین کاهش ویژگی - جدول ٦)

Classifier Alg	FS	cc	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Mean absolute error	Execution Time	Root mean squared error	Accuracy	Correctly Classified Instances	Incorrectly Classified Instances
Random Forest	Bat	۰,۹۸۴	۰,۹۹۲	۰,۰۰۸	۰,۹۹۲	۰,۹۹۲	۰,۹۹۲	۰,۹۸۴	۱,۰۰۰	۱,۰۰۰	۰,۰۲۱۷	۰,۲	۰,۰۸۳۸	۰,۹۹۲	۹۹,۱۹۳۲	۰,۸۰٦۸
C4.5	Genetic	۰,۹۷۲	۰,۹۸۶	۰,۰۱۴	۰,۹۸۶	۰,۹۸۶	۰,۹۸۶	۰,۹۷۲	۰,۹۸۸	۰,۹۸۳	۰,۰۱۸	۰,۰۹	۰,۱۱۷۵	۰,۹۸۶	۹۸,۵۸۸۱	۱,٤۱۱۹
NBTree	Genetic	۰,۹۷۶	۰,۹۸۹	۰,۰۱۲	۰,۹۸۹	۰,۹۸۹	۰,۹۸۹	۰,۹۷۷	۰,۹۹۷	۰,۹۹۶	۰,۰۱۵۹	۰,۵۲	۰,۱۰۰۸	۰,۹۸۸۵	۹۸,۸۷۰۵	۱,۱۲۹۵
BFTree	Bat	۰,۹۷۴	۰,۹۸۷	۰,۰۱۳	۰,۹۸۷	۰,۹۸۷	۰,۹۸۷	۰,۹۷۴	۰,۹۹۳	۰,۹۹۱	۰,۰۱۶۲	۰,۴۷	۰,۱۰۹۷	۰,۹۸۷	۰,۹۷۴۲	۰,۰۱۶۲
LADTree	Genetic	۰,۹۵۷	۰,۹۷۸	۰,۰۲۲	۰,۹۷۸	۰,۹۷۸	۰,۹۷۸	۰,۹۵۶	۰,۹۹۴	۰,۹۹۳	۰,۰۵۱۴	۰,۱۶	۰,۱۳۹۵	۰,۹۸۷	۹۷,۸۲۱۷	۲,۱۷۸۳
DT	Bee	۰,۹۵۷	۰,۹۷۸	۰,۰۲۲	۰,۹۷۸	۰,۹۷۸	۰,۹۷۸	۰,۹۵۶	۰,۹۹۴	۰,۹۹۴	۰,۰۷۰۵	۰,۱۳	۰,۱۵۵۶	۰,۹۸۷	۹۷,۸۲۱۷	۲,۱۷۸۳
LibSVM	Bee	۰,۹۳۱	۰,۹۶۵	۰,۰۳۶	۰,۹۶۵	۰,۹۶۵	۰,۹۶۵	۰,۹۳۰	۰,۹۶۵	۰,۹۴۸	۰,۰۳۵۱	۰,۴۷	۰,۱۸۷۳	۰,۹۶۴۵	۹۶,۴۹۰۵	۳,۵۰۹۵
MLP	Bat	۰,۹۴۴	۰,۹۷۱	۰,۰۲۹	۰,۹۷۱	۰,۹۷۱	۰,۹۷۱	۰,۹۴۳	۰,۹۸۳	۰,۹۸۰	۰,۰۴۸۵	۲,۷۷	۰,۱۵۸۲	۰,۹۷۱	۹۷,۱۳۵۹	۲,۸٦٤۱
Immunos99	Bat	۰,۸۲۷	۰,۹۱۶	۰,۰۸۹	۰,۹۲۶	۰,۹۱۶	۰,۹۱۶	–	۰,۹۱۴	–	۰,۰۸۳۵	۳,۳۴	۰,۲۸۹	۰,۹۱۳۵	۹۱,۶۴۹۹	۸,۳۵۰۱
CSCA	Genetic	۰,۹۱۲	۰,۹۵۷	۰,۰۴۴	۰,۹۵۷	۰,۹۵۷	۰,۹۵۷	–	۰,۹۵۶	–	۰,۰۴۳۲	۱۱,۸۱	۰,۲۰۷۸	۰,۹۵۶۵	۹۵,۶۸۳۷	٤,۳۱٦۳
AIRS2	Bat	۰,۹۴۴	۰,۹۷۱	۰,۰۲۹	۰,۹۷۱	۰,۹۷۱	۰,۹۷۱	–	۰,۹۷۱	–	۰,۰۲۸۶	۴۴,۰۲	۰,۱۶۹۲	۰,۹۷۱	۹۷,۱۳۵۹	۲,۸٦٤۱
AIRS2 Parallel	Bat	۰,۹۴۶	۰,۹۷۳	۰,۰۲۸	۰,۹۷۳	۰,۹۷۳	۰,۹۷۳	–	۰,۹۷۲	–	۰,۰۲۷۴	۱۶۷,۴۵	۰,۱۶۵۶	۰,۹۷۲۵	۹۷,۲۵۷	۲,۷٤۳

جهش نیز از ۰,۰۲ به ۰,۰۸ ارتقا داده شد. در مورد الگوریتم جستجوی مورچه نیز ، سرعت به accelerate ، مقادیر فرومون از ۲ به ۵ و تکرارها چهار برابر (۸۰) و جمعیت دو برابر گردید. (از ۲۰ به ٤۰)، همچنین نرخ گزارش دهی نیز از ۲۰ به ۳۰ افزایش داده شد. نرخ هوش ابتکاری (heuristic) مورچه ها نیز به ۱ افزایش داده شد. در مورد آخر (ژنتیک) نیز پارامترهای Crossover به ۰,۷ افزایش و maxGenerationبه ۳۰ ، اندازه جمعیت نیز به ۳۰ تنظیم و در نهایت جدول (٦) حاصل شد. این شش رویکرد کاهش ویژگی در دو

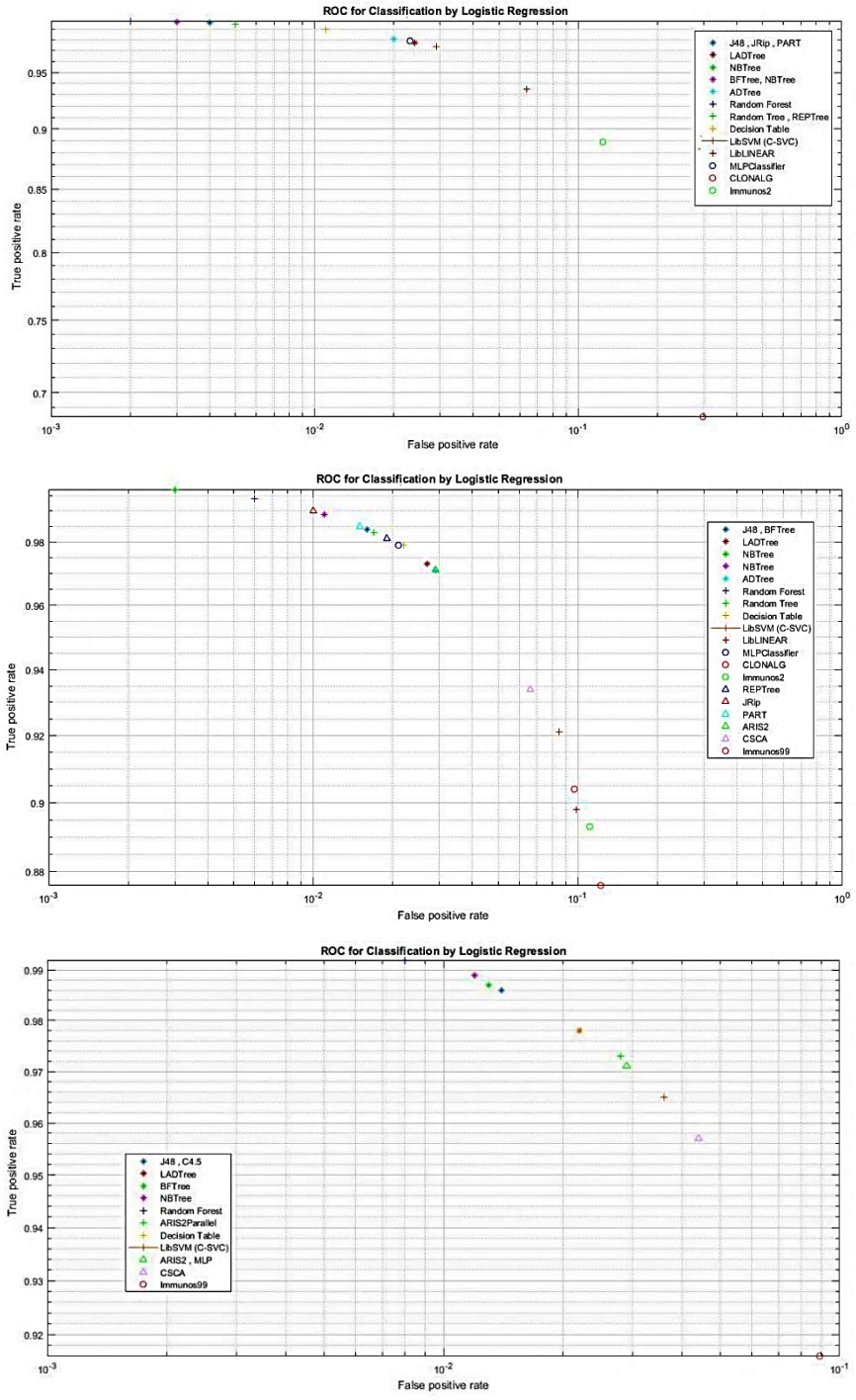
[Downloaded from ic4i-journal.ir on 2026-11-23]

جدول (۵) و (٦) به دسته بندهای منتخب از جدول (۲) اعمال گردید.

٤. یافته ها

با مقایسه دو جدول ۱و ۲ از فاز نخست با جدول ۷ در فاز دوم آزمایش، مشاهده می شود که تاثیر اعمال کاهش ویژگی به ترتیب بر سه الگوریتم immuno99 ،ARIS2Parallel ، CSCA ، LibSVM در بهبود نرخ های تشخیص و کارائی نسبت به سایر الگوریتم ها بیشتر بوده است. تغییر محسوس در نمودارهای $\mathbf{ROC-b,c}$ زیر قابل مشاهده می باشد.

نمودار (۲): سه نمودار ROC ،از بالا به ترتیب ، اجرای اول مطابق جدول (۱) ، اجرای دوم مطابق جدول (۲) ، با اعمال انتخاب ویژگی (از بالا به ترتیب $\mathbf{c,b,a}$)



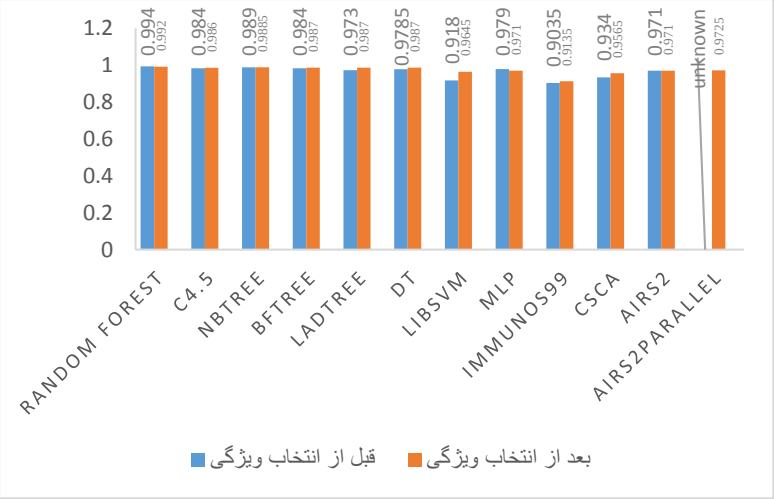
[Downloaded from ic4i-journal.ir on 2026-11-23]

همچنین در جدول ۷ ستون **cc** ضریب همبستگی را نشان می دهد. این معیار هر چه قدر به سمت عدد ۱ نزدیک تر باشد سیستم دسته بندی پایدارتر بوده و نتایج مشابهی را در مواجهه با داده عظیم در آینده ارائه خواهد داشت و نتایج بدست آمده دور از انتظار نخواهد بود. اما اگر از ۱ فاصله بگیرد نمایانگر ناپایداری سیستم و غیر قابل پیش بینی بودن آن است. بطوریکه با افزایش حجم داده جهت آزمایش و یا کاهش ویژگیهای غیر مرتبط و پارامتر دهی مناسب می توان این مقدار را به یک نزدیک تر نمود.

٤-١. ارائه رویکردِ پیشنهادی

با توجه به نتایج جداول (۲) تا (۷) در میان متدهای ایمنی مصنوعی رویکرد Bat+ ARIS2Paralell از ضریب همبستگی و نرخ های دسته بندی مطلوب تری در بین سایر متدهای مشابه برخوردار بوده و به دلیل نرخ همبستگی بالا قابلیت اطمینان در خصوص عملکرد دسته بندی و امکان توسعه در آینده را دارد. همچنین در میان متدهای الهام گرفته شده از طبیعت ، سیستم های تشخیص MLP+Bat در مقایسه با LibSVM+Bee از همبستگی و عملکرد بهتری برخوردار است.

نمودار (۳): مقایسه دقت (accuracy) دسته بندها قبل و بعد از اعمال رویکرد انتخاب ویژگی



به عنوان یک نتیجه گیری اولیه می توان اینگونه برداشت کرد که مطابق جدول ٦ ، رویکرد جستجو و انتخاب ویژگیِ Batsearch + ConsistencySubsetEval با ١٤ ویژگی در این مجموعه آزمایشات توانسته است بهترین بهبود را در نرخ های عملکردی دسته بندهای ارزیابی شده ارائه دهد. در میان متدهای ایمنی مصنوعی همانطور که بیان شد ، بهترین بهبود مربوط به رویکرد ARIS2Paralell+Bat+ MLP و Bat و در میان درخت ها نیز Bat + Randomforest می باشد. معمولاً به منظور ارزیابی مقایسه ای بهترِ دسته بندهای الهام گرفته شده از

[Downloaded from ic4i-journal.ir on 2026-11-23]

طبیعت (ایمنی مصنوعی ، متدهای مبتنی بر هوش ازدحامی جانداران و فرا ابتکاری) کار ارزیابی بهتر است با سایرِ دسته بندهای غیر ابتکاری نیز انجام شود. مقصود در اینجا درخت های تصمیم می باشند.

به عنوان یک نتیجه گیریِ کلّی می توان اینگونه بیان نمود که متد های ایمنی مصنوعی در مقایسه با سایر متدهای یادگیری ماشین (درختهای تصمیم ، متدهای فرا ابتکاری) به زیر مجموعه ویژگیهای انتخاب شده در الگوی ترافیک ورودی وابسته تر بوده بطوریکه تغییر/حذف یک ویژگی خاص تغییر محسوسی را در نرخ های تشخیص و خطاها منجر میشوند که یک چالش می باشد. این در حالیست که در مورد سایر الگوریتم ها تغییر چندان محسوسی رخ نمی دهد. حال مطابق نتیجه آزمایشهای انجام شده این چالش با انتخاب استراتژی جستجو و انتخاب ویژگیِ مناسب می تواند رفع شود. از طرفی نتیجه ارزیابی های آزمایشات حاکی از آنست که تغییرات قبل و بعد از تعبیه فاز انتخاب ویژگی در متدهای ایمنی مصنوعی به ترتیب در CSCA و Immunos99، ARIS2Paralell در میان توابع نیز بر روی متد **LibSVM** منجر به افزایش محسوسی در دقّت آنها شده است (نمودار ۳).

٤-۲. جمع بندی

در فرایند انتخاب ویژگی باید دقت کرد که زیر مجموعه هایی انتخاب شود که ذاتاً در کنار هم مفهوم کاملی برای سیستم تشخیص ارائه دهند. مثلاً دو ویژگی src_bytes و dst_bytes . این دو ویژگی معمولاً در کنار هم معنی پیدا می کند و در نتایج رویکرد های انتخاب ویژگی مشاهده شد که به جز الگوریتم Bat (خفاش) و ژنتیک ، بقیه الگوریتم ها این خصوصیت را نادیده می گیرند. این مورد نیز نیازمند پارامتردهی مناسب کاربر می باشد. پارامتر دهی باید بسته به مسئله پیکربندی شود، به عبارت بهتر باید به محض رو به رو شدن با مسئله مشخص کنیم که مقادیر پارامترها در چه رنجی تعیین شوند. این تا حدی به تجربه کار با این سیستم ها نیز وابسته است به منظور ارائه رویکردی نو با ترکیبِ دسته بندها ، آزمایشهای متعددی را می توان در نرم افزار وکا اجرا کرد. به طور کلی ازنظر نگارندگان این مقاله موفقیت یک رویکرد به عوامل زیر بستگی دارد :

فهم کامل سازوکار زیستی سیستم ایمنی مصنوعی و کسب تجربه لازم در بازه صحیح پارامترها.

استفاده از رویکرد های کاهش ویژگی و انتخاب استراتژی جستجوی مناسب، در این مورد پیشنهاد می شود که از الگوریتم های فرا ابتکاری استفاده گردد.

نتیجه ارزیابی های مقایسه ای این مقاله نشان داد که استراتژی جستجو و انتخاب ویژگی خفّاش در ترکیب با متد ایمنی مصنوعی ARIS2PARALELL بهتر عمل می کند که می تواند در آینده بر روی آن کار شده و توسعه پیدا کند. همچنین در مورد توابع نیز متد LiBSVM بهتر عمل نمود. در بین درخت های تصمیم نیز RandomForest عملکرد بهتری در ترکیب با متد خفّاش داشت. به عنوان یک پیشنهاد که به نظر می رسد می تواند در راستای توسعه و بهبود عملکرد زمانی رویکرد پیشنهادی Bat+ARIS2PARALELL از نظر بلادرنگ بودن آن در تولید و تکثیر آنتی بادی ها و تشخیص به موقع (آنلاین) مطرح شود ، استفاده از محیط پردازش ابری و یا پردازش تحت GPU می باشد. از طرفی حجم داده ورودی به

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال دوم، شمارهٔ ۱، بهار ۱۳۹۷

[Downloaded from ic4i-journal.ir on 2026-11-23]

دسته بند معمولاً در دادگان نفوذ مختلف ابعاد مسئله پیوسته تغییر می یابند اما بُعد ویژگیها معمولاً تغییر چندانی نمی کند. تغییرات پیوسته ویژگیها رخدادی است که در مجموعه آزمایشات این مقاله به دلیل ثابت بودن دادگان تست و یادگیری و محدودیت سخت افزاری و پردازشی ، امکان بررسی ابعاد متغیر وجود نداشت ولی پیشنهاد می شود که سیستم یادگیری و دسته بندی یک سیستم تشخیص نفوذ با این هدف توسعه داده شود که بتواند در حین یادگیری و ایجاد مدل دسته بندی ، توان تست مدل را با داده حجیم به صورت بلادرنگ یا نیمه بلادرنگ داشته باشد. به عبارت دیگر اهمیت برقراری نوعی **trade off** میان **time** و **performance** ضروری است. مسئله زمان بالای تشخیص در سیستم ایمنی مصنوعی وجود دارد. از نقطه نظر فناوری پیاده سازی نیز دربرخی سازمان ها ، زمان اهمیت بالایی دارد و در برخی دیگر نیز عملکرد به زمان اجرا ارجحیت دارد. امّا در مجموع امروزه هر دو پارامتر دارای اهمیت می باشند که باید توجه شوند. در برخی نیز مانند سازمان های نظامی ، به هر دوپارامتر زمان اجرا و تست و عملکرد باید توجه شود که کار پژوهشی و تخصصی زیادی را می طلبد.

۵. نتیجه گیری

الگوریتم های الهام گرفته شده از بیولوژیک و هوش ازدحامی جانداران به عنوان رویکرد نوین تحقیقاتی در نسل آینده سیستم های تشخیص نفوذ زیستی ، مورد بحث و بررسی قرار گرفت. همچنین مفهوم ایمنی و امنیت و تفاوت میان این دو بیان گردید. اصولاً سیستم های ایمنی مصنوعی با مبنای بیولوژیکی که دارند، با رویکرد برقراری ایمنی سیستم و حفظ آن سعی در کنترل امنیت دارند. از طرفی مفهوم مصونیت یا ایمنـــــی در سیستم ایمنی مصنوعی با دو واکنش اکتسابی (تطبیقی) و ذاتی بیان می شود و این دو واکنش در دراز مدت منجر به کنترل امنیت سیستم می گردند اما این پروسه در اولین مواجهه با آنتی ژنها به عنوان رشته های غیر خودی (نفوذ)، بسیار زمانبر بوده و به پارامترها و نرخ های ورودی کاربر نیز در مرحله پیاده سازی بستگی دارد. دلیل زمان بالای رویکردهای ایمنی مصنوعی بررسی شده نیز همین مسئله بوده و در واقع اوّلین فاز مواجهه آنتی بادیها با عوامل ترافیک شبکه غیر خودی می باشد که تکثیر و تشخیص آنها زمان زیادی می طلبد. همچنین مشاهده شد که اعمال فاز انتخاب ویژگی تاثیر زیادی در کاهش زمان ایجاد مدل دسته بند در **AIS** نسبت به بقیه الگوریتم های دسته بندی رایج می گذارد.

فهرست منابع

[1] Sharma, R. K., Kalita, H. K., & Issac, B. (2016). PIRIDS: A Model on Intrusion Response System Based on Biologically Inspired Response Mechanism in Plants. ***Innovations in Bio-Inspired Computing and Applications*** (pp. 105-116). Springer International Publishing.

[2] Thaseen, I. S., & Kumar, C. A. (2016). Intrusion detection model using fusion of chi-square feature selection and multi class SVM. ***Journal of King Saud University-Computer and Information Sciences***.

[3] Sunita, S., Chandrakanta, B. J., & Chinmayee, R. (2016). A Hybrid Approach of Intrusion Detection using ANN and FCM. ***European Journal of Advances in Engineering and Technology***, *3*(2), 6-14.

[Downloaded from ic4i-journal.ir on 2026-11-23]

[4] Blum, C., Lozano, J. A., & Davidson, P. P. (2015). An artificial bioindicator system for network intrusion detection. ***Artificial life***.

[5] Enache, A. C., & Sgarciu, V. (2015, July). A feature selection approach implemented with the Binary Bat Algorithm applied for intrusion detection. ***38th International Conference on Telecommunications and Signal Processing (TSP)*** (pp. 11-15). IEEE.

[6] Tama, B. A., & Rhee, K. H. (2015). A Combination of PSO-Based Feature Selection and Tree-Based Classifiers Ensemble for Intrusion Detection Systems. ***Advances in Computer Science and Ubiquitous Computing*** (pp. 489-495). Springer Singapore.

[7] Eesa, A. S., Orman, Z., & Brifcani, A. M. A. (2015). A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems. ***Expert Systems with Applications***, *42*(5), 2670-2679

[8] Rani, M. S., & Xavier, S. B. (2015). A Hybrid Intrusion Detection System Based on C5.0 Decision Tree and One-Class SVM. ***International Journal of Current Engineering and Technology*** 5(3), 2001-2007.

[9] Soliman, O. S., & Rassem, A. (2014). A Network Intrusions Detection System based on a Quantum Bio Inspired Algorithm. ***arXiv****:1405.1404*.

[10] Saurabh, P., Verma, B., & Sharma, S. (2012). Biologically Inspired Computer Security System: The Way Ahead. ***Recent Trends in Computer Networks and Distributed Systems Security*** (pp. 474-484). Springer Berlin Heidelberg.

[11] Alomari, O., & Othman, Z. A. (2012). Bees algorithm for feature selection in network anomaly detection. ***Journal of Applied Sciences Research***, *8*(3), 1748-1756.

[12] Kolias, C., Kambourakis, G., & Maragoudakis, M. (2011). Swarm intelligence in intrusion detection: A survey. ***Computers & security***, *30*(8), 625-642.

[13] Ma, W., Tran, D., & Sharma, D. (2008). Negative selection with antigen feedback in intrusion detection. ***Artificial Immune Systems*** (pp. 200-209). Springer Berlin Heidelberg.

[14] Brownlee, J. (2005). Immunos-81, the misunderstood artificial immune system. (*Technical Report*), ***Faculty of Information & Communication Technologies (ICT), Swinburne University of Technology, Melburne, Australia***.

[15] Enache, A. C., Sgarciu, V., & Petrescu-Nita, A. (2015, May). Intelligent feature selection method rooted in Binary Bat Algorithm for intrusion detection. ***10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI)*** (pp. 517 521). IEEE.

[16] Enache, A. C., & Sgarciu, V. (2015, May). Anomaly Intrusions Detection Based on Support Vector Machines with an Improved Bat Algorithm. ***20th International Conference on Control Systems and Computer Science (CSCS)*** (pp. 317-321). IEEE.

[17] Enache, A. C., & Patriciu, V. V. (2014, May). Intrusions detection based on support vector machine optimized with swarm intelligence, ***9th International Symposium on Applied Computational Intelligence and Informatics (SACI)*** (pp. 153-158). IEEE.

[18] Rathore, H. Feb, 10, (2016). Mapping Biological Systems to Network Systems, *Switzerland*: *Springer*.

[19] Song, J. (2016). Feature Selection for Intrusion Detection System, ***Retrivied from*** (Doctoral dissertation, Aberystwyth University).

[20] Hassanien, A. E., Kim, T. H., Kacprzyk, J., & Awad, A. I. (Eds.). (2014). ***Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*** (Vol. 70). Springer.

[21] Zekri, M., & Souici-Meslati, L. (2014). Immunological Approach for Intrusion Detection. ***Arima Journal***, *17*, 221-240.

[22] Yang, X. S. (2010). ***Nature-inspired metaheuristic algorithms***. Luniver press.

[23] Kayacık, H. G, Zincir-Heywood, A. N., & Heywood, M. I. (2005, October). Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets. ***In Proceedings of the third annual conference on privacy, security and trust***.

[24] Mukhopadhyay, M. (2014). A brief survey on bio inspired optimization algorithms for molecular docking. ***International Journal of Advances in Engineering & Technology***, 7(3), 868.

[25] Andersen.P. (Producer), & Andersen.P (Director). (March 19, 2012). ***The Immune System [Video podcast]***. US. Retrieved from http://www.bozemanscience.com

[26] Aickelin, U., Dasgupta, D. (2005). Articial Immune systems ***In Search methodologies***, (pp. 375-399). Springer, Boston, MA.

[Downloaded from ic4i-journal.ir on 2026-11-23]

[27] Brownlee, J, (2005). Clonal selection theory & clonalg-the clonal selection classification algorithm (CSCA). (*Technical Report*)**, *Swinburne University of Technology, Melburne, Australia***.

[28] Hofmeyr, S. A, & Forrest, S. (2000). Architecture for an artifiticl immune system. ***Evolutionary computation***, 8(4), 443-473.

[29] Farzadnia, E., Shirazi, H., (2017 September 21). The Black Hole Clustering Algorithm: A MATLAB Simulation. (*Technical Report*), ***Dept.of Communication and Information Security, Malek-Ashtar University of Technology (MUT), Tehran, Iran***.

[30] Shirazi, H., Namadchian, A., & khalili Tehrani, A., (2012). A Combined Anomaly Base Intrusion Detection Using Memetic Algorithm and Bayesian Networks. ***International Journal of Machine Learning and Computing,*** (pp. 706-710), doi: https://10.7763/IJMLC.2012.V2.219

[31] Shirazi, H., Madanipour, M., & Abolhassani, H., (2010). Improving Intrusion Detection Systems based on Feature Reduction via Data Mining. ***The 2010 International Conference on Electronics and Information Engineering (ICEIE 2010),*** at Japan.

[32] Sheikhan, M., Sharifi Rad, M., & Shirazi, H., (Dec 2011). Application of Fuzzy Association Rules-Based Feature Selection and Fuzzy ARTMAP to Intrusion Detection. ***Majlesi Journal of Electrical Engineering***, Vol.5, No. 4.

[33] Khadem, Z., Shirazi, H., & Farshchi, S. M. R., (2015 Feb 19). Detecting Control baesd Imperative Malwares in Network Traffic. ***2th National Conference on Applied Researches in Electronical, Mechanical and Mechatronics Engineering***, at Tehran, Iran.

[۳۴] سرایی، محمد مهدی؛ محمد رضا حجری و حسین شیرازی، ۱۳۸۹، استفاده از یادگیری ماشینی در بهبود تشخیص نفوذ، ***کنفرانس ملّی امنیت اطلاعات و ارتباطات***، اهواز، جهاد دانشگاهی خوزستان، https://www.civilica.com/Paper-CICS01-CICS01-012.html

[۳۵] هدایتی، علیرضا؛ حسین شیرازی و احمد خادم زاده، ۱۳۸۳، ارائه روشی برای بهبود سیستم تشخیص نفوذ snort در تشخیص رفتار غیر عادی شبکه با استفاده از پایگاه دانش، ***دهمین کنفرانس سالانه انجمن کامپیوتر ایران***، مرکز تحقیقات مخابرات ایران، https://www.civilica.com/Paper-ACCSI110-ACCSI10-158.html

[۳۶] خادم، زهرا؛ حسین شیرازی و سید محمدرضا فرشچی، ۱۳۹۳، تشخیص بدافزارهای کنترلی دستوری در ترافیک شبکه، ***دوّمین همایش ملّی پژوهش های کاربردی در برق، مکانیک و مکاترونیک***، تهران، دانشگاه جامع علمی کاربردی، https://www.civilica.com/Paper-ELEMECHCONF02-ELEMECHCONF02-001.html

[۳۷] شیرازی، حسین؛ جمالی فرد امینه، فرشچی سید محمدرضا، تشخیص حملات برنامه های کاربردی تحت وب با استفاده از ترکیب دسته بندهای تک کلاسی. ***مجلّه علمی- پژوهشی علوم و فناوریهای پدافند نوین***. ۱۳۹۳؛ ۵ (۲) :۱۱۹-۱۰۷.

https://adst.ir/article-1-574.fa.html

[Downloaded from ic4i-journal.ir on 2026-11-23]