مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۳، پاییز ۱۳۹۶، ص ۱۰۹-۹۵

ارائه چارچوب تخمین وضعیت در حملات منع خدمت توزیع‌شده با تلفیق اطلاعات حسگرهای فنی و بشری مبتنی بر منطق فازی

حمید اکبری[۱]، سیدمصطفی صفوی همامی[۲*]

۱- دانشجوی دکتری، دانشگاه جامع امام حسین (ع) ۲- دانشیار، دانشگاه صنعتی امیر کبیر

(دریافت: ۹۵/۱۰/۰۳، پذیرش: ۹۵/۱۱/۲۵)

چکیده

مهاجمین سایبری قادرند با استفاده از حملات جلوگیری از خدمت توزیع‌شده، تأثیرات بسزایی بر میزبان‌های شبکه رایانه‌ای بگذارند و در مقابل مدافعین با استفاده از انواع روش‌های دفاعی به دفاع می‌پردازند. در چنین شرایطی تعیین وضعیت شبکه قربانی سخت و پیچیده است. جهت ارزیابی وضعیت صحنه نبرد سایبری، ضروری است مهاجم و مدافع مورد ارزیابی قرار گیرند که تمرکز این مقاله در ارائه چارچوبی است که وضعیت قربانی را مورد ارزیابی قرار دهد. در این تحقیق رصد قربانی با استفاده از انواع حسگرهای سایبری اعم از فنی و بشری مورد مدل‌سازی و شبیه‌سازی قرارگرفته است. در ابتدا حسگرهای فضای سایبری مانند سایت‌های خبری، شبکه‌های اجتماعی و گزارش‌های مردمی و حسگر دیده‌بانی فنی مورد بررسی قرار گرفته و خصیصه‌های هر یک احصاء شده و درنهایت اهمیت هر یک با استفاده ازنظر خبرگان با استفاده از روش فرآیند تحلیل سلسله مراتبی، ارزش‌گذاری شده است. سپس ترکیبی از خصیصه‌ها را برای هریک از حسگرها تشکیل داده و وضعیت‌های قربانی را نسبت به آن تعیین کرده‌ایم. شرایط تلفیق اطلاعات با استفاده از روش دسته‌بندی براساس منطق فازی مهیا می‌گردد. با اجرای سه سناریو نشان داده شد که طرح فوق دارای کارایی مطلوب است. در سناریوی اول که حمله‌ای در کار نبوده است، تلفیق حسگرها با احتمال ۹۹/۳٪ و در سناریوی دوم که سرور قادر به خدمات‌رسانی به‌صورت کند بوده و تحت فشار است تلفیق حسگرها با احتمال ۷۸/۶٪ و در سناریوی سوم که سرور تحت حمله مؤثر قرار دارد تلفیق حسگرها با احتمال ۸۴/۲٪ بوده است وضعیت‌های خدمت‌رسانی را درست تخمین زده‌اند. فقدان اطلاعات هر یک از حسگرها، شرایط عدم قطعیت را موجب می‌گردد که در این تحقیق با ۱۵ حالت مختلف مورد ارزیابی قرارگرفته است. نتایج به‌دست‌آمده، نشان داد که روش پیشنهادی برای آگاهی از وضعیت میزبان تحت حمله، قابلیت ارزیابی را دارد.

واژه‌های کلیدی: حملات منع خدمت توزیع‌شده، تلفیق اطلاعات، دسته‌بندی براساس منطق فازی، شبکه حسگری سایبری، عدم قطعیت.

۱- مقدمه [۱]

امروزه حملات منع خدمت توزیع‌شده[1] معروف به DDoS، نقش اثرگذاری در جنگ سایبری دارد و یکی از مهم‌ترین تهدیدات مخرب محسوب می‌شود. صحنه نبرد سایبری متشکل از عناصر مهاجم سایبری، مدافع سایبری و بهره‌برداران در فضای سایبری است. به‌منظور ارزیابی این صحنه نبرد باید این فضا به‌خوبی ترسیم شود. از این‌رو، در این تحقیق درصدد هستیم تا چنین صحنه‌ای را مهندسی و ابعاد نهفته آن را روشن کرده و مورد تجزیه و تحلیل قرار دهیم. بدیهی است که نتیجه چنین ارزیابی موجب آگاهی مطلوب از وضعیت گردد. بنابراین، حسگرها یا دیده‌بان‌ها (فنی و بشری) یکی از ارکان مهم تأثیرگذار در آگاهی از وضعیت صحنه نبرد است. به‌طوری‌که بیش از ۶۵٪ خطاها مربوط به این بخش می‌باشند [۱]. مهم‌ترین علل این خطاها مربوط به خرابی حسگرها، تمهیدات دفاعی مانند مسدودسازی[2] و عوامل ناشناخته دیگر است که عدم قطعیت را موجب می‌گردد. بدیهی است دسترسی به منابع قربانی، بزرگ‌راه‌های ارتباطی می‌تواند در کاهش عدم قطعیت بسیار مؤثر باشد، در این تحقیق به منابعی که آثار این حملات را منعکس می‌کنند پرداخته و سپس تلاش می‌شود با تلفیق اطلاعات این منابع، موجب کاهش عدم قطعیت شد. در این مقاله در ابتدا کارهای انجام‌شده مرور می‌گردد و سپس مفاهیم و تعاریف، طرح پیشنهادی، احصای ویژگی‌های حسگرها و تلفیق آن‌ها پرداخته و در ادامه به مدل‌سازی و شبیه‌سازی و ارزیابی نتایج حاصله پرداخته می‌شود.

* رایانامه نویسنده مسئول: msafavi@aut.ac.ir

1- Distributed Denial of Service (DDoS)

2 - Filtering

۲- کارهای مرتبط

در حال حاضر، رصد حملات DDoS که به‌وسیله شبکه بات انجام می‌گیرد، با استفاده از دسترسی به مسیریاب‌های اصلی و بین‌المللی توسط صاحبان فن‌آوری و نیز توسط مالکان خدمات‌دهنده (قربانی) صورت می‌گیرد [۲]. لیکن این دسترسی نمی‌تواند توسط دیگران مورد استفاده قرار بگیرد. راه دیگر این‌که رصد قربانی با استفاده از شبکه دیده‌بانی صورت می‌گیرد که دیده‌بان‌ها مبادرت به اندازه‌گیری پاسخ زمانی خدمات قربانی و DNS[1] و سرعت انتقال اطلاعات می‌کنند که با توجه به خرابی حسگرها و احتمال وجود مسدودسازی در مسیر دیده‌بان‌ها شرایط عدم قطعیت به‌وجود می‌آید و اندازه‌گیری‌ها کم‌دقت می‌شوند [۳]. آثار این روش‌ها را می‌توان در برخی از سایت‌های مانیتورینگ معتبر مانند www.24x7.com ملاحظه نمود و شاهد بی‌دقتی‌های آن بود [۴]. در مقاله [۵،] آقای بن‌وارت[2] ادعا کرده که می‌توان از راه دور بدون نصب ابزاری در ماشین قربانی، مبادرت به اندازه‌گیری اثر حمله DDoS کرد. او در محیط آزمایشگاه نشان داد که حمله فلش‌کرود[3] بر روی دو معیار گذردهی مفید (داخلی) و زمان رفت و برگشت درخواست (خارجی) تأثیرگذار است و ضریب هم‌بستگی مثبتی بین آن‌ها وجود دارد. در مقاله [۶] آقای ولزل[4] و همکاران سرورهای فرماندهی و کنترل ۱۴ شبکه بات DIRTJUMPER و YODDS را مورد مانیتورینگ قرار داده و توانسته‌اند اهداف مورد حمله DDoS را روی شبکه فوق ضبط کنند. سپس آن‌ها با استفاده از انواع اندازه‌گیری‌ها ازقبیل زمان پاسخ TCP[5] و تحلیل محتوای HTTP[6] توانستند دسترس‌پذیری قربانی‌ها را ارزیابی کنند. آن‌ها نشان دادند که بیش از ۶۵٪ قربانی‌ها توسط حملات DDoS، به‌شدت آسیب‌پذیر هستند و حملات کم‌تری به شکست منجر می‌شوند. در مقاله پیش‌بینی حملات منع خدمات [۵]، نویسنده مبادرت به جمع‌آوری انواع معیارهای تأثیرگذار و پیامدها بر این نوع حملات داشته است. معیارهایی هم‌چون محاسبه هزینه خسارت، افت کیفیت خدمات، بازدهی تراکنش، تأخیر در خدمات و ... به چشم می‌خورد. یکی از معیارهای مورد ارزیابی، مربوط به کاهش کیفیت خدمات است که مورد توجه مهاجمان حملات منع خدمات است. راهنمای استانداردهای موجود برای پاسخ زمانی ایده‌آل صفحات وب عبارت‌اند از: [۱۹] یک‌دهم ثانیه، زمان ایده‌آل پاسخ کاربر که هیچ‌گونه تأخیری را حس نمی‌کند. یک ثانیه، حداکثر زمان قابل قبول است که زمان دانلود بیش از یک ثانیه کاربر را خسته می‌کند. ده ثانیه، زمان غیرقابل قبول که کاربر خسته شده و دوست دارد سایت را ترک کند. این اعداد برای طراحی ظرفیت سرور کاربرد زیادی دارند.

آقای شان[7] و همکاران [۸]، درصدد ارائه آگاهی وضعیتی دفاع سایبری هستند که بتوانند در لایه صفر ادغام با دریافت داده‌های هشداری از حسگرهای تشخیص نفوذ[8] و جلوگیری از نفوذ[9] و وقایع ثبت‌شده سامانه‌ی[10]، آن‌ها را مورد پالایش قرار دهند و در لایه یک، به ارزیابی هدف (شیء) پرداخته و در لایه‌های دوم و سوم با استفاده از مدل بازی مارکوف و مجموع موجودیت‌های سلسله مراتبی به ارزیابی وضعیت‌ها و تهدیدها دست یابند. ایشان روش بازی مارکوف را به‌منظور تخمین و باورپذیری هریک از الگوهای حملات سایبری مورد استفاده قرار داد. اشکال این روش این است که این آگاهی وضعیتی بر روی ماشین‌های قربانی قابل حصول است و از منظر دیده‌بانی قابل بهره‌برداری نیست. هم‌چنین آقای پنگ[11] و همکاران [۹] برای ارزیابی تأثیر حمله منع خدمت، شاخص‌هایی هم‌چون مصارف پهنای باند، پردازش، حافظه، تأخیر زمان پاسخ، گم‌شدن بسته، زمان (موردنیاز) بازیابی، روش‌های حمله (مصرف منابع، از کارانداختن خدمت و از کارانداختن سامانه) را در قالب یک ماتریس درآورده و تأثیر ده نوع حمله شبیه‌سازی‌شده را با استفاده از خوشه‌بندی ترکیبی خاکستری مورد ارزیابی قرار دادند و توانستند حملات ده‌گانه را به چهار دسته ضعیف، معمولی، خوب و خیلی‌خوب تقسیم نمایند. اشکال این روش آن است که نمی‌توان شاخص‌های فوق را (به‌جز تأخیر زمان) بدون همکاری از ماشین قربانی به‌دست آورد.

آقای ژانگ[12] و همکاران [۱۰] تلاش کرده‌اند از یک روش تلفیق داده چندمنبعی (حسگر) برای ارزیابی تأثیر حمله منع خدمت استفاده کنند. آن‌ها با استفاده از تعدادی ماشین در نقاط مختلف شبکه مبادرت به اندازه‌گیری پاسخ تأخیر زمانی ماشین قربانی کرده و داده‌های جمع‌آوری‌شده را بعد از پالایش، مورد ادغام قرار داده و سپس با استفاده از محاسبه آنتروپی (تأخیر قبل و بعد از حمله) به ارزیابی حمله پرداخته است. اشکال روش ژانگ

1- Domain Name System
2- Bannwart
3- Flash Crowd Attack
4- Welzel
5- Transmission Control Protocol
6- HyperText Transfer Protocol

7- Shen
8- Intrusion Detection Sensors (IDS)
9- Intrusion Prevention Sensors (IPS)
10- System logs
11- Peng
12- Zhang

زمانی آشکار می‌شود که تمامی حسگرها در معرض مسدودسازی قرار گرفته و ارزیابی نادرستی را از وضعیت قربانی ارائه می‌دهند. لذا روش پیشنهادی نویسنده، بهره‌مندی از حسگرهای بشری و به‌دست‌آوردن نتایج دقیق‌تری از وضعیت تأثیر حمله بر قربانی می‌باشد.

۲-۱- مفاهیم و تعاریف

حمله منع خدمت: تلاش برای از کارانداختن سامانه کاربر یا یک سازمان است. در حمله منع خدمت، مهاجم تلاش می‌کند تا سامانه‌ای را از حالت پایدار خارج کند و یا سرعت آن را به‌شدت کاهش دهد و کاربران نتوانند از منابع آن استفاده کنند. هدف از این حمله، این نیست که به سامانه یا داده‌های هدف دسترسی پیدا کنند، بلکه هدف این است که اجازه خدمت‌رسانی به کاربران قانونی را بگیرند. حملات **DDoS**، نوع پیشرفته‌ای از حملات **DoS** ساده است [۷]. به‌طورکلی می‌توان شدت اثر حمله را به دو دسته انسداد[1] و کاهش[2] خدمت دسته‌بندی کرد [۲، ۴ و ۱۱].

وضعیت‌های به‌وجودآمده برای یک خدمات‌دهنده که در مقام یک میزبان (قربانی) ممکن است مورد حمله قرار بگیرد، شامل: وضعیت خدمت‌رسانی خوب یا قابل قبول (حیثیتی)، وضعیت خدمت‌رسانی وخیم و درنهایت وضعیت قطع خدمت‌رسانی است که با توجه به معیار [۷] تبیین شده است.

دیده‌بانی: به‌منظور نظارت بر وضعیت خدمات ارائه‌شده از سوی میزبان‌های شبکه، نیاز است آن‌ها همواره مورد رصد دیده‌بان‌های فنی مستقل شبکه قرار بگیرند. در این‌جا دسترس‌پذیری خدمات، کیفیت خدمات[3] (زمان پاسخ) و .. انتظاراتی است که از دیده‌بانی فنی باید حاصل کرد.

تلفیق داده: فرآیندی است جهت ترکیب و تجمیع اطلاعات از منابع مختلف که درنتیجه آن دید جامع و دقیقی از محیط مورد نظر به‌دست خواهد آمد. به‌طورکلی در تلفیق داده‌ها، اطلاعات از یک یا چند منبع ورودی وارد می‌شوند و بعد از پالایش و تجزیه تحلیل اطلاعات نتیجه را به‌صورت برآیند داده‌ها نشان می‌دهد [۱۳-۱۲]. در حال حاضر روش‌ها و الگوریتم‌های به‌کار گرفته‌شده در تلفیق داده‌ها در سه دسته کلی شامل روش‌های مبتنی بر تخمین، کلاس‌بندی و قواعد تقسیم می‌شوند که می‌توان آن‌ها را در شکل (۱) ملاحظه نمود [۱۴].

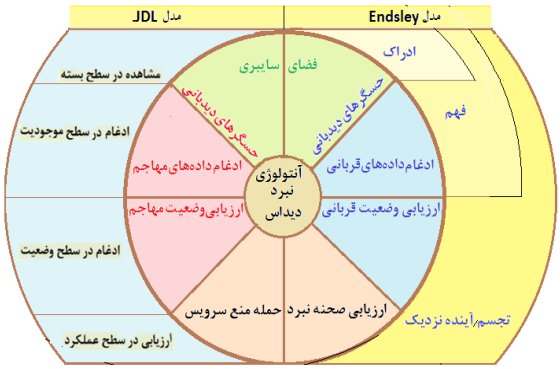
در طرح پیشنهادی این تحقیق، ترکیبی از روش‌های مبتنی بر کلاسه‌بندی و روش‌های مبتنی بر قواعد مورد استفاده قرار می‌گیرد.

شکل (۱): دسته‌بندی تلفیق داده براساس الگوریتم‌ها [۱۴]

منطق فازی: قادر است بسیاری از مفاهیم، متغیرها و سیستم‌هایی را که نادقیق و مبهم هستند (همان‌طورکه در عالم واقع نیز اکثراً چنین است) صورت‌بندی ریاضی کرده و زمینه را برای استدلال، استنتاج، کنترل و تصمیم‌گیری در شرایط عدم اطمینان، فراهم آورد. در سیستم‌های دارای عدم قطعیت زیاد و پیچیدگی‌های بالا، منطق فازی، روشی مناسب برای مدل‌سازی به شمار می‌رود.

۳- طرح پیشنهادی

حسگرها در فضای سایبری مبادرت به دیده‌بانی و رصد میزبان‌های خدمات‌دهنده (که قربانی مهاجم هستند) و شبکه بات مهاجم می‌کنند. در این میان، وجود یک هستان‌شناسی[4] کارآمد، تمامی بخش‌ها را پشتیبانی کرده و سؤال «چه کارهایی باید کرد؟» را پاسخ‌گو است [۱۵]. در حالت کلی، می‌توان ارزیابی وضعیت صحنه نبرد حمله DDoS را به‌صورت شکل (۲) متصور شد که سمت راست مربوط به قربانی و سمت چپ مربوط به مهاجم است. مدل پیشنهادی با مدل پنج لایه JDL[5] [۱۶] و مدل سه لایه آگاهی وضعیتی خانم اندسلی[6] [۱۷] دارای هم‌پوشانی است با این تفاوت که این مدل توسط یک هستان‌شناسی نبرد DDoS پشتیبانی می‌گردد.

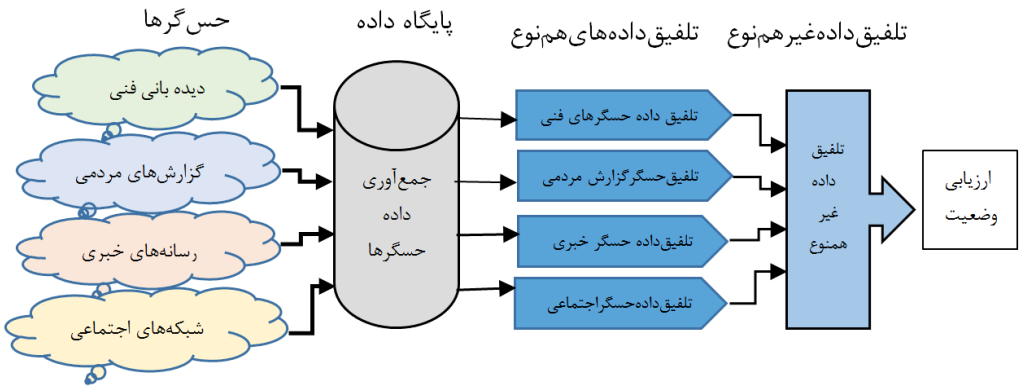


شکل (۲): شمای کلی طرح پیشنهادی ارزیابی صحنه نبرد حمله DDoS

1- Disruptive
2- Degrading
3- Quality of service (QoS)
4- Ontology
5- Joint Direction Literary
6- Endsley

هریک از طرفین درگیری بعد از انجام یک حمله، پیگیری خواهند کرد تا از وضعیت طرف مقابل آگاهی یابند و بدانند اثر حمله و دفاع آن‌ها به چه میزان بوده است. در صحنه جنگ‌های سایبری نیز به همین صورت است و حمله‌کننده تلاش خواهد کرد تا از وضعیت قربانی و اثر حمله خود مطلع شود تا بتواند تصمیمات مناسبی بگیرد. اما در این راستا مشکلات بسیاری وجود دارد، به‌عنوان‌مثال، ممکن است قربانی تمهیداتی درنظر گرفته و به‌کار بندد [۲۱] که حمله‌کننده را در مورد تأثیر حمله گمراه کند.

در طرح پیشنهادی با استفاده از حسگرهای فنی و بشری مبادرت به جمع‌آوری داده کرده و پس از چند مرحله تلفیق اطلاعات بتوان به ارزیابی وضعیت قربانی دست یافت که شکل (۳) نمای کلی از این طرح را نشان می‌دهد.



شکل (۳): شمای کلی از فرآیند ارزیابی وضعیت

در این طرح، اطلاعات حسگرهای هم نوع با یکدیگر تلفیق شده و در انتها نتایج ارزیابی هر یک از حسگرها با یکدیگر مورد تلفیق قرار می‌گیرند و ارزیابی نهایی را حاصل می‌کنند. در ادامه راجع به هریک از حسگرها و روش تلفیق و ارزیابی آن‌ها مطالبی ارائه می‌گردد.

۳-۱- بررسی نشانه‌ها در یک حمله واقعی

هنگامی‌که یک حمله منع خدمت صورت می‌گیرد، می‌توان آثار آن را در ابعاد گوناگون سیاسی، اقتصادی، اجتماعی به‌صورت نتایج و پیامدها ملاحظه کرد. اثر حمله به‌طور مستقیم در کمیت و کیفیت خدمت‌رسانی نمایان می‌گردد و متعاقب آن، بر روی ذی‌نفعان و خدمت‌گیرندگان اثر گذاشته و عکس‌العمل آن‌ها را از ابراز نارضایتی تا کاهش محبوبیت در پی خواهد داشت و مهم‌ترین پیامد آن بی‌اعتمادی و مهاجرت خدمت‌گیرندگان می‌باشد. با بررسی مهم‌ترین حملات منع خدمت در دنیا ملاحظه شد که این آثار در کلام مردم در شبکه‌های اجتماعی، سایت‌های خبری آنلاین و گزارش‌های مردمی به‌خوبی منعکس می‌گردد. به‌عنوان نمونه، حملاتی که در سال‌های ۲۰۱۲ و ۲۰۱۳ بر روی مؤسسات مالی و اعتباری صورت گرفته بود، انعکاس این حملات در صفحات اجتماعی فیس‌بوک و توئیتر قربانی‌ها (اعم از مدیران مؤسسات و مشتریان) مشاهده شد و در برخی سایت‌های معروف مانند سایت‌داون[1] (که گزارش‌های مردمی را منعکس می‌کردند) ملاحظه گردید. مشاهده این نظرات، ایده‌های بسیار خوبی چه ازنظر انتخاب حسگرها و چه ازنظر انتخاب نوع خصیصه‌های هر حسگر و دسته‌بندی آن در اختیار قرار داد. با مشاهده تعداد نظرات قبل از حمله و در هنگام حمله مشاهده شد که تعداد نظرات مردمی عاملی بسیار مهم است و این تعداد در هنگام اثر حمله نسبت به قبل از آن بسیار بیش‌تر است. هم‌چنین با مطالعه نظرات مردمی می‌توان متوجه شد که محتوای نظرات، ممکن است بسیار متفاوت باشد. کاربرانی ممکن است رضایت خود را از خدمت‌رسانی اعلام کنند، کاربرانی ممکن است با وجود اشاره به مشکلات، هم‌چنان از خدمت‌رسانی و نیز کاربرانی که بسیار خشمگین به انتقاد پرداخته و یا با زبانی ملتمسانه درخواست بهبود وضعیت را داشته باشند. در این تحقیق نیز بر همین اساس چه در حسگر نظرات مردمی و چه در حسگر شبکه‌های اجتماعی میزان رضایت کاربر به‌عنوان عاملی تعیین‌کننده در نظر گرفته شده است که ترکیب تعداد نظرات کاربران، می‌تواند گویای بسیاری از شرایط و نحوه تأثیر حمله باشد.

۳-۲- اصول و مبانی حسگرها

همان‌طورکه پیش از این نیز اشاره شد یکی از اهداف این طرح، درنظر گرفتن حسگرهایی است که براساس آن‌ها بتوان به اثر حملات DDoS پی برد. در ادامه به تعدادی از این حسگرها که در این طرح مورد استفاده قرارگرفته‌اند اشاره کرده و چگونگی رفتار آن‌ها شبیه‌سازی خواهد شد.

۳-۲-۱- دیده‌بانی کیفیت خدمت

دیده‌بانی از کیفیت خدمتی که قربانی ارائه می‌دهد را می‌توان به‌عنوان حسگر فنی برای سنجش تأثیر حمله درنظر گرفت و

1- https://sitedown.co

وضعیت قربانی را تخمین زد. در واقع این حسگرها در اقصی نقاط شبکه (برای بالابردن قابلیت اطمینان در برابر خرابی حسگرها و فیلترشدن برخی مسیرها) مستقر شده و مبادرت به رصد قربانی می‌کنند و هر یک تخمینی از وضعیت قربانی را احصاء کرده و با تلفیق داده‌های خود نسبت به وضعیت قربانی که در ادامه می‌آید، اعلام نظر می‌کنند.

۳-۲-۲- وضعیت کیفیت خدمت‌رسانی (تأخیر در پاسخ به خدمت):

حملات DDoS بر روی خدمات‌دهندگان، موجب قطع یا اختلال در کیفیت خدمت‌رسانی می‌شود. یکی از عوامل اثرگذار، ایجاد تأخیر در خدمت‌رسانی می‌باشد که نتیجه آن کاهش دسترسی کاربران مجاز به خدمت مورد نیاز است. از طرفی ممکن است خدمات‌دهنده در آن واحد انواع خدمات (Si) را ارائه دهد که یک یا چند مورد از آن‌ها مورد هدف قرار گیرد.

خدمت مورد هدف $Serv = S_i \{1, 2, \ldots\}$

S_1 = web service, S_2 = mail service, S_3 = FTP service, …

بنابراین می‌توان کیفیت خدمت هر یک را به‌صورت QoS_i درنظر گرفت. در این پژوهش، کیفیت خدمت فقط به خدمات وب محدود شده است و از معیارهایی هم‌چون تأخیر پاسخ زمان[۱]، گذردهی[۲]، گم‌شدن بسته[۳] و لغزش (تغییر) در تأخیر[۴]، [۲۰] فقط به معیار اول پرداخته می‌شود. زیرا اندازه‌گیری آن بدون دخالت خدمات‌دهنده، امکان‌پذیر است. در این‌جا بهترین کیفیت خدمت ($max\text{-}QoS_i$) از حداقل تأخیر زمانی برخوردار بوده و هم‌چنین پایین‌ترین کیفیت خدمت ($min\text{-}QoS_i$) از بالاترین تأخیر زمانی مجاز برخوردار است. از این‌رو، می‌توان وضعیت خدمت‌رسانی را متناسب با هر خدمت، مورد ارزیابی قرار داد که به چهار دسته زیر قابل تقسیم است:

۱- وضعیت خدمت‌رسانی خوب: در این وضعیت (Sit_i) تأخیر در پاسخ به خدمت (DTS)، در حداقل مقدار تعیین‌شده ($max\text{-}QoS_i$) است و خدمت‌دهنده، خدمات خود را باکیفیت عالی (GS[۵]) ارائه می‌دهد (کیفیت خدمت خوب یا عالی[۶]).

if ($0 < DTS^{7} < max\text{-}QoS_i$) then ($Sit_i$=GS)

۲- وضعیت خدمت‌رسانی قابل‌قبول (حیثیتی): در این وضعیت تأخیر در پاسخ به خدمت، در حداکثر مقدار قابل قبول ($min\text{-}QoS_i$) تعیین شده است و خدمت‌دهنده، خدمات خود را با حداکثر توان (FS[۸]) ارائه می‌دهد (کیفیت خدمت قابل قبول[۹]).

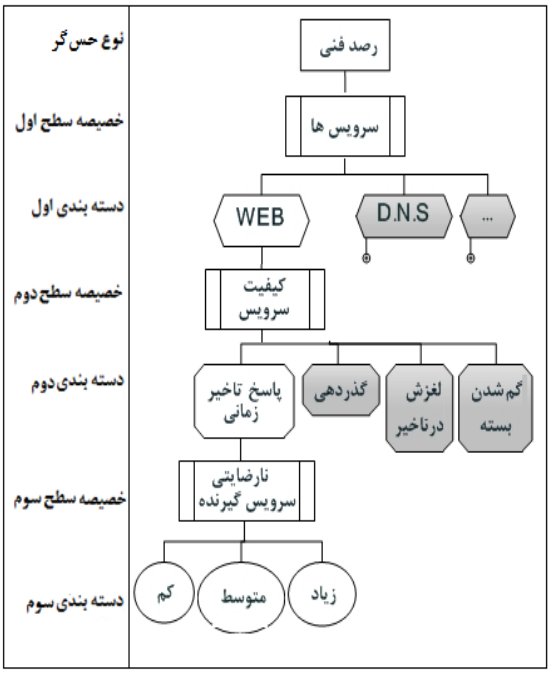
if ($max\_QoS_i <= DTS <= min\_QoS_i$) then ($Sit_i$=FS)

۳- وضعیت خدمت‌رسانی وخیم: در این وضعیت تأخیر در پاسخ به خدمت، فراتر از مقدار قابل قبول تعیین شده (کم‌تر از حد زمان پایان انتظار یعنی Time Out) است و خدمت‌دهنده، در خدمات خود دچار مشکل شده و حداقل (بد) خدمت (BS[۱۰]) را به کاربران مجاز ارائه می‌دهد (کیفیت خدمت وخیم[۱۱]).

if (Time Out > DTS > $min\text{-}QoS_i$) then (Sit_i=BS)

۴- وضعیت قطع خدمت‌رسانی: در این وضعیت تأخیر در پاسخ به خدمت، از حد زمان پایان انتظار (Time Out) فراتر می‌رود. به عبارتی، خدمت‌رسانی ازکارافتاده (DS) و دیگر پاسخ‌گو نمی‌باشد (خدمت‌رسانی قطع[۱۲]).

if (DTS >= Time Out) then (Sit_i=DS [13])



شکل (۴): دسته‌بندی خصیصه حسگر فنی

در طرح پیشنهادی، فرض می‌شود تلفیق داده‌های حسگر فنی، حاوی مقدار تأخیر زمان پاسخ‌دهی به یک خدمت (خدمت *i*ام) با

1- Delay Time
2- Throughput
3- Loss packet
4- Jitter
5- Good Service
6- Excellent QoS
7- Delay Time Service

8- Full Service
9- Full QoS
10- Bad Service
11- Bad QoS
12- Disrupt QoS
13- Disrupt Service

سه خصیصه کم، متوسط و زیاد باشد که بیان‌گر سه وضعیت خدمت‌رسانی خوب و قابل قبول، خدمت‌رسانی مختل و قطع خدمت‌رسانی است که در شکل (۴) نشان داده شده است و هم‌چنین وجود مسدودسازی وسیع دفاعی بتواند موجب عدم قطعیت در نتایج این حسگرها گردد.

۳-۳-۳- شبکه‌ها و رسانه‌های خبری[1]

بدون شک یکی از مسیرهایی که به سمت مطلع‌شدن از وضعیت قربانی و یا قربانیان، سوق می‌دهد شبکه‌ها و رسانه‌های خبری است. مخصوصاً اگر حملات DDoS در ابعاد وسیع انجام گیرد و قربانی حمله، سازمان و یا نهادی معتبر و مشهور باشد، طبعاً تمام رسانه‌های بزرگ و کوچک، این چنین خبری را در صدر اخبار خود قرار خواهند داد. البته بسیاری مواقع نیز در صورت شایعه‌بودن و یا دفع حمله توسط قربانی، باز این چنین شبکه‌هایی وظیفه اطلاع‌رسانی خود را انجام خواهند داد. در این پژوهش، تلاش بر آن است تا علاوه‌بر تقسیم‌بندی رسانه‌ها، تعداد رسانه‌هایی که خبرها را منتشر می‌کنند و نوع اظهارنظری که می‌کنند ملاک عمل قرار گیرند. در این‌جا رسانه به سه دسته اصلی پرمخاطب، متوسط مخاطب و کم‌مخاطب تقسیم شده است. حال هریک از این دسته‌ها می‌توانند درخصوص وضعیت اهداف مورد حمله سه نوع اظهارنظر با عناوین رد یا تکذیب، خنثی یا تحت تعمیر و تأیید اختلال یا قطع داشته باشند. هم‌چنین کثرت این اخبار با سه دسته کم، متوسط و زیاد تقسیم می‌شود. در شکل (۵) دسته‌بندی‌های مذکور نشان داده شده است.

Class MediaNews = {highFollowers, MediumFollowers, LowFollowers}
Class Statement = {Disrupt, Maintenance, Deny}
Class Volume = {Low, Medium, high}

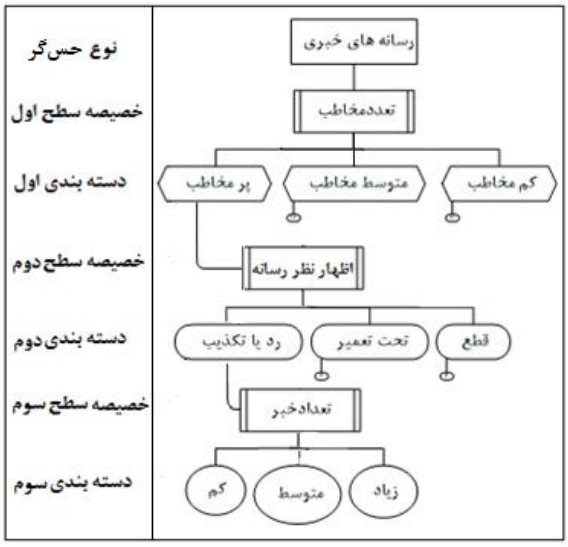
ترکیبات دسته‌های مذکور، ۲۷ حالت را نتیجه می‌دهند که به‌صورت سه‌تایی مرتب زیر به‌دست می‌آیند:

Combinations = {(a, b, c) ; a ∈ Class MediaNews, b ∈ Class Statement , c ∈ Class Volume}

به هر یک از موجودیت‌های هر کلاس، وزن‌هایی (w_i ,w_j ,w_k) اختصاص داده می‌شود[2] که رابطه زیر جهت تعیین سه وضعیت مطلوب (Situation A)، وضعیت تحت‌فشار (Situation B) و وضعیت از کار افتادن خدمت قربانی (Situation C)، می‌بایستی در بازه‌های مشخصی قرار گیرند.

1- Media news

۲- کلیه وزن‌دهی‌های این پژوهش با استفاده از فرم‌های نظرسنجی از خبرگان این حوزه احصاء شده است.



شکل (۵): دسته‌بندی خصیصه حسگر شبکه‌ها و رسانه‌های خبری

$Value\ Fusion_{ijk} = w_i * w_j * w_k$
if Value Fusion < α_{me} then Situation A
if α_{me} < Value Fusion < β_{me} then Situation B
if Value Fusion > β_{me} then Situation C

بنابراین، هر ترکیب دارای مقدار ارزشی است که ارزش ترکیب[3] نامیده می‌شود. اگر مقدار آن کم‌تر از α_{me} (آلفای مدیا) باشد در گروه وضعیت مطلوب قرار می‌گیرد و اگر مقدار آن بین α_{me} و β_{me} باشد در گروه وضعیت تحت‌فشار قرار می‌گیرد و درنهایت اگر مقدار آن بیش‌تر از β_{me} باشد در گروه وضعیت از کار افتادن خدمت قربانی قرار می‌گیرد. اولین مرحله تلفیق طبق رابطه زیر انجام می‌گیرد:

Total-Situation A= $\sum_{SituationA} Value\ Fusion$
Total-Situation B= $\sum_{SituationB} Value\ Fusion$
Total-Situation C= $\sum_{SituationC} Value\ Fusion$

مجموع ارزش ترکیب هر گروه جداگانه مورد محاسبه قرار می‌گیرد تا مشخص شود ترکیب غالب کدام است.

Final Fusion = Max (Total-Situation A, Total.Situation B, Total-Situation C)

۳-۲-۴- شبکه‌های اجتماعی[4]

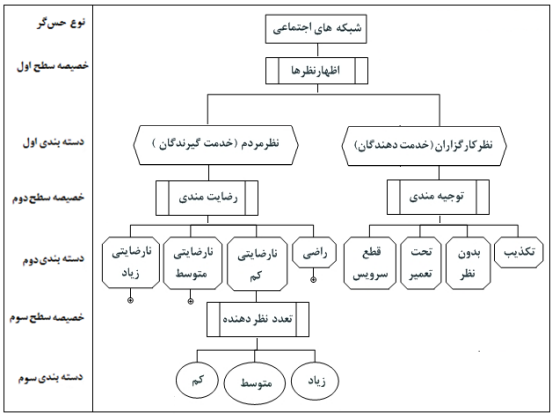
امروزه تمام سازمان‌ها، نهادها (چه بزرگ و یا کوچک)، دارای یک حساب کاربری و یا صفحه‌ای در شبکه‌های اجتماعی پرطرف‌دار بوده و از این بستر جهت تبلیغ و اطلاع‌رسانی به کاربران استفاده می‌کنند. آن‌ها از توییتر استفاده می‌کنند، در فیس‌بوک صفحه‌های طرف‌داران خود را ایجاد کرده‌اند، در یوتیوب فیلم ویدئویی

3- ValueFusion
4- Social networks

گذاشته‌اند، در لینکدین[1]، اینستاگرام و گوگل‌پلاس عضو بوده و دارای صفحات مخصوص به خود هستند. بنابراین، می‌توان از این بستر به اطلاعاتی دست یافت که نشان‌دهنده وضعیت (سرور) قربانی است، اگرچه این اطلاعات از طریق مسئولان سرور مورد حمله باشد که از طریق این شبکه‌ها وضعیت خود را برای طرف‌داران خود اعلام خواهند کرد و یا از طریق نظرات و اعتراض‌ها و یا حتی تعاریفی که کاربران نسبت به خدمات‌رسانی طرف مورد حمله بیان می‌کنند. بدین منظور، تلاش شد تا نشانه‌هایی که ممکن است در شبکه‌های اجتماعی راجع به وضعیت قربانی وجود داشته باشد، بررسی و شبیه‌سازی گردد.

در این‌جا شبکه‌های اجتماعی به دو دسته اصلی اظهارات مردمی و اظهارات اهداف (سوژه) تقسیم شده است. حال مسئولین خدمت‌دهنده می‌توانند درخصوص وضعیت اهداف مورد حمله چهار نوع اظهارنظر با عناوین رد یا تکذیب، بدون اظهارنظر، اظهار تعمیر و نگهداری و تأیید اختلال یا قطع داشته باشند و نیز اظهارات مردمی در چهار نوع اظهارنظر با عناوین ابراز رضایت، نارضایتی کم، نارضایتی متوسط و نارضایتی زیاد می‌باشد. همچنین کثرت این اخبار با سه دسته کم، متوسط و زیاد تقسیم می‌شود. در شکل (۶) دسته‌بندی‌های مذکور نشان داده شده است.

Class Admin Statement = {Disrupt, Maintenance, Deny, None}
Class Client Statement = {Consensus, Low UnConsensus, Medium UnConsensus, High UnConsensus}
Class Volume = {Low, Medium, high}



شکل (۶): دسته‌بندی خصیصه حسگر شبکه اجتماعی اهداف

ترکیبات دسته‌های مذکور، ۴۸ حالت را نتیجه می‌دهند که به‌صورت سه‌تایی مرتب زیر به‌دست می‌آیند:

Combinations = {(a, x) ; a ∈ Class Admin Statement, {x = (b,c); b ∈ Class Client Statement, c ∈ Class Volume}}

1- Linkedin

به هریک از موجودیت‌های هر کلاس، وزن‌هایی (w_i ,w_j ,w_k) اختصاص داده می‌شود که رابطه زیر جهت تعیین سه وضعیت مطلوب (Situation A)، وضعیت تحت‌فشار (Situation B) و وضعیت از کار افتادن خدمت قربانی (Situation C)، می‌بایستی در بازه‌های مشخصی قرار گیرند.

$Value\ Fusion_{ijk} = w_i + (w_j * w_k)$
if $Value\ Fusion < \alpha_{so}$ then Situation A
if $\alpha_{so} < Value\ Fusion < \beta_{so}$ then Situation B
if $Value\ Fusion > \beta_{so}$ then Situation C

بنابراین هر ترکیب دارای مقدار ارزشی است که آن را ارزش ترکیب نامیده می‌شود. اگر مقدار آن کم‌تر از α_{so} (آلفای سوشال) باشد در گروه وضعیت مطلوب قرار می‌گیرد و اگر مقدار آن بین α_{so} و β_{so} باشد در گروه وضعیت تحت‌فشار قرار می‌گیرد و درنهایت اگر مقدار آن بیش‌تر از β_{so} باشد، در گروه وضعیت از کار افتادن خدمت قربانی قرار می‌گیرد. اولین مرحله تلفیق طبق رابطه زیر انجام می‌گیرد:

Total-Situation A= $\sum_{SituationA} Value\ Fusion$
Total-Situation B= $\sum_{SituationB} Value\ Fusion$
Total-Situation C= $\sum_{SituationC} Value\ Fusion$

مجموع ارزش ترکیب هر گروه جداگانه مورد محاسبه قرار می‌گیرد تا مشخص شود ترکیب غالب کدام است.

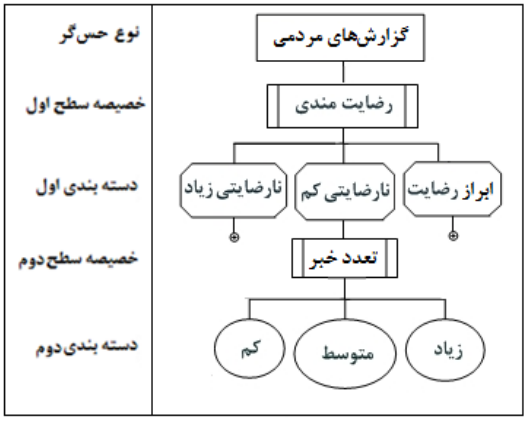
Final Fusion = Max (Total-Situation A, Total-Situation B, Total-Situation C)

۳-۲-۵- گزارش‌های مردمی[2]

یکی از مواردی‌که از طریق آن می‌توان به اطلاعاتی در مورد وضعیت خدمات‌رسانی سرور مورد هدف به کاربران بعد از حملات DDoS دست یافت، کمک‌گرفتن از نظرات کاربران است. به این ترتیب، که می‌توان وضعیت‌های از پیش تعریف‌شده‌ای را تعریف و از کاربران خواست تا یکی از وضعیت‌ها را انتخاب کنند، نظرات ارائه‌شده می‌تواند به‌عنوان یکی از گزینه‌ها جهت تأثیر حمله باشد. در این طرح نیز تلاش شد تا با استفاده از اطلاعات به‌دست‌آمده از گزارش‌های مردمی مبنی بر خرابی خدمات دهندگان مانند sitedown، ضمن دسته‌بندی نظرات مردمی، از آن‌ها به‌عنوان معیاری جهت سنجش تأثیر حملات DDoS استفاده شود. در شکل (۷) دسته‌بندی خصیصه‌های گزارش‌های مردمی نشان داده شده است. گزارش‌های مردمی می‌توانند درخصوص وضعیت اهداف مورد حمله سه نوع اظهارنظر با عناوین ابراز رضایت، نارضایتی کم و نارضایتی زیاد می‌باشد. همچنین

2- People Reports

کثرت این اخبار با سه دسته کم، متوسط و زیاد تقسیم می‌شود. در شکل (۷) دسته‌بندی‌های مذکور نشان داده شده است.



شکل (۷): دسته‌بندی خصیصه حسگر گزارش مردمی

Class Reporters People = {Consensus, Low UnConsensus, High UnConsensus}
Class Volume = {Low, Medium, high}

ترکیبات دسته‌های مذکور، نه حالت را نتیجه می‌دهند که به‌صورت دوتایی مرتب زیر به‌دست می‌آیند:

Combinations = {a ∈ Class Reporters People, b ∈ Class Volume}

به هر یک از موجودیت‌های هر کلاس، وزن‌هایی (w_i ,w_j) اختصاص داده می‌شود که رابطه زیر جهت تعیین سه وضعیت مطلوب (Situation A)، وضعیت تحت‌فشار (Situation B) و وضعیت از کار افتادن خدمت قربانی (Situation C)، می‌بایستی در بازه‌های مشخصی قرار گیرند.

$Value\ Fusion_{ij} = w_i * w_j$
if $Value\ Fusion < \alpha_{rep}$ then Situation A
if $\alpha_{rep} < Value\ Fusion < \beta_{rep}$ then Situation B
if $Value\ Fusion > \beta_{rep}$ then Situation C

بنابراین هر ترکیب دارای مقدار ارزشی است که آن‌را ارزش ترکیب نامیده می‌شود. اگر مقدار آن کمتر از α_{rep} (آلفای ری‌پورتر) باشد در گروه وضعیت مطلوب قرار می‌گیرد و اگر مقدار آن بین α_{rep} و β_{rep} باشد در گروه وضعیت تحت‌فشار قرار می‌گیرد و درنهایت اگر مقدار آن بیش‌تر از β_{rep} باشد، در گروه وضعیت از کار افتادن خدمت قربانی قرار می‌گیرد. اولین مرحله تلفیق طبق رابطه زیر انجام می‌گیرد:

Total-Situation A= $\sum_{SituationA}\ Value\ Fusion$
Total-Situation B= $\sum_{SituationB}\ Value\ Fusion$
Total-Situation C= $\sum_{SituationC}\ Value\ Fusion$

مجموع ارزش ترکیب هر گروه جداگانه مورد محاسبه قرار می‌گیرد تا مشخص شود ترکیب غالب کدام است.

Final Fusion = Max (Total-Situation A, Total-Situation B, Total-Situation C)

۳-۲-۶- تلفیق داده حسگرهای فنی و بشری

عملیات تلفیق داده‌های غیرهم‌نوع آخرین مرحله‌ای است که می‌تواند منجر به ارزیابی وضعیت شود. عدم حضور (یا صحت) هر یک از حسگرها می‌تواند موجب عدم قطعیت در تعیین وضعیت گردد. لذا برای کاهش اثر عدم قطعیت می‌توان حسگرهای فوق را از گردونه تلفیق اطلاعات کنار گذاشت و یا احتمال خطای آن‌ها را در محاسبات لحاظ کرد. بنابراین، می‌توان انتظار داشت تا تنوعی از ترکیب حسگرها پدید آید. بنابراین، لازم است به هریک از حسگرها، وزن‌هایی (w_{me} ,w_{so} ,w_{rep} ,w_{QoS}) اختصاص داده شود تا بتوان وضعیت‌های تلفیق را طبق روابط (۳-۱) محاسبه نمود که در جدول (۱) نشان داده شده است. با متعارف‌سازی[۱] مقادیر وضعیت طبق رابطه (۴)، می‌توان به ارزش قابلیت اطمینان هریک از وضعیت‌ها دست یافت.

$$Rel_{i_{\text{fusion}}} = \frac{\sum_{j=\{me.so.rep.ob\}}(S_{i_j})*(W_i)}{\sum_{i=\{A.B.C\}} S_{i_{fusion}}} \qquad (۴)$$

جدول (۱): تلفیق داده (غیرهم‌نوع) حسگرهای فنی و بشری

	Me	so	Rep	QoS	Total
SitA	$S_{A_{me}}$	$S_{A_{so}}$	$S_{A_{rep}}$	$S_{A_{QoS}}$	$S_{A_{\text{fusion}}} = \sum_{i=\{me.so.rep.ob\}} (S_{A_i}) * (W_i)$ (۱)
SitB	$S_{B_{me}}$	$S_{B_{so}}$	$S_{B_{rep}}$	$S_{B_{QoS}}$	$S_{B_{\text{fusion}}} = \sum_{i=\{me.so.rep.ob\}} (S_{B_i}) * (W_i)$ (۲)
SitC	$S_{C_{me}}$	$S_{C_{so}}$	$S_{C_{rep}}$	$S_{C_{QoS}}$	$S_{C_{\text{fusion}}} = \sum_{i=\{me.so.rep.ob\}} (S_{C_i}) * (W_i)$ (۳)

بدیهی است که ارزش قابلیت اطمینان منتخب، می‌تواند طبق رابطه (۵) بزرگ‌ترین آن‌ها باشد. بنابراین، می‌توان ارزیابی وضعیت را متناسب با مقدار قابلیت اطمینان منتخب طبق رابطه (۶) در نظر گرفت.

$$\text{Relselected} = \text{Max}(\text{Rel}_{\textbf{ifusion}}) \qquad (۵)$$

$$\text{SitAssessment} = \begin{cases} SitA\ ; & \text{Relselected} = RelA \\ SitB\ ; & \text{Relselected} = RelB \\ SitC\ ; & \text{Relselected} = RelC \end{cases} \qquad (۶)$$

قابلیت اطمینان مورد پذیرش لازم است شرط روابط (۸-۷) را احصاء کند:

$$VRS = min\left(1 - \frac{Reli_{fusion}}{Rel_{selected}}\right).i <> selected \qquad (۷)$$

۱- نرمالیزه یا تغییردادن مجموعه اعداد، به‌طوری‌که حاصل آن‌ها برابر عدد یک شود.

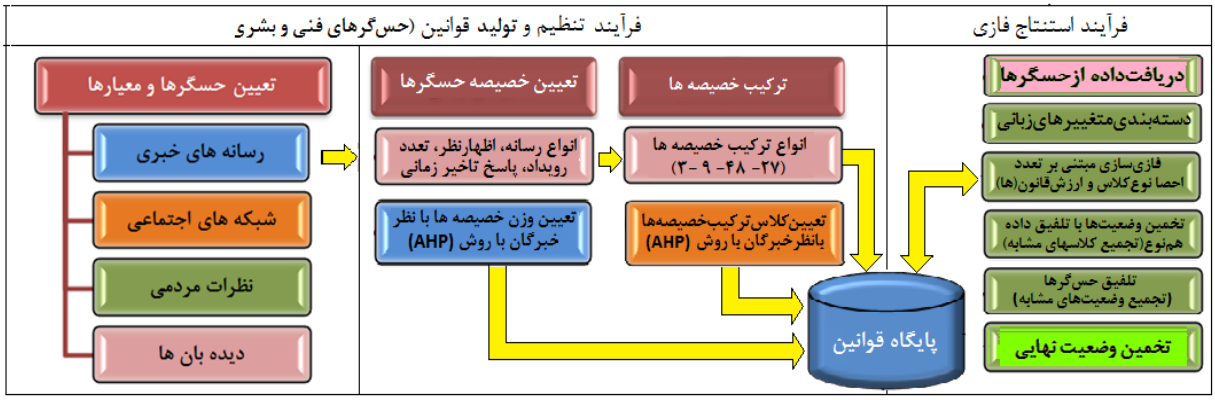
$TRS_{\text{accept}} = 0.5$

$$VRS \geq TRS_{accept} \ \ then \ Rel_{selected} \ is \ accept \qquad (۸)$$

با احراز شرط فوق، مقدار قابلیت اطمینان وضعیت منتخب می‌تواند برابر VRS باشد. بدیهی است اگر $Reli_{fusion}$ با یکدیگر برابر باشند شرط لازم را برای وضعیت انتخاب‌شده قابلیت اطمینان فراهم نمی‌کنند زیرا VRS کمتر از ۳٪ است.

۴- مدل‌سازی و شبیه‌سازی حسگرها با منطق فازی

همان‌طورکه پیش از این توضیح داده شد، برای اطلاع از تأثیر و یا عدم تأثیر و درصورت تأثیر، برای اطلاع از میزان مؤثربودن حملات سایبری باید از کانال‌ها و حسگرهای متعدد اطلاع شد. علاوه‌بر حسگرهای مربوط به دیده‌بان‌ها، سه نوع حسگر متفاوت دیگر نیز در این طرح مورد استفاده قرار گرفته است. این حسگرها، رسانه‌های خبری، شبکه‌های اجتماعی و همچنین نظرات مردمی موجود در سایت‌های مانیتورینگ وضعیت هستند. در این تحقیق با به‌کارگیری یکی از روش‌های معروف و مطمئن موجود در منطق فازی، تحت عنوان روش FRBCS [۳] برای تجمیع اطلاعات استفاده شده است. این روش ماهیت طبقه‌بندی را دارد و قرار است بیان کند که با توجه به اطلاعات موجود، وضعیت قربانی به چه صورت است. در این نوع سیستم‌ها از قوانین [۴] استفاده می‌شود. سمت راست این قوانین غیرفازی و سمت چپ، حالت فازی دارد که این، مشابه اطلاعات به‌دست‌آمده از حسگرهای به‌کاررفته در این طرح است. هم‌چنین با توجه به این‌که این نوع روش‌ها اغلب نتایج بسیار مطلوبی را ایجاد می‌کنند، در این طرح نیز روشی جدید ارائه خواهد شد که مبتنی بر چنین سامانه‌هایی است. شمای کلی این روش در شکل (۸) نشان داده شده است که این روش به دو قسمت کلی تقسیم می‌شود. در قسمت اول که فرآیند یادگیری است، پایگاه قوانین فازی استخراج خواهد شد. در قسمت دوم که شامل فرآیند استنتاج فازی است با استفاده از قوانین به‌دست‌آمده از مرحله قبل و ورودی‌های حسگرها، کار استنتاج با استفاده از روشی جدید ارائه می‌شود.



شکل (۸): نمای کلی تجمیع اطلاعات حسگرها با استفاده از منطق فازی

۴-۱- ایجاد پایگاه قوانین فازی

همان‌طورکه اشاره شد، سامانه‌های فازی به‌کاررفته در این طرح با استفاده از قوانین فازی عمل خواهند کرد، بنابراین باید با توجه به متغیرهای زبانی که پیش از این تعریف شد و در جدول (۳) مشخص شده‌اند، نواحی پوشش [۱] و نواحی تصمیم [۲] در فضا، تعیین شده و با توجه به داده‌های موجود در فضا، قوانین فازی طبق جدول (۲) تعیین گردند. اما به جهت این‌که اهمیت و میزان دقت این سامانه‌ها بسیار پراهمیت است، تلاش کردیم تا با دید خبرگی این قوانین را استخراج و مورد استفاده قرار دهیم.

دیده‌بان فنی: ازجمله حسگرهای مورد استفاده، دیده‌بان‌ها هستند که به‌نوعی نظرات فنی را بیان کرده یا به‌عبارت دیگر، با نگاه تخصصی، گزارشی از وضعیت سرور مورد حمله را ارائه می‌کنند که قوانین استخراج‌شده برای این مجموعه در جدول (۲) قسمت میانی سمت راست، قابل مشاهده است. همان‌طورکه در این جدول مشخص است، سه قانون برای این حسگر وجود دارد.

جدول فوق حاوی ستون شماره قوانین ($N.R$)، بازه تأخیر پاسخ زمانی ($D.T$) که با سه خصیصه کم (L) متوسط (M) و زیاد (H) می‌باشد.

رسانه‌های خبری: همان‌طورکه قبلاً اشاره شد، یکی از حسگرهای مورد استفاده، خروجی حاصل از رسانه‌های خبری

1- Covering Area
2- Decision Area
3- Fuzzy Rule Based Classification System
4- Rules

است که قوانین استخراج‌شده برای این مجموعه در جدول (۲) سمت راست، قابل‌مشاهده است.

همان‌طورکه در این شکل مشخص است با توجه به متغیرهای زبانی، ۲۷ قانون برای این حسگر وجود دارد. جدول فوق حاوی ستون شماره قوانین (N.R)، نوع رسانه (RAS) با سه خصیصه پرمخاطب (PM)، متوسط مخاطب (MM)، کم مخاطب (KM) و نوع اظهارنظر (NAZ) با سه خصیصه رد یا تکذیب (RT)، خنثی یا تحت تعمیر (TM)، تأیید اختلال یا قطع (TA) و تعداد محدوده خبر منعکس‌شده (NUM) با سه خصیصه کم (L)، متوسط (M)، زیاد (H) می‌باشد.

شبکه‌های اجتماعی: یکی از حسگرها مورد استفاده، خروجی حاصل از شبکه‌های اجتماعی است که قوانین استخراج‌شده برای این مجموعه در جدول (۲) سمت چپ قابل مشاهده است.

جدول (۳) حاوی ستون شماره قوانین (N.R)، اظهارنظر کارگزاران (MNG) با چهار خصیصه رد یا تکذیب (TZ)، بدون اظهارنظر (NS)، اظهار تعمیر و نگهداری (TN) و اختلال یا قطع (GH) و نوع اظهارنظر مردمی (PPL) با چهار خصیصه ابراز رضایت (RG)، نارضایتی‌کم (LR)، نارضایتی متوسط (MR) و نارضایتی زیاد (HR) و تعداد محدوده خبر منعکس‌شده (NUM) با سه خصیصه کم (L)، متوسط (M)، زیاد (H) می‌باشد.

نظرات مردمی: یکی از حسگرهای مورد استفاده، خروجی حاصل از نظرات مردمی است که از سایت‌های مانیتورینگ همانند sitedown قابل استخراج است که قوانین به‌دست‌آمده برای این مجموعه در جدول (۲) قسمت تحتانی سمت راست قابل مشاهده است. جدول فوق حاوی ستون شماره قوانین (N.R)، رضایتمندی (NAZ) با سه خصیصه ابراز رضایت (RT)، نارضایتی کم (NL)، نارضایتی زیاد (NH) و تعداد محدوده خبر منعکس‌شده (NUM) با سه خصیصه کم (L)، متوسط (M)، زیاد (H) می‌باشد.

جدول (۲): قوانین و وضعیت‌های مربوط به ترکیب خصیصه‌های هر حسگر

راست	حسگر رسانه‌ها سمت چپ قوانین			
St	NUM	NAZ	RAS	NR
A	L	RT	PM	۱
A	M	RT	PM	۲
A	H	RT	PM	۳
B	L	TM	PM	۴
C	M	TM	PM	۵
C	H	TM	PM	۶
C	L	TA	PM	۷
C	M	TA	PM	۸
C	H	TA	PM	۹
A	L	RT	MM	۱۰
A	M	RT	MM	۱۱
A	H	RT	MM	۱۲
B	L	TM	MM	۱۳
B	M	TM	MM	۱۴
B	H	TM	MM	۱۵
C	L	TA	MM	۱۶
C	M	TA	MM	۱۷
C	H	TA	MM	۱۸
A	L	RT	KM	۱۹
A	M	RT	KM	۲۰
A	H	RT	KM	۲۱
A	L	TM	KM	۲۲
A	M	TM	KM	۲۳
A	H	TM	KM	۲۴
B	L	TA	KM	۲۵
B	M	TA	KM	۲۶
B	H	TA	KM	۲۷

راست	حسگر شبکه اجتماعی سمت چپ قوانین			
st	NUM	PPL	MNG	NR
A	L	RG	TZ	۱
A	M	RG	TZ	۲
A	H	RG	TZ	۳
A	L	LR	TZ	۴
A	M	LR	TZ	۵
A	H	LR	TZ	۶
A	L	MR	TZ	۷
A	M	MR	TZ	۸
B	H	MR	TZ	۹
A	L	HR	TZ	۱۰
B	M	HR	TZ	۱۱
B	H	HR	TZ	۱۲
A	L	RG	NS	۱۳
A	M	RG	NS	۱۴
A	H	RG	NS	۱۵
A	L	LR	NS	۱۶
A	M	LR	NS	۱۷
A	H	LR	NS	۱۸
A	L	MR	NS	۱۹
A	M	MR	NS	۲۰
B	H	MR	NS	۲۱
A	L	HR	NS	۲۲
A	M	HR	NS	۲۳
B	H	HR	NS	۲۴
B	L	RG	TN	۲۵
B	M	RG	TN	۲۶
B	H	RG	TN	۲۷
B	L	LR	TN	۲۸
B	M	LR	TN	۲۹
B	H	LR	TN	۳۰
B	L	MR	TN	۳۱
B	M	MR	TN	۳۲
C	H	MR	TN	۳۳
B	L	HR	TN	۳۴
C	M	HR	TN	۳۵
C	H	HR	TN	۳۶
C	L	RG	GH	۳۷
C	M	RG	GH	۳۸
C	H	RG	GH	۳۹
C	L	LR	GH	۴۰
C	M	LR	GH	۴۱
C	H	LR	GH	۴۲
C	L	MR	GH	۴۳
C	M	MR	GH	۴۴
C	H	MR	GH	۴۵
C	L	HR	GH	۴۶
C	M	HR	GH	۴۷
C	H	HR	GH	۴۸

د) حسگر دیده‌بان فنی	
سمت چپ	راست
DT	St
L	A
M	B
H	C

ج) حسگر گزارش‌های مردمی			
سمت چپ قوانین			راست
NUM	NAZ	NR	St
L	RT	۱	A
M	RT	۲	A
H	RT	۳	A
L	NL	۴	A
M	NL	۵	A
H	NL	۶	B
L	NH	۷	B
M	NH	۸	C
H	NH	۹	C

جدول (۳): خصیصه انواع حسگرها و وزن دهی

رسانه های خبری												شبکه های اجتماعی										نظرات مردمی						دیده بان فنی		
تعددمخاطب			نظرمدیر			تعدادخبر			اظهارمدیرشبکه				اظهارنظرمردم				تعداداظهارنظر			میزان رضایت			تعداداظهارنظر			تاخیر پاسخ زمانی		
پر مخاطب	متوسط-مخاطب	کم مخاطب	رد یا تکذیب	تحت تعمیر	قطع	کم	متوسط	زیاد	رد یا تکذیب	بدون نظر	اظهار تعمیر	قطع سرویس	رضایت	نارضایتی کم	نارضایتی متوسط	نارضایتی زیاد	کم	متوسط	زیاد	رضایت	نارضایتی کم	نارضایتی زیاد	کم	متوسط	زیاد	کم	متوسط	زیاد
۰.۷	۰.۳	۰.۱	۰.۵	۰.۲۵	۰.۵	۰.۵	۱	۲	۰.۸	۰.۱	۰.۳	۱	۰.۵	۰.۲	۰.۲	۰.۵	۰.۵	۱	۲	۰.۳	۰.۴	۰.۵	۰.۵	۱	۲	۱	۰.۵	۱

۴-۲- وزن‌دهی به خصیصه‌ها[1] و قوانین

یکی از مواردی‌که به‌طور قطع روی عملکرد نهایی تأثیر مثبت خواهد گذاشت درنظرگرفتن وزن برای خصیصه‌ها و قوانین به‌دست آمده است. یکی از راه‌حل‌ها که می‌توان برای وزن‌دهی به قوانین استفاده کرد، درنظرگرفتن نسبت فراوانی داده در نواحی پوششی هر قانون نسبت به کل داده‌هاست. به‌عبارتی، هر قانونی که داده‌های بیش‌تری را پوشش می‌دهد معتبرتر است. یکی از روش‌های خبرگی، استفاده از وزن متخصص مربوطه است، به این صورت که به هریک از خصیصه‌ها با توجه به عبارت زبانی آن وزنی اختصاص می‌یابد، بعد از تنظیم کلیه وزن‌ها برای تمام متغیرها و عبارات زبانی می‌توان وزن هر قانون را نیز تعیین کرد. یک روش برای وزن هر قانون می‌تواند حاصل‌ضرب متغیرهای زبانی باشد که قانون مربوطه را تشکیل می‌دهند. این کار باعث خواهد شد تا به‌صورت خبرگی قوانینی که خیلی اعتبار ندارند. وزن کم‌تری بگیرند و قوانین پرمعتبر وزن بیش‌تری به خود اختصاص دهند. وزن هریک از قوانین از ضرب خصیصه‌ها به‌دست می‌آید. این وزن برای قوانین رسانه‌های خبری تشکیل شده است از:

۴-۳- وزن‌دهی حسگرها در تلفیق اطلاعات با استفاده از روش فرایند تحلیل سلسله مراتبی[2]

سطح اول فرایند تحلیل سلسله مراتب را معیارهای اصلی تشکیل می‌دهند. پرسش‌نامه خبره نخست با مقایسه زوجی معیارهای اصلی براساس هدف به تعیین اولویت هریک از معیارهای اصلی می‌پردازد. بنابراین معیارها براساس هدف دو به دو باهم مقایسه می‌شوند. وزن معیارهای اصلی (که همان حسگرها هستند) با استفاده از این روش تعیین می‌شود. بدین منظور، ماتریس مقایسه زوجی را شکل داده که در جدول (۴) ارائه شده است. آقایان اکزل و ساعتی[3] [۱۸] استفاده از میانگین هندسی را بهترین روش برای ترکیب مقایسه‌های زوجی معرفی کرده‌اند. بنابراین، از داده‌های هر سطر در جدول فوق میانگین هندسی گرفته می‌شود. وزن‌های به‌دست‌آمده متعارف[4] نیستند. بنابراین، میانگین هندسی به‌دست‌آمده در هر سطر را بر مجموع عناصر ستون میانگین هندسی تقسیم می‌کنیم. ستون جدید که حاوی وزن متعارف‌شده‌ی هر معیار است را بردار ویژه گویند.

این وزن‌دهی‌ها در ۱۵ حالت مختلف در جدول (۵) نمایش داده شده است. اعداد صفر در جدول ب عدم حضور حسگر مربوطه می‌باشد. وزن نهایی هر معیار همان ستون بردار ویژه است. در مواقعی نیز ممکن است حسگر و یا حسگرهایی موجود نباشند در این زمان نیاز است شیوه وزن‌دهی براساس حسگرهای موجود باشد.

جدول (۴): محاسبه وزن معیارها با استفاده از روش AHP

	رسانه‌های خبری	شبکه‌های اجتماعی	نظرات مردمی	دیده‌بان‌ها	میانگین هندسی	متعارف‌سازی	بردار ویژه
رسانه‌های خبری	۱	۲	۳	۱	$\sqrt[4]{۱*۲*۳*۱}=۱/۵۶۵$	$\frac{۱.۵۶۵}{۱/۵۶۵+۰/۸۴+۰/۴۹+۱/۵۶۵}$	۰/۳۵
شبکه‌های اجتماعی	۱/۲	۱	۲	۱/۲	$\sqrt[4]{۰/۵*۱*۲*۰/۵}=۰/۸۴$	$\frac{۰/۸۴}{۱/۵۶۵+۰/۸۴+۰/۴۹+۱/۵۶۵}$	۰/۱۹
نظرات مردمی	۱/۳	۱/۲	۱	۱/۳	$\sqrt[4]{۰/۳۳*۰.۵*۱*۰/۳۳}=۰/۴۹$	$\frac{۰/۴۹}{۱/۵۶۵+۰/۸۴+۰/۴۹+۱/۵۶۵}$	۰/۱۱
دیده‌بان‌ها	۱	۲	۳	۱	$\sqrt[4]{۱*۲*۳*۱}=۱/۵۶۵$	$\frac{۱/۵۶۵}{۱/۵۶۵+۰/۸۴+۰/۴۹+۱/۵۶۵}$	۰/۳۵

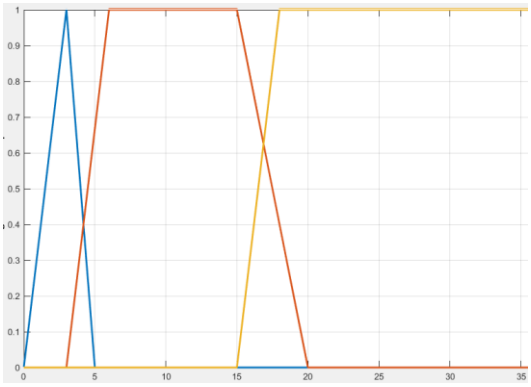
جدول (۵): ترکیب و وزن‌دهی حسگرها

ردیف	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
سایت‌خبری	۰/۳۵	۰/۵۴	۰/۴	۰/۴۳	۰	۰/۶۷	۰/۷۵	۰	۰/۵	۰	۰	۱	۰	۰	۰
شبکه‌اجتماعی	۰/۱۹	۰/۳	۰/۲	۰	۰/۳	۰/۳۳	۰	۰/۶۷	۰	۰/۳۳	۰	۰	۱	۰	۰
نظرات‌مردمی	۰/۱۱	۰/۱۶	۰	۰/۱۴	۰/۱۶	۰	۰/۲۵	۰/۳۳	۰	۰	۰/۲۵	۰	۰	۱	۰
دیده بان فنی	۰/۳۵	۰	۰/۴	۰/۴۳	۰/۵۴	۰	۰	۰	۰/۵	۰/۶۷	۰/۷۵	۰	۰	۰	۱

1- Feature weighting
2- Analytical Hierarchy Process-AHP
3- Axel & saati
4- Eigenvalue

۴-۴- مجموعه‌های فازی و توابع عضویت

قوانین فازی به‌کاررفته به‌گونه‌ای هستند که سمت چپ این قوانین، ترکیبی از حالت فازی و غیرفازی است. تنها خصیصه تعداد خبر در سمت چپ قوانین به‌صورت فازی می‌باشد که در شکل (۹) نشان داده شده است. بنابراین، باید برای سمت چپ قوانین تولیدشده در پایگاه قوانین، مجموعه‌های فازی و هم‌چنین تابع عضویت آن‌ها را تشکیل داد. بدین صورت‌که قسمت غیرفازی را هم‌چون یک درخت تصمیم به سمت قانون درست سوق می‌دهد و در این لحظه قسمت فازی این قوانین تعیین‌کننده وضعیت نهایی می‌باشند. با توجه به این مسئله نیاز است مجموعه‌های فازی و توابع عضویت برای تمام قوانین پایگاه، مشخص شوند. شکل (۹) مجموعه‌های فازی و روابط (۱۱-۹)، توابع عضویت را برای حسگرهای رسانه، شبکه اجتماعی و گزارش‌های مردمی نمایش می‌دهد. مجموعه اول یک مجموعه مثلثی است و دو مجموعه دیگر ذوزنقه‌ای می‌باشند.



شکل (۹): مجموعه‌های فازی مربوط به کلیه حسگرها

$$\begin{cases} 0 & x \le 0 \\ \frac{x-0}{a} & 0 \le x \le a \\ \frac{b-x}{b-a} & a \le x \le b \\ 0 & x \ge b \end{cases} \quad (۹)$$

$$\begin{cases} 0 & x \le a \\ \frac{x-a}{c-a} & a \le x \le c \\ 1 & c \le x \le d \\ \frac{e-x}{e-d} & d \le x \le e \\ 0 & x \ge e \end{cases} \quad (۱۰)$$

$$\begin{cases} 0 & x \le d \\ \frac{x-d}{f-d} & d \le x \le f \\ 1 & x \ge f \end{cases} \quad (۱۱)$$

در روابط بالا، که روابط فازی کلیه حسگرها را نشان می‌دهد، ضرایب a تا f برای هر یک از انواع حسگرها طبق جدول (۶) درنظر گرفته می‌شود. جدول (۷) مثالی از عملکرد سیستم در هنگام دریافت اطلاعات شبکه خبری را نشان می‌دهد که حسگر رسانه‌های خبری با دریافت تعدادی خبر در واحد زمان، با سیستم فازی نسبت به استنتاج کلاس وضعیت‌ها مبادرت کرده و با تجمیع وضعیت‌ها برآوردی را حاصل می‌کند

جدول (۶): ضرایب مربوط به روابط فازی هریک از حسگرها

انواع دیده بانی	a	b	c	d	e	f
رسانه‌های خبری	۳	۵	۶	۱۵	۲۰	۱۸
شبکه‌های اجتماعی	۳	۵	۶	۱۲	۱۵	۱۵
نظرات مردمی	۳	۵	۶	۱۵	۲۰	۱۸
دیده‌بان فنی	۳	۵	۶	۱۲	۱۵	۱۵

جدول (۷): ارائه سه سناریو در چهار گام زمانی مربوطه همه حسگرها

			NUM											
			سناریوی یک				سناریوی دو				سناریوی سه			
	Lay1	Lay2	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4
حسگر رسانه	PM	RT	۱	۱	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰
	PM	TM	۰	۰	۰	۰	۱	۱	۳	۳	۰	۰	۰	۰
	PM	TA	۰	۰	۰	۰	۰	۰	۰	۰	۲	۳	۴	۵
	MM	RT	۲	۴	۱۰	۲۰	۰	۰	۱	۲	۰	۰	۱	۱
	MM	TM	۰	۰	۱	۱	۵	۷	۱۴	۲۰	۲	۳	۳	۴
	MM	TA	۰	۰	۰	۰	۱	۱	۲	۲	۹	۱۴	۲۲	۲۸
	KM	RT	۵	۹	۱۵	۲۵	۰	۱	۳	۴	۲	۵	۶	۶
	KM	TM	۱	۲	۳	۳	۷	۱۲	۱۵	۲۵	۶	۸	۹	۱۰
	KM	TA	۰	۰	۰	۱	۱	۲	۴	۴	۹	۱۵	۲۲	۳۰
حسگر شبکه اجتماعی	TZ	RG	۱۰	۱۲	۲۰	۲۵	۰	۰	۰	۰	۰	۰	۰	۰
	TZ	LR	۱	۲	۲	۵	۰	۰	۰	۰	۰	۰	۰	۰
	TZ	MR	۱	۱	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰
	TZ	HR	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰
	NS	RG	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
	NS	LR	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
	NS	MR	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
	NS	HR	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
	TN	RG	۰	۰	۰	۰	۲	۲	۲	۳	۰	۰	۰	۰
	TN	LR	۰	۰	۰	۰	۵	۹	۱۲	۱۷	۰	۰	۰	۰
	TN	MR	۰	۰	۰	۰	۵	۷	۱۰	۱۲	۰	۰	۰	۰
	TN	HR	۰	۰	۰	۰	۲	۴	۵	۹	۰	۰	۰	۰
	GH	RG	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
	GH	LR	۰	۰	۰	۰	۰	۰	۰	۰	۴	۶	۶	۷
	GH	MR	۰	۰	۰	۰	۰	۰	۰	۰	۵	۸	۱۰	۱۵
	GH	HR	۰	۰	۰	۰	۰	۰	۰	۰	۷	۱۲	۲۰	۳۲
حسگر گزارش مردمی		RT	۵	۷	۱۲	۲۰	۱	۲	۲	۳	۰	۰	۰	۰
		NRK	۱	۱	۱	۲	۲۰	۲۵	۲۹	۳۵	۲۰	۲۱	۲۱	۲۳
		NRZ	۰	۰	۰	۰	۵	۷	۸	۹	۲۲	۲۷	۳۴	۴۵
دیده‌بان فنی		MTD	۲	۳	۳	۳	۶	۷	۹	۱۱	۱۶	۱۷	۱۷	۱۹

۵- ارزیابی طرح پیشنهادی تلفیق اطلاعات حسگرها

در این بخش با استفاده از منطق فازی به ارزیابی تلفیق اطلاعات حاصل از حسگرهای مختلف پرداخته شود. روش پیشنهادی، ابتدا فرآیند یادگیری و تولید قوانین فازی را پشت سر گذاشته و درنهایت با دریافت اطلاعات جدید از حسگرها به ارزیابی وضعیت فعلی سرور مورد هجوم می‌پردازد. با توجه به این‌که هیچ مجموعه داده‌ای در حوزه ارزیابی اثربخشی حملات منع خدمات را نمی‌توان یافت [۹] و در صورت موجودبودن نیز با شاخص‌های ارزیابی به‌کاررفته در این تحقیق هم‌خوانی ندارند لذا داده‌های مورد نیاز این پژوهش را می‌توان با استفاده از تجارب تأثیر حملات منع خدمات گذشته، در قالب سناریوها تولید کرد.

۵-۱- شبیه‌سازی سناریوها

حسگر دیده‌بان‌ها، رسانه‌های خبری، شبکه‌های اجتماعی و حسگر نظرات مردمی چهار حسگری هستند که در این طرح مورد استفاده و شبیه‌سازی قرارگرفته‌اند.

تنظیمات لازم جهت ایجاد خروجی: بعد از مشخص‌شدن حسگرها و خصیصه‌های هریک و هم‌چنین دسته‌بندی دامنه هر خصیصه با مفاهیم زبان‌شناسی معرفی‌شده در منطق فازی، خصیصه‌های هریک از حسگرها ترکیب‌شده و قوانین فازی استخراج خواهند شد. بعد از وزن‌دهی به خصیصه‌ها و هم‌چنین وزن‌دهی به قوانین استخراج‌شده، پایگاه قوانین فازی تولید و جهت استفاده برای پایش وضعیت‌های جدید آماده است.

تنظیم سناریوهای مختلف: برای به‌دست‌آوردن خروجی و مانیتورکردن وضعیت سرور و سایت‌های مورد هجوم با استفاده از داده‌هایی که از حسگرها می‌رسند سه سناریو مختلف در نظر گرفته‌شده که عبارت‌اند از:

۱. حالتی که سرور در وضعیت عادی به سر می‌برد.

۲. حالتی که سرور قادر به خدمات‌رسانی به‌صورت کند بوده و تحت فشار است.

۳. حالتی که سرور down شده است.

در این مرحله برای هر یک از سه سناریو و متناسب با هر یک از حسگرها، جریان داده رخدادها مقداردهی شده است که در جدول (۸) نشان داده شده است. بطوری‌که خصیصه‌های تعبیه‌شده (به‌صورت نمادگذاری) برای هریک از حسگرها (ستون اول) و هم‌چنین متغیرهای زبان‌شناسی (ستون‌های دوم و سوم) و ستون‌های بعدی تعداد رخدادهای مربوط به هر سناریو در چهار گام زمانی را نشان می‌دهد.

۵-۲- نتایج سناریوها

جدول (۹) نتایج تخمین سه وضعیت ازکارافتاده، کند و عادی در هر سه سناریوی فوق برای تمامی حسگرها (ستون اول) نشان داده شده است که در چهار زمان متفاوت (ستون دوم) و البته متوالی، اطلاعات از انواع حسگرها (ستون اول) دریافت شده است.

جدول (۸): نتایج تخمین وضعیت در سه سناریو

نوع حسگر	زمان	سناریو ۱			سناریو ۲			سناریو ۳		
		Down	Slow	UP	Down	Slow	UP	Down	Slow	UP
رسانه خبری	۱	۰	۰	۱۰۰	۱۸	۶۴	۱۸	۶۹	۲۰	۱۱
	۲	۰	۰	۱۰۰	۱۴	۶۷	۱۹	۶۹	۱۹	۱۲
	۳	۰	۴	۹۶	۱۷	۶۴	۱۹	۶۸	۱۹	۱۳
	۴	۰	۴	۹۶	۱۷	۶۲	۲۱	۶۹	۱۸	۱۳
شبکه اجتماعی	۱	۰	۰	۱۰۰	۰	۱۰۰	۰	۱۰۰	۰	۰
	۲	۰	۰	۱۰۰	۱۹	۸۱	۰	۱۰۰	۰	۰
	۳	۰	۰	۱۰۰	۳۷	۶۳	۰	۱۰۰	۰	۰
	۴	۰	۰	۱۰۰	۳۷	۶۳	۰	۱۰۰	۰	۰
نظرات مردمی	۱	۰	۰	۱۰۰	۲۸	۶۸	۴	۵۶	۴۴	۰
	۲	۰	۰	۱۰۰	۳۶	۵۷	۷	۵۶	۴۴	۰
	۳	۰	۰	۱۰۰	۳۶	۵۷	۷	۵۶	۴۴	۰
	۴	۰	۰	۱۰۰	۳۴	۵۶	۱۰	۵۶	۴۴	۰
حسگر دیده‌بان	۱	۰	۰	۱۰۰	۰	۱۰۰	۰	۱۰۰	۰	۰
	۲	۰	۰	۱۰۰	۰	۱۰۰	۰	۱۰۰	۰	۰
	۳	۰	۰	۱۰۰	۰	۱۰۰	۰	۱۰۰	۰	۰
	۴	۰	۰	۱۰۰	۰	۱۰۰	۰	۱۰۰	۰	۰

جدول (۹): نمونه‌ای از عملکرد سامانه در هنگام دریافت اطلاعات شبکه خبری

درصد نهایی	تجمیع کلاسها	ارزش کلاس	میزان تعلق به قانون	سمت راست قانون	وزن قانون	شماره قانون
۰.۳۵۰	۰.۱۱۷	۰.۱۱۷	۰.۶۶۷	A	۰.۱۷۵	۱
	۰.۱۵۰	۰.۰۵۸	۰.۳۳۳	C	۰.۱۷۵	۷
	۰.۰۳۳	۰.۱۵۰	۱.۰۰۰	A	۰.۱۵	۱۱
	۰.۰۵۰	۰.۰۷۵	۱.۰۰۰	B	۰.۰۷۵	۱۴
۰.۰۹۲	۰.۰۷۵	۰.۰۳۸	۰.۵۰۰	C	۰.۰۷۵	۱۶
	۰.۰۱۷	۰.۰۵۰	۰.۳۳۳	C	۰.۱۵	۱۷
۰.۱۴۶	۰.۰۵۸	۰.۰۳۳	۰.۶۶۷	A	۰.۰۵	۲۰
	۰.۰۳۸	۰.۰۵۰	۱.۰۰۰	A	۰.۰۵	۲۴
	۰.۰۵۰	۰.۰۱۷	۰.۶۶۷	B	۰.۰۲۵	۲۵

تعداد خبر	نوع اظهار	نوع رسانه
۲	رد یا تکذیب	رسانه پر مخاطب
۱	تایید اختلال یا قطع	رسانه پر مخاطب
۱۲	رد یا تکذیب	رسانه متوسط مخاطب
۱۲	خنثی یا تحت تعمیر	رسانه متوسط مخاطب
۴	تایید اختلال یا قطع	رسانه متوسط مخاطب
۵	رد یا تکذیب	رسانه کم مخاطب
۲۰	خنثی یا تحت تعمیر	رسانه کم مخاطب
۲	تایید اختلال یا قطع	رسانه کم مخاطب

۵-۳- مقایسه نتایج

خروجی به‌دست‌آمده از سامانه بعد از دریافت اطلاعات حسگرها مطابق جدول (۹) است، طبق انتظار در تمام لحظاتی که اطلاعات دریافت شد ملاحظه می‌گردد که در سناریوی اول، سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده بالابودن سرور است. در سناریوی دوم، سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده تحت فشار بودن سرور است.

از طرفی میزان درصدی که به پایین‌بودن سرور اختصاص یافته است کاملاً منطقی است. زیرا درجایی‌که خود مدیر سرور به این نکته اذعان دارد که سرور تحت فشار است و کاربران نیز که قاعدتاً به این مسئله اعتراض دارند سامانه باید درصدی را مطابق نظرات کاربران به پایین‌بودن سامانه اختصاص دهد که خروجی نیز همین امر را نشان می‌دهد. طبق انتظار در تمام لحظاتی که از حسگر گزارش مردمی اطلاعات دریافت شد، سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده تحت فشار بودن سرور است. البته طبیعی است چون نظرات مردم در این‌جا دخیل بوده و ممکن است با ایرادی حتی کوچک نظرات انتقادی تعداد کمی نداشته باشد و درنتیجه درصد قابل توجهی به پایین‌بودن و خوابیدن سرور تعلق گیرد.

در سناریوی سوم، خروجی به‌دست‌آمده از سامانه بعد از دریافت اطلاعات حسگر رسانه‌های خبری در تمام لحظاتی که اطلاعات دریافت شد، سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده خوابیده‌بودن سرور است. البته طبیعی است که حالت‌هایی مثل بالابودن سرور و یا تحت تعمیربودن نیز درصدهایی را به خود اختصاص دهند زیرا در حالتی که حمله رخ داده است بسیاری از رسانه‌های ذی‌نفع یا منکر این موضوع می‌شوند و یا به این‌که تنها مشکل کوچک پیش‌آمده اکتفا می‌کنند. هم‌چنین سناریوی سه برای حسگر شبکه‌های اجتماعی نشان می‌دهد که در چهار زمان متفاوت و البته متوالی اطلاعات از حسگر شبکه‌های اجتماعی دریافت شده است. طبق انتظار در تمام لحظاتی که اطلاعات از شبکه‌های اجتماعی دریافت شد، سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده پایین بودن سرور است. هم‌چنین خروجی به‌دست‌آمده از سامانه بعد از دریافت اطلاعات حسگر نظرات مردمی، طبق انتظار در تمام لحظاتی که اطلاعات دریافت شد سامانه بالاترین درصد را به حالتی می‌دهد که نشان‌دهنده افتادن و از دسترس خارج شدن سرور است. بنابراین می‌توان تخمین نهایی حاصل از سه سناریو برای تمامی حسگرها را با استفاده از روابط بخش ۵-۲-۳ را محاسبه کرد که نتایج حاصل در جدول (۱۰) نشان داده شده است. نتیجه نهایی حاصل، در سناریوی اول با احتمال ۹۹/۳٪ مبنی‌بر وضعیت بالابودن سامانه تخمین زده شده است و هم‌چنین در سناریوی دوم با احتمال ۷۸/۶٪ مبنی‌بر وضعیت تحت فشار بودن سامانه و در سناریوی سوم با احتمال ۸۴/۲٪ مبنی‌بر وضعیت پایین‌بودن سامانه تخمین زده می‌شود.

جدول (۱۰): تخمین نهایی حاصل از سه سناریو برای تمامی حسگرها

T-Total		سناریو ۱	سناریو ۲	سناریو ۳
Estimate Status	Down	۰	۱۶	۸۴
	Slow	۱۰	۷۹	۱۱
	UP	۹۸	۱	۱
Selected Status		۹۸	۷۹	۸۴
		UP	Slow	Down

۵-۴- ارزیابی کلی و طرح پیشنهادی

ارزیابی طرح پیشنهادی را می‌توان در چارچوب شکل (۸) مورد بررسی قرار داد. به‌طوری‌که با اجرای سه سناریو بتوان نشان داد که طرح فوق دارای کارایی مطلوب است. در سناریوی اول که حمله‌ای در کار نبوده است، تلفیق حسگرها با احتمال ۹۹/۳٪ وضعیت خدمت‌رسانی مطلوب و خوب را تشخیص دادند. در سناریوی دوم که سرور قادر به خدمات‌رسانی به‌صورت کند بوده و تحت فشار است تلفیق حسگرها با احتمال ۷۸/۶٪ وضعیت خدمت‌رسانی را تحت فشار تشخیص داده است. در سناریوی سوم که سرور تحت حمله مؤثر قرار دارد تلفیق حسگرها با احتمال ۸۴/۲٪ وضعیت قطع خدمت‌رسانی را تخمین زده‌اند. بدیهی است که طرح پیشنهادی باید بتواند در انواع شرایط عدم قطعیت، تخمین درستی از وضعیت قربانی را تشخیص دهد.

۶- نتیجه‌گیری

ایده به‌کارگیری تلفیق اطلاعات حسگرهای فنی و بشری نشان داد که می‌توان تخمین مناسبی از وضعیت (کمیت و کیفیت) خدمت‌رسانی قربانی به‌دست آورد. در این طرح نشان داده شد که می‌توان با استفاده از داده‌های (دارای عدم قطعیت) موجود در شبکه‌های اجتماعی، رسانه‌های خبری، گزارش‌های مردمی و مانیتورینگ‌های فنی در فضای سایبری می‌توان به رصد وضعیت یک قربانی تحت حمله سایبری DDoS پرداخت. به‌طوری‌که توانستیم این داده‌های هم‌نوع و غیرهم‌نوع را با استفاده از روش منطق فازی و امید ریاضی به‌صورت صوری یا رسمی[1] درآورده و به تخمین مناسبی از انواع وضعیت‌های قربانی رسید.

1- Formal

از طرفی تخمین کمیت و کیفیت خدمت‌رسانی قربانی در حین حمله برای تشخیص وضعیت قربانی، همواره یک چالش اساسی بوده و طرح‌های فعلی، برای شرایط عدم قطعیت (تمهیدات مدافع اعم از مسدودسازی و غیره) پاسخ‌گو نیست که طرح پیشنهادی درصدد رفع این چالش بوده است. بنابراین، نوآوری طرح شامل موارد ذیل است:

- امکان تخمین کمیت و کیفیت خدمت‌رسانی قربانی در حین حمله را با احتمال بیش از ۷۸٪ میسر می‌کند.
- نتایج تخمین پیشنهادی نسبت به گزارش‌های سایت‌های رصدگری (در روش‌های موجود) واقعی و قابل اطمینان‌تر است.
- یک چارچوب برای ارزیابی صحنه نبرد حملات DDoS، با استفاده از چهار حسگر فنی و بشری مطابق اشکال (۳-۲ و ۸)، ارائه گردید که با مدل‌های آگاهی وضعیتی خانم اندس‌لی و تلفیق داده JDL سازگاری دارد. برای ادامه کار و تحقیقات بعدی پیشنهاد می‌گردد با به‌کارگیری حسگرهای دیگر و با استفاده از روش‌های بیزین و مارکوف موجب کاهش ابهامات شد و دقت و قابلیت اطمینان تخمین وضعیت را بهبود بخشید.

۷- مراجع

[1] L. A. Petersen and H. Singh, “Understanding diagnostic errors in medicine: a lesson from aviation,” Qual Saf Health Care, vol.15, no. 3, pp. 159-164, Jun 2006.

[2] B. Saili Waichal, “Router Attacks-Detection And Defense Mechanisms,” International Journal of Scientific & Technology Research, vol. 2, Issue 6, June 2013.

[3] C. Kanich, K. Levchenko, B. Enright, G. M. Voelker, and S. Savage, “The Heisenbot Uncertainty Problem: Challenges in Separating Bots from Chaff,” University of California, San Diego, 2008.

[4] “https://www.site24x7.com/server-monitoring .html”.

[5] C. Bannwart, “Predicting the Impact of Denial of Service Attacks,” August 2012.

[6] C. Rossow, H. Bos, and A. Welzel, “On Measuring the Impact of DDoS Botnets,” EuroSec’14, Amsterdam, Netherlands, April 2014.

[7] K. Kumar, M. Sachdeva, and K. Arora, “Impact Analysis of Recent DDoS Attacks,” International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, vol. 3 no. 2, Feb. 2011.

[8] D. Shen, G. Chen, J. B. Cruz, Jr., L. Haynes, M. Kruger, and E. Blasch, “A markov game theoretic data fusion approach for cyber situational awareness,” Defense and Security Symposium, International Society for Optics and Photonics, p. 65710F, April 2007.

[9] Z. Peng, W. Zhao, and J. Long, “Grey synthetic clustering method for DoS attack effectiveness evaluation,” International Conference on Modeling Decisions for Artificial Intelligence, Springer Berlin Heidelberg, pp. 139-149, July 2011.

[10] L. J. Zhang, Y. Cao, and Q. X. Wang, “A DoS attack effect evaluation method based on multi-source data fusion,” Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1, pp. 91-96, IEEE, 2010.

[11] A. K. Igor kotenko and A. Shorov, “Agent based modeling & simulation of botnets and botnet defense,” Academic of sciences, Conference of cyber conflict proceeding, Petersburg, Russia, 2010.

[12] J. J. Alemán, “A Data Fusion Model for Ambient Assisted Living,” Volume 616 of the series Communications in Computer and Information Science, pp. 301-312, May 2016.

[13] N. A. Giacobe, “Application of the JDL Data Fusion Process Model for Cyber Security,” Proceedings of SPIE, The International Society for Optical Engineering 7710, April 2010.

[14] J. A. Rashidi and D. Khalil Nejad, “Concepts, theories and applications of data integration,” Malek Ashtar University of Technology, ISBN: 978-600-7736-14-2, 2016. (In Persian)

[15] S. A. M. Rizvi and S. K. Malik, “Ontology design and development using ontology editors along with semantic search patterns towards intelligent retrieval of information on web: case studies,” Journal International Journal of Autonomic Computing archive, vol. 2, Issue 1, February 2014.

[16] F. S. Yuan Yuan, “Data Fusion-based Resilient Control System under DoS Attacks: A Game Theoretic Approach,” International Journal of Control Automation and Systems, vol. 13, no. 3, June 2015.

[17] M. R. Endsley, “Final Reflections: Situation Awareness Models and Measures,” Journal of Cognitive Engineering and Decision Making, March 2015.

[18] M. Brunelli, “Introduction to the Analytic Hierarchy Process,” Springer Briefs in Operations Research, P. 83, 2015. 978-3-319-12502-2 (electronic), 10.1007/978-3-319-12502-2.

[19] http://cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/w/World_Wide_Web.htm

[20] T. Min, “QoS integration in Web services with the WS-QoS framework,” Doctoral thesis, p. 74, 2010.

[21] M. H. Hamza Kalai and M. R. M. J. shaman, “IP optimization ant colony algorithm for tracking denial of service attacks,” Journal of electronic and cyber defense, vol. 1, vol.4, 2014. (In Persian), IHU.AC.IR

Journal Of Electronical & Cyber Defence
Vol. 5, No. 3, 2017, Serial No. 19

A Framework For The Status Estimation In Distributed Denial-Of-Service Attacks By Data Fusion Of Human-And-Technical Sensors Based On Fuzzy Logic

V. Akbari, S. M. Safavi Homami*

*Imam Hossein University

(Received: 23/12/2016, Accepted: 13/02/2017)

ABSTRACT

Cyber attackers are able to have a significant impact on the computer networks' hosts by using DDoS attacks. whereas, defenders use different defensive methods to defend themselves. In such circumstances, it is difficult to determine the network status of the defender (victim). In order to assess the cyber battle scene, it is necessary to evaluate the attacker and defender. The focus of this paper is to provide a framework to assess the status of the victim. In this study, monitoring of the victim is done by using different types of cyber sensors including both technical and human sensors through modeling and simulation. Initially, we review the cyberspace sensors, such as news sites, social networks, reports of the people and technical sensors. The attributes of each sensor are extracted and finally the importance of each feature is evaluated by using the experts' analytic hierarchy process. Then the combination of attributes for each of the sensors is formed and status of the victim corresponding to the features is determined. The conditions of data fusion using the methods based on fuzzy logic are provided. Implementation of three scenarios show that the proposed method has the desired performance. In the first scenario, in which there was no attack, data fusion sensors have correctly estimated with a probability of 99.3%. In the second scenario, in which the server provides the service slowly and under pressure estimates with probability of 78.6%. In the third scenario, in which the server is under effective attack, data fusion sensors with a probability of 84.2% have estimated correctly. The lack of information about each of the sensors will cause conditions for uncertainty. In this study, we have evaluated 15 different cases. The results show that the proposed method for situation awareness of the host under attack has appropriate evaluation capabilities.

Keywords: DDos, Data Fusion, Fuzzy Rule Based Classification System, Human & Technical of Sensors

* Corresponding Author Email: msafavi@aut.ac.ir