دوفصلنامه محاسبات و سامانه‌های توزیع شده
www.jdcs.ir

ارائه یک روش جدید برای تشخیص حمله سیاهچاله در شبکه‌های سلامت اینترنت اشیاء

ابراهیم ظاهری عبده وند[1]، منوچهر کاظمی*[2]

گروه مهندسی کامپیوتر، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران[1]

گروه ریاضی، واحد آشتیان، دانشگاه آزاداسلامی، آشتیان، ایران[2]

چکیده

اینترنت اشیا کاربرد زیادی درامور روزمره پیدا کرده است رده ای از کاربرد های اینترنت اشیا در مصارف صنعتی را اینترنت اشیا صنعتی می‌نامند اینترنت اشیا صنعتی چشم انداز روشنی در آینده دارد و یکی از مهم ترین شاخه های اینترنت اشیا صنعتی بخش سلامت می‌باشد. در این شبکه اطلاعات بیماران به صورت مرتب به مراکز کنترل ارسال می شود تا سلامت بیمار دچار خطر نشود. این شبکه همچون تمام شبکه ها نیاز به بخش امنیتی دارد تا در مقابل حملات مختلف ایمن با شد. یکی از حملاتی که این شبکه را دچار مختل می‌کند، حمله سیاهچاله ا ست. ما دراین مقاله یک روش فازی برای کنترل حمله سیاهچاله ارائه کرده ایم و نتایج شبیه سازی نشان می‌دهد روش پیشنهادی عملکرد خوبی دارد.

Email:mkazemi@aiau.ac.ir

کلمات کلیدی: حمله سیاهچاله، شبکه اینترنت اشیا، شبکه سلامت، منطق فازی

Presenting a New Method for Detecting Black Hole Attack on Internet of Things (IoT) Health Networks

Ebrahim Zaheri Abdehvand[1], Manoochehr Kazemi*[2]

[1]Department of Computer Engineering, Qazvin branch, Islamic Azad University, Qazvin, Iran

[2]Department of Mathematics, Ashtian branch, Islamic Azad University, Ashtian, Iran

Abstract

IoT is used extensively in every day affairs. A category of IoT in industrial uses is called Industrial IoT. Industrial IoT has a bright outlook for the future. One of the most important branches of the industrial IoT is health sector. In this network, patients' information is regularly sent to the control centers, so that the patients' health is not compromised. Like all networks, this network needs a security section to be secured against various attacks. One of the attacks disrupting this network is the black hole attack. The paper presented a fuzzy method for controlling the black-hole attack, with the simulation results showing the good performance of the proposed method.

تاریخچه مقاله:

تاریخ ارسال: ۹۷/۱۲/۱

تاریخ اصلاحات: ۹۸/۳/۲۰

تاریخ پذیرش: ۹۸/۴/۲۰

تاریخ انتشار: ۹۸/۵/۱۵

Keywords:

Black hole attack
IoT network
Health network
Fuzzy logic

روش ارجاع به مقاله:

ا.ظاهری عبده وند، م.کاظمی، ارائه یک روش جدید برای تشخیص حمله سیاهچاله در شبکه‌های سلامت اینترنت اشیاء، دوفصلنامه محاسبات و سامانه‌های توزیع شده، سال دوم، شماره اول، شماره پیاپی ۳، سال ۱۳۹۸، ص ۹۵-۱۰۴

۱- مقدمه

اینترنت اشیاء، دستگاه های متعددی که ما به طور روزانه از آن ها استفاده می کنیم، ما را قادر می سازد از طریق اینترنت با هم تعامل داشته باشیم. این تضمین می دهد که دستگاه ها هوشمند باشند و اطلاعات را به سیستم مرکزی بفرستند که سپس طبق وظیفه‌ای که برای آن تعریف شده عکس العمل نشان دهد. اینترنت اشیاء می‌تواند در محدوده وسیعی از قلمروها از جمله مراقبت بهداشت، حمل و نقل، سرگرمی، شبکه های نیرو و ساختمان های هوشمند استفاده شود. انتظار می‌رود که اینترنت اشیاء به عنوان یک کاتالیزور برای ابتکارات تکنولوژی آینده عمل کند و انتظار می‌رود استفاده از آن به طور نهایی در طی سال‌های آینده بالا رود [1].

با میزان بالایی از دستگاه های متصل به اینترنت و داده های بسیار زیاد مرتبط با آن، نگرانی های در مورد امنیت باقی می‌ماند. به وسیله امنیت ما درجه پایداری یا حفاظت از زیر ساخت و کاربردهای اینترنت اشیاء را درک می‌کنیم. بسیاری از این دستگاه ها، اهداف ساده ای برای نفوذ هستند زیرا وابسته به منابع خارجی هستند و اغلب بدون مراقبت و توجه باقیمانده اند. به محض اینکه لایه شبکه درمعرض خطر افتاد، برای هکر بسیار ساده است که کنترل را به دست آورد و به طور بد اندیشانه ای از یک دستگاه استفاده کند و همچنین به دستگاه های دیگر از طریق گره اصلی تسخیر شده حمله کند. به ویژه، حمله به تجهیزاتی که یک حضور آنلاین را نگه می‌دارند آسان است. حمله سیاهچاله یکی از خطرناک ترین حملات فعال در شبکه های موردی بیسیم می باشد. گره سیاهچاله به این صورت عمل می کند که به تمام بسته های درخواست به مسیر پاسخ داده و طوری وانمود می کند که بهترین مسیر را تا گره مقصد دارد و سپس تمام بسته های دریافتی را از بین می برد.

۲- بیان مسأله

حمله سیاهچاله یک نوع از حمله های انکار سرویس است که در آن مسیریابی که قرار است بسته ها را ارسال کند، آن ها را دور می اندازد. این معمولاً از طرف مسیریابی که به دلایل مختلفی در معرض خطر قرار گرفته است، رخ می دهد. یکی از دلایلی که در پژوهش ذکر شده است از طریق یک حمله انکار سرویس در روتر است که از ابزار مشهور DDOS استفاده می‌کند[2].

از آنجا که معمولاً بسته ها در شبکه های پر اتلاف حذف می شوند، تشخیص و پیشگیری از حمله حذف بسته ها بسیار مشکل است. در یک سیستم IOT پزشکی، مهاجم می تواند از پویایی پروتکل جهت شنود بسته های درخواست (RREQ) به نفع خود استفاده کند. برای این کار، مهاجم از یک بسته RREP جعل شده به عنوان پاسخ استفاده می‌کند که کوتاه ترین مسیر به سمت مقصد را نشان می‌دهد و به اینصورت یک اتصال را بین گره مبدأ و گره مخاطره آمیز برقرار می‌سازد. بنابراین سرنوشت تمام بسته‌های موجود به روی این مسیر، دردستان گره مخاطره آمیز است.

۳- سوابق

مقاله [3] سیستم تشخیص و تسکین حمله سیاهچاله مبتنی بر الگوریتم ژنتیک در شبکه‌های IOT می‌باشد، تمرکز این مقاله بر روی حملات پروتکل

امنیتی است. الگوریتم ژنتیک برای ایجاد IP های پویا در شبکه مورد استفاده قرار می‌گیرد.

از اهداف استفاده این الگوریتم می‌توان به موارد زیر اشاره کرد:

- جلوگیری از ارسال داده‌های غیرمجاز
- جلوگیری از حمله

از جمله ویژگی‌های روش ارائه شده می‌توان به موارد زیر اشاره کرد:

- تولید قوانین پویا با توجه به شرایط تغییر پذیر سیستم های تشخیص نفوذ
- افزایش داده‌های جمع شده با گذشت زمان در سیستم و بهبود تصمیم گیری‌ها به کمک این پایگاه داده
- مدل ارائه شده مبتنی بر رفتار است. این نوع مدل‌ها دقیق‌تر هستند و بازدهی بیشتری دارند.

معماری کلی این روش به این صورت است که ابتدا بخش Network sniffer آنالیز مجموعه داده‌ای سیستم را بر عهده دارد. نتیجه این بخش به الگوریتم ژنتیک ارسال می‌شود. پس از ارزیابی الگوریتم ژنتیک، قوانین ایجاد می‌شوند و در پایگاه داده ذخیره می‌گردد.

مزایا:

۱- الگوریتم‌های ژنتیک فی نفسه موازی هستند. به دلیل چندین زاد و ولد آن‌ها می‌توانند فضای راه حل را در چندین جهت با هم جستجو کنند.

۲- موازی سازی به الگوریتم ژنتیک اجازه می‌دهد تا به طور تلویحی طرح‌های بسیاری را یک دفعه و با هم ارزیابی کند. این امر آن‌ها را مناسب برای حل مسائلی که فضای راه حل بالقوه، حقیقتاً بزرگ هست، می‌سازد.

۳- سیستم های مبتنی بر الگوریتم ژنتیک می‌توانند به‌آسانی دوباره آموزش (retraining) ببینند. این امر امکان افزودن قوانین جدید را توسعه می‌دهد و سیستم تشخیص نفوذ را پیشرفت می‌دهد.

معایب:

- اشکال اصلی آن مصرف زیاد منابع درگیر است.

پژوهشگران [4] از یک شبکه عصبی بازگشت کننده[1] که سایز آن کاهش یافته است و بر اساس گروه بندی ورودی‌ها استفاده کرده اند. کاهش سایز شبکه سرعت آن را بالا می برد. ویژگی‌های ورودی را به چهار دسته تقسیم کرده اند: ویژگی های محتوی[2]، ویژگی های پایه[3]، ویژگی های ترافیکی مبتنی بر زمان[4] و ویژگی‌های ترافیکی مبتنی بر میزبان[5]. در این شبکه اتصال بین لایه ورودی و لایه مخفی بر اساس دسته مربوط به ویژگی‌ها می باشد.

در مقاله [5] پژوهشی صورت گرفت که در آن دو روش مختلف از نظر دقت و زمان مورد بررسی قرار گرفتند. بخشی از مجموعه داده KDD به عنوان داده آموزشی انتخاب گردید و سپس برای نتیجه بهتر الگوریتم انتخاب ویژگی که در این تحقیق PCA بود بر روی مجموعه داده اعمال می‌شود، در مرحله بعد الگوریتم طبقه بندی ترکیبی SVM + DT+ Boosting و SVM + DT +Bagging برای مقایسه اعمال میشود و مورد ارزیابی قرار می‌گیرد.

در مقاله [6] نیز تحقیقی در زمینه الگوریتم های مختلف یادگیری ماشین ارائه کرد. در روش ارائه شده توسط او، در ابتدا با استفاده از الگوریتم ژنتیک، ویژگی‌های موثر مجموعه داده KDD که ۴۱ عدد است به ۱۵ کاهش می‌یابد و از چندین الگوریتم طبقه بندی کننده متفاوت جهت بررسی و مقایسه نتایج استفاده می شود، در این تحقیق مشاهده می شود که استفاده از ماژول انتخاب گر ویژگی، باعث بالا

[1] Recurrent
[2] Content Features
[3] Basic Features
[4] Time-based Traffic Features
[5] Host- based Traffic Features

رفتن سرعت و دقت عملکرد بخش طبقه بندی می‌شود و در نهایت چند روش یادگیری ماشین به عنوان طبقه بندی کننده با یکدیگر مقایسه می‌شود، که نتایج کامل آن در [7] آورده شده است.

در مقاله [8] برای تشخیص نفوذ حمله از الگوریتم فرا اکتشافی و اجتماع پرندگان استفاده شده است. در این الگوریتم هر ذره در محیط شبکه توزیع می‌شود و در صورت مشاهده حالت‌های غیر نرمال، مقدار فرمول آن بیشتر می شود و در انتها ذره های که مقدار بیشتری از حد میانگین دارند دچار حالات نفوذ هستند

در مقاله [9] برای تشخیص نفوذ از ترکیب سه الگوریتم ژنتیک، درخت تصمیم و شبکه عصبی استفاده شده است در این الگوریتم ورودی شبکه عصبی با ژنتیک و درخت تصمیم بهینه شده است و شبکه عصبی پنج لایه استفاده شده است.

در [10] از تکنیک های داده کاوی جهت آنالیز داده‌های شبکه استفاده شده است. در واقع این تحقیق با مطالعه جامع تمامی مقالات موجود در این مبحث، یک مقاله مروری جهت جمع‌بندی متدهای ارائه شده در ارزیابی سیستم تشخیص نفوذ ارائه نموده است. در نهایت مقایسه‌ای جامع بین روش‌های موجود ارائه شده است.

در پژوهشی [11] که انجام گرفت، روشهای متعدد رتبه‌بندی اعتباری از جمله رگرسیون لجستیک، تحلیل ممیز خطی، k امین همسایه نزدیک، شبکه عصبی، درخت تصمیم، ماشین بردار پشتیبان روی ۸ مجموعه داده واقعی با یکدیگر مقایسه شده اند و نتیجه‌گیری بدین صورت بوده که روش‌های شبکه عصبی و ماشین بردار پشتیبان بهتر از سایر روش‌ها در کلاس‌بندی موفق بوده‌اند.

محققین در مقاله [12] روشی دادند که الگوها به صورت خودکار یافت می‌شوند و این الگوها در دیتابیس های سیستم‌های تشخیص نفوذ ذخیره و مورد استفاده قرار می‌گیرند. همچنین زمان انسان و همچنین تلاش برای یادگیری الگوی حملات جدید به صورت دستی را کاهش می‌دهد. اشکالات اصلی شبکه عصبی مصنوعی مبتنی بر سیستم تشخیص نفوذ در دو جنبه وجود دارد. دقت تشخیص پایین تر به ویژه برای حمله های مکرر کم به عنوان مثال ریموت به محلی، کاربر ریشه و ثبات تشخیص ضعیف می‌باشد و دلیل اصلی این است که توزیع انواع مختلف حمله‌ها نا متوازن است. روش اف. سی.ان.ان بکار گرفته شده در این مقاله در بالا بردن دقت تشخیص برای حملات مکرر کم و ثبات تشخیص موثر می‌باشد.

نویسندگان یک سیستم تشخیص نفوذ متشکل از خوشه بند KNN و شبکه عصبی توسعه داده‌اند. از این خوشه بند برای بهبود آموزش شبکه عصبی بهره برده شده است. این مساله موجب بهود دقت در تصمیم گیری نهایی شبکه عصبی خواهد گردید [13].

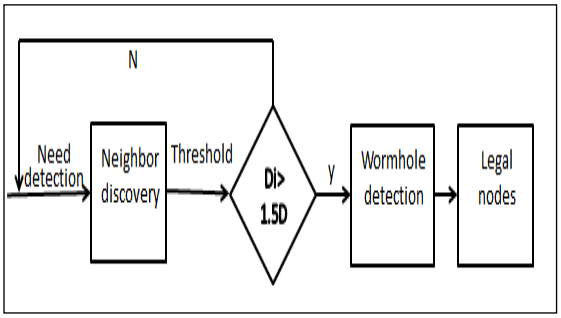
محققین مقاله [14] یک سیستم تشخیص نفوذ در لایه های زیر ساخت و نرم افزار معرفی کرده‌اند. برای بهبود بازدهی این سیستم تشخیص نفوذ از ساختار پردازش شبکه ای نیز بهره برده شده است.

محققین مقاله [15] در مقاله عنوان نمودند که سیستم تشخیص نفوذ بطور عمده شامل چند لایه رو به جلو در شبکه عصبی است. از شبکه‌های عصبی ام.ال.اف.اف برای تشخیص ناهنجاری مبتنی بر رفتار کاربر استفاده شده اما درعمل، تعداد مجموعه آموزشی بسیار بزرگ بوده و توزیع مجموعه نامتعادل است. شبکه‌های عصبی ام.ال.اف.اف برای رسیدن به مینیمم محلی آسان تر ولی ثبات آن پایین تر است. بخصوص دقت تشخیص در حمله مکرر با دوره تکرار کم، پایین است.

۴- روش پیشنهادی

در این قسمت جزئیات روش پیشنهادی توضیح داده می‌شود.

قرار است روشی ارائه شود که با بررسی یک شرط و ارائه یک الگوریتم در دو مرحله به جلوگیری و کشف حمله سیاهچاله بپردازد.



شکل (۱): پروسیجر کشف

مطابق شکل (۱) گره‌های را که دچار حمله شده‌اند را در ۴ مرحله شناسایی می‌کنیم:

۱- گره i بسته کشف همسایه را همه پخشی می‌کند و پیام اکوی همسایه‌ها را جمع می‌کند.
۲- اگر تراکم داده‌ها در همسایگی $D_i>1.5D$ باشد، تصمیم به اجرای فرآیند تشخیص نفوذ می‌گیرد.
۳- از الگوریتم منطق فازی برای کشف استفاده می‌کند.
۴- گره‌های همسایه را به دو دسته تقسیم می‌کند: گره‌های مجاز و گره‌های غیرمجاز.

این مرحله خود شامل دو زیر مرحله می‌باشد. ساختن لیست همسایگی و محاسبه سربار زمان وارد شدن (TOA)[۶].

اگر مقیاس های اندازه گیری برای شاخص‌ها از نوع کمّی باشند و داده‌ها نیز استاندارد شده باشند، روش‌های گوناگونی برای پیدا کردن این فاصله وجود دارد. یکی از معروف ترین و پرکاربرد ترین نوع فاصله، فاصله اقلیدسی می‌باشد. فاصله اقلیدسی برای دو نقطه x وy، در فضایی با d بُعد (شاخص) از رابطه (۱) به دست می‌آید:

رابطه $\mathbf{d(x,y)} = \sqrt{(x-x1)^2+(y-y1)^2}$ (۱)

هر نود قبل از اینکه به ارسال بسته بپردازد یک زمان به ا سم T_{init} ثبت می‌کند سپس پیغام Hello را بین نودهای همسایه، بلافاصله بعد از استقرار در شبکه پخش همگانی[۷] می‌کند. هر نود، لیست همسایگی خود که ممکن است شامل همسایه‌های دور که توسط سیاهچاله متصل شده باشند را ساخته و سربار زمان TOA مربوط به آن گره را محاسبه می‌کند.

۴-۱- محاسبه سرآیند زمان وارد شدن

هر گره زمانی بنام زمان ارسال دارد. هرگاه قرار است همسایگی برای هر گره مشخص شود سرآیند زمان ارسال باید محاسبه شود، یعنی فاصله زمانی ارسال تا دریافت پیام. نتیجه‌ی محاسبه TOA ممکن است دو حالت داشته باشیم:

- TOA مجاز: فاصله زمانی است که بسته در زمان قانونی بین مبدأ و مقصد مهاجرت کرده است.
- TOA غیرمجاز: فاصله زمانی است که بسته بین مبدأ و مقصد در زمان غیرمجاز و با تأخیر رد و بدل شده است.

۴-۲- مرحله دوم: شناسایی سیاهچاله

در این مرحله جهت شناسایی سیاهچاله و تشخیص نفوذ از منطق فازیاستفاده می‌کنیم. روشی که برای انتخاب گره مشکوک ارائه کرده‌ایم از سه آیتم تشکیل شده است:

- انرژی باقی مانده گره: گره‌ای که انرژی زیادی مصرف کرده است، احتمال دارد دچار حمله شده باشد.

[6]Time Of Arrive overhead

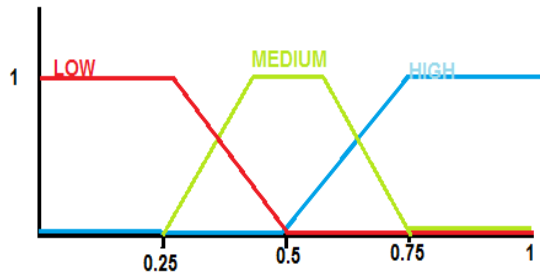
[7]Broadcast

- تعداد داده ارسالی به یک مقصد: این عامل نیز می‌تواند نشان دهنده حمله باشد.
- TOA: فاصله زمانی است که بسته در زمانی بین مبدأ و مقصد مهاجرت کرده است.

برای انتخاب گره جعلی و غیر جعلی این سه آیتم ورودی‌های سیستم فازی هستند.

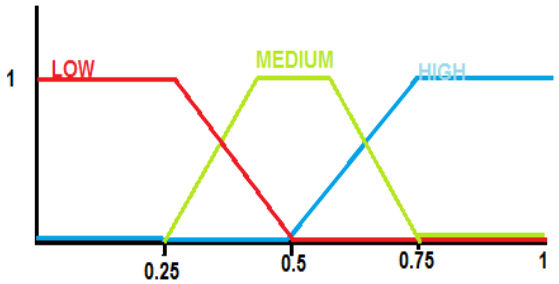
۴-۳- مراحل فازی سازی

همان‌طور که گفته شد برای قسمت فازی سازی از سه آیتم استفاده می‌شود که برای هریک تابع عضویتی باید در نظر گرفته شود.تابع عضویت مربوط به انرژی باقی مانده در شکل (۲) نمایش داده شده است.



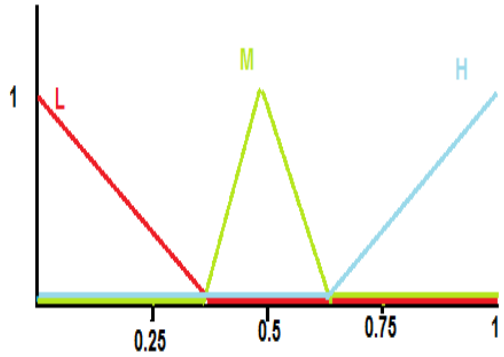
شکل (۲) : تابع عضویت برای ورودی انرژی باقی مانده

همان‌طور که گفته شد شکل (۲) برای انرژی باقی مانده است در این نمودار مقدار HIGH برای حالت ایده آل می‌با شد به طوری که انرژی در بالاترین مقدار خود قرار دارد. تابع عضویت مربوط به تعداد ار سال در شکل (۳) نمایش داده شده است.



شکل (۳): تابع عضویت مربوط به تعداد ارسال

در تابع تعداد ارسال ایده آل برای حالتی می‌باشد که تعداد ار سال کمترین مقدار با شد زیرا تعداد ار سال بالا انرژی زیادی مصرف می‌کند.



شکل (۴) : تابع عضویت برای TOA

۴-۴ مرحله استنتاج فازی

با توجه به سه ورودی گفته شده در مرحله استنتاج فازی از موتور ممدانی استفاده می‌شود و تعدادی از پارامترهای این موتور در جدول (۱) قابل مشاهده می‌باشد.

جدول (۲) : تعدادی از خروجی قوانین فازی

میزان مشکوک بودن	TOA	تعداد ارسال به یک مقصد خاصی	انرژی باقی مانده
Very High	high	High	Low
Medium	Low	Low	Low
High	Medium	Medium	Low
Medium	Medium	High	Medium
High	Low	Low	Medium
Medium	high	Medium	High

برای تعیین مقدار قطعی ما از سیستم استنتاج TSK استفاده کرده‌ایم. این سیستم به شکل زیر عمل می‌کند. دراین سیستم قسمت مقدم قواعد فازی است اما قسمت نتیجه غیرفازی و ترکیبی خطی از متغیرهای ورودی ا ست. خروجی‌ها به کمک رابطه (۲) به دست می‌آید:

رابطه (۲)

$$y = \frac{\sum_{i=1}^{c} w_i y_i}{\sum_{i=1}^{c} w_i}$$

در این رابطه yi طبق رابطه گفته شـــده در زیر به دست می‌آید:

$$R_i: If\ x_1\ is\ \tilde{A}_{t1}\ and\ (or) x_2\ is\ \tilde{A}_{t2}\ and\ (or)\ \dots x_m\ is\ \tilde{A}_{tm}\ Then\ y_t = a_{i1}x_1 + a_{i2}x_2 + \cdots a_{im}x_m$$

(i= 1,2,…c) رابطه (۳)

که xiها مقدار ورودی هســـتند و Aiها پارامترهای فازی (انرژی، تعداد ارسال و زمان).

در جدول (۲) خروجی منطق فازی به صـــورت عددی برای چند حالت نمایش داده شده است.

جدول (۲) : خروجی منطق فازی به‌صورت عددی برای چند حالت

میزان مشکوک بودن	TOA	تعداد ارسال به یک مقصد خاصی	انرژی باقی مانده
0.5	0	0	0
1	1	1	0
0.25	0.25	0	0.25
0.75	0.5	1	0.5
0.75	0	1	0.75
0.75	0.75	0.25	1
0.75	0.25	0.75	1

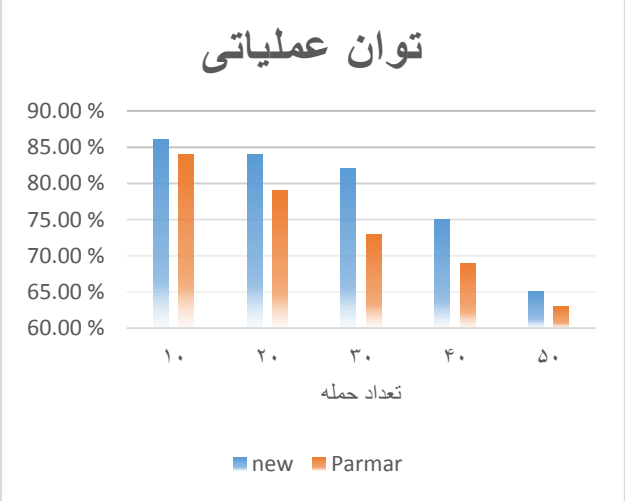
با توجه به خروجی منطق فازی که به صـــورت عدد مطرح می‌شود گره‌ها به دو قسمت جعلی و عادی تقسیم می‌شوند.

۵- ارزیابی و مقایسه روش پیشنهادی

در این قســـمت از مقاله روش پیشـــنهادی با یک روش دیگر تحت شـــرایط مشـــابه و برابر مورد شـــبیه سازی و مقایسه قرار گرفته‌اند که در ادامه توضیح داده شده‌اند برای مقایسه از مقاله [16] استفاده شده است در این مقاله یک روش جدید برای مقابله با حمله کرم چاله ارائه شده است و از پروتکل AOMDV استفاده شـــده اســـت که از بردار فاصـــله و زمان رفت و برگشت[8] RTT برای تشخیص حمله استفاده می‌کند. یکی از معیارهای ارزیابی توان عملیاتی می‌باشـــد این معیار از حاصـــل تقســـیم میزان داده دریافت شـــده در مقصد به مدت زمان رساندن داده‌ها به دست می‌آید در توان عملیاتی معیارهایی مانند نرخ تحویل بســـته و تأخیر انتها به انتها نیز دخیل هســـتند هر چقدر این معیارها بهتر باشـــند توان عملیاتی شـــبکه بالاتر خواهد بود. سناریو شبیه سازی برای این معیار به شکل زیر می‌باشد.

- چند گره به صورت تصادفی دچار حمله می‌شوند.
- شبکه شروع به کار می‌کند.
- توان عملیاتی زمانی که کل شـــبکه از بین رفت ارزیابی می‌شود.
- اندازه شبکه ثابت است.
- تعداد گره ثابت است.

نتیجه مقایســـه این معیار در شـــکل (۵) قابل مشاهده می‌باشد.

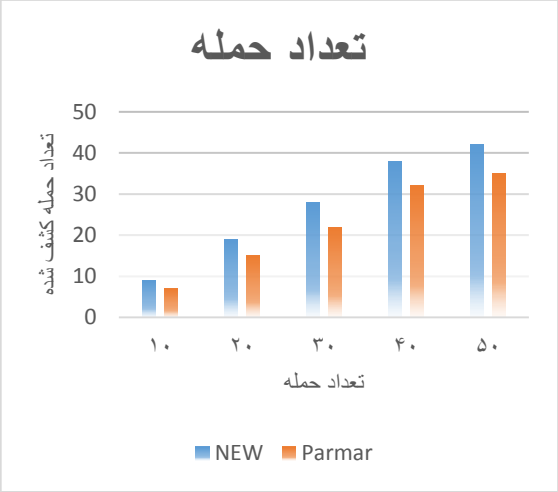


شکل (۵) : توان عملیاتی

نتیجه شبیه سازی نشان می‌دهد روش پیشنهادی عملکرد خوبی دارد، دلیل بالا بودن توان عملیاتی روش پیشـــنهادی این اســـت که از چندین عامل مهم برای تشخیص حمله استفاده می‌کند.

[8] round trip time

معیار بعدی کشـــف تعداد حمله می‌باشـــد در این معیار هدف این اســت که تعداد گره‌های جعلی موجود در شبکه را شناسایی کنیم. سناریو شبیه سازی به این صـــورت می‌باشـــد که تعداد نود و تعداد حمله در هر مرحله بیشـتر می‌شـود و سـیسـتم میزان شـناسـایی گره‌های جعلی یا حمله را نمایش می‌دهد.

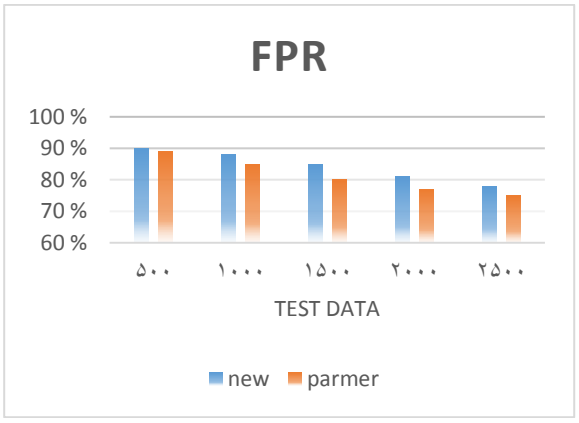


شکل (۶): تعداد حمله کشف شده

روش پیشـــنهادی تعداد حمله بیشـــتری را کشـــف کرده اسـت زیرا با اسـتفاده از منطق فازی دقت بالایی برای شناسایی حمله دارد.

معیار نرخ مثبت کاذب (FPR)

این معیار نشان می‌دهد که چه درصد از هشدارها به‌ا شتباه اعلام شده‌اند. برای شبیه سازی این سناریو در هر مرحله تعداد حملات در دیتاســـت افزایش پیدا کرده ا ست. نتیجه شبیه سازی در شکل (۷) نمایش داده شده است.

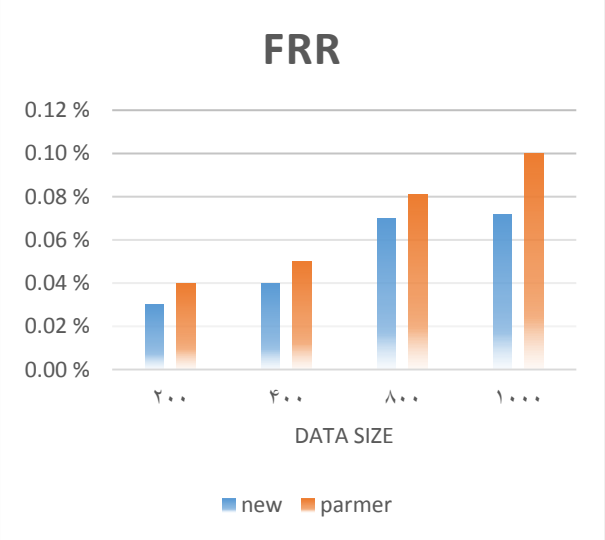


شکل (۷): معیار FPR

با توجه به نتایج به دسـت آمده از شـبیه سـازی روش پیشنهادی از عملکرد بهتری برخوردار می‌باشد.

معیار عدم پذیرش اشتباه

این خطا زمانی رخ می‌دهد که یک سـیسـتم کاربر دارای مجوز را به اشـــتباه نپذیرد. FRR یا False Reject Rate به معنی نرخ عدم پذیرش اشـــتباه که خطای شماره یک هم نامیده می شود و درصد دفعاتی که عدم پذیرش اشتباه رخ می‌دهد را نشان می‌دهد.

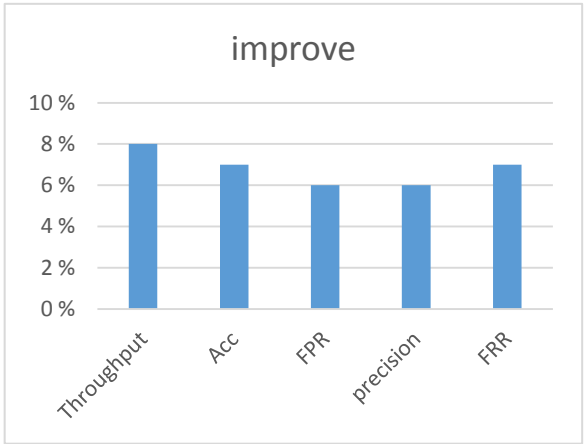


شکل (۸) : معیارFRR

۶- نتیجه گیری

صـــنعت مراقبت بهداشـــتی نیازمند پیشـــرفت‌های تخصـصـی در WSN ها و برنامه‌های IOT اسـت تا در ازای درخواســـت های آتی و احتیاجات بیماران و کارمندان پزشکی فراهم آورده شوند. این درخواست‌ها

می‌توانند توسط اکثر سیستم‌های پزشکی IOT پاسخ داده شوند، اما لازم به ذکر است که اکثر سیستم‌های فعلی، امنیت مناسب را برای داده‌ها ارائه نمی‌دهند. حملهٔ DoS بروی مسیر یابی داده ها می‌تواند تأثیر چشمگیری به روی سیستم‌های WSN پزشکی داشته باشد. در این مقاله، رویکردی برای ارائهٔ یک رویه پیشنهاد شده است که می‌تواند از حملات سیاهچاله اجتناب کرده و سبب ارتقا امنیت گردد. روش پیشنهادی بر مبنای منطق فازی عمل می‌کند و بر اساس پارامترهای تعداد ارسال داده، زمان ارسال داده و انرژی مصرف گره‌ها عمل می‌کند در این سیستم پارامتر های گفته شده برای ورودی منطق فازی پیشنهادی هستند و براساس خروجی سیستم فازی گره‌های دچار حمله شناسای می شود، روش پیشنهاد با یک روش دیگر مقایسه شده است و در شکل زیر قابل مشاهده است که چه مقدار روش پیشنهادی بهبودی داشته است.



(شکل- ۹): میزان بهبود روش پیشنهادی در هر معیار

۷- مراجع

[1] *Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism." In 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), pp. 115-120. IEEE, 2016.*

[2] *Borgohain, Tuhin, Uday Kumar, and Sugata Sanyal. "Survey of security and privacy issues of internet of things." arXiv preprint arXiv:1501.02211 (2015).*

[3] *Mathur, Avijit, Thomas Newe, and Muzaffar Rao. "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT." Sensors 16, no. 1 (2016): 118.*

[4] *Sharma, Divya, Ishani Mishra, and Sanjay Jain. "A detailed classification of routing attacks against RPL in Internet of Things." International Journal of Advance Research, Ideas and Innovations in Technology 3, no. 1 (2017): 692-703.*

[5] *Bostani, Hamid, and Mansour Sheikhan. "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach." Computer Communications 98 (2017): 52-71.*

[6] *Mathur, Avijit, Thomas Newe, and Muzaffar Rao. "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT." Sensors 16, no. 1 (2016): 118.*

[7] *Bashir, Adil, and Ajaz Hussain Mir. "Internet of Things Security Issues, Threats, Attacks and Counter Measures." International Journal of Computing and Digital Systems 7, no. 02 (2018): 111-120.*

[8] *Shahabi, Sina, Mahdieh Ghazvini, and Mehdi Bakhtiarian. "A modified algorithm to improve security and performance of AODV protocol against black hole attack." Wireless Networks 22, no. 5 (2016): 1505-1511.*

[9] *Khare, Ashish Kumar, J. L. Rana, and R. C. Jain. "Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology." International Journal of Computer Network and Information Security 9, no. 7 (2017): 29.*

[10] *Daza, V., A. Lozano, and M. Richardson. "Routing Over Low-Power and Lossy Networks T. Tsao Internet-Draft R. Alexander Intended status: Informational Cooper Power Systems Expires: December 12, 2014 M. Dohler CTTC." (2014).*

[11] *Mayzaud, Anthea, Remi Badonnel, and Isabelle Chrisment. "A Taxonomy of Attacks in RPL-based Internet of Things." (2016).*

[12] *Sharma, Divya, Ishani Mishra, and Sanjay Jain. "A detailed classification of routing attacks against RPL in Internet of Things." International Journal of Advance Research, Ideas and Innovations in Technology 3, no. 1 (2017): 692-703.*

[13] *Airehrour, David, Jairo Gutierrez, and S. Ray. "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks." (2017).*

[14] *Taylor, Vincent F., and Daniel T. Fokum. "Mitigating black hole attacks in wireless sensor networks using node-resident expert systems." In 2014 wireless telecommunications symposium, pp. 1-7. IEEE, 2014.*

[15] *Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on Emerging Topics in Computing 5, no. 4 (2016): 586-602.*

[16] *Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1, no. 1 (2011): 4.*

ابراهیم ظاهری عبده وند کارشناسی خود را در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات در سال۱۳۹۴ اخذ نموده و مدرک کارشناسی ارشد خود را در رشته مهندسی فناوری اطلاعات گرایش مدیریت سیستم های اطلاعاتی در سال ۱۳۹۷ به اتمام رسانده و اکنون دانشجوی دکتری در دانشگاه آزاد قزوین میباشد در سال ۲۰۱۸ توانست پس از سپری کردن مراحل مختلف آموزش و ممیزی شرکتها در حوزه امنیت اطلاعات TUV Nord مدرک سرممیزی بین‌المللی را از شرکت آلمان اخذ نماید و همچنین با گذراندن دوره و قبولی موفق به کسب استاندارد NDA در آزمون استاندارد آلمان TUV Nord عدم افشاء اطلاعات از شرکت گردید در حال حاظر ایشان در زمینه جراحی هارد و بازیابی اطلاعات و رمز گشایی فایلهای آسیب دیده توسط باج‌گیرها به عنوان مدیر فنی و توسعه تکنولوژی کلینیک تخصصی بازیابی اطلاعات بهره ور فعالیت دارد و همچنین بعنوان مشاور در زمینه امنیت اطلاعات مشغول به فعالیت میباشد. نشانی رایانامه: SERVER_KIA@Yahoo.com

منوچهر کاظمی مدرک کارشناسی خود را در رشته ریاضی کاربردی گرایش کامپیوتر از دانشگاه صنعتی خواجه نصرالدین طوسی در سال ۱۳۷۸ و مدرک کارشناسی ارشد را در رشته ریاضی کاربردی از دانشگاه تحصیلات تکمیلی زنجان در سال ۱۳۸۰ و همچنین دکترای خود را در رشته محاسبات عددی در سال ۱۳۹۳ از دانشگاه آزاد اسلامی کرج اخذ کرده است. در حال حاضر ایشان عضو هیأت علمی و استادیار پایه ۱۵ در دانشکده فنی و مهندسی دانشگاه آزاد آشتیان است. زمینه‌های پژوهشی مورد علاقه ایشان عبارتند از: محاسبات عددی، شبکه‌های عصبی، هوش مصنوعی و تجزیه، نظریه فازی، موجک ها Wavelent، Hoyar و تحلیل الگوریتم ها.

نشانی رایانامه ایشان عبارت است از:

mkazemi@aiau.ac.ir
unirer_ka@yahoo.com