فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال ششم، شماره ۸۶، پاییز ۱۴۰۱، ص ۹۵۸-۹۳۲

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

بهره‌گیری از منطق فازی در جهت تأمین امنیت شبکه‌های بی‌سیم

احد تفضلی [۱]

تاریخ دریافت: ۱۴۰۱/۰۷/۰۴ تاریخ چاپ: ۱۴۰۱/۰۹/۲۵

چکیده

در دهه‌های گذشته شبکه‌هایی حسگر بی‌سیم به دلایل کاربردهای وسیع در علوم مختلف مانند علوم نظامی، کشاورزی وغیره، در بین محققان بسیار مورد توجه قرار گرفته است و همچنین با پیشرفت روزافزون این تکنولوژی و قوی‌تر شدن آن بحث تأمین امنیت این شبکه‌ها و جلوگیری از نفوذ به آن‌ها توسط گروه‌های مهاجم دارای اهمیت دوچندان شده است. در این پژوهش با استفاده از منطق فازی که یک منطق چند ارزشی، بین ۰ و ۱ می‌باشد به بحث شناسایی خطرات موجود در این شبکه‌ها و همچنین برخورد متناسب نسبت به مهاجمان برای تأمین بهتر امنیت پرداخته شده است، سیستم فازی نام برده که بر اساس استنتاج ممدانی می‌باشد و می‌تواند نیازهای امنیتی شبکه را برای مقابله با نوع‌های متفاوت با اهداف و تکنیک‌های مختلفی از مهاجمان را برآورده سازد و به عنوان ابزاری مناسب برای عملکرد متقابل در برابر این حمله‌ها عمل کند. نتایج عددی برای دو حالت از حملات فرضی به شبکه به صورت (۵؛ و ۸۱۲؛ و ۸۱۲) و (۱۵۴؛ و ۴۴؛ و ۳۸۵.) می‌باشد که به ترتیب کنترل خاص سخت‌افزارها، بانک اطلاعات ملی برای نرم‌افزارها و کنترل افراد برای حالت اول و کنترل فیزیکی سخت‌افزارها، آپدیت سیستم برای نرم‌افزارها و آموزش افراد را برای حالت دوم را نتیجه می‌دهد.

واژگان کلیدی

شبکه‌های حسگر بی‌سیم، امنیت سایبری، نفوذ، منطق فازی، تهاجم سایبری

۱. کارشناسی ارشد مهندسی فناوری اطلاعات-مدیریت سیستم های اطلاعاتی، دانشگاه غیاث الدین جمشید کاشانی، قزوین، ایران.

مقدمه

شبکه‌های حسگر بی‌سیم از موضوعات بدیع و بسیاربا اهمیت در دانش روز پردازش و فناوری اطلاعات محسوب می‌گردد (Islam andWada,2013). این شبکه‌ها در مواردی مانند نظارت بر شرایط محیطی، جمع‌آوری داده‌هایی نظیر دما و فشار، کاربردهای نظامی کاربرد دارند (Felemban,2013)، شبکه‌های حسگر بی‌سیم از نظر تهدیدات و حملات مخرب بسیار آسیب‌پذیر هستند. شبکه‌های حسگر بی‌سیم از موضوعات بدیع و بسیاربا اهمیت در دانش روز پردازش و فناوری اطلاعات محسوب می‌گردد که این شبکه‌ها گزینه مناسبی برای حالتی است که ما به محیط هدایت شده دسترسی نداشته باشیم. این شبکه‌ها مستقل و خود گردان بوده و بدون دخالت انسان کار می‌کنند. شبکه‌های حسگر بی‌سیم، شبکه‌هایی هستند که معمولاً برای نظارت و کنترل محیط‌های اطراف مورد استفاده قرار می‌گیرند. این شبکه‌ها، یک سیستم توزیع شده، خود مختار و خود سازمانده هستند که از تعداد زیادی گره‌های حسگر کوچک با عملیاتی که به انرژی کمی نیاز دارند تشکیل شده است (Islam andWada,2013) امنیت شبکه[1] در حالت کلی به مجموعه اقداماتی گفته می‌شود که به منظور جلوگیری از بروز مشکلات امنیتی در بستر شبکه صورت می‌گیرد. این مجموعه اقدامات می‌تواند بصورت راهکارهای متعددی در غالب سرویس‌های سخت‌افزاری و نرم‌افزاری پیاده‌سازی شوند. در این پژوهش حفظ امنیت شبکه‌های بی‌سیم به کمک منطق فازی[2] بررسی خواهدشد. منطق‌فازی شکلی از منطق‌های چند ارزشی بوده که در آن ارزش منطقی متغیرها می‌تواند هر عدد حقیقی بین ۰ و ۱ و خود آن‌ها باشد. ساختار سیستم‌های منطق فازی، ساده و قابل درک است.

سیستم‌های منطق فازی در دنیای امروز در گروه وسیعی از علوم و فنون کاربرد دارند یکی از کاربردهای اصلی این سیستم‌ها کمک به بهبود سیستم‌های تشخیص در شبکه‌های ارتباطی و اطلاعاتی است (مرادی و همکاران، ۱۳۹۰). از این‌روی در مطالعه پیش رو به بررسی حفظ امنیت شبکه‌های حسگر بی‌سیم به کمک منطق‌فازی پرداخته خواهدشد.

از آنجایی که شبکه‌های حسگر بی‌سیم در زمینه‌های پزشکی، صنعت، کشاورزی، نظامی، محیط زیست، ساختمان، سلامت و بهداشت و... کاربرد دارند، لذا حفظ امنیت این شبکه‌ها از اهمیت بالایی برخوردار است؛ بنابراین نتایج این پژوهش می‌تواند به حفظ امنیت و بهبود کارکرد شبکه‌های بی‌سیم در زمینه‌های ذکر شده کمک‌کننده باشد. از دیگر کاربردهای نتایج این پژوهش افزایش امنیت شبکه‌های بی‌سیم در نظارت بر آلودگی هوا، نظارت بر آتش‌سوزی جنگل‌ها، نظارت بر رانش زمین، نظارت بر میزان آلودگی آب‌ها، نظارت بر تغییرات جوی جهت جلوگیری و کم کردن عواقب حوادث طبیعی مثل سیلاب‌ها و طوفان‌ها، صحت کارکرد و سلامت ماشین آلات، نظارت بر کارکرد سیستم‌ها که حتی می‌توان بر کارکرد یک حسگر شبکه دیگر نظارت کرد، نظارت بر کارکرد مراکز داده، نظارت بر سلامتی سازه‌های مهندسی می‌باشد.

[1] Network Security
[2] Fuzzy Logic

نتایج این پژوهش همچنین در پژوهشگاه‌های علوم پزشکی، بیمارستان‌ها، پادگان‌های نظامی، دستگاه‌های مربوط به انرژی هسته‌ای، کارخانه‌جات و مراکز صنعتی، ساختمان‌های هوشمند، سازمان محیط‌زیست، استانداری و شهرداری مراکز استان‌ها، مراکز اداری دولتی و خصوصی، دانشگاه‌ها و مراکز آموزش عالی مورد استفاده قرار می‌گیرد.

هدف این پژوهش، بررسی کاربرد منطق‌فازی در حفظ امنیت شبکه‌های بی‌سیم و ارائه راهکارهایی جهت جلوگیری از حملات آسیب‌زا به شبکه می باشد. همچنین در این پژوهش برآنیم تا به ارائه‌ی رفتار متناسب نسبت به حملات خاص و بررسی نقاط ضعف شبکه‌های بی‌سیم در راستای حفظ امنیت بپردازیم. از همین رو در پی پاسخ به سوالاتی نظیر این موارد هستیم که چگونه به کمک منطق فازی می‌توان امنیت شبکه‌های بی‌سیم را ارتقا داد؟ نقاط ضعف و قوت شبکه‌های بی‌سیم در حفظ امنیت شبکه چیست و دامنه و کاربرد منطق فازی در حفظ امنیت شبکه‌های بی‌سیم چیست؟

فرضیه های پژوهش به این شرح است کهبه کمک منطق فازی می‌توان امنیت شبکه‌های بی‌سیم را افزایش داد؟ با استفاده از منطق فازی می‌توان شبکه‌های بی‌سیم را در برابر حملات آسیب‌زا ایمن کرد.

پیشینه پژوهش

در مقاله Shin و همکاران که در سال ۲۰۱۰ منتشر شد (Shin,et all,2010) یک چارچوب سلسله مراتبی برای تشخیص نفوذ و همچنین پردازش داده‌ها پیشنهاد شده است. در طول آزمایشات بر روی چارچوب پیشنهادی، آن‌ها بر اهمیت خوشه‌بندی یکپارچه تأکید کردند. نویسندگان معتقد بودند چارچوب سلسله مراتبی آن‌ها برای تأمین برنامه‌های کاربردی صنعتی شبکه حسگرهای بی‌سیم در رابطه با دو خط دفاعی مفید است. در (Chen, et all. 2009) نویسندگان یک جدول جداسازی را برای تشخیص نفوذها در شبکه حسگر بی‌سیم سلسله مراتبی از طریق یک روش با بهره‌وری انرژی پیشنهاد کرده‌اند. پیشنهاد آن‌ها نیاز به دو لایه خوشه‌بندی دارد. با توجه به آزمایش آن‌ها، روش تشخیص نفوذ با استفاده از جداول جداسازی می‌تواند حملات را به طور مؤثر تشخیص دهد. مشکل این پیشنهاد به شرح زیر است: نویسندگان ادعا می‌کنند که هر سطح، سطح دیگری را نظارت می‌کند و هر گونه ناهنجاری را به ایستگاه پایه گزارش می‌دهد. از آنجا که این یک شبکه سلسله مراتبی است، هر هشدار تولید شده توسط گره‌های سطح پایین باید از طریق گره‌های سطح بالاتر عبور کند. در صورتی که گره سطح بالاتر خود نفوذکننده باشد، ایستگاه پایه به دلیل سوء استفاده گره‌های بالاتر نفوذکننده از طریق مسدود کردن پیام‌های هشدار که از گره‌های سطح پایین دریافت می‌کنند، نمی‌تواند از سوء رفتار نفوذکننده آگاه شود. در (Su et all,2005) سیستم تشخیص نفوذ مبتنی بر رویکرد خوشه‌بندی پیشنهاد شده است. پیشنهاد آن‌ها همچنین امنیت سرخوشه‌ها را نیز تضمین می‌کند. در رویکرد آن‌ها، اعضای یک خوشه، سرخوشه خود را در زمان برنامه‌ریزی شده نظارت می‌کنند. به این ترتیب انرژی برای تمام اعضای خوشه ذخیره می‌شود. از طرف دیگر، اعضای خوشه تحت نظارت سرخوشه‌ها هستند، این همچنین موجب صرفه‌جویی در انرژی اعضای خوشه می‌شود. نویسندگان از طریق شبیه‌سازی، نشان دادند که الگوریتم پیشنهادی آن‌ها نسبت به الگوریتم‌های دیگر در طراحی بسیار کارآمدتر است. مشکل این رویکرد مکانیسم مدیریت کلید آن است. این بخشی از سیستم تشخیص نفوذ است و به آن کمک می‌کند تا جفت کلیدهایی در

میان گره‌ها ایجاد کند. سیستم تشخیص نفوذ از این کلیدها برای احراز هویت پیام‌ها استفاده می‌کند. مدیریت کلید فرض می‌کند که گره‌ها ثابت هستند و گره‌های جدید نمی‌توانند پس از ایجاد جفت کلیدها ایجاد شوند. این مسأله برای شبکه حسگرهای بی‌سیم به نوعی نقص در طراحی به حساب می‌آید زیرا در این شبکه دایما نیاز به تغییر گره‌ها و تعویض آن‌ها وجود دارد.

به کارگیری منطق فازی در انتخاب مناسب گره بعدی برای پیکربندی مسیر با پروتکل LEAP در شبکه‌های حسگر بی‌سیم تحقیقی است که ستاری و همکاران آن را به انجام رساندند با توجه به این که در شبکه‌های حسگر بی‌سیم، انتخاب مناسب گره بعدی جهت پیشگیری از حملات و کاهش سطح مصرف انرژی دارای اهمیت است، در این تحقیق روشی مبتنی بر منطق فازی برای انتخاب گره گام بعدی با در نظرگرفتن وضعیت و انتقال گزارش به گره‌های مختلف ارائه گردید. در این روش به صورتی مؤثر گره گام بعدی با چهار عامل بر مبنای سیستم منطق فازی انتخاب گردید. این ۴ عامل، بیان‌کننده ۴ پارامتر بهینه شده از نظر انرژی، یعنی درجه نزدیکی گره به کوتاه‌ترین مسیر، درجه نزدیکی گره به سرخوشه، نسبت انرژی باقیمانده هر گره و تعداد پیام‌های غلط فیلترشده است. روش پیشنهادی با افزایش سطح انرژی و حفظ سطح همسانی از امنیت در مقایسه با پروتکل LEAP همراه است (نایینی و همکاران، ۱۳۹۶).

افزایش امنیت شبکه‌های حسگر بی‌سیم با بهره‌گیری از روش جداول عددهای ترکیبی توزیع شده و منطق فازی عنوان پژوهشی است که در سال ۱۳۹۷ در شهر شیراز انجام شد. آنان دریافتند نگهداری و افزایش امنیت، خودکارآمد بودن گره‌های شبکه‌های حسگر بی‌سیم و عدم کنترل از مرکز بر روی آن‌ها از اصلی‌ترین مشکلات پیش روی استفاده از این شبکه‌ها به ویژه در اقدامات حساس و امنیتی و یا کارهای استراتژیک محسوب می‌گردد (دشتی و همکاران، ۱۳۹۷).

ارتقای امنیت، خود کارآمد بودن گره‌های شبکه‌های حسگر بی‌سیم و کنترل نکردن از مرکز از مهمترین معضلات در توسعه این شبکه‌ها به خصوص در گروه کارهای حساسیت بالا و امنیتی و یا اقدامات استراتژیک محسوب می‌گردد. ترکیب جداول توزیع شده (DHT) با شبکه‌های حسگر بی‌سیم راه حل مناسبی برای حل چالش‌ها است. فایده اصلی جدول هش توزیع شده سرویس جستجوی کارآمدش می‌باشد. با استفاده از منطق فازی می‌توانیم ارتباط گزاره‌های واقعی را با گزاره‌های ماشینی برقرار کنیم (قاضی‌زاده و همکاران، ۱۳۹۲).

هوش مصنوعی و الگوهای داده کاوی برای حل این مشکلات تکنیک‌های متعددی را ارائه داده‌اند. در این مقاله تکنیک‌های فازی که در زمینه آموزش بسیار مورد توجه بوده مورد بررسی قرار گرفته است. در سیستم‌های آموزش الکترونیکی، نقش آفرینان اصلی دانش‌آموزان و معلمان هستند و داده مورد پردازش مرتبط با مدل‌سازی و نتایج فعالیت‌های آن هاست. تکنیک‌های فازی بازنمایی این دانش و دستکاری آن تحت رویکردهای انسانی که به خوبی توسط نقش آفرینان این دامنه قابل درک است را امکان‌پذیر می‌سازد. در این تحقیق، مروری بر تکنیک‌های مورد استفاده از جنبه‌های مختلف منطق فازی صورت گرفته است و نتایج به دست آمده در مقالات، نشان می‌دهد تکنیک فازی می‌تواند کارایی

سیستم‌های تدریس را افزایش داده و باعث بهبود روند یادگیری فراگیران و سهولت و اثربخشی تدریس مدرسان شود (جمالیان و همکاران، ۱۴۰۰).

جدول ۱- مرورمطالعات انجام شده

نویسندگان	سال	راهکارهای پیشنهادی	مزایا و معایب
حامد و همکاران	۱۳۹۵	معرفی روش جدیدی از پروتکل مسیریابی می‌پردازد که بر مبنای سطح امنیت گره‌ها و با استفاده از قانون منطق فازی طراحی شده است. در این پروتکل مسیریابی که با عنوان مسیریابی سطح امنیتی بر اساس منطق فازی شناخته می‌شود، با بهره‌گیری از منطق فازی سعی بر آن است ت اروند مسیریابی از طریق مسیرهایی که بیشترین امنیت را دارند انجام شود.	بالابردن سطح امنیت شبکه به کمک منطق فازی مقایسه‌ی این پروتکل با پروتکل مسیریابی AODV در یک کار پژوهشی مجزا و عطف به پژوهش‌های گذشته و عدم انجام دو آلترناتیو و مقایسه آن‌ها با یکدیگر در همین پژوهش
حسنی و همکاران	۱۳۹۷	با ارایه یک شبکه عصبی فازی و تعیین قوانین پایگاه دانش، اقدام به تخمین امنیت شبکه بی‌سیم نموده و از طریق مانع دسترسی غیرمجاز به این شبکه می‌شود.	از منطق فازی در راستای پوشش دادن به پارامترهایی که جنبه غیرقطعی دارند استفاده می‌شود. همچنین در راستای افزایش دقت و تسریع در جواب خروجی نیز از شبکه عصبی استفاده می‌شود
جمالیان و همکاران	۱۴۰۰	در این مقاله تکنیک‌های فازی که در زمینه آموزش بسیار مورد توجه بوده مورد بررسی قرار گرفته است. در سیستم‌های آموزش الکترونیکی، نقش آفرینان اصلی دانش‌آموزان و معلمان هستند و داده مورد پردازش مرتبط با مدلسازی و نتایج فعالیت‌های آن هاست. نتایج به دست آمده در مقالات، نشان می‌دهد تکنیک فازی می‌تواند کارایی سیستم‌های تدریس را افزایش داده و باعث بهبود روند یادگیری فراگیران و سهولت و اثربخشی تدریس مدرسان شود	فقط فعالیت معلمان و دانش‌آموزان مدلسازی شده است و عوامل مؤثر دیگر مانند کارکنان مدرسه و رفتار آن‌ها در نظر گرفته نشده است.
دشتی و همکاران	۱۳۹۷	افزایش امنیت شبکه‌های حسگر بی‌سیم با بهره‌گیری از روش جداول عددهای ترکیبی توزیع شده و منطق فازی	خودکارآمد بودن گره‌های شبکه‌های حسگر بی‌سیم به کمک منطق فازی
قاضی‌زاده و همکاران	۱۳۹۲	ترکیب جداول توزیع شده (DHT) با شبکه‌های حسگر بی‌سیم	فایده اصلی جدول هش توزیع شده سرویس جستجوی کارآمدش می‌باشد. با استفاده از منطق فازی می‌توانیم ارتباط

نویسندگان	سال	راهکارهای پیشنهادی	مزایا و معایب
			گزاره‌های واقعی را با گزاره‌های ماشینی برقرار کنیم
نایینی و همکاران	۱۳۹۶	به کارگیری منطق فازی در انتخاب مناسب گره بعدی برای پیکربندی مسیر با پروتکل LEAP در شبکه‌های حسگر بی‌سیم	در این روش به صورتی مؤثر گره گام بعدی با چهار عامل بر مبنای سیستم منطق فازی انتخاب گردید. این ۴ عامل، بیان‌کننده ۴ پارامتر بهینه شده از نظر انرژی، یعنی درجه نزدیکی گره به کوتاه‌ترین مسیر، درجه نزدیکی گره به سرخوشه، نسبت انرژی باقیمانده هر گره و تعداد پیام‌های غلط فیلترشده است
قره جانلو و همکاران	۱۳۹۰	یک روش بر پایه قواعد منطق فازی با هدف افزایش ذخیره‌سازی توان در شبکه‌های حسگر بی‌سیم ارائه نمودند. در شیوه پیشنهادی آنان هر گره برای مصرف توان، از یک پردازنده فازی بهره می‌برد که فاصله خود تا هدف را به عنوان ورودی به پردازنده فازی داده و مقدار انرژی مصرفی خود و تقویت‌کننده را به عنوان خروجی از پردازنده فازی می‌گیرد	در طراحی روش مورد نظر فقط ذخیره‌سازی توان در نظر گرفته شده است و به امنیت شبکه توجه نشده است.
سروش نیا	۱۳۹۰	مروری بر مطالعات شبکه بی‌سیم	مطالعه مروری بوده و روش جدیدی ارائه نداده است.
مرادی و همکاران	۱۳۹۰	مروری بر مطالعات سیستم منطق فازی	به بیان کاربردهای منطق فازی پرداخته اما مطالعه مروری بوده و روش جدیدی ارائه نداده است.
حسین نژاد و همکاران	۱۳۹۳	پیشرفت‌های اخیر حاکی از آنست که توجه و علاقه به کاربرد شبکه‌های حسگر بی‌سیم بیشتر شده است از قبیل مدیریت مشکلات، شناسایی میدان رزم، محافظت حاشی‌های و نظارت-امنیتی. حسگرها در این کاربردها در مقیاس زیاد گسترش یافته باشند و در محیط‌های نا امن به کار گرفته شدند.	مطالعه مروری بوده و به مطالعات انجام شده در زمینه شبکه‌های حسگر بی‌سیم پرداخته و روش جدیدی ارائه نداده است.

نویسندگان	سال	راهکارهای پیشنهادی	مزایا و معایب
مؤمن‌زاده و همکاران	۱۳۹۹	درصد خطای پایین روش پیشنهادی در تعیین میزان اعتماد یک گره در شبکه نکته بارز این مقاله است که توانسته است پس از بروز حمله گره‌های مخرب را تشخیص داده و با قرنطینه‌سازی آن‌ها از ادامه فعالیت آن‌ها جلوگیری کند.	راهکار و مکانیسم پیشنهادی با استفاده از نرم‌افزار شبیه ساز ۲NS مورد ارزیابی قرارگرفته است.
موسوی	۱۳۹۹	در این مقاله، روش‌های خوشه بندی مبتنی بر منطق فازی در شبکه حسگر بی‌سیم مرور می‌شوند	به بیان کاربردهای منطق فازی پرداخته اما مطالعه مروری بوده و روش جدیدی ارائه نداده است.

مبانی نظری

شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم از موضوعات بدیع و بسیاربا اهمیت در دانش روز پردازش و فناوری اطلاعات محسوب می‌گردد که این شبکه‌ها گزینه مناسبی برای حالتی است که ما به محیط هدایت شده دسترسی نداشته باشیم. این شبکه‌ها مستقل و خود گردان بوده و بدون دخالت انسان کار می‌کنند (Islam and Wada,2013). شبکه‌های حسگر بی‌سیم، شبکه‌هایی هستند که معمولاً برای نظارت و کنترل محیط‌های اطراف مورد استفاده قرار می‌گیرند. این شبکه‌ها، یک سیستم توزیع شده، خود مختار و خود سازمانده هستند که از تعداد زیادی گره‌های حسگر کوچک با عملیاتی که به انرژی کمی نیاز دارند تشکیل شده است (Islam and Wada,2013) گره‌های حسگر دارای محدودیت در منابع انرژی، پردازش و محاسباتی هستند. این شبکه‌ها در مواردی مانند نظارت بر شرایط محیطی، جمع‌آوری داده‌هایی نظیر دما و فشار، کاربردهای نظامی کاربرد دارند (Felemban,2013). سپس داده‌های جمع‌آوری شده توسط این حسگرها به ایستگاه پایه یا سینک ارسال می‌شوند. برای اداره کردن این شبکه‌های متراکم و توزیع شده باید چالش‌هایی نظیر مقیاس‌پذیری، تحمل خرابی، استحکام و ارایه راه حل‌های کارآمد از نظر انرژی مورد توجه قرار گیرد (Karenos et all,2007). شبکه‌های حسگر بی‌سیم نیز از نظر تهدیدات و حملات مخرب بسیار آسیب‌پذیر هستند و طراحی ساده سخت‌افزار از این ابزارهای الکترونیکی، مانع از بکارگیری مکانیسم‌های دفاعی مرسوم شبکه‌ها می‌شود. شبکه‌های حسگر بی‌سیم در بسیاری از حوزه‌ها شامل ماشینی‌سازی یا اتوماسیون صنعتی، امنیت، تحلیل شرایط آب و هوا، دامنه وسیعی از سناریوهای نظامی کاربرد دارند.

منطق فازی

منطق فازی شـکلی از منطق چند ارزشـی بوده که در آن ارزش منطقی متغیرها می‌تواند هر عدد حقیقی بین ۰ و ۱ و خود آن‌ها با شد. ساختار سیستم‌های منطق فازی، ساده و قابل درک ا ست. همچنین منطق فازی امروزه در مقیاس تجاری و آزمایشگاهی، امنیتی و... بسیار به کار گرفته می‌شود. از طرفی کنترل بهتر و مؤثرتر ماشین‌ها و صرفه‌جویی در هزینه‌ها را

با استفاده از منطق فازی می‌توان امکان‌پذیر می‌باشد. همچنین در زمینه امنیت می‌توان براساس منطق فازی، برنامه‌ریزی را به شکل انجام داد که با از تداخل و نفوذ در شبکه فرآیند سیستم متوقف نشود. به این ترتیب در همین زمینه، بالا بردن کارایی سیستم‌ها با منطق فازی امکان‌پذیر است، بطوری که با استفاده از حسگرهای ارزان قیمت فرآیند کنترل امنیت سیستم به خوبی و با هزینه کم صورت می‌پذیرد. در انتها، شاید بتوان بهترین دلیل استفاده از منطق فازی را حل مسائل پیچیده با راه حل‌های مؤثر بیان کرد.

روش تحقیق

منطق فازی و سیستم فازی

منطق فازی شکلی از منطق‌های چند ارزشی بوده که در آن ارزش منطقی متغیرها می‌تواند هر عدد حقیقی بین ۰ و ۱ باشد. این منطق به منظور به‌کارگیری مفهوم درستی جزئی به‌کارگیری می‌شود، به طوری که میزان درستی می‌تواند هر مقداری بین کاملاً درست و کاملاً غلط باشد. اصطلاح منطق فازی اولین بار در پی تنظیم نظریه‌ی مجموعه‌های فازی توسط پرفسور لطفی‌زاده ارائه شد. واژه فازی به معنای غیردقیق، ناواضح و مبهم (شناور) است. منطق فازی براساس این مشاهدات استوار است که اکثر مواقع، افراد بر اساس اطلاعات غیر دقیق و غیر عددی تصمیم‌گیری می‌کنند. مدل‌ها یا مجموعه‌های فازی، روشی ریاضی برای نشان دادن و بیان اطلاعات مبهم و غیر دقیق هستند.

اجزای یک سیستم فازی را می‌توان به صورت زیر خلاصه کرد

فازی ساز: مقدار عددی متغیرها را به یک مجموعه فازی تبدیل می‌کند.

- پایگاه قواعد فازی: که مجموعه‌ای از قواعد (اگر-آنگاه) است.
- موتور استنتاج فازی: که ورودی‌ها را با یک سری اعمال به خروجی تبدیل می‌کند.
- دیفازی ساز: خروجی فازی را به یک عدد قطعی تبدیل می‌کند.

نمودار ۱- روند سیستم فازی

تبدیل ورودی‌های قطعی[۳] به یک متغیر زبانی[۴] با استفاده از توابع عضویت[۵] ذخیره شده در پایگاه دانش فازی می‌باشد. در این مرحله برای هر متغیر ورودی، توابع عضویت در نظر می‌گیریم تا ورودی‌های قطعی تبدیل به فازی شوند و در سیستم استنتاج فازی قرار بگیرند. اعداد فازی انواع مختلفی دارند، مانند مثلثی، ذوزنقه‌ای، گوسین و غیره؛ که در این کار از تابع عضویت مثلثی استفاده می‌شود که در ادامه با توضیح نشان داده می‌شوند.

پایگاه قواعد به مجموعه اگر -آنگاه‌های فازی گفته می‌شود که قلب سیستم استنتاج فازی را تشکیل می‌دهد. یک قانون اگر-آنگاه به صورت اگر X برابر A باشد، آنگاه Y برابر B است تعریف می‌شود که X و Y متغیرهای ورودی و خروجی و A و B مقادیر زبانی (توابع عضویت) نوشته شده برای این متغیرهاست.

طراحی یک سیستم کارشناس امنیت سایبری مبتنی بر قاعده فازی امنیت سایبری

مراحل طراحی شامل تعریف متغیرهای سیستم کارشناس امنیت سایبری، جمع‌آوری داده‌ها برای تهدیدهای سایبری، طراحی و اجرای سیستم می‌باشد. این مراحل در بخش‌های زیر توضیح داده می‌شوند (Goztepe,2012). داده‌های استفاده شده برای به‌دست آوردن متغیرها و قواعد از داده‌های آورده شده در (Goztepe,2012) استفاده شده که در ادامه خود داده‌ها به همراه روش به‌دست آوردن آن‌ها توسط Goztepe درکار ارائه شده است و در این پژوهش از همین داده‌های به‌دست آمده برای طراحی سیستم ممدانی استفاده می‌کنیم.

تعریف متغیرهای سیستم کارشناس امنیتی سایبری

اولین گام در مدل پیشنهادی ایجاد متغیرهای ورودی و خروجی فازی است. برای به‌دست آوردن متغیرهای فازی ابتدا باید در مورد انواع حمله، انواع گروه‌های مهاجم سایبری و نمودها و مکان‌های حمله اطلاعات کسب کرد و این با مطالعه حوزه مشکلات سایبری و همچنین با مشورت با متخصصان سایبری انجام می‌شود. (Goztepe,2012) تعداد نامحدودی از داوطلبان بالقوه وجود دارند که برای به‌دست آوردن اطلاعات می‌توان با آن‌ها مصاحبه کرد. در این کار متغیرهای کلیدی ورودی و خروجی با استناد به مصاحبه با کارشناسان امنیت سایبری تعریف شده است. نام ورودی و خروجی‌های مدل پیشنهادی در شکل زیر داده شده است؛ که ورودی‌ها تکنیک حمله[۶]، هدف حمله[۷]، نوع گروه مهاجم[۸] و هدف از حمله[۹] می‌باشد و خروجی‌ها اقدامات بر روی سخت‌افزارهای[۱۰] خاص، برنامه‌های[۱۱] و افراد اپراتور سیستم[۱۲] می‌باشند؛ که نام توابع عضویت هر کدام از ورودی و خروجی‌ها در جداول ۱ تا ۳ زیر آمده است.

---

[3] Crisp
[4] Linguist Variables
[5] Mebership fcn
[6] Cyber techniques
[7] Cyber intrudes target
[8] Cyber intrudrs
[9] Aim of cyber intruders
[10] Sophisticated hardware
[11] Software
[12] Users

جدول ۲- ورودی‌های اول و دوم به همراه تابع عضویت‌های آن

تکنیک‌های سایبری (T)	هدف گروه از آسیب رساندن (A)
حمله به شبکه A_N	خارج از سرویس OoS
انکار سرویس DoS	گرفتن صفحه‌ی وب S_W_P
ویروس V	کنترل سیستم‌های مهم CoCS
ویروس پست الکترونیکی E - V	به‌دست آوردن اطلاعات مهم CCI
بمب منطقی b – l	کنترل سیستم CS
اسب تروجان T_H	
مهندسی اجتماعی s	
بدافزار m	

جدول ۳-ورودی سوم و چهارم

انوع گروه مهاجمان (CI)	هدف مهاجم (CIT)
گروه حرفه‌ای SS	سیستم مخابراتی CC
هکر H	سیستم اقتصادی FC
دشمن سیستم ES	سیستم برق PP
فعال سابری CA	سیستم ضروری ES
	سیستم حمل و نقل PT
	مجموعه‌ی عمومی PI
	سیستم‌های آب WW
	سیستم نفت و گاز OND

جدول ٤- خروجی‌ها

سخت‌افزارهای (H)	برنامه‌ها (S)	افراد (U)
کنترل فیزیکی PC	برنامه‌های خاص SS	آموزش افراد UT
کنترل خاص SpC	آپدیت سیستم SU	اطلاع دادن AW
ساپورت تکنیکی TS	بانک اطلاعات کلی NDB	کنترل افراد UC

جمع‌آوری داده‌ها

سیستم استنتاج دانش متخصص انسانی را مدل می‌کند. همچنین توضیحات مشابه با کارشناس انسانی ارائه می‌دهد. این سیستم می‌تواند سؤالات مختلفی را که توسط کاربر پرسیده می‌شود را توصیف کند. داده‌های مورد استفاده برای این کار از مجموع‌های اطلاعات جمع‌آوری شده از کارشناسان اینترنتی و مدیران سیستم استخراج شده‌است. این داده‌ها توسط ابزارهایی چون مصاحبه و سؤال و جواب از کارشناسان و افراد متخصص به‌دست آمده است (Goztepe,2012) که این اطلاعات را به صورت قواعد بین ورودی و خروجی‌ها می‌نویسیم. این قواعد در واقع رابطه‌ی بین ورودی‌ها و خروجی‌ها را نشان می‌دهد.

داده‌های به‌دست آمده به خصوص با موضوعات زیر مرتبط هستند:

انواع حملات: ویروس، بدافزار، بمب منطق، مهندسی‌اجتماعی، اسب تروجان، خارج کردن سیستم از سرویس، گرفتن صفحه وب، حمله به شرکت‌ها، توقیف سیستم‌های حیاتی، ثبت اطلاعات محرمانه، کنترل سیستم‌ها.

طراحی سیستم با استفاده از داده‌ها و متغیرهای به‌دست آمده

در این جا دو حالت برای طراحی سیستم استفاده می‌شود روش حرکت به جلو که برای طراحی آن با استفاده از ورودی می‌خواهیم به خروجی دلخواهمان برسیم. در روش حرکت به عقب خروجی دلخواه را داریم و نسبت به آن ورودی را انتخاب می‌کنیم؛ یعنی در واقع در این مرحله دو قسمت قبل را به هم ربط می‌دهیم.

مدل مبتنی بر قانون فازی

معماری کلی سیستم خبره بر قاعده و اجزای یک سیستم استنباط فازی مبتنی بر قواعد می‌باشد؛ که آین قواعد بر اساس اطلاعات به‌دست آمده از تجربه‌ی شخصی افراد متخصص بنا می‌شود. قواعد بین ورودی‌ها و خروجی‌ها با الگوی حرکت رو به جلو تنظیم می‌کنیم این قواعد به صورت اما و اگر می‌آیند که این قواعد براساس مصاحبه با افراد کارشناس سیستم طراحی شده‌اند و با استفاده از این قوانین می‌توان ارتباط بین توابع عضویت ورودی و خروجی را نشان داد. قواعد با استفاده از تجربه‌ی شخصی افراد متخصص بوجود آمده‌اند و بر پایه‌ی دانش انسانی می‌باشند. در ادامه مصاحبه از مقاله استخراج شده است

این مصاحبه با توجه به اطلاعات آورده شده در (Goztepe,2012) طراحی شده است با توجه به پژوهش Goztepe مصاحبه حول سؤالات به موضوعات زیر مربوط می‌باشد، سؤالات به صورت باز طراحی شده است.

انواع حملات: ویروس، بدافزار، بمب منطق، مهندسی‌اجتماعی، اسب تروجان، خارج کردن سیستم از سرویس، گرفتن صفحه وب، حمله به شرکت‌ها، توقیف سیستم‌های حیاتی، ثبت اطلاعات محرمانه، کنترل سیستم‌ها.

سؤالات باتوجه به متغیرهای ورودی و خروجی سیستم طراحی شده است.

جدول ۵- مصاحبه جمع‌آوری شده از مقاله

سؤالات زیر را باتوجه به دانش و تجربه‌ی خود در رابطه به انواع گروه‌های مهاجم جواب دهید
۱ –باتوجه به تجربه‌ی شما هر کدام از گروه‌های مهاجم سایبری (گروه حرفه‌ای، هکر، دشمن سیستم و فعال سایبری) به چه صورت به یک سیستم حمله می‌کند؟
۲- باتوجه به تجربه‌ی شما هر کدام از گروه‌های مهاجم سایبری (گروه حرفه‌ای، هکر، دشمن سیستم و فعال سایبری) چه هدف‌هایی را به صورت معمول برای حمله انتخاب می‌کند؟(مکان)
۳- باتوجه به تجربه‌ی شما هر کدام از گروه‌های مهاجم سایبری (گروه حرفه‌ای، هکر، دشمن سیستم و فعال سایبری) به چه دلیل به یک سیستم حمله خواهد کرد؟
۴- باتوجه به تجربه‌ی شما در مقابل گروه‌های مهاجم سایبری (گروه حرفه‌ای، هکر، دشمن سیستم و فعال سایبری) بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم چیست؟
سؤالات زیر را باتوجه به دانش و تجربه‌ی خود در رابطه با انواع تکنیک‌های استفاده شده توسط گروه‌های مهاجم جواب دهید
۵- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام منع دسترسی به سیستم چیست؟
۶- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام بروز ویروس در سیستم چیست؟
۷- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام بروز بمب منطقی در به سیستم چیست؟
۸- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام بروز تروجان در به سیستم چیست؟
۹-باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام بروز مهندسی جمعی در به سیستم چیست؟
۱۰- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام بروز بدافزار در به سیستم چیست؟
سؤالات زیر را با توجه به دانش خود در رابطه با اهداف گروه‌های مهاجم به سیستم جواب دهید
۱۱ - باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام خارج سیستم از کار کرد چیست؟

۱۲-گروه‌های مهاجم معمولاً کدام مکان‌ها و تأسیسات را به منظور خارج کردن از سیستم مورد هدف قرار می‌دهند؟
۱۳- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام کنترل سیستم توسط گروه مهاجم چیست؟
۱۴- گروه‌های مهاجم معمولاً کدام مکان‌ها و تأسیسات را به منظور کنترل سیستم مورد هدف قرار می‌دهند؟
۱۵- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام کنترل سیستم‌های حیاطی توسط گروه مهاجم چیست؟
۱۶-گروه‌های مهاجم معمولاً کدام مکان‌ها و تأسیسات را به منظور کنترل سیستم‌های حیاطی مورد هدف قرار می‌دهند؟
۱۷- باتوجه به تجربه‌ی شما بهترین عمل کرد دفاعی در رابطه با افراد، نرم‌افزارهای استفاده شده در سیستم و سخت‌افزارهای سیستم در هنگام به‌دست آوردن اطلاعات مهم توسط گروه مهاجم چیست؟
۱۸-گروه‌های مهاجم معمولاً کدام مکان‌ها و تأسیسات را به منظور به‌دست آوردن اطلاعات مهم مورد هدف قرار می‌دهند؟
با توجه به تجربه‌ی خود و مکان‌های هدف به سؤالات زیر جواب دهید
۱۹- بهترین استراتژی دفاعی در رابطه باحمله به سیستم مخابراتی چیست؟
۲۰-بهترین استراتژی دفاعی در رابطه باحمله به سیستم اقتصادی چیست؟
۲۱-بهترین استراتژی دفاعی در رابطه باحمله به سیستم برق چیست؟
۲۲-بهترین استراتژی دفاعی در رابطه باحمله به سیستم اضطراری چیست؟
۲۳-بهترین استراتژی دفاعی در رابطه باحمله به سیستم‌های عمومی چیست؟
۲۴-بهترین استراتژی دفاعی در رابطه باحمله به سیستم حمل و نقل عمومی چیست؟
۲۵- بهترین استراتژی دفاعی در رابطه باحمله به سیستم نفت و گاز چیست چیست؟

لازم به توجه می‌باشد که سیستم طراحی شده در بخش ۳ با توجه به دیتای جمع‌آوری شده در (Goztepe,2012) می‌باشد و قواعد فازی آورده شده متناسب با همین دیتا است

که دراینجا قواعد بر اساس داده‌های آورده شده در (Goztepe,2012) آورده شده‌اند

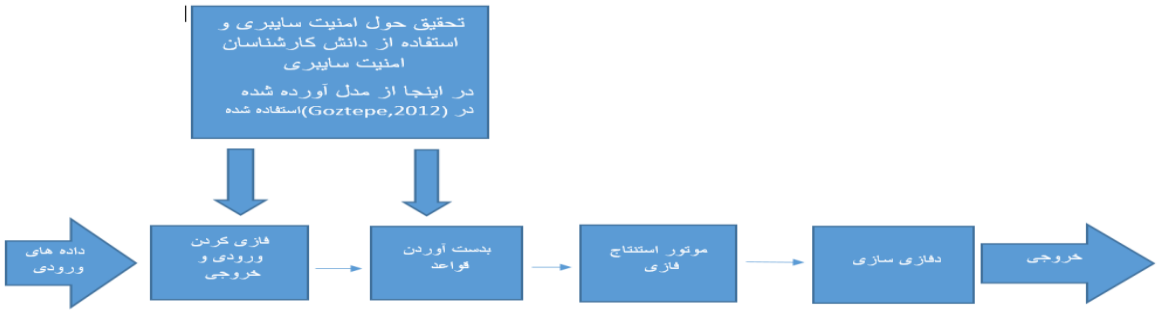
- If(T is N-A) and(A is OoS) and(CIT is CC) then(H is TC)(1)
- If(T is E-V) then(S is SpS)(H is SpC)(U is UT)(1)
- If(T is N-A) and(A is S-W-P) and(CIT is Kl) and(CI is CI) then(S is SpS)(H is TC)(1)
- If(T is M) and(A is CS) and(CIT is Kl) and(CI is SS) then(S is SpS)(H is SpC)(U is UT)(1)

- If(T is S-E) and(A is CS) and(CIT is CC) and(CI is CH) then(S is SU)(1)
- If(T is DoS) and(A is OoS) and(CIT is WW) and(CI is CH) then(S is NDB)(H is TC)(1)
- If(T is S-E) and(A is CCI) and(CIT is FC) and(CI is CH) then(U is UT)(1)
- If(T is S-E) and(A is CCI) and(CIT is Kl) and(CI is CI) then(U is UT)(1)
- If(A is S-W-P) and(CIT is CC) and(CI is CI) then(S is SU)(1)
- If(A is P) and(CIT is Kl) and(CI is SS) then(S is SpS)(H is TC)(0.8)
- If(A is P) and(CIT is TR) and(CI is SS) then(S is SpS)(H is TC)(1)
- If(A is P) and(CIT is CC) and(CI is ES) then(S is SU)(U is AW)(1)
- If(A is CS) and(CIT is Kl) and(CI is SS) then(H is PC)(1)
- If(A is CS) and(CIT is Kl) and(CI is CI) then(S is SpS)(H is SpC)(U is UT)(1)
- If(A is CCI) and(CIT is FC) and(CI is CH) then(S is SU)(H is TC)(U is UsC)(1)
- If(CI is Kl) and(CI is SS) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CI is Kl) and(CI is ES) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CI is Kl) and(CI is CI) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CI is Kl) and(CI is CH) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CI is FC) and(CI is SS) then(S is SU)(H is TC)(U is UsC)(1)
- If(CI is FO and(CI is CHI then(S is SU)(H is TC)(U is UsO(1)
- If(CI is TR) and(CI is SS) then(S is SpS)(H is SpC)(U is AW)(1)
- If(CI is ES) and(CI is SS) then(S is SpS)(H is SpC)(U is AW)(1)
- If(CIT is Kl) and(T is L-B) and(CI is CH) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CIT is CC) and(T is L-B) and(CI is ES) then(S is SU)(H is TC)(U is AW)(1)
- If(CIT is Kl) and(CI is SS) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CIT is Kl) and(CI is ES) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CIT is Kl) and(CI is CI) then(S is SpS)(H is SpC)(U is UT)(1)
- If(CIT is Kl) and(CI is CH) then(S is SpS)(H is SpC)(U is UT)(1)

پس از به‌دست آوردن قواعد استنتاج فازی فعال می‌شود و داده‌های ورودی را با استفاده از منطق فازی بررسی می‌کند و نسبت به قواعد خروجی مورد نظر را به‌دست می‌آورد

دفازی‌سازی

مرحله دفازی‌سازی که در آن داده‌های فازی خروجی به ریاضیات قطعی تبدیل می‌شود؛ و در واقع عکس مرحله‌ی فازی‌سازی می‌باشد و پس از آن فرایند فازی خاتمه یافته است.



نمودار ۲- فرایند کلی کار کرد مدل ارائه شده

با توجه به نمودار ۲ برای به‌دست آوردن متغیرها و قوانین سیستم فازی طبق (Goztepe,2012) ابتدا نیاز به تحقیق حول تهاجمات انجام شده می‌باشد و که این امر توسط استفاده از دانش کارشناسان فازی می‌باشد و خبرگان این امر می‌باشد و پس از آن سیستم استنتاج فازی طبق قسمت‌های گفته شده در قبل طراحی می‌شود. در این پژوهش برای طراحی مدل فازی ممدانی از اطلاعات آورده شده در رابطه با امنیت سیستم در (Goztepe,2012) استفاده شده است.

یافته ها و نتایج

در این بخش ابتدا به طراحی سیستم کارشناس امنیت شبکه‌ی فازی ارائه شده در فصل قبل می‌پردازیم و سپس سیستم طراحی شده طی دو حالت از تهاجم بررسی می‌کنیم. شبیه‌سازی با نرم‌افزار matlab و توسط ابزار fuzzy logic designer انجام شده است که یک ابزار گرافیکی برای طراحی سیستم‌های فازی ممدانی[۱۳] و سوگینو[۱۴] می‌باشد.

جعبه ابزار فازی متلب[۱۵]

جعبه ابزار فازی مجموعه‌ای از توابع است که بر روی متلب ساخته شده است و محیط محاسبات عددی ابزارهایی برای ایجاد و ویرایش استنتاج فازی فراهم می‌کند. این جعبه ابزار به شدت به رابط کاربری گرافیکی متکی است ابزار گرافیکی سه دسته از ابزارها را ارائه می‌دهد: توابع خط فرمان، ابزارهای تعاملی گرافیکی، بلوک‌ها و مثال‌های سیمولینک[۱۶]. پنج هستند ابزارهای اولیه رابط کاربری گرافیکی برای ساخت، ویرایش و مشاهده سیستم‌های استنتاج فازی در جعبه ابزار منطق فازی شامل سیستم استنتاج فازی یا ویرایشگر فازی[۱۷]، ویرایشگر تابع عضویت، ویرایشگر قوانین، نمایشگر قوانین و سطح بیننده می‌باشد (Rachmat,Haris,2017).

[13] Mamdani
[14] Sugino
[15] Fuzzy Logic Toolbox
[16] SIMULINK
[17] FIS

مراحل شبیه‌سازی با fuzzy logic designer

مرحله‌ی اول

ورودی‌ها و خروجی‌های سیستم را مشخص می‌کنیم و برای هر کدام از آن‌ها توابع عضویت متناسب تعیین می‌کنیم. در جدول ۶ نام ورودی‌های، تعداد توابع عضویت آن‌ها، دامنه و نوع تابع عضویت مشخص شده است. همچنین در جدول ۷ اطلاعات مربوط به خروجی‌ها را آورده شده است.

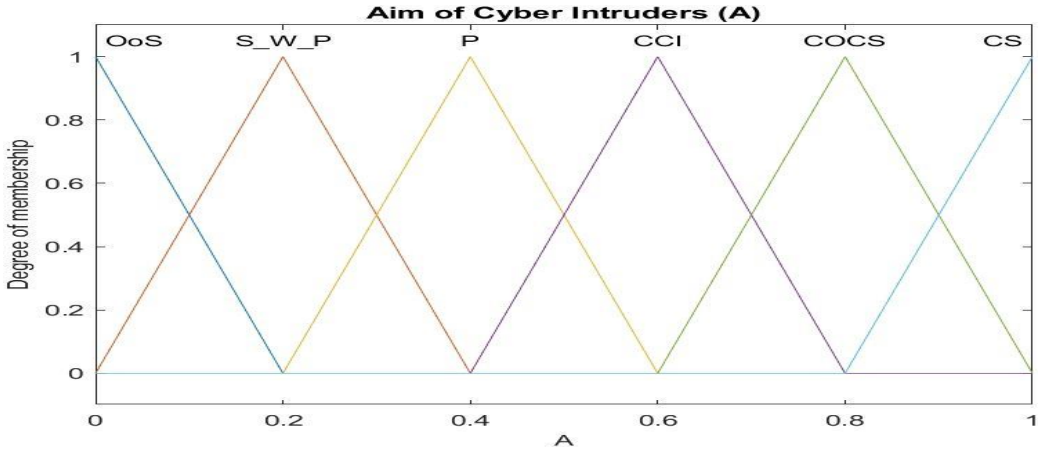
جدول ٦- ورودی‌ها به همراه اطلاعات

نام ورودی‌ها	تکنیک سایبری (T)	هدف از آسیب (A)	نوع گروه (CI)	هدف حمله (CIT)
تعداد تابع عضویت	۸	۶	۴	۸
نوع تابع عضویت	مثلثی	مثلثی	مثلثی	مثلثی
دامنه ورودی	[۰-۱]	[۰-۱]	[۰-۱]	[۰-۱]

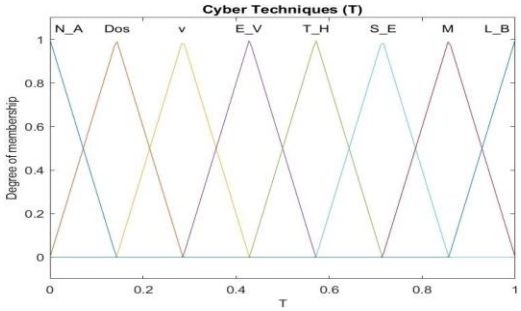
جدول ۷-خروجی‌ها به همراه اطلاعات

نام خروجی‌ها	سخت‌افزار (H)	نرم‌افزار (S)	افراد (U)
تعداد تابع عضویت	۳	۳	۳
نوع تابع عضویت	مثلثی	مثلثی	مثلثی
دامنه خروجی	[۰-۱]	[۰-۱]	[۰-۱]

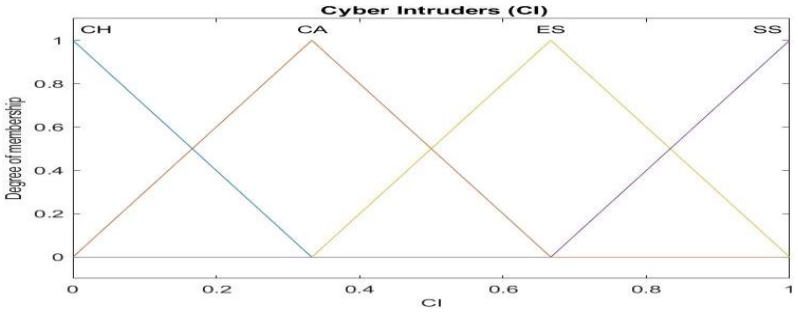
تصاویر ۱ تا ۴ ورودی‌های سیستم فازی را به همراه تابع عضویت آن‌ها نشان می‌دهند و همچنین تصاویر ۵ تا ۷ خروجی‌ها را به همراه تابع عضویت‌های آن‌ها نشان می‌دهند.



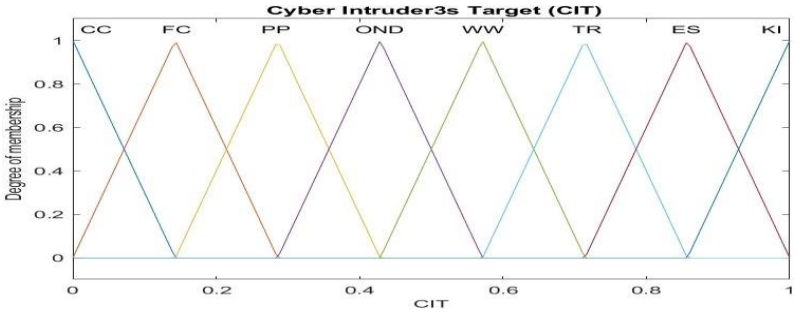
تصویر ۱- تکنیک های سایبری



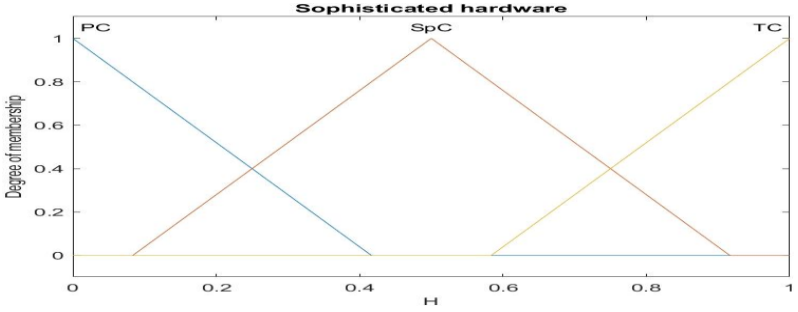
تصویر ۲- هدف از حمله



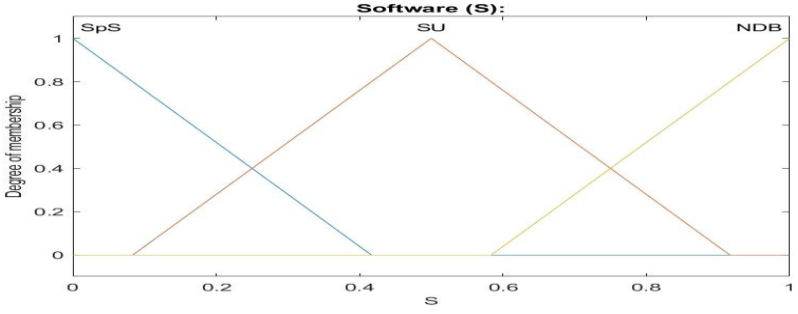
تصویر ۳- نوع گروه مهاجم



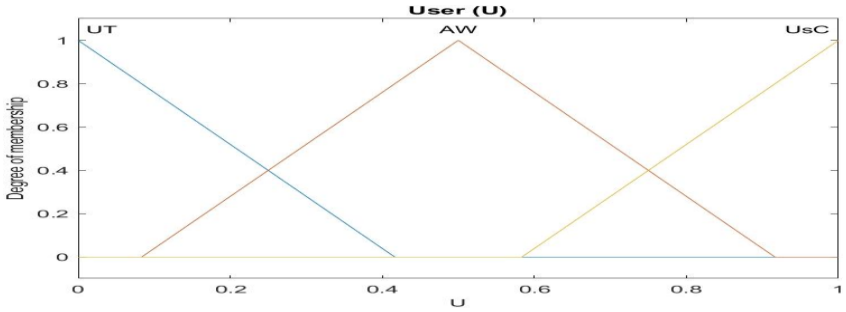
تصویر ٤- هدف حمله به



تصویر ٥- خروجی سخت‌افزار



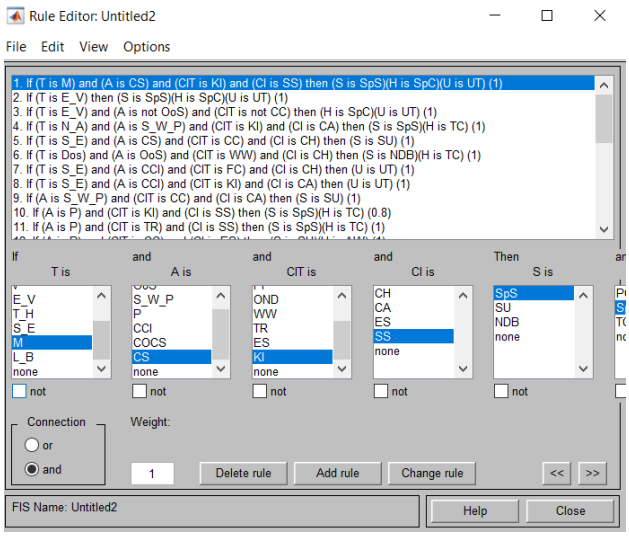
تصویر ٦- خروجی نرم‌افزار



تصویر ۷- خروجی افراد

مرحله‌ی دوم

قواعد بین ورودی‌ها و خروجی‌ها با الگوی یاد شده تنظیم می‌کنیم این قواعد به صورت اما و اگر می‌آیند که این قواعد براساس مصاحبه با افراد کارشناس سیستم طراحی شده‌اند و با استفاده از این قوانین می‌توان ارتباط بین توابع عضویت ورودی و خروجی را نشان داد. قواعد با استفاده از تجربه‌ی شخصی افراد متخصص بوجود آمده‌اند و بر پایه‌ی دانش انسانی می‌باشند که تصویر ۸ نمای قوانین در ابزار گرافیکی آورده شده است.

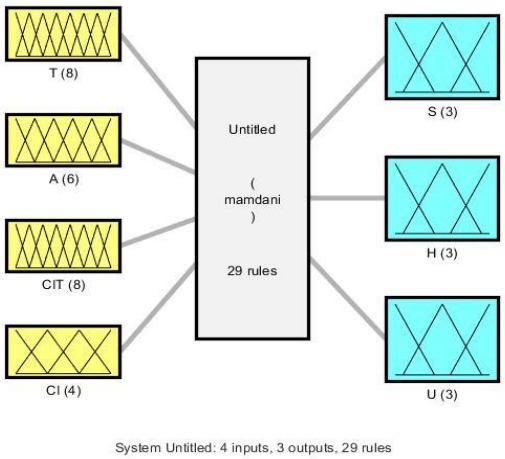


تصویر ۹- قوانین در ابزار گرافیکی

مرحله‌ی سوم

دراین مرحله دفازی‌سازی است که در آن عکس یک فراید فازی اتفاق خواهد افتاد و داده‌های فازی به ریاضیات قطعی تبدیل می‌شود و سیستم یک عدد به ما ارائه می‌دهد که در این سیستم از دفازی ساز[18] ممدانی استفاده شده است که به نام دفازی ساز سنتروید[19] نیز معروف است.

[18] Defuzzification
[19] Centroid

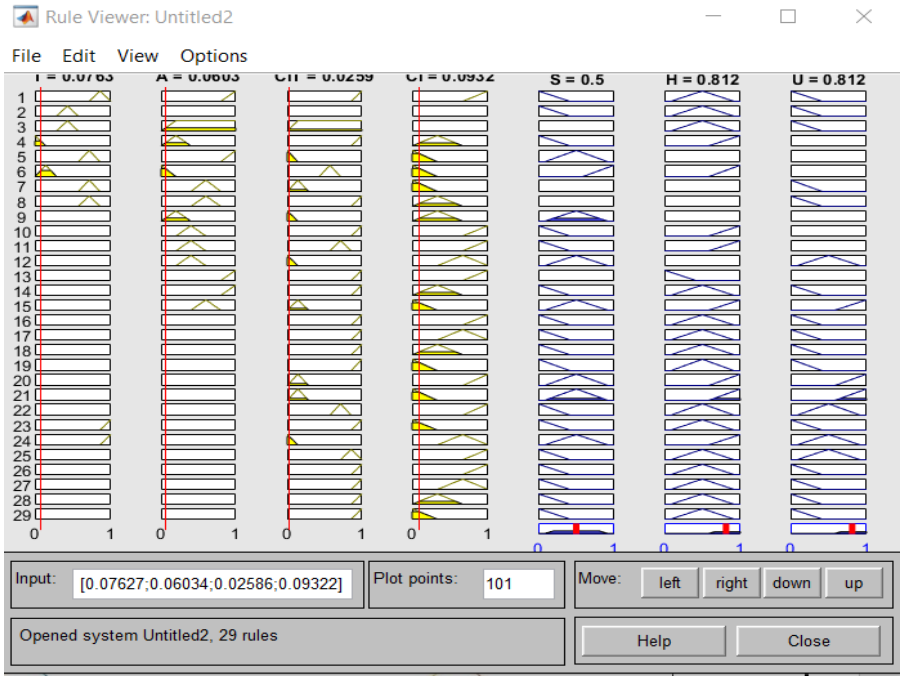


تصویر ۱۰- نمای کلی سیستم

تصویر ۱۰ فرایند کلی سیستم طراحی شده را نشان می‌دهد که به همراه ورودی خروجی‌ها، توابع عضویت آن‌ها و تعداد قواعد بنا شده آورده شده است.

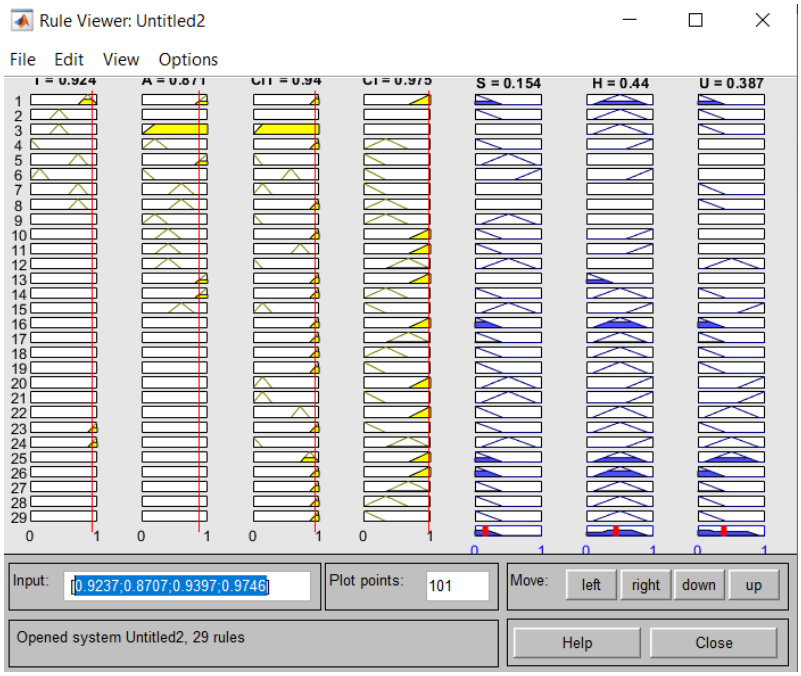
نتایج سیستم طراحی شده

حال سیستم طراحی‌سازی شده را برای دو حالت تهاجم شبیه‌سازی کرده و نتایج به همراه شکل تحلیل می‌کنیم. جدول ۸ ورودی‌ها خروجی‌ها را برای این دو حالت نسان می‌دهد. فرض کنید که داده‌ها نشان می‌دهند که یک گروه هکر کامپیوتری با تکنیک آسیب رساندن به سیستم قصد خارج کردن سیستم مخابراتی از سرویس را دارند. سیستم ارائه شده به سرعت نسبت به داده‌های جمع‌آوری شده درمیابد که بهترین عملکرد در مقابل چنین حمله‌ای کنترل خاص سخت‌افزارها، بوجود آوردن بانک ملی اطلاعات و کنترل افرادی که از شبکه استفاده می‌کنند می‌باشد.



تصویر ۱۱- خروجی نسبت به حالت اول

برای حالت دوم فرض کنید که یک گروه حرفه‌ای با تکنیک بوجود آوردن بمب منطقی قصد کنترل مجموعه‌های عمومی رادارند در این صورت خروجی سیستم نسبت به حمله کنترل فیزیکی سخت‌افزارها، آپدیت سیستم‌های نرم‌افزاری و اطلاع و آموزش به افراد می‌باشد.



تصویر ۱۲-خروجی نسبت به حالت دوم

T	A	CIT	CT	S	H	U
.۹۲۳۷	.۸۷۰۷	.۹۳۹۷	.۹۷۴۶	.۱۵۴	.۴۴	.۳۸۷
.۰۷۶۲۷	.۰۶۰۳۴	.۰۲۵۸۶	.۰۹۳۳۲۲	.۵	.۸۱۲	.۸۱۲

جدول ۸- خروجی سیستم فازی نسبت به دو حالت فرض شده

با توجه به تصاویر ۱۱ و ۱۲ برای مقدار دهی به سیستم طراحی شده از قسمت پایین منوی ابزار گرافیکی برای مقدار دهی به ۴ متغیر ورودی استفاده می‌کنیم همچنین می‌توان با استفاده از خود شکل مقدار دهی را انجام داد و مقادیر خروجی در بالای شکل نمایان خواهند شد و نمودار تصویری روی شکل نشان داده می‌شود

بحث و نتیجه گیری

در این بخش سیستم طراحی شده در فصل قبل را با روش‌های قدیمی‌تر مانند استفاده از شخص متخصص برای بررسی امنیت شبکه بررسی می‌کنیم و مشکلات سیستم رابیان خواهیم کرد همچنین برای حل مشکلات نام برده روش‌هایی برپایه هوش مصنوعی ارائه داده می‌شود. همچنین در بخش انتهایی کار نتیجه‌گیری برای کل کار انجام می‌گیرد.

مقایسه‌ی سیستم فازی با سیستم‌های امنیت شبکه‌ی قدیمی‌تر

استفاده از منطق فازی برای تشخیص و تأمین امنیت شبکه می‌تواند بازده فرایند را بالاتر ببرد و همچنین سرعت تشخیص و عکس العمل را بسیار بهبود می‌بخشد. لازم به ذکر است که استفاده از سیستم فازی برای شناسایی و عملکرد در حوضه‌ی امنیت سایبری می‌تواند فرایند شناسایی و عملکرد را برای مدیران شبکه سریع‌تر کرده و هم چنین با وجودی که برپایه‌ی قواعد تهیه شده توسط دانش انسانی می‌باشد می‌تواند خطاهای انسانی را شامل مشکلات ناشی از عدم تجربه و عدم آگاهی، مشکلات شامل کم بود نیروی تحلیل و تفسیر اطلاعات و غیره را کاهش می‌دهد و راندمان عملکردی بهتری نسبت به استفاده از خود کارشناسان به صورت روش قدیمی را دارا می‌باشد. جدول ۹ به بررسی مزایا و معایب این سیستم می‌پردازد.

جدول ۹- معایب و مزایا

مزایا	معایب
سیستم فازی دقت بهتری نسبت به انسان دارد	قابلیت پیش‌بینی حالات جدیدی از تهدید را ندارد
سیستم فازی سرعت عمکرد بهتری نسبت به انسان دارد	ممکن است به راحتی توسط مهاجمان شناسایی شود
سیستم فازی راندمان بالاتری نسبت به انسان دارد	قابلیت عملکرد در محیط جدید را ندارد
این سیستم برپایه قواعد دانش انسانی است و از تجربه‌های افراد متخصص استفاده می کند (برای قواعد)	

همانطور که در جدول ۹ مشاهده می‌شود مهم‌ترین و بزرگ‌ترین مشکل سیستم ارائه شده نسبت به روش‌های قدیمی‌تر عدم وجود پویایی و توانایی شناخت خطرات جدید و روش‌های جدید برای شناسایی می‌باشد و برای حل کردن این مشکل در قسمت بعد راهکارهای با استفاده از هوش مصنوعی برای بهبود این سیستم ارائه شده است.

پیشنهادات برای بهبود مشکلات سیستم ارائه شده

پیشنهادات ارائه شده در این قسمت در دو تیپ هوش مصنوعی[۲۰] آورده می‌شوند که شامل آلگوریتم‌های فرا ابتکاری و سیستم‌های فازی بهبود یافته[۲۱] می‌باشند

پیشنهاد اول: استفاده از الگوریتم ژنتیک با منطق فازی

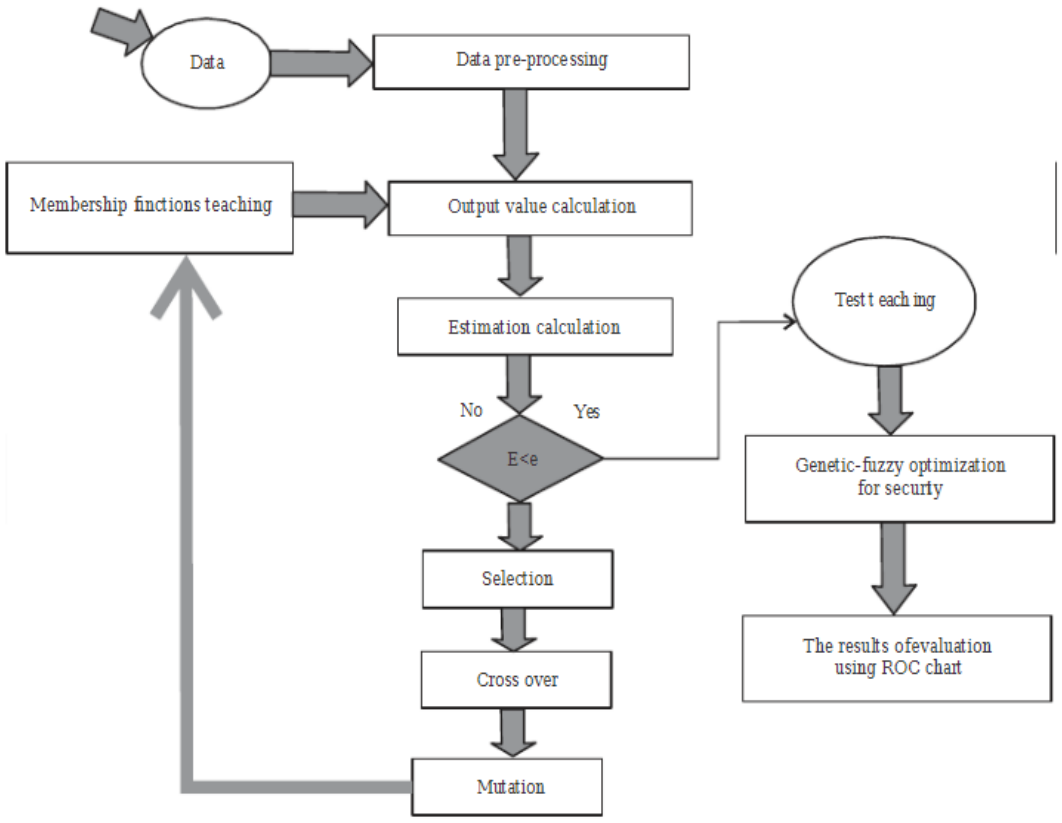
دسترسی به دانش متخصصانی که برنامه حمله را اجرا می‌کنند، به طوری که به محض ورود متجاوزان، می‌توان آن‌ها را شناسایی کرد و زنگ هشدار به پایگاه داده ارسال شد اما در کسب و کارهای سنتی اینگونه نبود زیرا امنیت به صورت فیزیکی تأمین می‌شد. تاکنون اقدامات پیشگیرانه زیادی برای بهبود عملکرد این کسب و کار و حفظ امنیت و اعتماد انجام شده است که از میان آن‌ها می‌توان به نصب نرم‌افزار، آنتی ویروس و رمزگذار به عنوان موارد تأثیرگذار اشاره کرد.

[20] Artificial intelligence
[21] Extended fuzzy systems

امروزه، تکنیک‌های بهینه‌سازی بهتری توسعه یافته‌اند که می‌توانند امنیت بیشتری را از طریق الگوریتم‌های ژنتیک فازی فراهم کنند، اگرچه این تکنیک‌ها به زیرساخت هوشمندتر نیاز دارند. الگوریتم‌های ژنتیک فازی یک راه قدرتمند برای توسعه امنیت تجارت الکترونیک ارائه کرده‌اند. در این قسمت سعی شده است در مورد تکنیک‌های ژنتیک فازی برای بهینه‌سازی امنیت و اعتماد در تجارت الکترونیک بیشتر بحث شود.

الگوریتم ژنتیک از علم ژنتیک و نظریه تکامل داروین الهام گرفته شده و بر اساس بقای بهترین‌ها توسط انتخاب طبیعی است. الگوریتم‌های ژنتیکی نوع خاصی از الگوریتم‌های تکاملی هستند که از تکنیک‌های بیولوژیکی مانند وراثت و جهش استفاده می کنند.

این الگوریتم اولین بار توسط جان هولاند[۲۲] معرفی شد. بعدها با تلاش گلدبرگ[۲۳] در سال ۱۹۸۹ این روش جایگاه خود را پیدا کرد و امروزه به دلیل ویژگی‌های منحصر به فرد خود در بین روش‌های دیگر جای گرفته است. در واقع، الگوریتم‌های ژنتیک از اصول انتخاب طبیعی داروین برای یافتن فرمول بهینه برای پیش‌بینی یا تطبیق الگو استفاده می کنند. تصویر ۱۳ روند استفاده از الگوریتم فازی ژنتیک می‌باشد (Najaafi. et al,2020).



تصویر ۱۳- الگوریتم فازی ژنتیک

[22] Jan holland
[23] Goldberg

پیشنهاد دوم: تشخیص بات‌نت در شبکه بر پایه ترکیب ویژگی‌های فازی‌سازی شده و شبکه عصبی[۲۴] چند لایه

در دو دهه اخیر با رشد تصاعدی استفاده از شبکه‌ها بی‌سیم مانند اینترنت، حملات سایبری به سرعت در حال افزایش است. این حجم از رشد در واقع از تولید و تکثیر داده‌ها نشات می‌گیرد. انواع جدیدی از داده‌ها هر روز از طریق رسانه‌های اجتماعی، کلاس‌های آنلاین، موتورهای جستجو و برنامه‌های موبایل و غیره، تولید می‌شوند. برای انجام این کار، مهاجمان انواع گوناگونی از حملات را گاهاً حتی به صورت ترکیبی، از طریق بدافزارها، ویروس‌ها، فیشینگ و غیره اجرا می‌کنند. همه این نوع حملات را می‌توان به راحتی با استفاده از بات‌نت[۲۵] انجام داد. بات‌نت شبکه‌ای از ربات‌ها است که بر اساس دستور بات مستر[۲۶] کار می‌کند. آن‌ها از بات‌نت برای تعبیه انواع مختلفی از حملات سایبری استفاده می‌کنند که به راحتی برای بات مستر می‌تواند در میان سایر کاربران واقعی پنهان شود. در دهه اخیر، بات‌نت به یکی از مخرب‌ترین انواع نفوذ و تخریب در شبکه‌های بی‌سیم تبدیل شده است. به دلیل نوع پنهان بودن بات‌ها و ظرفیت بالای قابل حمل آن‌ها، شناسایی بات‌نت‌ها به یک صورت مسأله بسیار مهم در امنیت شبکه تبدیل شده است. تاکنون روش‌های مختلفی برای شناسایی منبع بات‌نت ارائه شده است که از آن میان روش‌هایی مبتنی بر یادگیری ماشین و یادگیری نتایج بهتری ارائه داده‌اند محدودیت اصلی در این حوزه که بر دقت شناسایی هم تأثیر منفی می‌گذارد عدم وجود ویژگی‌های کافی در پایگاه داده‌های بات‌نت است. در این جا یک متد کلی بر مبنای ترکیب منطق فازی و شبکه‌های عصبی پیشنهاد داده می‌شود

در واقع پیشنهاد می‌شود که به دلیل محدودیت تعداد ویژگی‌های پایگاه‌های بات‌نت، از منطق فازی برای تولید ویژگی از درون همین مجموعه داده بات‌نت استفاده شود تا حجم و تنوع داده‌ها بیشتر شود و در ادامه هر تکنیکی یادگیری ماشینی هم که استفاده گردد، بتواند بهتر آموزش داده شود. در ادامه ویژگی‌های ایجاد شده، می‌تواند برای آموزش یک شبکه عصبی مصنوعی استفاده می‌شود. برای تولید ویژگی‌ها، ابتدا برخی از ویژگی‌های واضح شناسایی می‌شوند و سپس قوانین فازی را به کار ببریم تا آن ویژگی‌های واضح به تعداد بیشتری ویژگی‌های فازی تبدیل گردد. سپس، هر یک از ویژگی‌های فازی تبدیل شده برای مشارکت آن‌ها در مجموعه داده بررسی می‌شود. برای تولید ویژگی‌های فازی پیشنهاد می‌شود که از مجموعه داده‌های (CTU-13)، استفاده گردد.

مدل پیشنهادی در شکل زیر به صورت دیاگرام نشان داده شده است. مدل پیشنهادی شامل بخش‌های زیر می‌باشد:

۱. مهندسی ویژگی مبتنی بر منطق فازی برای تولید ویژگی‌های جدید.

۲. طبقه‌بندی مبتنی بر شبکه عصبی مصنوعی

---

[24] Neural network
[25] Botnet
[26] Botmaster

تصویر ١٤- مدل فازی عصبی

امنیت سیستم با ظهور موج‌های جدید از تهدیدات سایبری به یکی از مهم‌ترین مسائل تکنولوژی بدل شده است و همچنین در صورت عدم بررسی آن می‌تواند ضررهای مالی و جانی زیادی را برای افراد بوجود آورد. در این کار سعی شد با بررسی منطق فازی به ارائه سیستم جدیدتری برای فرایند شناخت و عمکرد متقابل در برابر خطرات شبکه حسگر بی‌سیم پرداخته شود و همچنین با شبیه‌سازی این سیستم توانستیم به صورت سریع و همزمان به تحلیل این شبکه‌ها بپردازیم. با مقایسه سیستم فازی نسبت به این شبکه‌های دانستیم که استفاده از سیستم فازی دارای مزایای بیشتری نسبت به حالات قدیمی‌تر می‌باشد و این امر توانسته سیستم فازی را که براساس دانش انسانی است را به یکی‌از بهترین ابزارها برای امنیت شبکه تبدیل کند. همچنین برای بهبود عملکرد این سیستم برای حالات جدید تهاجم دو پیشنهاد در سبک‌های متفاوت هوش مصنوعی ارائه گردید.

منابع

[۱]. تشتریان، فرزاد، شاکری، حسن، یغمایی مقدم، محمد حسین، قائمی بافقی، عباس، ارائه یک الگوریتم کارا در جهت کشف حمله wormhole در شبکه‌های حسگر بی‌سیم. اولین کنفرانس ملی دانش پژوهشان کامپیوتر و فناوری اطلاعات، دانشگاه تبریز، ۱۳۹۰

[۲]. سروش نیا محمد، شبکه‌های حسگر بی‌سیم، پروژه مقطع کارشناسی دانشگاه مهاباد، ۱۳۹۱

[۳]. مرادی، زهرا و تشنه لب، محمد، ۱۳۸۹، کاربرد منطق فازی در ارتقای امنیت مسیریابی درشبکه‌های موردی سیار، اولین کنفرانس دانشجویی فناوری اطلاعات ایران، سنندج، https://civilica.com/doc/88160

[۴]. قره جانلو، مسعود و نصرت آبادی، مسعود و یغمایی مقدم، محمدحسین، ۱۳۸۸، ارائه‌ی یک روش فازی جهت کاهش مصرف انرژی در پروتکل‌های مسیریابی شبکه‌های حسگر بی‌سیم، پانزدهمین کنفرانس کامپیوتر سالانه انجمن کامپیوتر ایران، تهران، https://civilica.com/doc/79194

[۵]. ستاری نائینی و؛ و موحدی، ف. (۱۳۹۶). به کارگیری منطق فازی در انتخاب مناسب گره بعدی برای پیکربندی مسیر با پروتکل LEAP در شبکه‌های حسگر بی‌سیم. مهندسی برق و مهندسی کامپیوتر ایران - ب مهندسی کامپیوتر، ۱۵(۴), ۳۰۴-۲۹۵. https://www.sid.ir/fa/journal/ViewPaper. aspx?id=۳۱۲۹۶۱

[۶]. افزایش امنیت شبکه‌های حسگر بی‌سیم با استفاده از جدول اعداد ترکیبی توزیع شده و منطق فازی، امید خلعتی، سید ابراهیم دشتی، محمدرضا اسلامی نژاد، ۱۳۹۷

[۷]. ثابت، مریم و قاضی‌زاده، مهدی و ناجی، حمیدرضا، ۱۳۹۲، ارائه یک روش سلسله مراتبی بهینه برای تشخیص حملات انکار سرویس با استفاده از شبکه عصبی در شبکه‌های حسگر بی‌سیم، همایش مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدلسازی و امنیت سیستم‌ها، مشهد، https://civilica.com/doc/238867

[۸]. جمالیان، الهام و قائمی، رضا، ۱۴۰۰، مروری بر کاربرد منطق فازی در سیستم‌های آموزش الکترونیکی، چهارمین همایش بین‌المللی مهندسی فناوری اطلاعات، کامپیوتر و مخابرات ایران، تهران، https://civilica.com/doc/1259789

[۹]. حسنی، سیدامین و اسماعیل دوست، محمد، ۱۳۹۷، ارایه الگوریتمی ترکیبی از منطق فازی و شبکه عصبی در راستای تخمین میزان امنیت در شبکه‌های بی‌سیم، دومین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی، اهواز، https://civilica.com/doc/849143

[۱۰]. حامد، محسن و صداقت، رضوان، ۱۳۹۵، یک پروتکل مسیریابی بر اساس منطق فازی برای بهبود امنیت داده‌ها در شبکه‌های بی‌سیم Ad Hoc، دومین همایش ملی علوم و فناوری‌های نوین ایران، تهران، https://civilica.com/doc/583370

[۱۱]. حسن نژاد مرزونی، حمیدرضا و دهقان، بختیار و رضاحسینی، زهرا، ۱۳۹۳، مسیریابی فازی در شبکه‌های حسگر بی‌سیم، همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات، تهران

[۱۲]. مؤمن‌زاده حقیقی، حسین و باوی، فاطمه و اعتصامی، مسعود، ۱۳۹۹، مسیریابی مبتنی بر اعتماد در شبکه‌های حسگر بی‌سیم با استفاده از منطق فازی، https://civilica.com/doc/1241440

[۱۳]. موسوی، صغری، ۱۳۹۹، مروری بر روش‌های خوشه‌بندی مبتنی بر منطق فازی در شبکه حسگر بی‌سیم، کنفرانس بین‌المللی پژوهش‌های نوین در مهندسی برق، کامپیوتر، مکانیک و مکاترونیک در ایران و جهان اسلام، کرج، https://civilica.com/doc/1118453

[۱٤] P. Gope, J. Lee,” Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Network”, DOI 10.1109/JSEN. 2016.2628413, IEEE Sensors Journal. 2016.

[۱۵] K. Kaushal, V. Sahni," Early Detection of DDoS Attack in WSN" International Journal of Computer Applications (0975 – 8887), 134(13). 2016.
[۱۶] A. K. M. M. Islam and K. Wada, "Communication Protocols on Dynamic Cluster-based Wireless Sensor Network," Informatics, Electronics & Vision (ICIEV), 2013 International Conference on. Dhaka, 1-6.2013.
[۱۷] Felemban, "Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology" Int'l J. Of Communications, Network and System Sciences, 6(5), pp. 251-259.2013.
[۱۸] K. Karenos, V. Kalogeraki and S. Krishnamurthy, "Cluster-based Congestion Control for Sensor Networks" ACM Transactions on Sensor Networks, 4(5), 1-31.2007.
[۱۹] J. Sen, "Security in Wireless Sensor Networks", Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA. 2012.
[۲۰] Hill, J. R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. "System Architecture Directions for Networked Sensors." In Proceedings of the 9th International Conference on 87 Architectural Support for Programming Languages and Operating Systems, 93-104, New York: ACM Press. 2000.
[۲۱] A Kellner, K Behrends, and D Hogrefe, Challenges of Secure Routing in WSNs: A Survey Technical Report No. IFI-TB-2010-06, Institute of Computer Science, Georg-AugustUniversität Göttingen, Germany. ISSN 1611- 1044.2010.
[۲۲] Reshma I. Tandel, "Leach Protocol in Wireless Sensor Network: A Survey" International Journal of Computer Science and Information Technologies, 7(4). 2016.
[۲۳] B. Mbarek, A. Meddeb, W. Ben Jaballah, M. Mosbah, "An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks" The 8th International Conference on Ambient Systems, Networks and Technologies. 2017.
[۲۴] Q. Monnet, L. Mokdad, "DoS detection in WSNs: Energy-efficient designs and modeling tools for choosing monitoring nodes". 2016.
[۲۵] S. Shin, T. Kwon, G. Y. Jo, Y. Park, H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks", IEEE Trans. Ind. Informat. 6(4), 744-757.2010.
[۲۶] R. C. Chen, C. F. Hsieh, Y. F. Huang, "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", in Proc. ACM ICUIMC-09.2009.
[۲۷] C. C. Su, K. M. Chang, Y. H. Kuo and M. F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in Proc. IEEE Wireless Communications and Networking Conference. 2005.
[۲۸] Neda Najaafi, Mohammadsaeid Zahedi, Fatemeh Mokhtari Esfidvjani and Arash Hedayati, 2020. A Genetic Fuzzy Model for Investigating Security and Trust in E-Commerce with Genetic Algorithm. Journal of Engineering and Applied Sciences, 15:1445-1450.
[۲۹] S. M. Bridges, and R. B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection", In Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, 2000, pp. 16-19
[۳۰] Gozepe, Kerim. "Designing fuzzy rule based expert system for cyber security." International Journal of Information Security Science 1.1(2012): 13-19.

[۳۱] Rachmat, Haris & Mulyana, Tatang & Hasan, Sulaiman & Ibrahim, Mohd. (2017). Design Selection of In-UVAT Using MATLAB Fuzzy Logic Toolbox. 538-545.10.1007/978-3-319-51281-5_5

[۳۲] Nguyen, Thanh Thi, and Vijay Janapa Reddi. "Deep reinforcement learning for cyber security." IEEE Transactions on Neural Networks and Learning Systems (2019).

[۳۳] Banković, Zorana, et al. "Improving network security using genetic algorithm approach." Computers & Electrical Engineering 33.5-6(2007): 438-451.

[۳٤] Hosseini, S. Nezhad, A. E. Seilani, H., (2022), “Botnet detection using negative selection algorithm, convolution neural network and classification methods”, *Evolving Systems*, 13(1), 101-115.