مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۱، بهار ۱۳۹۶، ص ۹۸-۸۵

ارائه مدل فازی ارزیابی میزان اثربخشی حملات منع سرویس‌دهی توزیع‌یافته، مبتنی بر منابع آشکار

اردشیر قاسم‌زاده[۱]، مجید غیوری ثالث*[۲]

۱- کارشناس ارشد، ۲- استادیار، دانشکده جنگ الکترونیک و دفاع سایبری، دانشگاه امام حسین(ع)

(دریافت: ۹۵/۰۲/۲۱، پذیرش: ۹۵/۰۸/۱۰)

چکیده

عملیات‌های سایبری، که عملیات منع سرویس‌دهی توزیع‌یافته (DDoS) یکی از مهمترین انواع آنها هستند، با فرض این‌که مبتنی بر اصول عملیات تاثیرمحور باشند، پیامدهای متنوعی ایجاد می‌کنند. اندازه‌گیری میزان و ابعاد پیامدهای یک عملیات سایبری از پیچیدگی بالایی برخوردار است. یکی از روش‌های استخراج پیامدها، ارزیابی میزان اثربخشی عملیات می‌باشد. از طرفی ارزیابی میزان اثربخشی نیز پیچیده و سخت می‌باشد، چرا که فضای تاثیرات عملیات سایبری، دارای شرایطی مثل عدم قطعیت بالا، گسترده بودن و غیرخطی بودن رابطه قدرت و کارایی عملیات با اثرات وضعی آنها می‌باشد. عموما برای غلبه بر چالش فوق از تلفیق داده‌های دریافتی از چند حسگر استفاده می‌شود. در فضای عملیات، حسگرها به دو نوع حسگر آشکار و پنهان تقسیم می‌شوند ولی در فضای سایبر حسگرهای آشکار از اهمیت بالاتری برخوردار هستند. در این تحقیق یک سازوکار مناسب برای اندازه‌گیری میزان موفقیت حملات DDoS طراحی شده است. جهت بازخوردگیری و اندازه‌گیری اثر نهایی عملیات DDoS، از منابع آشکار به‌عنوان حسگرها در مشاهده و دریافت میزان تاثیرات این نوع از عملیات، استفاده شده است. از آنجا که داده‌های منابع آشکار نزدیک به زبان شناختی بوده و همچنین به‌صورت دامنه‌ای و غیر دقیق بیان می‌گردد، لذا از روش فازی که یکی از بهترین روش‌های حل مسائل عدم قطعیتی و ابهام‌آلود می‌باشد، استفاده شده است. همچنین از منطق فازی و دلفی فازی وزن‌دار به صورت توامان جهت تلفیق و ادغام داده‌های حسگرها استفاده شده است. نتیجه ارزیابی‌ها به‌خوبی نشان می‌دهد سازوکار ارائه‌شده برای انتخاب و مقیاس‌بندی داده‌های آشکار به خوبی تدوین شده است و روش پیشنهادی برای تلفیق داده‌ها به دلیل توانایی عمل در محیط‌های عدم قطعیتی و مبهم، خطای کمتری نسبت به منطق کلاسیک و تک‌حسگری دارد.

واژه‌های کلیدی: عملیات سایبری، عملیات DDoS، اثربخشی عملیات، پیامد، استنتاج فازی

۱- مقدمه

اکثر صاحب‌نظران سایبری اذعان دارند که فضای سایبری به عنوان یک قلمروی جدید ظهور پیدا کرده است. لذا به‌وجود آمدن جنگ در این قلمرو قابل پیش‌بینی و طبیعی بوده و لذا وجود نگاشتی از فرایندها، اجزاء، مفاهیم و مولفه‌های جنگ‌های سخت و سنتی در این عرصه منطقی و عقلایی است [۱]. یکی از مفاهیم مطرح و ضروری در جنگ‌های غیر سایبری، فرماندهی و کنترل صحنه نبرد می‌باشد. پس می‌توان نگاشتی از مراحل و فرایندهای فرماندهی و کنترل را در قلمروی سایبری متصور بود. یکی از مهم‌ترین بخش‌های سامانه‌های فرماندهی و کنترل، آگاهی از وضعیت و اشراف بر صحنه نبرد می‌باشد. در حوزه آگاهی از وضعیت نبردهای سایبری، اندازه‌گیری و ارزیابی میزان اثربخشی عملیات سایبری بسیار با اهمیت‌تر از نبردهای سنتی است. بنا به دلایل ذیل پرداختن به موضوع اندازه‌گیری میزان اثربخشی عملیات سایبری، ضروری است:

- یکی از شاخص‌های پیامدسنجی عملیات سایبری، ارزیابی و احصاء میزان اثربخشی وضعی و مستقیم می‌باشد.
- ماهیت عدم قطعیتی و پیچیدگی فضای سایبری، موجب غیرخطی شدن رابطه بین ابعاد و قدرت عملیات سایبری با ابعاد و میزان اثر وضعی آنها شده است. لذا مولفه ارزیابی میزان اثربخشی عملیات سایبری نسبت به ارزیابی میزان کارایی، قضاوت درستی نسبت به تحقق یافتن اهداف عملیات فراهم می‌نماید.
- امروزه مبانی و مفاهیم مرتبط با فضای سایبری و همچنین ابعاد فضای سایبری دوران بلوغ خود را طی می‌کند. از این‌رو تا حدی شاکله و کلیات این قلمرو مشخص و آشکار

* رایانامه نویسنده مسئول: ghayoori@ihu.ac.ir

شده است. ولی به دلیل ماهیت عدم قطعیتی این فضا و عدم وجود سامانه‌ها و سازوکارهای دقیق، مقوله اثرسنجی عملیات سایبری همچنان جزء مسائل پیچیده و حل نشده باقی مانده است. همچنین در اکثر عملیات‌های سایبری، نه مهاجمان و نه قربانیان ارزیابی دقیقی از میزان اثربخشی این نوع عملیات ندارند.

- مطابق تحقیقات انجام شده توسط شرکت سیمانتیک، تعداد جرائم سایبری به مراتب بیشتر از جرائم غیرسایبری است. از طرفی تخمین درستی از میزان جرائم سایبری وجود ندارد. تا بتوان در تهیه و تدوین اسناد حقوقی فضای سایبری، اندازه‌گیری میزان اثربخشی عملیات سایبری را فراهم نمود [۲]. طبق اعلام شرکت هیولت پاکارد، در سال ۲۰۱۳ میزان خسارت حملات سایبری بالغ بر ۴۶۵ میلیارد دلار ارزیابی شده که روزانه یک میلیون نفر در دنیا قربانی حملات سایبری می‌شوند [۳].
- طبق گزارش منابع معتبر و رسمی حملات DDoS روزبه‌روز و به سرعت در حال افزایش هستند و این نوع حملات در رده دوم حملات سایبری می‌باشند [۱]. این نوع حملات در عین سادگی، بسیار قدرتمند و موثر بوده و تهدیدی بر قابلیت "دسترس‌پذیری" منابع شبکه‌ای و اینترنتی می‌باشند. لذا در این تحقیق، اندازه‌گیری میزان اثربخشی عملیات و حملات DDoS مورد بررسی و مطالعه قرار گرفته است.

حال با توجه به ضرورت‌های بیان شده، مسئله این است که چطور می‌توان میزان اثربخشی عملیات سایبری DDoS را تعیین نمود؟ جهت پاسخ به این سوال بایستی سوالات فرعی مطرح شده و پاسخی علمی به آنها داده شود. سوالات فرعی عبارتند از:

- حسگرهای مرتبط جهت تعیین میزان اثربخشی حملات DDoS را چطور معماری گردد؟
- چه معیارهایی برای تعیین میزان حملات DDoS، مورد نیاز است؟
- چطور می‌توان ارزیابی نهایی میزان اثربخشی حملات DDoS بر قربانی را مدل کرد؟

فرآیند کار انجام شده در این تحقیق عبارت است از: ابتدا، با استفاده از حسگرهای سایبری و براساس شاخص‌ها، پارامترها و معیارهای اصولی و علمی مرتبط با اثربخشی عملیات DDoS، اطلاعات و داده در رابطه با میزان اثربخشی حملات بر مقصد و قربانی حملات از محیط دریافت می‌شود. سپس داده‌ها پالایش و دسته‌بندی شده و در انباره‌ای ذخیره می‌گردد. با پردازش داده‌های موجود در انباره دانش، از طریق الگوریتم‌ها و روش‌های تلفیق و ترکیب داده، میزان اثربخشی عملیات، مدل‌سازی می‌گردد.

حسگرهای مورد استفاده در این تحقیق، مبتنی منابع آشکار می‌باشند. با توجه به عدم‌قطعیتی بودن فضای سایبری و شناختی بودن قالب داده‌ای منابع آشکار، مناسب‌ترین روش ارزیابی میزان اثربخشی عملیات DDoS، استنتاج فازی است، که در این تحقیق از این روش استفاده شده است. به طور مختصر ساختار ادامه تحقیق، بدین شرح است: ابتدا در بخش ۲، به مرور ادبیات و مفاهیم مرتبط با موضوع تحقیق پرداخته شده است. این بخش شامل بررسی تفصیلی حملات DDoS به همراه اثر وضعی آن، مفاهیم منطق فازی و دلفی فازی (با توجه به این‌که مدل‌سازی ترکیب و تلفیق داده در این تحقیق با روش منطق فازی و دلفی فازی انجام شده است.) می‌باشد. در بخش۳ به کارهای مرتبط با موضوع پژوهش پرداخته می‌شود. در بخش ۴، طرح پیشنهادی تحقیق ارائه شده است. در طرح پیشنهادی، ابتدا معماری پیکربندی حسگرها که مبتنی بر منابع آشکار است ارائه می‌شود، سپس با استفاده از منطق فازی و دلفی فازی، ارزیابی میزان اثربخشی حملات DDoS، مدل‌سازی می‌شود. در بخش ۵، طرح پیشنهادی مورد ارزیابی قرار گرفته است. سرانجام در بخش ۶، نتایج و یافته‌های تحقیق، در قالب نتیجه‌گیری و ارائه پیشنهادها، جهت انجام کارهای آتی مورد اشاره قرار گرفته است.

۲- مفاهیم پایه

۲-۱- حملات DDoS

حملات DDoS که معماری آنها در شکل (۱) آمده است [۴]، تهدیدی بر قابلیت "دسترس‌پذیری" منابع شبکه‌ای و اینترنتی می‌باشند. در این نوع عملیات، سرویس‌های سامانه مورد حمله، "قربانی اولیه" و سیستم‌های به تصرف آمده جهت پیاده‌سازی سناریوی عملیات گسترده و توزیع‌یافته، "قربانیان ثانویه" نامیده می‌شوند. با استفاده از قربانیان ثانویه، رهگیری و ردیابی منشاء عملیات بسیار سخت و دشوار خواهد بود.

اثرات وضعی عملیات جلوگیری از سرویس‌دهی توزیع یافته بر ابعاد سه‌گانه سایبری به‌شرح ذیل خواهد بود [۵]:

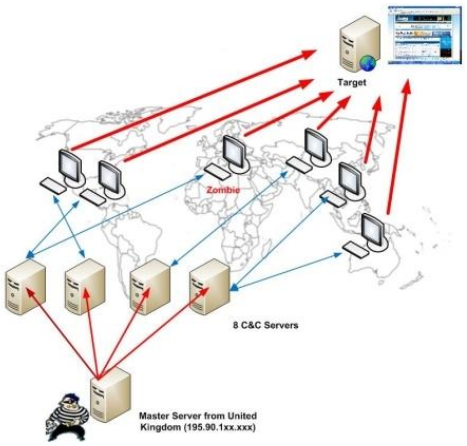
۱. اثرات وضعی در لایه زیرساختی (فیزیکی)
- اختلال و/یا قطع سرویس‌دهی روترها
- اختلال و/یا قطع سرویس‌دهی سوئیچ‌ها
- اختلال و/یا قطع سرویس‌دهی پهنای باند
- اختلال و/یا سرویس‌دهی فایروال‌ها و IPS/IDSها

۲. اثرات وضعی در لایه برنامه‌های کاربردی (اطلاعاتی)
- اختلال و/یا قطع سرویس‌دهی سوئیچ‌های ADC/content
- اختلال و/یا قطع سرویس‌دهی WAF
- اختلال و/یا قطع سرویس‌دهی سرورها
- اختلال و/یا قطع سرویس‌دهی برنامه‌های کاربردی

- اختلال و/یا قطع سرویس‌دهی پایگاه‌دادها

۳. اثرات وضعی در لایه شناختی (ادراکی)

- ایجاد بهت و ترس در جامعه قربانی
- ایجاد خسارت اقتصادی
- ایجاد خسارت سیاسی
- تاثیرگذاری منفی روانی بر جامعه قربانی
- ایجاد تغییرات تصمیمات جامعه قربانی
- ایجاد تغییر رفتار جامعه قربانی
- ایجاد افزایش نارضایتی در مشتریان قربانی



شکل (۱). معماری عملیات DDoS

۲-۲- منطق فازی

نظریهٔ مجموعه‌های فازی، نظریه‌ای است که در شرایط عدم اطمینان و عدم قطعیت مورد استفاده قرار می‌گیرد؛ این نظریه قادر است بسیاری از مفاهیم و متغیرها و سیستم‌هایی را که نادقیق هستند، صورت‌بندی ریاضی ببخشد و زمینه را برای استدلال، استنتاج، کنترل و تصمیم‌گیری در شرایط عدم اطمینان فراهم آورد.

به‌طور کلی یک سیستم خبره فازی از پنج بخش زیر تشکیل شده است [۶]:

۱. فازی‌ساز[1]: اعداد ورودی را به درجه‌ای از مقادیر کلامی مرتبط می‌کند.
۲. لغت‌نامه[2]: توابع عضویت مجموعه‌های فازی را که در قوانین به‌کار برده می‌شوند، تعریف می‌کند.
۳. پایگاه دانش[3]: قوانین اگر-آن‌گاه فازی به همراه لغت‌نامه، پایگاه دانش سیستم فازی را تشکیل می‌دهد.
۴. تصمیم‌گیرنده: عملیات استنتاج را روی قوانین اجرا می‌کند.
۵. فازی‌زدا[4]: نتایج استنتاج فازی را به اعداد واقعی تبدیل می‌کند.

چهار نوع فازی‌ساز به‌کار برده می‌شود که عبارتند از: فازی‌ساز مثلثی[5]، فازی‌ساز ذوزنقه‌ای[6]، فازی‌ساز منفرد[7] و فازی‌ساز گاوسی[8]، که در این پژوهش از فازی‌ساز مثلثی استفاده شده است.

۲-۳- دلفی فازی

روش دلفی فازی در دهه ۱۹۸۰ میلادی توسط کافمن و گوپتا ابداع شد [۶]. کاربرد این روش به منظور تصمیم‌گیری و اجماع بر مسائلی که اهداف و پارامترها به صراحت مشخص نیستند، منجر به نتایج بسیار ارزنده‌ای می‌شود. ویژگی مهم این روش، ارائه چارچوبی انعطاف‌پذیر است. که بسیاری از موانع مربوط به عدم دقت و صراحت را تحت پوشش قرار می‌دهد.

اجرای فرآیند دلفی فازی با استفاده از اعداد فازی مثلثی، مراحل زیر را شامل می‌شود [۷]:

در گام نخست از افراد خبره خواسته می‌شود که نظرات خود را در قالب حداقل مقدار، ممکن‌ترین مقدار و حداکثر مقدار ارائه دهند.

$$\left(A_1^{(i)}, B_1^{(i)}, C_1^{(i)}\right) \ , \ \mathrm{i} = 1,2,3, \dots, \mathrm{n} \qquad (۱)$$

در این رابطه i بیانگر فرد خبره iام و عدد ۱ نشانگر اولین پیش‌بینی دلفی است.

در گام دوم پاسخ‌های n فرد دسته‌ای را تشکیل می‌دهند. میانگین این دسته که خود یک عدد فازی مثلثی است محاسبه می‌شود.

$$(A_1^m, B_1^m, C_1^m) \quad m = \frac{1}{n}\sum_{i=1}^{n} a^{(i)} \qquad (۲)$$

در گام سوم برای هر فرد خبره، میزان اختلاف از میانگین دسته محاسبه می‌شود.

$$\left(A_1^m - A_1^{(i)}, B_1^m - B_1^{(i)}, C_1^m - C_1^{(i)}\right) \qquad (۳)$$

در گام چهارم هر فرد خبره براساس اطلاعات و نتایج تحلیل آماری به‌دست‌آمده از مرحله قبل، یک پیش‌بینی جدید ارائه می‌نماید. طبق رابطه (۴)، مراحل فوق تا دست‌یابی به انحراف معیار مناسب یا تا هنگامی که تکرار فرآیند تغییری در نتایج

1 -Fuzzifier
2 -Dictionary
3 -Rule Base

4 -Defuzzifier
5 -Triangular fuzzifiers
6 -Trapezoidal fuzzier
7 -Singleton fuzzier
8 -Gaussian fuzzier

ایجاد نکند، ادامه می‌یابد.

$$\left(A_2^{(i)}, B_2^{(i)}, C_2^{(i)}\right) \ , \ \mathrm{i} = 1,2,3,\dots,\mathrm{n} \qquad (۴)$$

در پایان به منظور تعیین ارزش قطعی اعداد فازی حاصل از اجرای فرایند دلفی فازی، روش‌های فازی‌زدایی مورد استفاده قرار می‌گیرد. در این تحقیق از روش ارائه شده توسط گوپتا و همکارانش [۶] برای فازی‌زدایی اعداد فازی مثلثی نامتقارن استفاده شده است.(رابطه ۵)

$$X = \frac{(c-a)+(b-a)}{3} + a \qquad (۵)$$

در این رابطه، X عدد قطعی نهایی، a مرز پایین تابع عضویت، b مولفه دارای بیشترین درجه عضویت و c مرز بالای تابع عضویت است.

۳- کارهای مرتبط

در عمده کارهای صورت گرفته در حوزه این تحقیق صرفا یک-بعدی به مسئله نگریسته شده است. به‌این ترتیب اگر هدف حمله‌ای کشورهای در حال توسعه باشد و همان حمله با همان ویژگی در کشورهای پیشرفته، که عموما متکی بر خدمات الکترونیکی هستند، صورت گیرد کارهای صورت گرفته قبلی قضاوت و اندازه‌گیری یکسانی را خواهند داشت. در صورتی که اثرات این نوع حملات در کشورهای پیشرفته به مراتب بیشتر و گسترده‌تر از کشورهای در حال توسعه خواهد بود. لذا در این تحقیق علاوه رفع مشکلات منطق کلاسیک در اندازه‌گیری و ارزیابی محیط‌های غیرخطی و عدم قطعیتی، نقیصه بیان شده برطرف شده است.

با توجه به مطالعات انجام گرفته، اغلب کارهای علمی صورت پذیرفته در این زمینه در مقیاس آزمایشگاهی پیاده‌سازی شده‌اند. لذا فرایند حملات و اندازه‌گیری میزان اثربخشی در یک محیط شبیه‌سازی شده انجام گرفته است. در محیط آزمایشگاهی و شبیه‌سازی شده، ابتدا در وضعیت عادی مقادیر پارامترهای میزان کارایی وب‌سایت‌ها و پارامترهای کیفیت سرویس‌دهنده‌ها، اندازه‌گیری شده سپس حملات DDoS را انجام داده و در حین حملات مقادیر همان پارامترها دوباره اندازه‌گیری شده، و درنهایت با مقایسه مقادیر دو وضعیت بیان شده، میزان اثربخشی حملات DDoS اندازه‌گیری می‌گردد. به بیان دیگر اغلب استراتژی‌های موجود با مقایسه ترافیک شبکه را در زمان حمله و بدون حمله میزان اثربخشی حملات DDoS را اندازه‌گیری می‌کنند [۸]. بعضی از رویکردهای دفاعی، زمان پاسخ سرویس مورد حمله را محاسبه می‌کنند [۹]. با اندازه‌گیری میزان بقای بسته‌های نرمال ثابت می‌شود که این پارامتر مهم است، چرا که به‌طور واضح منعکس کننده دقت و صحت سازوکارهای دفاعی و میزان بسته‌های عادی از دست‌رفته می‌باشد[۱۱-۱۰]. در [۹ و ۱۲] از پارامتر درصد تراکنش‌های شکست‌خورده (تراکنش‌هایی که از مقادیر آستانه QOS تبعیت نمی‌کنند) به عنوان پارامتری جهت اندازه‌گیری تاثیر حملات DDoS استفاده شده است. در این مقالات مدل مبتنی بر مقدار آستانه برای اندازه‌گیری ترافیک مرتبط با یک برنامه کاربردی خاص تعریف و استفاده شده است. همچنین کیفیت سرویس‌های ضعیف و نامرغوب را وقتی که میزان اندازه‌گیری به مقدار آستانه می‌رسد، را مشخص می‌کند. پارامتر دیگری بنام زمان انقضای سرور در [۱۳] مورد استفاده قرار گرفته است. به دلیل دور انداخته شدن ترافیک مجاز و قانونی، صدمات جانبی مشخص نمی‌شود. در [۱۴] از ورودی خوب و زمان متوسط بین زمان پاسخ متوسط و شکست به عنوان پارامترهای کارایی استفاده شده در حالی‌که در [۱۵] از دو پارامتر آماری بنام حجم و جریان جهت تشخیص حملات DDoS بهره برده است. پارامترهای آورده شده در [۱۲] از جمله ورودی خوب، ورودی بد، زمان پاسخ، تعداد ارتباطات فعال، نرخ متوسط میزان سرویس‌دهی و درخواست سرویس و شاخص ابقاء بسته نرمال (که در [۱۱] معرفی شده است) به طور مناسب نشانگر حملات DDoS برای برنامه‌های کاربردی دوطرفه از قبیل HTTP، FTP و DNS می‌باشد، ولی برای ترافیک رسانه که به تاخیرات یک طرفه و بسته‌ها حساس هستند، مناسب نیست.

در [۸] یک مدل ریاضی سه‌بعدی جهت ارزیابی درجه تاثیر حملات DoS مبتنی بر شاخص‌های کیفیت سرویس استاندارد 3GPP، ارائه شده است. مدل ارائه شده در یک محیط آزمایشگاهی مورد تست و ارزیابی قرار گرفته است. در محیط آزمایشگاه بعد از انجام انواع حملات DoS و اندازه‌گیری شاخص‌ها و مقایسه آن با شاخص‌های 3GPP در وضعیت‌های مختلف مکانیزم‌های امنیتی، میزان اثربخشی حملات DoS مورد ارزیابی قرار گرفته است.

مدل ارائه شده در [۱۶]، تاثیرات حملات سایبری به‌خصوص حملات DDoS را مبتنی بر خسارت اقتصادی حاصل از این نوع حملات، از قبیل هزینه زمان پایین بودن[1] سرویس وب، هزینه بازیابی حادثه[2] حمله، تعهد[3] به مشتریان و میزان از دست دادن مشتریان[4] را مورد بررسی قرار داده است.

در پایان این بخش، به عنوان جمع‌بندی می‌توان ادعا کرد که در کارهای صورت گرفته، کار انجام شده مرتبط با موضوع تحقیق، عمدتا به صورت یک بعدی و یا محدود مورد بررسی قرار گرفته است. در ضمن به دلیل ماهیت عدم قطعیتی فضای

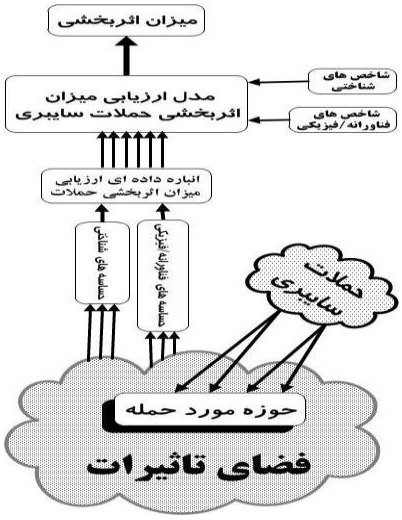
1 -Downtime Loss
2 -Disaster Recovery
3 -Liability
4 -Customer Loss

سایبری، نمی‌توان با روش‌های ریاضیاتی کلاسیک و آماری، میزان اثربخشی حملات DDoS را اندازه‌گیری نمود. این مسئله یکی از کاستی‌های کارهای قبلی در این زمینه است. استفاده از زبان شناختی و بهره‌گیری از تلفیق اطلاعات چندحسگری از جمله روش‌های موثر جهت تقلیل میزان عدم‌قطعیتی است. درکارهای صورت گرفته از این دو راه‌حل استفاده نشده است. از طرفی با توجه به این‌که یکی از مجموعه حسگرها، عوامل انسانی می‌باشد. در این تحقیق با استفاده از معماری چندحسگری و بهره‌گیری از زبان شناختی استنتاج فازی، بخش قابل توجهی از این نقایص، برطرف شده است. خلاصه موارد بیان شده، در جدول (۱) آمده است.

۴- متدولوژی تحقیق

در شکل (۲)، متدلوژی ارزیابی میزان اثربخشی عملیات سایبری، ارائه شده است.

براساس سوالات مطرح شده در بخش مقدمه ابتدا لازم است معماری و پیکربندی حسگرهای سایبری استخراج گردد. که این معماری در شکل (۳) نمایش داده شده است. در گراف مورد اشاره، گره‌های انتهایی نمایانگر خود حسگرها می‌باشد. که این گره‌ها در دسته‌های مختلف سازماندهی شده‌اند. گره‌های میانی بیانگر گروهی از حسگرهای از یک نوع می‌باشد و گره وسطی گراف، محل ترکیب و تلفیق نتیجه و اندازه‌گیری نهایی میزان اثربخشی می‌باشد. بر اساس این معماری، ابتدا حسگرهای هر گروه در رابطه با میزان اثربخشی حملات سایبری اطلاعات و داده را از محیط دریافت می‌کنند. جمع رای‌گیری شورایی تمام حسگرها یک قضاوت در مورد میزان اثربخشی حملات سایبری استخراج می‌گردد. همچنین با توجه به میزان اهمیت و دقت هر حسگر، برای حسگرهای هر گروه، یک وزن اعتباری داده می‌شود.



شکل (۲). مدل ارزیابی اثربخشی حملات سایبری

جدول (۱). شاخص‌های ارزیابی

ردیف	نام پارامتر و شاخص	مراجع
۱	مدل خسارت اقتصادی	[۱۶]
۲	عامل مقیاسMIDAS2007	[۱۷]
۳	عاملMIDAS2007NET	[۱۷]
۴	استهلاک حافظه	[۱۸]
۵	استهلاک پردازشگر	[۱۸]
۶	متوسط خروجی خوب	[۱۹]
۷	Average congestion window	[۱۹]
۸	میزان بسته‌های ارسال و دریافت در ثانیه	[۱۹]
۹	میزان متوسط رشد صف	[۲۰]و[۲۱]
۱۰	میزان امکان در دسترس بودن	[۲۰]و [۲۲]
۱۱	زمان پاسخ	[۲۰]
۱۲	تاخیر، تعداد تاخیر و اطلاعات اطلاعات از دست رفته گفتگو	[۲۳]
۱۳	تاخیر و اطلاعات اطلاعات از دست رفته ویدئو یکطرفه	[۲۳]
۱۴	تاخیر و اطلاعات از دست رفته ویدئو یکطرفه	[۲۳]
۱۵	تاخیر و اطلاعات از دست رفته ارسال/دریافت داده حجیم	[۲۳]
۱۶	تاخیر و اطلاعات از دست رفته تصویر	[۲۳]
۱۷	تاخیر و اطلاعات از دست رفته Telemetry-monitoring	[۲۳]
۱۸	تاخیر و اطلاعات از دست رفته ایمیل(دسترسی سرویس)	[۲۳]
۱۹	تاخیر و اطلاعات از دست رفته ایمیل(انتقال از سرور به سرور)	[۲۳]
۲۰	تاخیر و اطلاعات از دست رفته تراکنش‌های با اولویت پایین از قبیل SMS	[۲۳]
۲۱	تاخیرو تعداد تاخیر ,اطلاعات از دست رفته پیام صوتی	[۲۴]
۲۲	تاخیرو تعداد تاخیر ,اطلاعات از دست رفته جریان صدا با کیفیت بالا	[۲۴]
۲۳	legitimate packet survival ratio	[۲۴]
۲۴	درصد تراکنش‌های از بین رفته	[۲۴]
۲۵	پهنای باند مفید	[۲۴]

اگر مجموعه حسگرها را با S_{ti} نمایش داده شود، آنگاه این مجموعه به‌صورت زیر تعریف می‌گردد:

$$S_{ti} = \{S_{t1}, S_{t2}, S_{t3}, \dots, S_{tn}\} \qquad (۶)$$

به‌نحوی که S_{ij} عبارتست از حسگر jام از مجموعه حسگر i.

هر حسگر با استفاده از مقادیر مجموعه شاخص I_i، میزان اثربخشی را ارزیابی می‌کند. مجموعه شاخص I_i به صورت زیر تعریف می‌شود:

$$I = \{I_1, I_2, I_3, \dots, I_m\} \quad (۷)$$

به‌قسمی که هر I یک شاخص ارزیابی است که توسط حسگر S_n ارزیابی می‌شود. جهت ارزیابی میزان اثربخشی شاخص‌های I_m توسط حسگر S_n تابع μ (مطابق آنچه در شکل (۴) نمایش داده شده است) به صورت زیر تعریف می‌شود:

$$\mu_j = f(I_1, I_2, I_3, \dots, I_m) \quad (۸)$$

شاخص‌های استفاده شده در این تحقیق به شرح ذیل می‌باشد:

- شاخص‌های اقتصادی
- شاخص‌های اطلاعاتی
- شاخص‌های ادراکی

شکل (۴) توسعه‌یافته شکل (۳) است، که معماری نهایی حسگرها را نمایش می‌دهد. براساس شکل (۴)، اجرای فرآیند ارزیابی میزان اثربخشی حملات DDoS با استفاده از استنتاج فازی شامل مراحل زیر است:

۱- در گام نخست با توجه به کارکرد و ماهیت حسگرهای سایبری، شاخص‌های مرتبط تعیین گردید. در این تحقیق مجموعه شاخص‌های بعد اقتصادی با I_{Eco}، و مجموعه شاخص‌های بعد اطلاعاتی فضای سایبری با I_{info}، و مجموعه شاخص‌های ادراکی و شناختی با I_{cogn} نشان داده شده است. بنابراین داریم:

$$I_{Eco} = \{I_{Eco_1}, I_{Eco_2}, \dots, I_{Eco_l}\} \quad (۹)$$

$$I_{info} = \{I_{info_1}, I_{info_2}, \dots, I_{infi_p}\} \quad (۱۰)$$

$$I_{cogn} = \{I_{cogn_1}, I_{cogn_2}, \dots, I_{cogn_q}\} \quad (۱۱)$$

در این تحقیق، شاخص میزان خسارت اقتصادی[1] (FL) به عنوان شاخص اقتصادی، شاخص میزان نارضایتی مشتریان[2] به عنوان شاخص شناختی و شاخص مدت زمان پایین بودن وب‌سایت[3] (DT) مورد حمله به عنوان شاخص اطلاعاتی در نظر گرفته شده است. با توجه به فرض این پژوهش، ابعاد فضای تاثیرات (E_s) مورد نظر سه‌بعدی بوده و برای هر بعد آن یک شاخص در نظر گرفته شده است. اگر شاخص‌های ذکر شده با علایم اختصاری نمایش داده شده است. آن‌گاه، $I_{Eco_1} = FL$، و $I_{info_1} = DT$ و $I_{cogn_1} = CL$

۲- در این گام با توجه به شاخص‌های انتخاب شده در مرحله قبل، از دید یک حسگر میزان اثربخشی حملات DDoS، مقادیر شاخص‌های آن حسگر ترکیب و تلفیق شده، استنتاج می‌شود. ترکیب و تلفیق مقادیر حسگر براساس شاخص‌های مربوطه، به روش منطق فازی صورت می‌گیرد. حال اگر مقدار استنتاج شده به روش منطق فازی از دید حسگر j را با تابع μ_j نشان داده شود، خواهیم داشت:

$$\mu_j = f(I_{Eco}, I_{Info}, I_{Cogn}) \quad (۱۲)$$

۳- پس از آن‌که تمام مقادیر حسگرهای یک گروه حسگری محاسبه و تعیین گردید، با استفاده از روش دلفی فازی مقادیر استنتاج شده حسگرهای گروه حسگری باهم تلفیق و ترکیب می‌شوند. در روش دلفی فازی که در آن با استفاده تکرار اخذ داده، انحراف معیار قابل قبولی استخراج شده و براساس مقدار نسبت به نظرات خبرگان قضاوت صورت می‌گیرد. در این تحقیق، بجای انحراف معیار دلفی فازی، از معدل‌گیری شده است. مقدار استنتاج شده حسگرهای گروه حسگری i با تابع γ_i نشان داده شده است، لذا خواهیم داشت:

$$\gamma_i = g(\mu_1, \mu_2, \mu_3, \dots, \mu_n) \quad (۱۳)$$

۴- در مرحله بعدی، پس از آن‌که مقادیر تمام گروه‌های حسگری محاسبه گردید، با استفاده از روش دلفی فازی مقادیر استنتاج شده گروه‌های حسگری مجددا ترکیب شده تا مقدار نهایی میزان اثربخشی حملات DDoS در نقطه R_{Effect} بدست آید. لذا اگر این مقدار را با تابع β_k که k تعداد گروه‌های حسگری می‌باشد، نشان دهیم، خواهیم داشت:

$$\beta_k = h(\gamma_1, \gamma_2, \gamma_3, \dots, \gamma_k) \quad (۱۴)$$

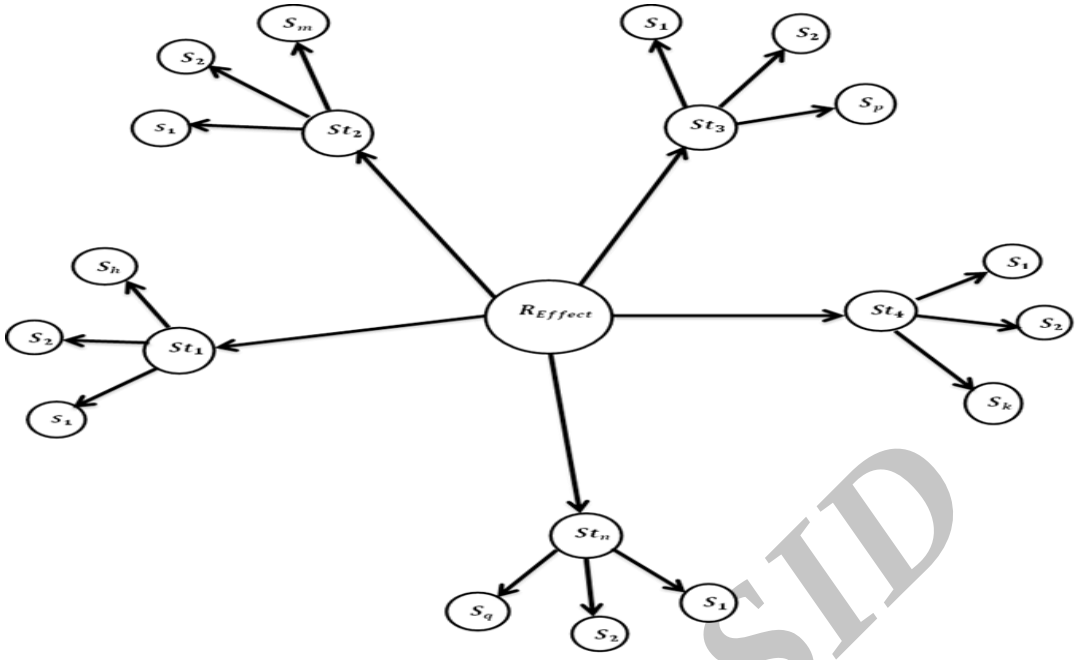
در مدل پیشنهادی توابع فوق به صورت زیر در نظر گرفته شده‌اند:

- توابع μ_j براساس منطق فازی محاسبه می‌شوند.
- توابع γ_i براساس دلفی فازی محاسبه می‌شوند.
- توابع β_k براساس دلفی فازی محاسبه می‌شوند.

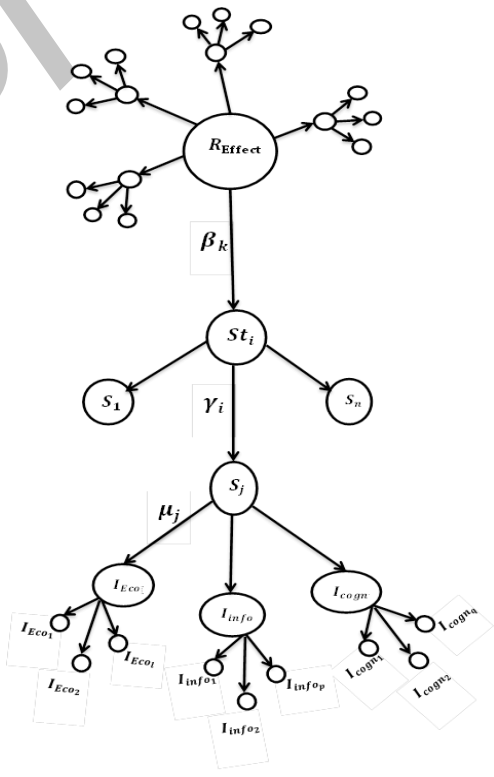
پس از محاسبه توابع فوق مقدار R_{Effect} که میزان اثربخشی عملیات DDoS را بیان می‌کند، از طریق رابطه زیر به‌دست می‌آید:

$$R_{Effect} = w_1 \sum \beta_1 + w_2 \sum \beta_2 + \dots + w_k \sum \beta_k \quad (۱۵)$$

1 -Finance Loss
2 -Customer Loss
3 -Down Time



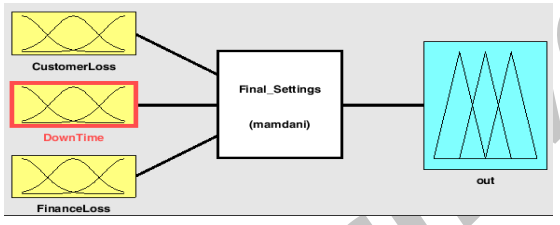
شکل (۳). گراف حسگرهای سایبری



شکل (۴). معماری حسگرها

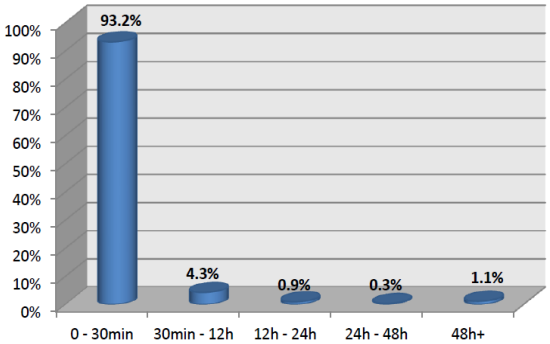
۵- پیاده‌سازی طرح پیشنهادی

در این تحقیق برای پیاده سازی و شبیه‌سازی روش فوق از متلب استفاده شده است. بدین‌منظور در گام نخست مطابق شکل (۵)، به روش منطق فازی مقادیر بازه‌های شاخص‌های میزان از دست دادن مشتریان (CL)، زمان پایین بودن وب‌سایت (DT) و میزان خسارت اقتصادی (FL) باید تعیین گردد.



شکل (۵). تلفیق فازی متغیرهای هر حسگر

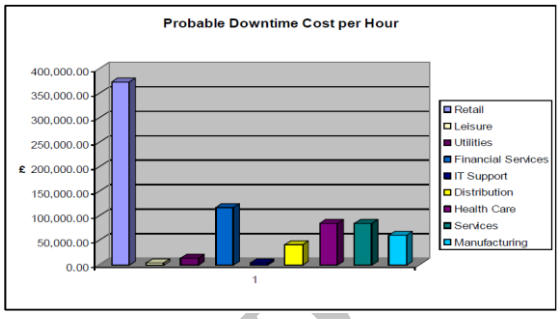
طبق بررسی‌های صورت‌گرفته [۵] که نتیجه آن در شکل (۶) آمده است، ۹۳ درصد حملات موفق DDoS، ۳۰ دقیقه طول کشیده است. لذا بازه فازی به‌دست‌آمده برای شاخص DT، بر اساس یافته‌های آورده شده در شکل (۶) محاسبه شده است.



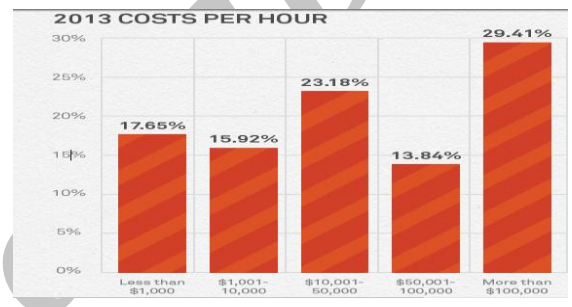
شکل (۶). آمار زمان پایین بودن

طبق پژوهش صورت‌گرفته که نتیجه آن در شکل‌های (۷ و ۸) نشان داده است، متوسط میزان خسارت اقتصادی به وب‌سایت‌های

مالی و بانکی برابر با ۱۰۰۰۰۰دلار می‌باشد. براساس این معیار بازه‌های فازی براساس مقادیر شکل‌های (۷ و ۸) [۱, ۲۶] تعریف می‌گردد.



شکل (۷). میزان خسارت اقتصادی حملات در ساعت



شکل (۸). میزان خسارت اقتصادی حملات

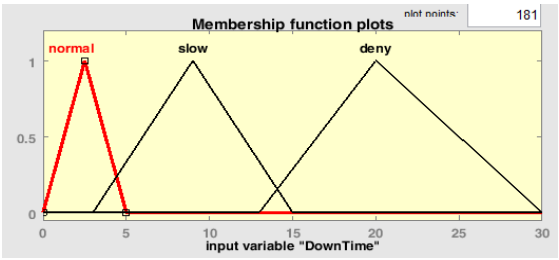
با توجه به این‌که سند معتبری در خصوص تاثیر حملات DDoS برای شاخص از دست دادن مشتریان به‌دست نیامد لذا برای تعیین بازه‌های فازی شاخص میزان از دست دادن مشتریان (CL) از مصاحبه با خبرگان فن و تخمین‌های کلی استفاده گردید. تخمین دقیق‌تر این موضوع یک کار تحقیقاتی است که نیاز به زمان مناسبی دارد. جمع‌بندی پژوهش‌های صورت گرفته در جدول (۲) آورده شده است.

جدول (۲). جمع‌بندی متغیرهای فازی مورد استفاده

متغیرهای ورودی	مقادیر کلامی	بازه فازی
زمان پایین بودن وب‌سایت	عادی	۰-۵ دقیقه
	مختل	۴-۱۵ دقیقه
	قطع	بزرگتر از ۱۵
میزان نارضایتی مشتریان	کم	۰-٪۱۰
	متوسط	٪۸-٪۳۰
	زیاد	بیشتر از ٪۲۵
میزان خسارت اقتصادی	کم	۰-٪۱۶۰۰۰ دلار
	متوسط	۱۲۰۰۰-۵۰۰۰۰ دلار
	موثر	بیشتر از ۴۰۰۰۰دلار

۵-۱- تعریف متغیرها بر اساس شاخص‌ها:

مدت زمان پایین بودن وب‌سایت[1]: که از این به بعد به‌صورت (DT) نمایش داده خواهد شد، جزء معیارهای فناورانه در نظر گرفته شده است. این شاخص بیانگر مدت زمان پایین بودن وب‌سایت پس از انجام یک حمله DDoS می‌باشد. شکل (۹) تابع عضویت این متغیر فازی را نمایش می‌دهد.

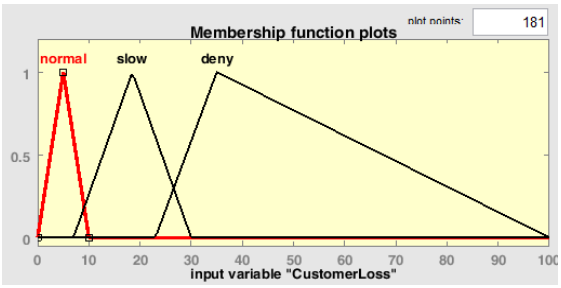


شکل (۹). تابع عضویت متغیر DT

میزان از دست دادن مشتریان (CL): منظور از این متغیر، نسبت مشتریان ناراضی بر کل مشتریان وب سایت هدف می باشد [۲۸]. اگر سرویسی در مدت زمان مشخصی غیرقابل دسترس باشد، ممکن است مشتریان دیگر از این سرویس‌دهنده منتقل شده و یا حداقل بیشتر از این سرویس استفاده نکنند. این نوع از دست دادن موجب خسارت شده و شامل از دست دادن مشتریان جدید نیز می‌شود.

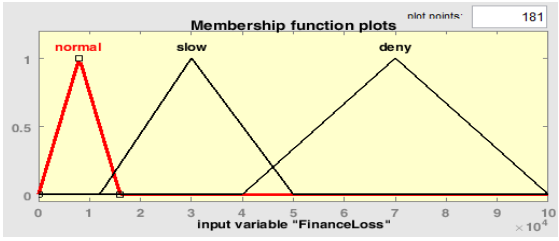
شکل (۱۰)، تابع عضویت مربوط به میزان نارضایتی مشتریان (CL) را نشان می‌دهد. این تابع در سه وضعیت کم، متوسط و زیاد تعریف شده است. که براساس مقادیر بازه‌ها نوع این وضعیت‌ها مشخص می‌گردد.

میزان خسارت اقتصادی (FL): منظور از این متغیر، خسارت اقتصادی و مالی وب سایت هدف بدلیل اثر حملات است. شکل (۱۱)، تابع عضویت مربوط به میزان خسارت اقتصادی (FL) را نشان می‌دهد. این تابع نیز در سه وضعیت کم، متوسط و زیاد تعریف شده است که براساس مقادیر بازه‌ها نوع این وضعیت‌ها مشخص می‌گردد.



شکل (۱۰). تابع عضویت متغیرCL

1 -Down Time



شکل (۱۱). تابع عضویت متغیر FL

۵-۲- تشکیل پایگاه قانون اگر...آن‌گاه اگر

با توجه به این‌که تعداد متغیرهای زبانی ۳ متغیر بوده و هرکدام ۳ حالت بی‌تاثیر، متوسط و موثر را به عنوان ورودی می‌گیرند، خروجی تلفیق متغیرهای فوق، ۳ خروجی بی‌تاثیر، متوسط و موثر را دارد. لذا تعداد قواعد و یا به عبارتی تعداد قوانین پایگاه قواعد فازی ۲۷ عدد خواهد شد. با توجه به نظرات خبرگان و تجارب خبرگی، پایگاه قواعد تشکیل شده است که در جدول شماره (۲) لیست قواعد آمده است.

با توجه به جدول فوق، به دلیل واضح بودن نحوه استنتاج قواعد ۲۷،۱۹،۱۶،۱۷،۱۸،۱۳،۱۵،۱۱،۱۰،۲،۱ در چگونگی ترکیب گزاره‌های متناظر آنها، نیازی به استدلال نیست. در مورد قاعده شماره ۳، در نگاه اول شاید بی‌معنی و غیرممکن به نظر برسد، ولی با توجه به این‌که متولیان بعضی از وب‌سایت‌ها بتوانند در زمان حمله، پایداری و کیفیت سرویس‌دهی خود را مثل زمان غیرحمله، حفظ کنند بایستی مبالغی را جهت تقلیل و یا حذف اثر حمله، هزینه کنند. لذا با وجود این‌که در زمان حمله، گزاره‌های کیفیت بالا آمدن صفحه وب و میزان مشتریان عادی و نرمال هستند ولی هزینه نگهداری وب‌سایت در حالت پایدار، موجب اعمال خسارت اقتصادی بر متولیان وب‌سایت می‌گردد. اگر مبنای طرح‌ریزی عملیات سایبری، جنگ اقتصادی صرف باشد آنگاه قواعد شماره ۴، ۷ و ۸ قابل قبول و ممکن خواهد بود. دلیل ممکن بودن قاعده شماره ۷ این است که در این حالت کیفیت و بالا آمدن صفحه وب عادی و نرمال بوده ولی اثر حملات بر سرویس‌های تعاملی کاربر با وب‌سایت متمرکز شده است.

از طرفی متولیان وب‌سایت جهت نگهداری وب‌سایت در حالت عادی و نرمال اقدامی نکرده‌اند، لذا در این قاعده امکان نارضایتی مشتریان بوجود آمده است. چرا که براساس اصول عملیات تاثیرمحور، مبنای پیروزی و موفقیت تصورات قربانی و فرضیات مهاجمان از تاثیر نهایی عملیات خواهد بود. با توجه به اینکه صفحات وب حاوی سرویس‌هایی از قبیل ایمیل، استعلام حساب بانکی و هر چیزی که حاوی فیلدهای تعاملی با کاربر هستند، لذا با فرض این‌که گزاره کیفیت بالا آمدن صفحه وب نرمال و عادی هست، ممکن است کاربران نتوانند با بخش‌ها و فیلدهای تعاملی و پرس‌وجویی آن کار کنند و این موضوع موجب سرخوردگی و نارضایتی مشتریان خواهد شد. در حالت قاعده ۹، ممکن است شدت اثرحمله سایبری DDoS، موجب اختلال و یا قطع سرویس‌های تعاملی با کاربر و همچنین ایجاد خسارت اقتصادی از طریق اعمال خسارت بابت نگهداری وب‌سایت در حالت عادی شده است. ولی این هزینه در حدی نبوده است که سرویس‌های تعاملی کاربر را در حالت عادی نگه دارد. در قواعد ۱۰،۱۹ و ۲۲ با وجود این‌که زمان و کیفیت بالا آمدن وب‌سایت مختل یا قطع شده است، ولی به‌دلیل عدم تاثیر در شاخص‌های میزان نارضایتی مشتریان و میزان خسارت اقتصادی، اثر حمله نادیده گرفته شده است. دلیل ممکن بودن این قواعد این است که عملیات سایبری در غیر از زمان پیک و بیشینه کارکرد مفید وب‌سایت، انجام گرفته است. و یا وب‌سایت مورد حمله در منطقه‌ای قرار گرفته است که اساسا زیرساخت و فرهنگ دولت الکترونیک در انجام وجود ندارد.

۵-۳- تلفیق و ادغام مقادیر ورودی به حسگرهای هر گروه با استفاده از منطق فازی

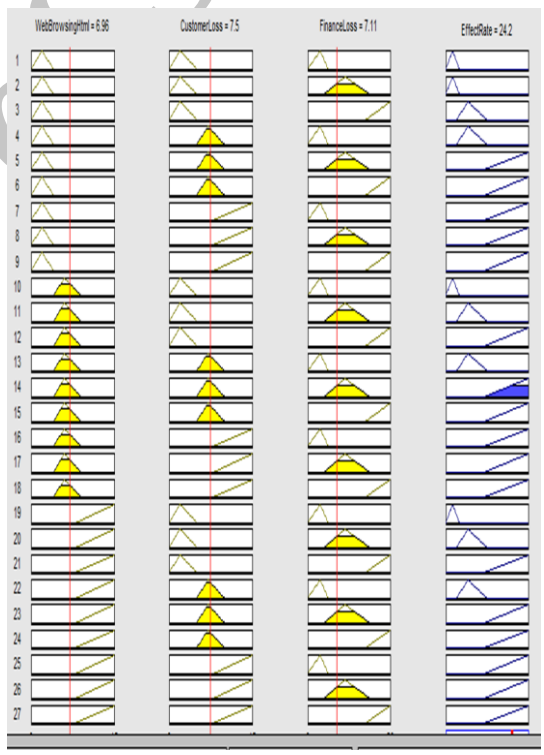
میزان اثربخشی حملات از دید حسگر تنها خروجی سیستم بوده که به صورت فازی در نظر گرفته شده و در آخر فازی زدایی شده و میزان اثربخشی حملات از دید حسگر به‌صورت یک عدد به‌دست می‌آید.

در جدول (۳) و شکل (۱۲)، نتیجه حاصل از اعمال قوانین بر روی ورودی‌ها و خروجی‌ها مشاهده می‌شود. ورودی‌ها در حالت مختلف و نتیجه حاصل از این ورودی‌ها آورده شده است. با استفاده از روش مرکز ثقل، مقادیر فازی ورودی شاخص‌های ارزیابی دی‌فازی شده و میزان اثربخشی حملات DDoS در قالب عناوین سه‌گانه بی‌تاثیر، متوسط و موثر از دید یک حسگر محاسبه شده است.

جدول (۳). پایگاه قوانین

ردیف	μ_j	I_{Eco_1}	I_{cogn_1}	I_{info_1}
۱	بی‌تاثیر	بی‌تاثیر	بی‌تاثیر	بی‌تاثیر
۲	بی‌تاثیر	متوسط	بی‌تاثیر	بی‌تاثیر
۳	موثر	موثر	بی‌تاثیر	بی‌تاثیر
۴	متوسط	بی‌تاثیر	متوسط	بی‌تاثیر
۵	موثر	متوسط	متوسط	بی‌تاثیر
۶	موثر	موثر	متوسط	بی‌تاثیر
۷	موثر	بی‌تاثیر	موثر	بی‌تاثیر
۸	موثر	متوسط	موثر	بی‌تاثیر
۹	موثر	موثر	موثر	بی‌تاثیر
۱۰	بی‌تاثیر	بی‌تاثیر	بی‌تاثیر	متوسط
۱۱	متوسط	متوسط	بی‌تاثیر	متوسط

ادامه جدول (۳). پایگاه قوانین				
ردیف	μ_j	I_{Eco_1}	I_{cogn_1}	I_{info_1}
۱۲	موثر	موثر	بی‌تاثیر	متوسط
۱۳	متوسط	بی‌تاثیر	متوسط	متوسط
۱۴	موثر	متوسط	متوسط	متوسط
۱۵	موثر	موثر	متوسط	متوسط
۱۶	موثر	بی‌تاثیر	موثر	متوسط
۱۷	موثر	متوسط	موثر	متوسط
۱۸	موثر	موثر	موثر	متوسط
۱۹	بی‌تاثیر	بی‌تاثیر	بی‌تاثیر	موثر
۲۰	متوسط	متوسط	بی‌تاثیر	موثر
۲۱	موثر	موثر	بی‌تاثیر	موثر
۲۲	متوسط	بی‌تاثیر	متوسط	موثر
۲۳	موثر	متوسط	متوسط	موثر
۲۴	موثر	موثر	متوسط	موثر
۲۵	موثر	بی‌تاثیر	موثر	موثر
۲۶	موثر	متوسط	موثر	موثر
۲۷	موثر	موثر	موثر	موثر



شکل (۱۲). تلفیق قواعد فازی و خروجی آن بروش مرکز ثقل

۵-۴- ترکیب مقادیر حسگرهای هر مجموعه حسگری بر اساس دلفی فازی

در مرحله قبل از طریق استنتاج به روش منطق فازی، میزان اثربخشی هر حسگر در داخل مجموعه حسگرها در قالب زبان شناختی بی‌تاثیر، متوسط و موثر محاسبه شد. با توجه به نزدیک بودن قالب و ادبیات خروجی هر حسگر به زبان شناختی انسانی و وجود عدم قطعیت، با توجه به مطالعات صورت گرفته مناسب‌ترین روش جهت تلفیق مقادیر حسگرها در یک مجموعه حسگری، روش دلفی فازی می‌باشد. لذا در این بخش جهت تجمیع و تلفیق اندازه‌گیری کل حسگرهای موجود در یک گروه از روش دلفی فازی استفاده شده است. لذا ابتدا باید متغیرهای کلامی را در قالب طیف پنج‌گانه لیکرت که در جدول (۴) مقادیر آن آورده شده، را تعریف و مشخص گردد. البته به دلیل سه حالته خروجی حسگرها، سه طیف از طیف‌های لیکرت (بی‌تاثیر، متوسط، موثر) را انتخاب شده و متغیرها به شکل اعداد مثلثی تعریف شده است.

جدول (۴). مقادیر لیکرت

متغیرهای کلامی	عدد فازی مثلثی	عدد فازی قطعی‌شده
موثر	(۰/۷۵،۰/۵، ۱)	۰/۵۶۲۵
متوسط	(۰/۵،۰/۲۵، ۰/۷۵)	۰/۳۱۲۵
بی‌تاثیر	(۰/۲۵،۰، ۰/۵)	۰/۰۶۲۵

۵-۵- ترکیب مقادیر مجموعه‌های حسگرها بر اساس دلفی فازی

در مرحله قبل از طریق استنتاج دلفی فازی، میزان اثربخشی هر مجموعه حسگر در قالب زبان شناختی بی‌تاثیر، متوسط و موثر محاسبه شد. بازهم با توجه به نزدیک بودن قالب و ادبیات خروجی هر مجموعه حسگر به زبان شناختی انسانی و وجود عدم قطعیت، در این بخش نیز جهت تجمیع و تلفیق اندازه‌گیری کل مقادیر مجموعه حسگرهای موجود در گراف مجددا از روش دلفی فازی استفاده شده است. لذا باز هم مثل مرحله قبل، باید متغیرهای کلامی در قالب طیف پنج‌گانه لیکرت تعریف و مشخص گردند. مقادیر عبارات در جدول (۳) آورده شده است.

البته به دلیل سه حالته خروجی حسگرها، سه طیف از طیف‌های لیکرت (بی‌تاثیر، متوسط، موثر) را انتخاب نموده و متغیرها به شکل اعداد مثلثی تعریف می‌نماییم.

۶- ارزیابی مدل ارائه‌شده

در این بخش ابتدا داده‌های مورد نیاز جهت ارزیابی تهیه و جمع‌آوری شد. سپس مبنای ارزیابی و مقایسه بین روش فازی و کلاسیک تعریف گردید. منظور از کلاسیک همان منطق گزاره‌هاست که برای استنتاج استفاده می‌شود. پس از آن شاخص‌های ارزیابی دقت و سرعت انتخاب شده، براساس این دو شاخص روش فازی و کلاسیک مورد ارزیابی قرار گرفته‌اند. در نهایت با استفاده از نرم‌افزار متلب سناریوی این تحقیق پیاده‌سازی شده و در نهایت در قالب نمودارها، تفاوت دو روش فوق نشان داده شده است.

۶-۱- تهیه داده‌های مورد نیاز

جهت ارزیابی مدل پیشنهادی نیاز به داده می‌باشد. بدین منظور براساس مطالعات صورت گرفته سه منبع داده مشخص و تهیه گردید:

- وب‌سایت‌های مرتبط
- مقاله‌ها
- تولید داده براساس الگوی مشخص، جهت رفع نواقص بند ۲ و۳.

براساس گراف حسگرهایی که در شکل (۳) آمده است، پنج مجموعه حسگری در نظر گرفته شده است. اولین مجموعه حسگر وب‌سایت‌های پایش وضعیت وب‌سایت و حملات می‌باشد. تعداد حسگرهای این مجموعه حسگر ۵ عدد می‌باشد که عبارتنداز:

- 24x7
- Akamai
- Site Down
- BankInfoSecurity
- dotcom monitoring

دومین مجموعه حسگر وب‌سایت‌های خبری هستند، که دارای چهار حسگر می‌باشد. حسگرهای انتخاب شده برای این مجموعه حسگر عبارتند از: رویترز، هافینگتون‌پست، شبکه‌های اجتماعی، وبلاگ‌ها.

سومین مجموعه حسگر، وب‌سایت‌های تحلیلی می‌باشد. این مجموعه حسگر دارای پنج حسگر می‌باشد، که عبارتند از: DDoSInfo، neuster، prolexic، Riorey، Radware

به‌دلیل انعکاس اخبار حملات در خود وب‌سایت قربانی حملات، یکی از مجموعه حسگرها خود این وب‌سایت‌ها انتخاب شده است. قاعدتا این مجموعه حسگر دارای یک حسگر می‌باشد. بنابراین چهارمین حسگر خود وب‌سایت قربانی حملات می‌باشد.

پنجمین مجموعه حسگر، عوامل انسانی می‌باشد. چهار نفر از نقاط مختلف دنیا به وب‌سایت قربانی حملات وصل شده و وضعیت آن را مشخص و ذخیره نموده‌اند.

منبع دوم تهیه و تامین داده‌ها، مقالات می‌باشد. نوشته‌ها و مقالات [۸ و ۳۱-۲۸] حاوی داده‌هایی بودند که در این تحقیق از آنها استفاده شد.

در نهایت با توجه به مطالعات صورت گرفته و با توجه به قالب ورودی داده‌ها جهت شبیه‌سازی، نواقصات بخش‌های قبل با تولید داده، برطرف گردید. جهت ارزیابی نیاز به داده خطادار می‌باشد. در این بخش داده‌های خطادار نیز تولید شد.

بر اساس مطالعات و پژوهش‌های صورت گرفته، حمله موفق و مشهوری که در این چند سال اخیر رخ داد و در منابع آشکار انعکاس قابل ملاحظه‌ای پیدا کرد، مجموعه حملات موسوم به ابابیل بود. این حملات در سال‌های ۲۰۱۲ و ۲۰۱۳ رخ داده است. نتایج فعالیت‌های صورت گرفته در جدول (۵) آورده شده است.

۶-۲- مبنا و معیار مقایسه

با توجه به داده‌های جمع‌آوری شده، ابتدا مقادیر شاخص‌های سه‌گانه ارزیابی میزان اثربخشی حملات DDoS یعنی CL،DT و FL براساس قوانینی که در جدول (۲) تعریف شده و براساس بازه‌های تعریف شده، تعیین می‌گردد. سپس وضعیت وب‌سایت قربانی مشخص می‌گردد.

جدول (۵). مجموعه داده مورد آزمون

ردیف	شماره قانون	وضعیت وب‌سایت	مشتریان از دست رفته	پایین بودن وب سایت	خسارت اقتصادی	مشتریان از دست رفته خطادار	پایین بودن وب سایت خطادار	خسارت اقتصادی خطادار	نتایج روش کلاسیک	نتایج روش فازی
۱	۹	۲	۳/۸۸۷	۱۹/۵۳۶	۵۵۰۲۲/۵	۳۲/۹۵	۱۶/۱۲	۴۸۲۷۷/۳	۳	۰/۸۲۸
۲	۹	۲	۶/۳۱۰	۲۷/۴۵۴	۵۰۲۹۴/۵	۰/۱	۱۷/۲۲	۵۳۷۴۸/۹	۲	۰/۵
۳	۹	۲	۵/۸۶۱	۲۰/۱۹۲	۹۶۵۴۸/۹	۰/۱	۲۹	۹۶۰۶۹/۷	۲	۰/۵
۴	۹	۲	۶/۹۶۱	۲۳/۵۴۱	۷۴۱۷۷/۶	۰/۱	۲۱/۲۸	۶۸۴۰۴/۲	۲	۰/۵
۵	۹	۲	۹/۲۶۷	۱۵/۵۳۷	۹۷۰۹۸/۷	۰/۱	۲۰/۳۳	۹۳۲۳۴/۹	۲	۰/۵
۶	۹	۲	۹/۴۸۲	۲۷/۷۰۲	۹۳۰۹۵/۴	۹۹	۲۷/۶۶	۹۳۷۲۷/۵	۳	۰/۸۰۵
۷	۸	۲	۰/۸۲۱	۲۷/۵۶۷	۴۴۷۰۴/۴	۰/۱	۳/۶۹	۳۷۳۴۷/۲	۱	۰/۴۴۵
۸	۸	۲	۱/۱۳۸	۱۶/۶۷۰	۱۸۷۷۶/۲	۰/۱	۲۲/۴۳	۸۸۳۷/۰۷	۳	۰/۸۰۵
۹	...	...	....	....	....	....	....	....	....	....
۲۹۹۸	۱	۱	۲/۲۷۲	۲/۷۳۱	۱۰۵۷۷/۳	۱۶/۹۶۹	۰/۱	۲۰۴۸/۲	۲	۰/۵
۲۹۹۹	۱	۱	۵/۵۳۳	۱/۳۵۳	۱۰۶۲۳/۹	۰/۱	۰/۱	۱۳۲۰۹/۲	۱	۰/۱۹۵
۳۰۰۰	۱	۱	۷/۰۴۱	۳/۵۱۷	۳۷۱۰/۴	۰/۱	۰/۱	۰/۱	۱	۰/۱۹۵
۳۰۰۱	۱	۱	۸/۰۶۹	۰/۸۹۷	۱۰۳۹۶/۵	۰/۱	۱/۲	۱۲۹۴۲/۹	۱	۰/۱۹۵
۳۰۰۲	۱	۱	۰/۶۷۴	۳/۶۲۵	۶۳۲۱/۵	۹۹	۱۸/۳۰	۱۴۴۴/۷	۳	۰/۸۰۵
۳۰۰۳	۱	۱	۹/۶۷۳	۴/۷۸۱	۶۱۵۲/۲	۰/۸۲۳	۰/۱	۱۳۲۹۴/۳	۱	۰/۱۹۳

دو حالت مبنا جهت مقایسه در نظر گرفته شده است: ۱- با تولید نویز و ایجاد خطا به داده‌هایی که از قبل وضعیت خروجی‌اش معلوم است، تا آن حدی که منجر به تغییر وضعیت وب‌سایت نگردد. ۲- با تولید و و ایجاد خطا به داده‌های مبنا تا اندازه‌ای که منجر به تغییر وضعیت وب‌سایت گردد. اگر خروجی یکی از روش‌ها در حالت ۱ مغایر با وضعیت وب‌سایت گردد، آن‌گاه روش مذکور دچار خطا شده است. درغیر این‌صورت درست تشخیص داده شده است.

در حالت ۲ اگر مقادیر یکی از روش‌ها مغایر با خروجی وب‌سایت، باشد آن روش درست تشخیص داده است در غیر این‌صورت با خطا مواجه شده است.

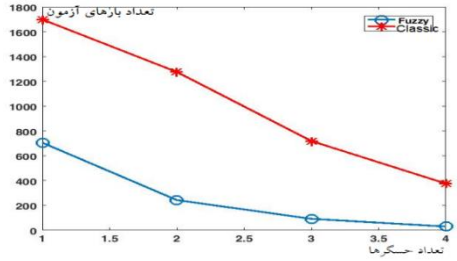
۶-۳- شاخص‌های ارزیابی

با توجه به ماهیت روش‌های فازی و کلاسیک، شاخص‌های میزان خطا و سرعت جهت ارزیابی این دو روش انتخاب گردید. شاخص میزان خطا بیانگر تعداد خطاهایی است که براساس مبنای تعریف شده در یکی از روش‌های کلاسیک و فازی رخ می‌دهد.

زمان پردازش هر دو روش در محیط شبیه‌سازی شده اندازه‌گیری شد. لذا از طریق به‌دست آوردن زمان پردازش دو الگوریتم، شاخص ارزیابی سرعت در هر دو روش اندازه‌گیری و مقایسه می‌گردد.

۶-۴- تحلیل نتایج

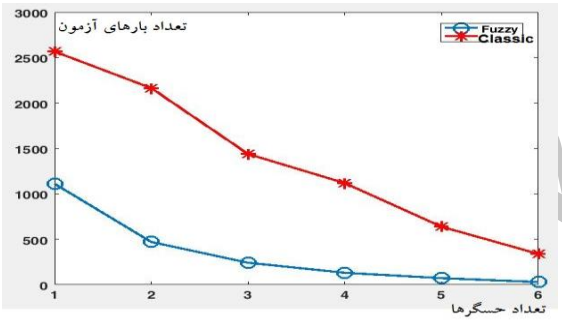
جهت استنتاج دقیق ارزیابی علاوه بر داده‌های مورد بحث در بخش ۱-۷، در خود نرم‌افزار متلب بصورت تصادفی، داده تولید شد. با استفاده از تابع rand در نرم‌افزار متلب و با استفاده از بازه‌های مقادیر شاخص‌ها که با مطالعه داده‌های مشابه به‌دست آمده، مقادیر تصادفی تولید شده است. به‌عنوان مثال در جدول (۴) به تعداد ۳۰۰۰ رکورد داده تولید شد. میزان خطای رخ داده شده در هر دو روش توسط نرم‌افزار متلب در قالب نمودار که در شکل (۱۳) نمایش داده شده، استخراج شد. با توجه به خصوصیات مجموعه‌های فازی در مقابل مجموعه‌های کلاسیک می‌توان گفت که اولا مرز مشخصی برای اعداد وجود ندارند و میزان تعلق هر عدد به یک مجموعه با تابع عضویت تعیین می‌شود، ثانیا تطابق بیشتر با طبیعت واقعی حوادث دارند و ثالثا امکان توصیف کامل علوم نادقیق و بطورکلی عدم‌قطعیت‌ها وجود دارد، لذا با توجه به شکل (۱۳) مدل فازی دقت بسیار زیادی از اندازه‌گیری پارامترهای طبیعی که دارای رفتارهای پیچیده هستند، به‌دست می‌دهد.



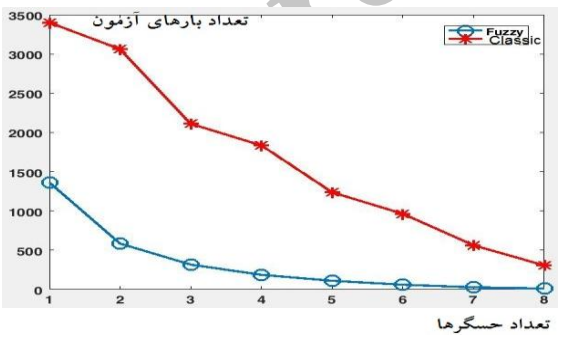
شکل (۱۳). میزان خطا در چهار جسگر

علاوه بر این‌که میزان خطای فازی که با خط آبی نمایش داده شده، نسبت به میزان خطای روش کلاسیک که با خط قرمز نشان داده شده است، کمتر است. با افزایش تعداد جسگرها میزان خطا در هر دو روش سیر نزولی دارد.

از طرفی با توجه به شکل‌های (۱۵-۱۴) با افزایش تعداد جسگرها اختلاف میزان خطای دو روش فازی و کلاسیک کاهش می‌یابد. این وضعیت بیانگر آن است که در حالتی که تعداد جسگرها زیاد است و اختلاف خطا برای متولیان زیاد مهم نیست، می‌توان به اختیار از هرکدام از روش‌های کلاسیک و فازی استفاده نمود.



شکل (۱۴). میزان خطا در شش جسگر



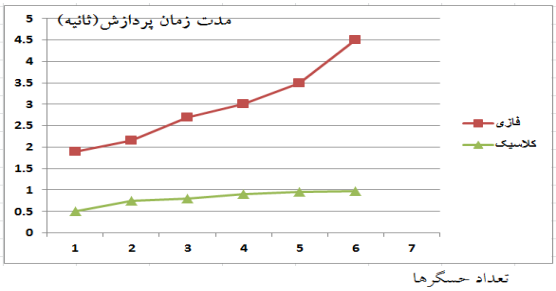
شکل (۱۵). میزان خطا در هشت جسگر

با توجه به شکل‌های (۱۵-۱۳) و ادامه آن برای تعداد جسگرهای زیادتر در محیط شبیه‌سازی متلب یک نتیجه جالبی بدست آمد. این نتیجه عبارت است از این‌که نمودار خطا در روش فازی را به سهولت می‌توان با عبارت ریاضی مدل نمود. اشکال فوق و ادامه آنها بسیار شبیه و نزدیک نمودار معادله زیر می‌باشد:

$$f(s) = Be^{-ks} \qquad (۱۶)$$

در معادله فوق، متغیر s بیانگر حسگر و $f(s)$ تعداد خطای رخ داده در حالت فازی می‌باشد. مقادیر ثابت B و k ثابت و مثبت هستند. عدد B محل تلاقی نمودار با محور تعداد خطا یا همان $f(s)$ می‌باشد. این تابع مشهور به تابع طبیعی نزولی زنگوله‌دار است.

شاخص ارزیابی دیگری که مورد بحث این نوشته است، سرعت پردازش دو روش کلاسیک و فازی می‌باشد. با اندازه‌گیری مدت زمان پردازش هر دو روش با افزایش تعداد حسگرها نمودار شکل (۱۶) استخراج شد.



شکل (۱۶). مدت زمان پردازش

با توجه به نمودار شکل (۱۶)، مدت زمان پردازش فازی به مراتب بیشتر از کلاسیک می‌باشد. همچنین با افزایش تعداد حسگرها مدت زمان پردازش فازی به صورت نمایی زیاد می‌شود، در حالیکه در روش کلاسیک به صورت نزدیک به خطی مدت زمان افزایش می‌یابد. لذا نتیجه می‌گیریم روش فازی برای حالت‌هایی که نیاز فوری به اندازه‌گیری پاسخ میزان اثربخشی نیست، مناسب می‌باشد. البته با افزایش ظرفیت پردازشی به‌صورت سخت‌افزاری می‌توان بر این نقیصه فائق آمد.

۷- نتیجه‌گیری

تلفیق منطق فازی، دلفی فازی و چندحسگری این امکان را می‌دهد که با اطمینان بیشتری نسبت به تعیین مقادیر پرداخته شده و مقادیر خود را نه فقط به‌صورت یک ارزش یا مقدار صریح بلکه به صورت بازه‌ای از مقادیر بیان کرد.

روش ارائه‌شده در این پژوهش، یک چارچوب منسجم و یکپارچه‌ای را فراهم می‌کند که باعث پیوند قابلیت‌های عملیات تاثیرمحور با ماهیت عدم قطعیتی فضای سایبری می‌گردد. از مزیت روش ارائه شده نسبت به روش‌های قبلی، می‌توان به موارد ذیل اشاره کرد: در پژوهش‌های پیشین اغلب رویکرد آزمایشگاهی اتخاذ شده بود، و این درحالی است که در این پژوهش با بهره‌گیری از رویکرد چندحسگری، به‌صورت شبیه‌سازی عمل شده است. روش‌های پیشین عمدتا به فضای تاثیرات به طور یک‌بعدی که همان اندازه‌گیری اثرفناورانه است، پرداخته است. در حالی‌که روش ارائه شده در این پژوهش ابعاد فضای تاثیرات سه‌بعدی در نظر گرفته است. در عین حال به‌دلیل منعطف و جامع بودن معماری ارائه‌شده در این پژوهش گسترش ابعاد فضای تاثیرات به‌صورت دلخواه وجود دارد.

در رابطه با موضوع این مقاله پنج حوزه قابل تحقیق در آینده پیشنهاد می‌گردد: اول اینکه این پژوهش مقدمه پژوهشی با عنوان "ارائه مدل پیامدسنجی عملیات سایبری" می‌باشد، لذا پیشنهاد می‌گردد تحقیق یا مجموعه تحقیقات گسترده‌ای در این زمینه صورت گیرد. دوم این‌که این مدل ارائه شده مختص حملات DDoS ارائه شده است، لذا می‌توان برای تک‌تک انواع دیگر حملات سایبری مدل خاص آن حمله را ارائه داد. سوم: با توجه به این‌که مجموعه حسگرهای آورده شده در نمودار دارای ارزش‌ها و وزن‌های اعتباری هستند، به عنوان حوزه پنجم فعالیتی مرتبط با موضوع این مقاله، می‌توان با استفاده از الگوریتم‌های آموزش‌پذیر از قبیل رگرسیون و غیره می‌توان به‌همراه روش‌هایی ازقبیل داده‌کاوی و نظرات خبرگان میزان وزن و ارزش دقیق نسبی حسگرها را به‌دست آورد. ۱- تاثیر پارامتر میزان خسارت اقتصادی و میزان مشتریان ناراضی بر میزان اثربخشی حملات زیاد بوده و لذا با وارد کردن آن در تخمین و بازسازی داده‌ها می‌توان از میزان خطا در اندازه‌گیری داده‌های مفقود کاست. ۲- می‌توان برای تخمین و بازسازی داده‌هایی که تحت تاثیر چند پارامتر می‌باشد، از مدل فازی استفاده نمود.

۸- مراجع

[1] "https://www.akamai.com/us/en/resources/ddos.jsp" *2015*.

[2] "http://www8.hp.com/emea_middle_east/ar/home.html" "https://www.symantec.com/solutions/financial-services"

[3] Hp-ponemon, "Hewlett-Packard," *2014*.

[4] J. Mirkovic, "D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks," Ph.D Thesis,

[5] "http://www.prolexic.com/resources/ddos.jsp," 2013.

[6] T. Ross and j. Wiley, "Fuzzy Logic with Engineering Application," The Atrium, Southern Gate, Chichester, West Sussex, vol. United Kingdom, 2005.

[7] C. Hsue, "Evaluating the Best Main Battle Tank Using Fuzzy Decision Theory with Linguistic Criteria Evaluation," European Journal Of Operational Research, vol. 142, 2002.

[8] X. Peng Su and H. Tang, "DoS Attack Impact Assessment based on 3GPP QoS Indexes," Institute of Electronic Technology, The PLA Information Engineering University, P. R. China, 2008.

[9] P. Mirkovic, S. Fahmy, R. Thomas, A. Hussain, and S. Schwab, "Measuring Impact of denial Of service," 2nd ACM workshop on Quality of protection QoP, pp. 53 - 58, 2006.

[10] S. Kumar, M. Sachdeva, and K. Kumar, "Flooding based DDoS attacks and their influence on web services," International Journal of Computer Science and Information Technology, vol. 2, no. 3, pp. 1131-1136, 2011.

[11] K. Kumar, "Protection from Distributed Denial of Service (DDoS) Attacks in ISP Domain," Indian Institute of Technology, Roorkee, 2007.

[12] J. Mirkovic, B. Wilson, S. Fahmy, P. Reiher, R Thomas, W. Yao, and S. Schwab, "Towards user-centric metrics for denial-of-service measurement," In proceedings of the workshop on Experimental computer science, San Diego, California, 2007.

[13] S. Schwab, R. Thomas, and B. Wilson, "Towards systematic IDS evaluation," In Proceedings of DETER Community Workshop, pp. 20-23, June 2006.

[14] C. Joshi, "An Integrated Honeypot Framework for Proactive Detection, Characterization and Redirection of DDoS Attacks at ISP level," International Journal of Information Assurance and Security (JIAS), vol. 3, no. 1, pp. 1-15, March 2008.

[15] B. Gupta and M. Misra, "An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach," Journal of Information Assurance and Security, vol. 3, no. 2, pp. 102-110, June 2008.

[16] W. T. Dubendorfer and B. Plattner, "An economic damage model for large-scale Internet attacks," In 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, vol. IEEE Comput. Soc., pp. 223-228, 2004.

[17] D. Merwe, "MIDAS: An Impact Scale for DDoS attacks," 15th IEEE Workshop on Local & Metropolitan Area Networks, pp. 200–205, 2007.

[18] V. Raja, S. Reddy Gade, and S. Kumar, "Performance of Win-dows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," In Fourth International Conference on Digital Society, pp. 188-191, IEEE, February 2010, 2010.

[19] F. Roman Chertov and B. Shroff, "Emulation versus Simula-tion: A Case Study TCP-Targeted Denial of Service Attacks," 2nd International Conference on Testbeds and Research Infrastructures for the Development of Net-works and Communities, pp. 316–325, 2006.

[20] I. Traore, "Queue-based analysis of DoS attacks," In Information Assurance Workshop, IAW'05, pp. 266-273 2005.

[21] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoid-ance," IEEE/ACM Transactions on Networking, vol. 1, no. 4, pp. 397-413, 1993.

[22] H. Alefiya Hussain and C. Papadopoulos, "A framework for classi-fying denial of service attacks," In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications- SIGCOMM New York, USA ACM Press, p. 99, 2003.

[23] H. Jelena Mirkovic, S. Fahmy, P. Reiher, and R. Thomas, "Accurately Measuring Denial of Service in Simulation and Testbed Experiments," IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 2, pp. 81-95, April 2009.

[24] G. Monika Sachdeva and K. Kumar, "An emulation based impact analysis of DDoS attacks on web services during flash events," 2nd International Conference on Computer and Communication Technology (ICCCT-2011), pp. 479-484, 2011.

[25] K. Monika Sachdeva, G. Singh, and K. Singh, "Performance Analysis of Web Service under DDoS Attacks," IEEE International Advance Computing Conference, number March, pp. 1002-1007, 2009.

[26] "https://www.neustar.biz/security/ddos-protection", 2012.

[27] H. Builder and C. Nordin, "Alternative Models of Command and Control," In: Command Concepts: A Theory Derived from the Practice of Command and Control, Rand Corp., 1999.

[28] K. Monika Sachdeva, G. Singh, and K. Singh, "Performance Analysis of Web Service under DDoS Attacks," IEEE International Advance Computing Conference (IACC 2009), March 2009.

[29] C. Rither, "Predicting the Impact of Denial of Service Attacks," Department of Electrical and Computer Engineering, THESIS: Degree of Master of Science, Air University, Ohio, 2012.

[30] G. Monika Sachdeva, K. Kumar1, and K. Singh, "Measuring Impact of DDOS Attacks on Web Services," Information Assurance and Security, 2010.

[31] H. Teodor Sommestad and M. Ekstedt, "Estimates of success rates of Denial-of-Service attacks," Royal Institute of Technology (KTH), 2011.

Model of Fuzzy Evaluation of the Effectiveness of the Distributed Denial of Service Attacks, Based on Open Source

A. Ghasemzadeh, M. Gayoori Sales*

*Imam Hossein University

(Received: 27/01/2016, Accepted: 31/10/2016)

ABSTRACT

Cyber operations, which the operation of distributed denial of service (DDoS) are the most important type of impact can cause a variety of effects. Measuring the success of a cyber-attack is hard; because of the complexity of the effects of the attacks have conditions like high uncertainty, widespread and nonlinear relationship between power and efficiency of operations with the effects of their condition. Generally to overcome the above challenges of integrating data from multiple sensors are used. In the operations, the sensors are divided into two types: Open and Closed sensor, but sensors detected in cyberspace are more important. In this study a suitable mechanism is designed to measure the success of DDoS attacks. For feedback and measure the ultimate effect of the DDoS, from open sources as sensors and receive the effects of this type of operation is used. The data open sources close to linguistically and also expressed as a range imprecise and fuzzy method so that one of the best ways of solving problems is uncertainty been used. The weighted fuzzy logic and fuzzy Delphi sensors have been used simultaneously for data integration.

Keywords: Cyber Operations, DDoS Attacks, Effects Of Attacks, Fuzzy Inference

* Corresponding Author Email: ghayoori@ihu.ac.ir