ارائه راه‌کاری مبتنی بر منطق فازی به‌منظور افزایش نرخ تحویل بسته در سیستم تشخیص نفوذ

محمد اخلاق‌پور، دانشجوی کارشناسی‌ارشد مهندسی کامپیوتر، باشگاه پژوهشگران جوان و نخبگان واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران
M.Akhlaghpour@khuisf.ac.ir
محمدرضا سلطان‌آقائی، استادیار دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)
Soltan@khuisf.ac.ir

چکیده

در تشخیص نفوذ، رفتار طبیعی فعالیت‌های انجام شده توسط کاربر یک مسئله مهم می‌باشد، از این‌رو دانش اندک درمورد یک حمله از میان انبوه حملات برای سیستم تشخیص نفوذ شامل، نرخ تشخیص کم و هم‌چنین نرخ بالای هشدارهای کاذب می‌باشند. در این مقاله، روشی مرکب، برگرفته از روش‌های تحلیل علت ریشه‌ای و تشخیص ناهنجاری در جهت بهبود و کاهش هشدارهای مثبت‌کاذب در سیستم تشخیص نفوذ با استفاده از منطق فازی، به‌منظور شناسایی و تفکیک هشدارهای صحیح از هشدارهای کاذب بیان گردیده است. نتایج به‌دست آمده در این پژوهش، نشان می‌دهد، نسبت تحویل بسته می‌تواند با استفاده از الگوریتم سه ورودی فازی، مقداری برابر با 100 درصد و کاهش میزان هشدارهای کاذب را به مقداری برابر صفر را به‌همراه داشته باشد.

کلیدواژه‌ها: هشدار کاذب، سیستم تشخیص نفوذ، منطق فازی.

1- مقدمه

منبع داده‌های شبکه، شامل مقدار زیادی از اطلاعات متنی می‌باشد که تجزیه و تحلیل، آن‌ها را دشوار می‌نماید. بنابراین شناسائی نفوذ، براساس منابع مختلفی از جمله کسب اطلاعات و وقایع شکل می‌گیرد. این اطلاعات در تشخیص سوءاستفاده، دانش گسترده‌ای از الگوهای مرتبط با حملات شناخته‌شده توسط کارشناسان می‌باشد. بنابراین روش‌هایی هم‌چون، تطبیق الگو، تجزیه و تحلیل انتقال حالت در تشخیص نفوذ[1]، کاربرد دارند. به‌منظور مقابله با نفوذ به سیستم و شبکه‌های کامپیوتری، روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ ایجاد گردیده است، که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم به شبکه‌ی کامپیوتری را برعهده دارند.

از این‌رو شبکه تشخیص نفوذ، برای نظارت بر یک منطقه وسیع و دوردست استفاده می‌شوند[1]. سیستم تشخیص نفوذ، از گره‌های حسگر کوچک تشکیل شده است، که باهم همکاری می‌کنند. توپولوژی کنترل در سیستم‌های تشخیص نفوذ، برای دست‌یابی به صرفه‌جویی در انرژی و افزایش طول عمر شبکه استفاده می‌شود. این روش، رویکرد منطق فازی را برای توپولوژی کنترل شبکه اعمال می‌نماید. تمام گره‌ها در یک شبکه به‌طور تصادفی و یکنواخت مستقر می‌شوند. بنابراین، ابتدا از دو ورودی استفاده شده است، که تفاوت بین تعداد گره‌ها با شعاع کم‌ترین و حداکثر حساسیت می‌باشند. با این حال، به علت چند عیب، یک ورودی دیگر یعنی مجاورت سینک اضافه شده است.

هدف اصلی این پژوهش، افزایش تحویل بسته و کاهش هشدارهای کاذب با استفاده از منطق فازی[2] در سیستم تشخیص نفوذ می‌باشد. هم‌چنین در بخش 2، به راه‌کارهای پیشین، سپس در بخش 3، روش پیشنهادی، پس از آن در بخش 4، ارزیابی پژوهش و در بخش 5، نتیجه‌گیری و کارهای پیشین پرداخته شده است.

2- کارهای پیشین

در تحقیق هامامتو و همکاران‌اش در سال 2018، یک طرح ترکیبی از الگوریتم ژنتیکی[3] و یک منطق فازی برای تشخیص ناهنجاری شبکه مطرح گردیده است. در این تحقیق، الگوریتم ژنتیک برای تولید یک پارامتر دیجیتال شبکه با استفاده از تحلیل جریان استفاده شده است، از این رو، جایی‌که اطلاعات از داده‌های جریان شبکه استخراج شده است، به‌منظور پیش‌رفتار ترافیک شبکه برای یک بازه زمانی استفاده شده است. علاوه بر این، یک طرح منطقی فازی برای تصمیم‌گیری درمورد این‌که یک نمونه، یک انحراف متفاوت از برخی رویکردهای موجود در ادبیات است، اعمال گردیده است. در واقع، یک سیستم متخصص با قابلیت نظارت بر ترافیک شبکه با جریان‌های IP پیشنهاد شده است، در حالی‌که رفتارهای پیش‌بینی شده در بازه زمانی منظم تولید شده و زمانی‌که یک مشکل احتمالی وجود دارد،

1- Intrusion Detection
2- Fuzzy Logic
3- Genetic Algorithm

هشدار را صادر می‌نماید. سیستم تشخیص ناهنجاری پیشنهاد شده، مستقل از مشکلات شبکه می‌باشد. در نتایج به‌دست آمده، اشاره شده است، با استفاده از رویکرد پیشنهادی در یک جریان واقعی ترافیک شبکه ، دقت 96/54 درصد و نرخ مثبت کاذب 0.56 درصد می‌باشد. هم‌چنین، این روش در دستیابی به عملکرد بالاتری در مقایسه با چندین روش دیگر موفق بوده است[2].

در تحقیق هایدر و همکاران‌اش در سال 2017، یک ماتریس با استفاده از یک سیستم منطقی فازی مبتنی بر مدل استنتاج فازی Sugeno، برای ارزیابی کیفیت واقع‌گرایی، مجموعه داده‌های سیستم تشخیص نفوذ ارائه شده است. در این تحقیق، براساس نتایج متریک پیشنهادی، مجموعه‌ای از مجموعه داده‌های سیستم تشخیص نفوذ نسل آینده واقع‌گرایانه، طراحی و تولید شده است و یک تحلیل اولیه انجام شده، که جهت کمک به طراحی سیستم‌های تشخیص نفوذ آینده است. این مجموعه داده تولید شامل، بازتاب‌های عادی و غریزی از فعالیت‌های شبکه فعلی می‌باشد که در سطوح مهم زیرساخت‌های سایبری در شرکت‌های مختلف انجام می‌شود. درنهایت، با استفاده از معیار پیشنهاد شده، مجموعه داده تولید شده برای ارزیابی کیفیت واقع‌گرایی آن، با مقایسه آن با مجموعه داده‌های سیستم تشخیص نفوذ، در دسترس عمومی برای تأیید برتری آن تحلیل شده است[3].

در تحقیق لی و همکاران‌اش در سال 2016 آمده است، سیستم تشخیص نفوذ شبکه، برای بیش از بیست سال توسعه یافته‌اند و به‌طور گسترده‌ای در شبکه‌های کامپیوتری برای تشخیص تنوع حملات مستقر شده‌اند. اما یکی از محدودیت‌های عمده، تعداد زیاد سیستم‌های هشدار، به‌خصوص هشدارهای کاذب است، که در طول تشخیص تولید می‌کنند. برای پرداختن به این موضوع، بسیاری از روش‌های یادگیری‌ماشین[1] به‌منظور کاهش سیستم تشخیص نفوذ شبکه و مثبت کاذب استفاده شده است. با این حال در مقاله فوق، به رویکرد مبتنی بر چند نظریه که اغلب توسط ادبیات، با استفاده از یک تابع به مدل، یک دیدگاه خاص و به‌طور مشترک بهینه‌سازی شده است، تمام توابع برای بهینه‌سازی و بهبود عملکرد یادگیری استفاده می‌کنند. نتایج به‌دست آمده در این مقاله، نشان داده است که سیستم می‌تواند یک قدرت فیلتراسیون‌پایدار[2]، با بهبود بیش از 95% به‌دست آورده شد [4].

در تحقیق اِلحاق و همکاران‌اش در سال 2015، به‌منظور توسعه چندین سیستم، از سیستم‌های فازی ژنتیکی در یک چارچوب یادگیری دوگانه استفاده شده است. مزایای استفاده از این رویکرد دوگانه است: اول، استفاده از مجموعه‌های فازی و به‌ویژه برچسب‌های زبانی، مرز نرمی بین مفاهیم را فراهم می‌کند و امکان تفسیر بیشتر از مجموعه قوانین را فراهم می‌آورد. دوم، طرح یادگیری تقسیم و تسخیر، که در آن تمام جفت‌های ممکن کلاس‌ها را با اهداف تطبیق می‌کند، برای رویدادهای حمله ناشناخته بهبود بخشد. هم‌چنین اشاره شده است، بین جدایی «فعالیت عادی» و انواع مختلف حمله، بهتر می‌شود[5].

1- Machine Learning
2 - Stable Filtration

در تحقیق فنگ و همکاران‌اش در سال 2014، یک الگوریتم طبقه‌بندی داده مبتنی بر یادگیری ماشین اعمال شده به شبکه تشخیص نفوذ ارائه شده است. وظیفه این طبقه‌بندی، به حداقل رساندن اشتباه در فعالیت‌های شبکه عادی و غیرعادی می‌باشد. نتایج این تحقیق، نرخ طبقه‌بندی و زمان اجرا بهبود داده شده است[6].

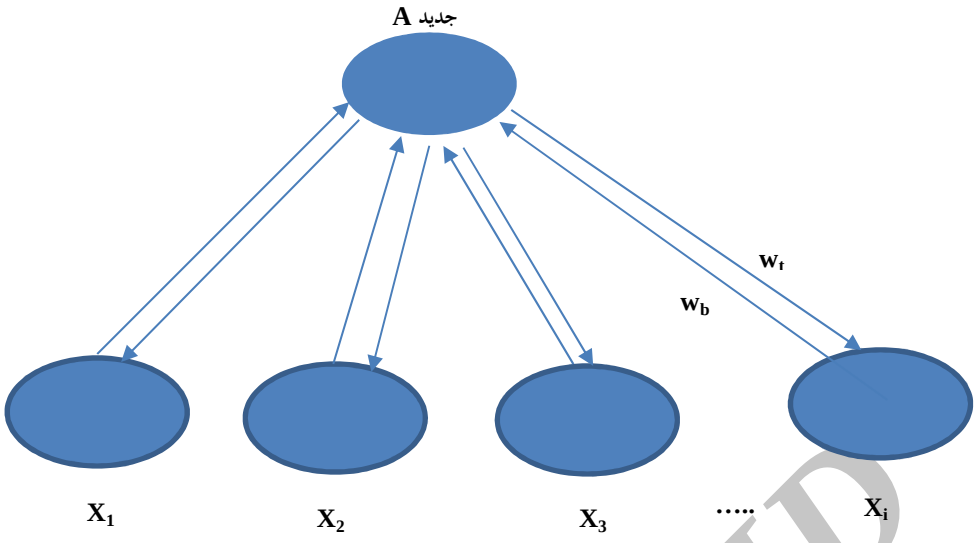
در تحقیق کورانا و همکاران‌اش در سال 2013، به کمک‌های فرضیه‌های اصلی سه مرحله را ارائه شده است: الف) طبقه‌بندی کلی از تکنیک‌های حمله در برابر سیستم تشخیص نفوذ پشتیبان. ب) شرح گسترده‌ای از چگونگی حملات، با بهره‌برداری از نقاط ضعف سیستم تشخیص نفوذ در سطح انتزاعی مختلف اجرا. ج) انجام یک تحقیق انتقادی، برای هریک از راه‌حل‌های پیشنهادی و نقاط باز است [7].

جدول 1- پیشینه تحقیق به‌طور اختصاری

مرجع	تکنیک	هدف	نتیجه
هامامتو و همکاران‌اش 2018، [2]	طرح ترکیبی از الگوریتم ژنتیکی و یک منطق فازی	تولید یک پارامتر دیجیتال شبکه با استفاده از تحلیل جریان	بهبود با دقت 96/54 درصد و نرخ مثبت کاذب 0.56 درصد
هایدر و همکاران‌اش 2017، [3]	استفاده از ماتریس با استفاده از یک سیستم منطقی فازی مبتنی بر مدل استنتاج فازی Sugeno	ارزیابی کیفیت واقع‌گرایی	بهبود در مقایسه با مجموعه داده‌های سیستم تشخیص نفوذ
لی و همکاران‌اش 2016، [4]	رویکرد مبتنی بر چند نظریه	کاهش سیستم تشخیص نفوذ شبکه و مثبت کاذب	بهبود بیش از 95%
اِلحاق و همکاران‌اش 2015، [5]	استفاده از سیستم‌های فازی ژنتیکی در یک چارچوب یادگیری دوگانه	استفاده از مجموعه‌های فازی و طرح یادگیری تقسیم و تسخیر	بهبود فعالیت عادی
فنگ و همکاران‌اش 2014، [6]	استفاده از الگوریتم طبقه‌بندی داده مبتنی بر یادگیری ماشین	حداقل رساندن اشتباه در فعالیت‌های شبکه عادی و غیرعادی	بهبود نرخ طبقه‌بندی و زمان اجرا
کورانا و همکاران‌اش 2013، [7]	استفاده از فرضیه‌های اصلی سیستم تشخیص نفوذ	انجام یک تحقیق انتقادی	ارائه راه‌حل‌های پیشنهادی و نقطه باز

3- روش پیشنهادی

باتوجه به این‌که حملات در افراد مختلف و تکنولوژی‌های مختلف متفاوت می‌باشد، از این رو، اگر سیستم نتواند پیشرفت نماید، سیستم تشخیص نفوذ نیز نمی‌تواند امنیت را بهبود ببخشد. برای حل این مشکل، سیستم تشخیص نفوذ ترکیبی هوشمند مطرح شده در [8]، باید یک سیستم تشخیص هوشمند باشد. وقتی سیستم با یک حمله جدید مواجه می‌شود، مکانیزم یادگیری این توانایی را در تشخیص و یادگیری نوع جدیدی از حمله خواهد داشت. در شکل 1، مدلی از معماری مکانیزم یادگیری سیستم‌های تشخیص نفوذ ترکیبی هوشمند نشان داده شده است.



شکل 1- معماری مکانیزم یادگیری سیستم‌های تشخیص نفوذ ترکیبی هوشمند

از آن‌جایی که نمی‌توان نمونه‌های واقعی را در شبکه‌های حسگر بی‌سیم خوشه‌بندی شده به‌دست آورد، از مجموعه داده دانش 1999[1]، به‌عنوان نمونه برای بررسی کارایی ماژول تشخیص سوءاستفاده، استفاده می‌شود. مجموعه داده دانش 1999 در Columbia University در سال 1998، برای محیط‌های نظامی در پروژه DARPA ساخته شد، که شامل 34 نوع امکانات عددی و 7 نوع امکانات نمادی می‌باشند.

علاوه براین، این مجموعه داده، شامل تعداد زیادی رفتارهای حملات مختلف می‌باشد که در 4 گروه دسته‌بندی شده‌اند: پروب[2]، حمله کاربر به ریشه[3]، حمله کاربر محلی[4] و نیز شامل یک نوع ارتباط نرمال می‌باشد. بنابراین 5 نوع رفتار در آزمایشات برای دسته‌بندی سیستم‌های تشخیص نفوذ ترکیبی استفاده می‌شوند. حمله‌هایی مانند، Spoofed, Altered, Replayed rooting information, Sinkhole, Wormholes و Acknowledmnet Spoofing، نیاز به ایجاد مرحله پروب، قبل از انجام حمله دارد. در این مقاله از kddcup.data_10_percent.gz به‌عنوان نمونه آموزشی و آزمایشی مجموعه داده، استفاده می‌شود، که شامل 10% از مجموعه داده دانش 1999و 494021 ارتباط ثبت شده می‌باشد.

3-1- تعیین مقادیر احتیاطی تشدید انطباقی شبکه

یک بسته وقتی به‌عنوان یک حمله ناشناخته، شناسایی می‌شود که مقدار خروجی زیر حد آستانه باشد، در چنین حالتی، بسته به مکانیزم یادگیری جهت شناخت نوع آن ارسال می‌شود. برای پیدا

1- Knowledge Discovery Data Mining (KDD)
2- Prob
3- User to Root (U2R)
4- User to Local (U2L)

کردن میانگین تعداد خوشه‌ها، مقادیر احتیاطی باید تعیین شوند، زیرا این مقادیر احتیاطی مهم‌ترین فاکتور جهت تعیین تعداد خوشه‌ها هستند. مقادیر احتیاطی، بین 0 و1 هستند و به‌منظور ایجاد دسته‌بندی‌های مختلف، باید مقادیر مختلفی برای آن تعیین نمود.

3-2- شبیه‌سازی تشدید انطباقی شبکه

مشاهده شده است، اگر مقدار حدآستانه بیشتر 0/99 باشد، باید توانست به دقت بالای 95% نیز دست یافت، به‌علاوه اگر مقدار احتیاطی 0/05 باشد، تعداد خوشه‌ها در یک حد کنترل شده و حد میانگین خواهد بود و دسته‌بندی به‌خوبی انجام می‌گیرد.

3-3- سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

در واقعیت یک شبکه ساخته می‌شود، که مهاجمان نتوانند خط دفاعی آن را بشکنند، این کاری واقعاً مشکل است، زیرا در حقیقت شبکه‌ها باید ادغام خودآگاهی و توانایی تحمل‌پذیری خطا را درنظر داشته باشند. به‌عبارتی، باید یک مکانیزم طراحی شود که حملات را تشخیص داده و اثرات آن‌ها را کاهش دهد. از این‌رو، یک خط دوم دفاعی موردنیاز می‌باشد که حملات و یا گره‌های مهاجم را تشخیص دهد. یک سیستم تشخیص نفوذ قادر است، گره‌های بدرفتار را تشخیص داده و سایر گره‌های همسایه را برای اقدام متقابل مناسب، آگاه سازد. مکانیزم تشخیص نفوذ واقعی، در عناصری که به آن‌ها عامل سیستم تشخیص نفوذ می‌گویند، پیاده‌سازی می‌شود.

اگرچه بعضی از انواع سیستم‌های تشخیص نفوذ، به‌عنوان مکانیزم جلوگیری کننده اصلی در شبکه‌های سیمی و adhoc استفاده می‌شوند، اما توجه داشته باشید، پیاده‌سازی این سیستم‌ها در شبکه‌های بی‌سیم به‌دلیل تفاوت زیاد این شبکه‌ها، امکان‌پذیر نمی‌باشد. این یکی از پیچیدگی‌های طراحی مکانیزم‌های امنیتی می‌باشد. بنابراین شبکه‌های حسگر بی‌سیم، نیاز به یک طراحی جدید و سبک وزن از سیستم‌های تشخیص نفوذ دارند.

3-4- شبیه‌سازی

در شبیه‌سازی، از 3 ورودی فازی استفاده شده است که شامل، 25 قانون برای 2 ورودی و 125 قانون برای 3 ورودی در استنتاج فازی است. شکل قوانین به این‌صورت است:

اگر A و B و C (C برای 3 ورودی استفاده می‌شود) آن‌گاه D، جایی‌که A، B، C، D نشان‌دهنده درصد انرژی باقی‌مانده و تفاوت حداکثر حداقل پوشش، نزدیک به تخلیه و فاصله فعلی است. بعضی مثال‌ها از قوانین در جدول 2 نشان داده شده است.

جدول2- مثال از قوانین

فاصله کانونی	نزدیکی	میانگین Max/Min	درصد انرژی باقی‌مانده
بالا	دور	بالا	بالا
متوسط	میانه	کم	بالا
خیلی بالا	خیلی دور	بالا	متوسط
بالا	خیلی دور	خیلی بالا	کم

در جدول 3، پنج شبکه را نشان می‌دهد که تعداد تکرار برنامه گره اول از بین می‌رود. به‌عنوان مثال، در الگوریتم MIN در شبکه به اندازه 80*80 بعد از 1344 بار تکرار برنامه در گره اول از بین می رود.

جدول 3- پنج شبکه که تعداد تکرار برنامه در گره اول از بین می‌رود

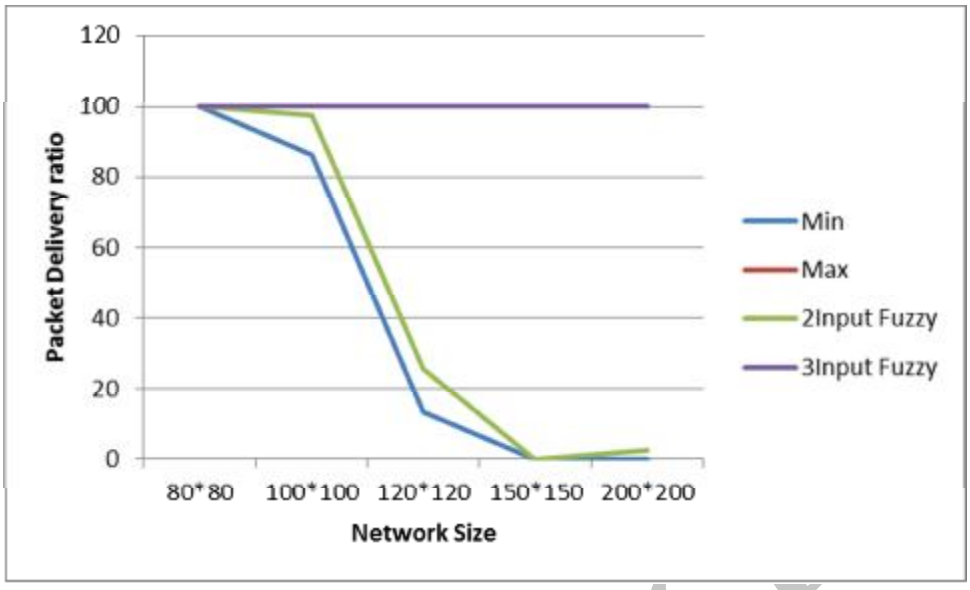
سایز شبکه	80*80	100*100	120*120	150*150	200*200
Min	1344	1616	875	-	-
Max	967	1264	1464	1097	966
2 ورودی فازی	2844	988	568	-	-
3 ورودی فازی	3023	3812	1013	1019	622

به‌طور کلی می‌توان بیان نمود، هنگامی که اندازه شبکه بزرگ‌تر شود، در الگوریتم‌های فازی Min و 2 ورودی، گره اول زودتر از 2 الگوریتم دیگر می‌میرد . "-" نشان‌دهنده شکست شبکه است. به‌دلیل توازن بار در الگوریتم فازی سه ورودی، گره‌های حسگر با یک‌دیگر همکاری می‌کنند، بنابراین طول عمر گره‌های حسگر می‌تواند طولانی باشند.

4- ارزیابی پژوهش

در مطالعات انجام شده که در بخش 2 به آن‌ها اشاره گردیده است، با استفاده از منطق فازی به‌منظور قابلیت نظارت بر ترافیک شبکه با جریان‌های IP و تفسیر مجموعه داده بودند. در این تحقیق با استفاده از روش‌های پیشین تلاش گردید تا راه‌حل جدیدی جهت افزایش نرخ تحویل بسته و کاهش هشدارهای کاذب با استفاده از 3 ورودی فازی انجام پذیرد.

نتایج به‌دست آمده در این تحقیق نشان داده است، با استفاده از 3 ورودی فازی می‌توان نرخ تحویل بسته را تا میزان برابر با 100 درصد افزایش داد و از این رو میزان کاهش هشدار کاذب به صفر خواهد رسید. شکل 2، نسبت تحویل بسته به‌صورت تابعی از اندازه‌ی شبکه را نشان می‌دهد.



شکل 2 - میزان تحویل بسته

درجدول 4، مقادیر به‌دست آمده، با 3 ورودی فازی به نسبت2 ورودی فازی با حداقل 50 گره و حداکثر 100 گره به‌صورت عددی نشان داده است.

جدول4- نسبت تحویل بسته

الگوریتم	Min	Max	2 ورودی فازی	3 ورودی فازی
50 گره	86.5	100	97.6	100
100 گره	100	100	100	100

باتوجه به الگوریتم‌های فازی، Max و 3 ورودی، گره غیرقابل دست‌یابی رخ نمی‌دهد و تمام بسته‌ها دریافت می‌شوند. بنابراین نسبت تحویل بسته 100% می‌باشد، که در Min و 2 ورودی فازی، کوچک‌ترین نسبت است.

5- نتیجه‌گیری و کارهای آینده

در این تحقیق باتوجه به شبیه‌سازی، الگوریتم‌هایی که از منطق فازی استفاده می‌کنند، براساس قوانین تعریف شده باعث می‌شوند تا گره‌ها با یک‌دیگر همکاری داشته باشند، که این همکاری موجب ایجاد تعادل‌بار در شبکه می‌شود. بنابراین گره‌ها در این الگوریتم طولانی‌تر از دیگران زنده خواهند ماند و موجب افزایش نسبت تحویل بسته می‌شوند. در الگوریتم Min، به علت حداقل شعاع حسگر، گره‌های غیرقابل دسترس بیشتر خواهد بود. این باعث کم‌شدن مقدار بسته‌بندی می‌شود. سیستم

منطق فازی مطابق با محیط‌های در حال تغییر با مشکلی مواجه است. به‌منظور کارهای آینده توصیه می‌گردد، با استفاده از مفاهیم یادگیری شبکه‌های عصبی در سیستم‌های فازی، اغلب به نام مدل‌سازی عصبی، می‌تواند جایگزینی خوب در شبکه‌های آینده باشد.

مراجع

[1] Srithar S. Karuppasamy K. (2015), ***Energy Efficient Adaptive Weighted Fuzzy Clustering Based Routing Protocol in Sensor Networks***, International Journal of Engineering Research and General Science Vol. 3, pp.825-830.

[2] Hamamoto, A. H. Carvalho, L. F. Sampaio, L. D. H. Abrão, T. Proença M. L. (2018), ***Network Anomaly* Detection System *using Genetic Algorithm and* Fuzzy *Logic*,** Expert Systems With Applications, , Vol. 92, pp. 390-402.

[3] Haider, W. Hu, J. Slay, J. Turnbull, B.P. Xie, Y. (2017), ***Generating Ralistic Intrusion Detection System Dataset Based on Fuzzy Qualitative Modeling,*** Journal of Network and Computer Applications, Vol.87, pp. 185-192.

[4] Li, W. Meng, W. Lue, X. Kwok L. F. (2016) ***MYPSys: Toward practical Multy – View Based False Alaram Reduction System in Network Intrusion Detection,*** Computer & Security, Vol. 60, pp. 177-192.

[5] Elhag, S. Fernanes, A. Bawakid, A. Alshomrani, S. Herrera, F. (2015), ***On the Combination of Genetic Fuzzy systems and Pairwise Learning for Improving Detection Rates on inteusion Detection System,*** Expert Systems With Applications, Vol. 42, Issuses pp. 193-202.

[6] Feng, W. Zhang, Q. Hu, G. Huang, J. X. (2014), ***Mining network data for intrusion detection through combining SVMs with antcolony networks,*** Future Generation Computer Systems, Vol. 37, pp. 127-140.

[7] Corona, I. Giacinto, G. Roli, F. (2013), ***Adversarial attacks against* intrusion detection systems: Taxonomy, solutions and open issues,** Information Sciences, Vol. 239, pp. 201-225.

[8] Das, A. Gorthim R. (2015), ***knowledge Based Routing Protocol in Wireless Sensor Network,*** 7th International Conference on Computational Intelligence, Communication Systems and Networks (CICSYN), PP. 35-38.