فصلنامه فرماندهی و کنترل، سال اول، شماره ۲، زمستان ۱۳۹۵

تعیین وضعیت ماشین قربانی با استفاده از تلفیق دادهٔ حس‌گرهای سایبری در سطح بسته

حمید اکبری[۱]، سیدمصطفی صفوی همامی[۲]

تاریخ دریافت: ۹۵/۹/۷ تاریخ پذیرش: ۹۵/۱۰/۲۰

چکیده

مهاجمان سایبری قادرند با استفاده از حمله‌های جلوگیری از خدمت‌رسانی، تأثیرهای بسزایی بر میزبان‌های شبکهٔ رایانه‌ای بگذارند. مدافعان با استفاده از انواع روش‌های دفاعی ازجمله فیلترینگ به دفاع می‌پردازند. در چنین شرایطی تعیین وضعیت شبکهٔ قربانی سخت و پیچیده می‌گردد. برای ارزیابی وضعیت صحنهٔ نبرد سایبری ضروری است، مهاجم و مدافع مورد ارزیابی قرار گیرند که این مقاله، چارچوبی کلی را برای این منظور پیشنهاد داده و در ادامه، تنها وضعیت قربانی مورد ارزیابی قرارگرفته است. در این تحقیق، رصد قربانی در دو حالت تک حس‌گری و شبکهٔ حس‌گری با انواع احتمال‌های فیلترینگ و خرابی حس‌گر مورد مدل‌سازی و شبیه‌سازی قرارگرفته است. در حالت تک حس‌گری میزان دقت تشخیص حس‌گر با افزایش فیلترینگ و میزان خرابی، کاهش می‌یابد؛ به‌گونه‌ای که در ۵٪ فیلترینگ، با افزایش خرابی حس‌گر از صفرتا ۵۰٪، دقت اندازه‌گیری از ۹۷٪ به ۷۳٪ کاهش می‌یابد. با افزایش فیلترینگ مشاهده می‌شود که تأثیرگذاری خرابی حس‌گر، کاهش می‌یابد؛ به‌گونه‌ای‌که اثرگذاری در ۱۰۰٪ فیلترینگ، دقت اندازه‌گیری در ٤۹٪ ثابت مانده است، همچنین با استفاده از روش n گرام (با n های ۲ تا ٤) تلاش شد با امکان خطایابی، دقت تشخیص را از ۵۰٪ به ۷۸٪ بهبود داد. در حالت شبکهٔ حس‌گری ملاحظه شد که بخشی از حس‌گرها قادرند قربانی را رصد کنند و از این‌رو جدول نگاشتی تهیه شد تا رابطهٔ حس‌گرهای بینا را با میزان فیلترینگ و خرابی نشان دهد. در ادامه تحقیق، داده حس‌گرها با روش‌های میانگین‌گیری و رأی‌گیری مورد تلفیق قرار گرفت که رأی‌گیری ٤ تایی بیشترین دقت (۹۰٪) را نسبت به سایرین داشت. بااین‌حال عدم قطعیت باقی‌مانده، با ارائهٔ دو روش تشخیص روند فیلترینگ و تشخیص روند تأخیر پاسخ خدمت‌رسانی، پیشنهاد گردید. در پایان برای آگاهی از وضعیت میزبان تحت حمله، چارچوبی ارائه شده است.

واژگان کلیدی: ادغام داده، شبکهٔ حس‌گری سایبری، عدم قطعیت، فیلترینگ، حمله‌های منع خدمت توزیع‌شده، تشخیص صحیح خدمت‌رسانی

۱. دانشجوی دکتری، دانشکده جنگ الکترونیک و دفاع سایبری، دانشگاه امام حسین (ع)، hamidakbari@ihu.ac.ir

۲. دانشیار، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر، msafavi@aut.ac.ir

۱. کلیات

۱-۱. بیان مسئله

شبکهٔ بات[1]، مجموعه‌ای از میزبان‌هایی[2] است که تحت تسلط سامانهٔ فرماندهی و کنترل مهاجم سایبری برای مقاصد گوناگونی ازجمله شناسایی، رصدگری و حملهٔ منع خدمت توزیع‌شده[3] مورد استفاده قرار می‌گیرند (Hohlfeld, et.al, 2014:3). در حملهٔ منع خدمت توزیع‌شده مهاجمان با فرمان به شبکهٔ بات، سیلی از بسته‌ها را به سمت قربانی گسیل کرده و آن را از کار می‌اندازند (Daniel, et.al, 2013). در رصد و آگاهی از وضعیت حمله‌های دی داس و تأثیر آن بر روی قربانی، باوجود تمهیدهای امنیتی ازجمله فیلترینگ[4] و غیره شرایط عدم قطعیت حاکم است (Kanich, et.al, 2008). بدیهی است دسترسی به منابع قربانی و شاهراه‌های ارتباطی می‌تواند در کاهش عدم قطعیت بسیار مؤثر باشد، ولی به علت عدم دسترسی به منابع بالا، رصد اثرگذاری حمله‌ها در هاله‌ای از ابهام باقی می‌ماند. حس‌گرها (فنی و بشری) یا دیدبان‌ها وظیفهٔ رصدگری را بر عهده داشته و تأثیرگذاری بسزایی در آگاهی وضعیتی صحنهٔ نبرد دارند؛ به‌گونه‌ای که تأثیر آن بیش از ٦٥ درصد بوده (Petersen, et.al, 2006:159-164) و بخش مهم خطاها (خرابی حس‌گرها، عوامل ناشناخته و ...) شرایط عدم قطعیت را به وجود آورده و موجب تشخیص غلط می‌گردد، بنابراین ارزیابی از خدمت‌رسانی قربانی در شرایط عدم قطعیت، مسئلهٔ اصلی تحقیق حاضر است که محقق به‌دنبال حل علمی آن است.

۱-۲. اهمیت و ضرورت موضوع تحقیق

مهاجم سایبری، زمانی می‌تواند اقدام‌های مؤثری داشته باشد که بتواند اثر حملات خود را بر روی خدمت رسانی‌های قربانی مشاهده کند، از این‌رو آگاهی یافتن از وضعیت صحنهٔ نبرد سایبری ضرورت پیدا می‌کند و نیاز است چالش‌های این حوزه، شناسایی شده و برای آن راهکارهای ارائه شود.

۱-۳. هدف تحقیق

هدف اصلی این پژوهش، ایجاد آگاهی وضعیتی از صحنهٔ نبرد سایبری است؛ به‌گونه‌ای که بتوان وضعیت هدف‌هایی که مورد هجوم هستند را به‌درستی درک کرد و تأثیر حملات آنها را در چگونگی خدمت‌رسانی قربانی، مشاهده نمود، از این‌رو هدف‌های فرعی پی‌بردن به چالش‌های رصدگری توسط حس‌گرهای سایبری (در سطح بسته) و شناسایی عوامل عدم قطعیت و یافتن راه‌حل‌هایی است که بتواند موجب کاهش بی‌دقتی در تشخیص وضعیت ماشین‌های تحت حمله شود و در نهایت، چارچوبی ارائه شود که آگاهی از وضعیت صحنهٔ نبرد سایبری را با دقت ترسیم کند.

۱-٤. پیشینهٔ تحقیق

مانیتورینگ یا پایش شبکه از پرکاربردترین فعالیت‌هایی است که مدیر شبکه برای مدیریت بهتر و بالابردن کارایی شبکه به آن نیاز دارد که پایش تمامی دستگاه‌ها اعم از ماشین‌های خدمات‌دهنده، مسیریاب‌ها، سوئیچ‌ها، دیواره‌های آتش، منبع تغذیه بدون وقفه و ... را شامل می‌شوند، از این‌رو به‌راحتی می‌توان از ابزارهای مانیتورینگ برای صحت یا عدم صحت کارکرد دستگاه‌های فوق آگاه شد و حتی با پایش

1. Botnet
2. Host
3. Distributed Denial of Service (DDoS)
4. Filtering

پردازنده‌ها، حافظه و ذخیره‌سازهای سخت[1]، می‌توان از میزان مصرف آنها آگاه شد و وضعیت‌های بحرانی سامانه را کشف و مورد رسیدگی قرار داد (Barth, 2008). بدیهی است کارکرد ابزارهای بالا، وابسته به دسترسی‌های مجاز به تمامی سامانه‌ها بوده و برای سایر پایش‌کنندگان امکان‌پذیر نمی‌باشد. در حال حاضر در مواجه با حملات دی داس، امکان رصد و پایش، فقط با استفاده از دسترسی به مسیریاب‌های اصلی و بین‌المللی و آن هم فقط توسط صاحبان فناوری و نیز توسط مالکان ماشین خدمات‌دهنده (قربانی) امکان‌پذیر است (Waichal, et.al, 2013)، ولی این دسترسی نمی‌تواند توسط دیگران مورد استفاده قرار گیرد. راه دیگر این است که رصد قربانی با استفاده از شبکهٔ دیدبانی انجام می‌شود که دیدبان‌ها مبادرت به اندازه‌گیری پاسخ زمانی خدمت‌رسانی قربانی و DNS و سرعت انتقال اطلاعات می‌کنند که با توجه به خرابی حس‌گرها و احتمال وجود فیلترینگ در مسیر دیدبان‌ها شرایط عدم قطعیت به وجود می‌آید و اندازه‌گیری‌ها کم‌دقت می‌شوند (Kanich, et.al, 2008). آثار این روش‌ها را می‌توان در برخی از وبگاه‌های مانیتورینگ معتبر مانند www.24x7.com ملاحظه نمود و شاهد بی‌دقتی‌های آن بود. آقای شان و همکاران (Shen, et.al, 2007)، در صدد ارائهٔ آگاهی وضعیتی دفاع سایبری هستند که بتوانند در لایهٔ صفر ادغام با دریافت داده‌های هشداری از حس‌گرهای تشخیص نفوذ[2] و جلوگیری از نفوذ[3] و وقایع ثبت‌شدهٔ سامانه[4]، آنها را مورد پالایش قرار دهند و در لایهٔ یک، به ارزیابی هدف (شی) پرداخته و در لایه‌های دوم و سوم با استفاده از مدل بازی مارکوف و مجموع موجودیت‌های سلسله‌مراتبی به ارزیابی وضعیت‌ها و تهدیدها دست یابند. ایشان روش بازی مارکوف[5] را به‌منظور تخمین و باورپذیری هر یک 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 دیدبانی قابل بهره‌برداری نیست. در مقاله‌ای آقای ارنه ولزل و همکاران سرورهای فرماندهی و کنترل[6] ۱٤ شبکهٔ بات DIRTJUMPER و YODDS را مورد مانیتورینگ قرار داده و توانسته‌اند، هدف‌های مورد حملهٔ منع خدمت توزیع‌شده را روی شبکه فوق ضبط کنند(Welzel, et.al, 2014)، سپس آنها با استفاده از انواع اندازه‌گیری‌ها از قبیل زمان پاسخ TCP و تحلیل محتوای HTTP توانستند دسترس‌پذیری قربانی‌ها را ارزیابی کنند. آنها نشان دادند که بیش از ٦٥٪ قربانی‌ها توسط حملات DDOS به‌شدت آسیب‌پذیر هستند و حملات کمتری به شکست منجر می‌شوند. در تحقیق یادشده، مبنای کار محقق، بهره‌مندی از دسترسی به مسیریاب‌های کلیدی بوده است که برای همگان میسر نمی‌باشد. در مقاله آقای سایریل بن‌وارت ادعا کرده که می‌توان از راه دور بدون نصب ابزاری در ماشین قربانی، مبادرت به‌اندازه گیری اثر حملهٔ دی‌داس[7] کرد (Bannwart, 2012). او در محیط آزمایشگاه نشان داد که حملهٔ فلش‌کرود بر روی دو معیار گذردهی مفید (داخلی) و زمان رفت‌وبرگشت

1. Hard Disk
2. Intrusion Detection Sensors (IDS)
3. Intrusion Prevention Sensors (IPS)
4. System Logs

5. Markov
6. Command & Control
7. DDoS

خدمت‌رسانی (خارجی) تأثیرگذار است و ضریب همبستگی مثبتی بین آنها وجود دارد. طرح پیشنهادی وی، برای محیط‌هایی که دارای عدم قطعیت (شرایط فیلترینگ) است، پاسخگو نمی‌باشد. آقای پنگ و همکاران نیز برای ارزیابی تأثیر حملهٔ منع خدمت، شاخص‌هایی همچون مصارف پهنای باند، پردازش، حافظه، تأخیر زمان پاسخ، گم‌شدن بسته، زمان (موردنیاز) بازیابی، روش‌های حمله (مصرف منابع، از کار انداختن خدمت و از کار انداختن سامانه) را در قالب یک ماتریس در آورده و تأثیر ۱۰ نوع حملهٔ شبیه‌سازی‌شده را با استفاده از خوشه‌بندی ترکیبی خاکستری مورد ارزیابی قرار دادند و توانستند حملات ده‌گانه را به چهار دسته ضعیف، معمولی، خوب و خیلی خوب تقسیم نمایند (Peng, et.al, 2011:139-149). اشکال این روش آن است که نمی‌توان شاخص‌های فوق را (به‌جز تأخیر زمان) بدون همکاری از ماشین قربانی به دست آورد. آقای ژانگ و همکاران تلاش کرده‌اند از یک روش تلفیق داده چند منبعی (حس‌گر) برای ارزیابی تأثیر حملهٔ منع خدمت استفاده کنند (Zhang, et.al, 2010:91-96). آنها با استفاده از تعدادی ماشین در نقاط مختلف شبکهٔ مبادرت به اندازه‌گیری پاسخ تأخیر زمانی ماشین قربانی کرده و داده‌های گردآوری‌شده را پس از پالایش، مورد ادغام قرار داده و سپس با استفاده از محاسبهٔ آنتروپی (تأخیر پیش و پس از حمله) به ارزیابی حمله پرداخته‌اند. اشکال روش ژانگ زمانی آشکار می‌شود که تأخیر زمانی یک یا اندکی از حسگرها در مقایسه با سایر حسگرها بسیار کمتر باشد که در این صورت برآیند حاصل از طرح پیشنهادی وی، عدد بزرگی خواهد بود؛ به‌عبارتی تأثیر حمله، مثبت ارزیابی خواهد شد در حالی که این، کل حقیقت نیست، همچنین اگر تمامی حس‌گرها در معرض فیلترینگ قرار بگیرند، طبق طرح پیشنهادی، تمامی حسگرها از روند محاسبه‌ها خارج شده و قادر به اندازه‌گیری تأثیر حمله نخواهند بود و ارزیابی نادرستی را از وضعیت قربانی اعلام می‌کنند. بنابراین روش پیشنهادی نویسنده، برای دو مشکل بالا، دارای راه‌حل می‌باشد، بنابراین می‌توان نتیجه گرفت که کارهای انجام‌شده در مورد مانیتورینگ، پاسخگوی شرایط عدم قطعیت نمی‌باشند و عموم آنها نیز نیازمند همکاری خدمات‌دهندگان و همچنین دسترسی به مسیریاب‌های کلیدی می‌باشند، از این‌رو تحقیق پیش‌رو در نظر دارد چالش‌های رصدگری ماشین‌های خدمات‌دهنده را با استفاده از مدل پیشنهادی هموار کند.

۵-۱. پرسش تحقیق

۱-۵-۱. پرسش اصلی

رصد خدمت‌رسانی قربانی تحت حملهٔ منع خدمت توزیع‌شده چگونه است؟

۲-۵-۱. پرسش‌های فرعی

(۱) چالش‌ها و موانع شبکهٔ حس‌گری سایبری در مواجه با دسترس‌پذیری به ماشین‌های تحت حملهٔ منع خدمت چیست؟

(۲) چگونه می‌توان عوامل عدم قطعیت در شبکهٔ حس‌گری را کاهش داد؟

٦-۱. روش تحقیق

در این تحقیق با استفاده از مدل‌سازی و شبیه‌سازی شبکهٔ حس‌گری سایبری در سطح بسته به بررسی عوامل عدم قطعیت، تبیین وضعیت‌های متصور و پیشنهادهای کاهش عدم قطعیت و ارزیابی نتایج حاصل

پرداخته می‌شود و داده‌های مورد نیاز با استفاده از کد برنامه نویسی C++ تهیه شده است.

۷-۱. سازماندهی تحقیق

ساختار این پژوهش در چهار بخش تنظم شده است که فصل اول شامل بیان مسئله، ضرورت و اهمیت، اهداف، پیشینه، پرسش و روش تحقیق است.

در فصل دوم به مبانی نظری در قالب چارچوب کلی ارزیابی صحنهٔ نبرد اشاره شده و در فصل سوم به یافته‌های تحقیق اعم از مدل‌سازی و شبیه‌سازی شبکهٔ حسگری سایبری، چالش‌ها و راه‌حل‌ها پرداخته می‌شود و در پایان در فصل نتیجه‌گیری به جمع‌بندی و پیشنهاد کارهای آتی اشاره می‌گردد.

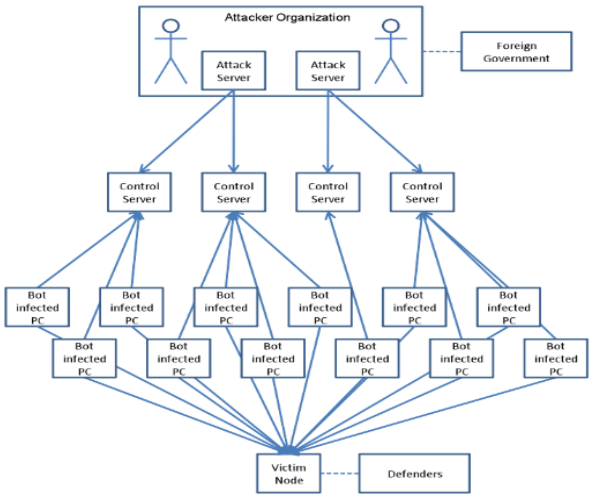
۲. ادبیات تحقیق

۱-۲. حمله‌های منع خدمت توزیع‌شده

حملهٔ منع خدمت، تلاش برای از کار انداختن سامانهٔ کاربر یا سازمان است. در حملهٔ منع خدمت، مهاجم تلاش می‌کند تا سامانه‌ای را از حالت پایدار خارج کند و یا سرعت سامانه 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 کند، بلکه هدف این است که اجازهٔ خدمت‌رسانی به کاربران قانونی را بگیرد. هدف‌های حمله‌های منع خدمت شامل گسیل ترافیک عظیم (بسته‌های سیل‌آسا) به‌سوی شبکهٔ قربانی برای جلوگیری از ترافیک مجاز شبکه، قطع ارتباط بین دو ماشین جهت عدم دسترسی به خدمات، منع دسترسی افراد به خدمات است. حملهٔ منع خدمت به‌عنوان یک حملهٔ غیرپیچیده شناخته می‌شود به این‌علت که مهاجم نمی‌تواند به اطلاعات دسترسی پیدا کند و فقط در خدمت‌رسانی آن، اختلال به وجود می‌آورد. حمله‌های منع سرویس دو نوع می‌باشند: نوع اول حملاتی که توسط یک سامانه به یک سامانهٔ دیگر انجام می‌شود (منع خدمت ساده) و نوع دوم حملاتی که توسط چندین سامانه به یک سامانه انجام می‌شود (منع خدمت توزیع‌شده) که پیشرفته‌تر از نوع اول است.

حملات منع خدمت در مقیاس‌های بسیار بزرگ و توزیع‌شده علیه یک سامانه انجام می‌شود (Charalampos, et.al, 2004). در این حملات، تعداد زیادی بسته از طریق صدها یا هزاران ماشین برای از کار انداختن منابع قربانی (شامل پردازنده، حافظه و پهنای باند شبکه) ارسال می‌شود. گفتنی است که این ماشین‌های مهاجم، تحت عنوان شبکهٔ بات سازماندهی می‌شوند. انواع روش‌های حمله وجود دارند که می‌توانند هر یک از منابع شبکه را مورد هدف قرار دهند که به‌طور نمونه می‌توان به syn flood و udp flood اشاره کرد. در شکل (۱) معماری حملات جلوگیری از خدمات توزیع‌شده ارائه گردیده است.

شکل ۱. معماری حملات منع خدمت توزیع‌شده
(Charalampos, et.al, 2004)



ماشین این حملات، قدرتمندتر از سایر حملات بوده و تشخیص و مقابله با آنها نیز سخت‌تر است. برای ارزیابی تأثیر این نوع حملات، از معیارهایی همچون محاسبه هزینهٔ خسارت، افت کیفیت خدمت، بازدهی تراکنش، تأخیر در خدمت و غیره استفاده می‌شود.

۲-۲. دیدبانی

به‌منظور نظارت بر وضعیت خدمات ارائه‌شده از سوی خدمت‌دهندگان (میزبان‌ها)، نیاز است آنها همواره مورد رصد دیدبان‌های مستقل شبکه قرار بگیرند. در اینجا دیدبان‌ها وظیفه‌دارند از اقصی نقاط (جهان) در بازه‌های زمانی مشخص نسبت به دسترس‌پذیر بودن خدمت‌رسانی پایش کنند. بدیهی است اگر از نقاطی، عدم دسترسی وجود داشته باشد، لازم است ماشین خدمت‌رسان (میزبان) به سرعت مطلع شده و نسبت به رفع مشکل اقدام نماید. گفتنی است در مواجهه با حملات دی داس، مهاجم نیز درصدد دیدبانی از قربانی (خدمات مورد حمله) است. در اینجا دسترس‌پذیری خدمات، کیفیت خدمت (زمان پاسخ) و غیره انتظاراتی است که از دیدبانی باید حاصل کرد، همچنین دیدبانی را می‌توان برای اقدام‌های مهاجم در نظر گرفت؛ به‌گونه‌ای که بتوان مشخص کرد که از چه نقاطی، با چه تعداد ماشین مهاجم، با چه پهنای باندی و با چه روشی (متدی) به کدام‌یک از خدمات قربانی حمله می‌کند. در اینترنت این دیدبانی‌ها توسط سازمان‌هایی انجام می‌گیرد که به ترافیک شاهراه‌ها و مسیریاب‌های اصلی دسترسی دارند. از این جمله می‌توان به شرکت‌هایی مانند اکاما[1] و پرولگزیک[2] و یا دانشگاه آلاباما[3] اشاره کرد.

۳-۲. انواع روش‌های دیدبانی

دیدبانی از ماشین‌های خدمت‌رسان (قربانی) از چند منظر قابل دسته‌بندی است:

دستهٔ اول: با استفاده از یک یا چند کاربر، ماشین قربانی مورد رصد قرار می‌گیرد.

دستهٔ دوم: با استفاده از شبکهٔ بات (ربات‌ها) در اقصی نقاط جهان به‌صورت منظم، مدافع یا قربانی رصد می‌شود. هم‌اکنون وبگاه‌هایی مانند www.24x7.com یا host_tracker.com یا alertra.com این کار را انجام می‌دهند.

دستهٔ سوم: با استفاده از صفحات اجتماعی که میزبان (قربانی)ها ممکن است وضعیت وبگاه خود را در آنجا اعلام کنند.

دستهٔ چهارم: با استفاده از اظهارنظر مردمی در وبگاه‌هایی مانند sitedown.co و غیره.

دستهٔ پنجم: با استفاده از اظهارنظرهای مردمی نسبت به وضعیت ماشین‌های خدمت‌رسان در شبکه‌های اجتماعی، وبگاه‌های خبری و غیره.

این تحقیق در نظر دارد دیدبانی‌های دستهٔ اول و دوم را مورد کنکاش قرار دهد.

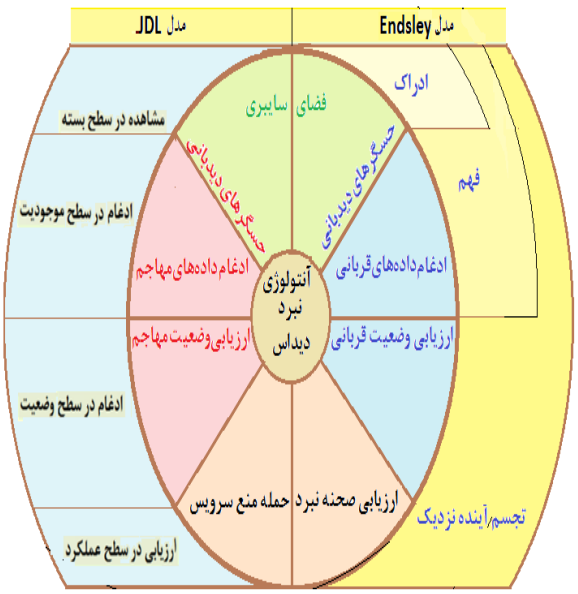
٤-۲. مدل مفهومی آگاهی از وضعیت صحنهٔ نبرد سایبری

حس‌گرهای رصد قربانی و شبکهٔ بات مهاجم در فضای سایبری قرار دارند که مبادرت به دیدبانی

1. Akama
2. Prolexic
3. Alabama

می‌کنند. در ادامه لازم است ادغام داده انجام شود تا به ارزیابی وضعیت صحنهٔ نبرد طرفین نزدیک شد. در این میان، وجود یک آنتولوژی کارآمد، تمامی بخش‌ها را پشتیبانی کرده و پرسش «چه کارهایی باید کرد؟» را پاسخگو است (Rizvi et.al, 2014). در حالت کلی می‌توان ارزیابی وضعیت صحنهٔ نبرد حملهٔ دی‌داس را به‌صورت شکل (۲) متصور شد. مدل پیشنهادی با مدل پنج لایهٔ JDL[1] (Yuan, 2015) و مدل سه لایهٔ آگاهی وضعیتی اندسلی[2] (Endsley, 2015) دارای هم‌پوشانی است با این تفاوت که این مدل توسط یک آنتولوژی نبرد دی‌داس پشتیبانی می‌گردد.

شکل ۲. شمای کلی طرح پیشنهادی برای ارزیابی صحنهٔ نبرد حمله دی داس



سمت راست مربوط به قربانی و سمت چپ مربوط به مهاجم است. به‌منظور تجزیه و تحلیل و ارزیابی دیدبان‌های حملات دی‌داس لازم است مدل‌سازی در این خصوص انجام می‌شود. در ابتدا به ارزیابی وضعیت قربانی پرداخته می‌شود. از این رو رصدگری تک حسگری و در ادامه چند حسگری (شبکه‌ای) مدل‌سازی شده و مورد شبیه‌سازی قرار می‌گیرند. در ادامه با انجام آزمایش در محیط شبیه‌سازی، نتایج ارزیابی‌شده و میزان دقت و خطای مدل‌ها، اندازه‌گیری می‌شوند. در انجام آزمایش‌های مربوط، چند راهکار (بهره‌مندی از چند الگوریتم) برای تشخیص وضعیت صحنهٔ نبرد پیشنهاد می‌گردد و برای صحت و درست‌یابی آنها اقدام به شبیه‌سازی جامع کرده و با استفاده از معیارهای کارایی، آنها مورد سنجش و ارزیابی قرار می‌گیرند.

۳. یافته‌های تحقیق، مدل‌سازی و شبیه‌سازی حس‌گرهای سایبری

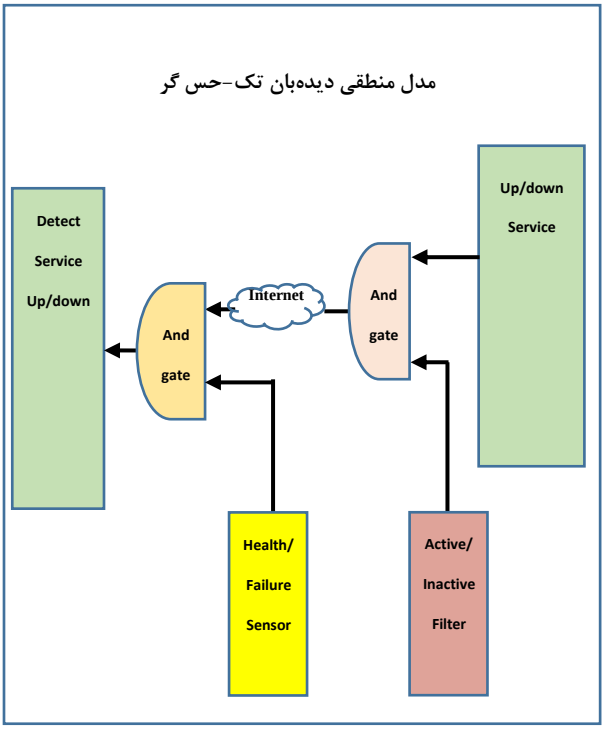
همان‌گونه که در بخش پیش اشاره شد، نیاز است دیدبان‌های سایبری مورد مدل‌سازی قرار گیرند، بنابراین در دو مرحله مدل‌سازی تک حس‌گر و مدل‌سازی شبکهٔ حس‌گری انجام می‌شود.

۳-۱. مدل‌سازی تک حس‌گر

به‌منظور ارزیابی دیدبان تک حس‌گر دی‌داس، مدل منطقی مربوط به شکل (۳) ارائه شده است.

1. Joint Direction Literary
2. Endsley

شکل ۳. مدل منطقی دیدبان تک حس‌گر



عناصر مدل پیشنهادی شامل یک ماشین خدمت‌رسان (قربانی) و سازوکار امنیتی فیلترینگ آن و دیدبان است که نقش هر یک از عناصر به شرح زیر است:

ماشین خدمت‌رسان (قربانی): دارای دو نقش خدمت‌رسانی[1] و عدم خدمت‌رسانی[2] است.

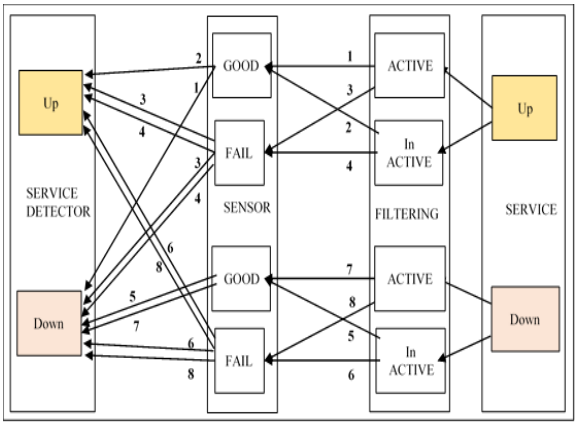
مکانیسم دفاعی فیلترینگ: دارای دو نقش اعمال فیلترینگ[3] و یا عدم اعمال فیلترینگ[4] از سوی ماشین خدمت‌رسان یا عوامل کمکی آنهاست، بنابراین فعال بودن آن موجب حجاب حس‌گر از قربانی می‌گردد.

1. Up
2. Down
3. Active
4. In Active

دیدبان (حس‌گر): دارای دو وضعیت حس‌گر سالم[5] یا خراب[6] است که نتایج کارش تشخیص وضعیت خدمت‌رسانی (قربانی) است.

تحلیل این مدل در شکل (٤) در چهار قسمت آمده است:

شکل ٤. مدل‌سازی دیدبانی حملات دی داس از خدمت‌رسانی (قربانی) در شرایط احتمالی فیلترینگ و خرابی حس‌گر



قسمت اول (سمت راست) وضعیت خدمت‌رسانی را در دو حالت ارائه خدمت‌رسانی و عدم خدمت‌رسانی نشان می‌دهد که لازم است توسط حس‌گر در قسمت چهارم تشخیص داده شود. قسمت دوم مربوط به اعمال یا عدم اعمال فیلترینگ توسط قربانی یا مسیریاب‌های پشتیبان است. قسمت سوم مربوط به وضعیت صحت حس‌گر است در دو حالت سالم یا خراب است و درنهایت، قسمت چهارم مربوط به سامانهٔ تشخیص است که تعیین کند خدمت‌رسانی توسط قربانی ارائه می‌گردد یا خیر؟

انتظار می‌رود در صورت عدم فیلترینگ و صحت حس‌گر، میزان تشخیص دقیق بوده و در صورت

5. Health
6. Fail

برقراری خدمت‌رسانی، حس‌گر وجود خدمت‌رسانی را تشخیص بدهد و بالعکس.

رفتار فیلترینگ به این‌صورت است که اگر در مسیر حس‌گر قرار گیرد، حس‌گر کور شده و می‌تواند خدمت‌رسانی قربانی را رصد نماید. با خراب بودن حس‌گر نیز سامانه تشخیص نمی‌تواند قربانی را به‌درستی رؤیت نماید و وضعیت آن را به‌طور صحیح اطلاع دهد. تمامی حالات بالا را می‌توان به‌صورت جدول (۱) در نظر گرفت که دارای احتمال وقوع مشخصی می‌باشند.

جدول ۱. نتایج حاصل از شبیه‌سازی حس‌گر حملات دی داس در حالت‌های مختلف فیلترینگ و خرابی حس‌گر

احتمال دقت و خطا						درصد فراوانی‌ها				فراوانی دقت و خطاها در شرایط خرابی حس‌گر و فیلترینگ‌های مختلف							
ETotal	EF	ET	TotalA	ATnS	ATS	%GTT	%GFF	TF+FT	TT+FF	GTT	GFF	TF	FT	TT	FF	FILTERING	FAIL SENS
0	0	0	1	1	1	0	0	0	100	0	0	0	0	500472	499528	0	0
0.025	0.045	0.003	0.975	0.955	1	0.3	4.7	2	97	1520	23403	23551	1496	476921	498032	0	5
0.05	0.086	0.007	0.95	0.914	0.99	0.7	9.5	5	94	3054	46939	47012	3016	453460	496512	0	10
0.1	0.16	0.015	0.9	0.84	0.99	1.5	19	9	90	6068	94003	93953	6040	406519	493488	0	20
0.2	0.278	0.037	0.8	0.722	0.96	3.9	38.5	20	79	12073	187797	187935	12088	312537	487440	0	40
0.25	0.327	0.054	0.75	0.673	0.95	5.7	48.5	25	74	15008	235061	235025	15176	265447	484352	0	50

۲-۳. شبیه‌سازی رصدگر تک حس‌گر

به‌منظور درست‌یابی و ارزیابی مدل و مشخص شدن رفتار آن، نیاز است تا مدل بالا با استفاده از شبیه‌سازی در یک محیط عملیات دیدبانی سایبری آزمایش‌شده تا رفتار حس‌گر مورد بررسی قرار گیرد، ازاین‌رو مدل فوق با استفاده از برنامهٔ موجود در پیوست (الف) که با زبان C++ نوشته شده است، مورد پیاده‌سازی و اجرا قرار گرفت. این برنامه یک‌میلیون بار اجرا گردید؛ به‌گونه‌ای که در هر بار، وضعیت خدمت‌رسانی را در دو حالت وجود خدمت‌رسانی و عدم خدمت‌رسانی به‌صورت تصادفی (با رعایت الگوی تغییرات) در نظر می‌گیرد، همچنین با احتمال‌های مفروض و سفارشی (حداکثر فیلترینگ مشخص)، اعمال یا عدم اعمال فیلترینگ را به‌صورت تصادفی تولید کرده و نتیجه را در اختیار حس‌گر موردنظر قرار می‌دهد. حال با حداکثر احتمال خرابی مشخص، وضعیت صحت حس‌گر معین می‌گردد و در نهایت، موجب تشخیص وضعیت‌های وجود خدمت‌رسانی یا عدم خدمت‌رسانی را فراهم می‌آورد.

۱-۲-۳. میزان اندازه‌گیری دقت و خطای تک حس گر

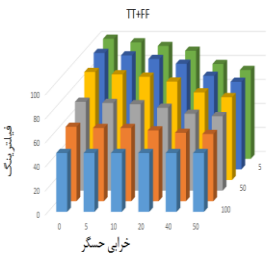
به‌منظور ارزیابی دقیق مدل، در یک‌میلیون بار اجرا، میزان احتمال فیلترینگ و خرابی حس‌گر طبق جدول شمارهٔ (۲- سمت چپ) با گام‌های کوچک و مشخص در ۳۶ شبیه‌سازی، افزایش‌یافته و نتایج استخراج‌شده است. در جدول (۱- سمت چپ)، FF مربوط به تعداد نتایج خروجی حس‌گر است که وقتی خدمت‌رسانی برقرار نبوده، حس‌گر نیز آن را درست (عدم خدمت‌رسانی) تشخیص داده است و TT مربوط به

تعداد نتایجی است که وقتی خدمت‌رسانی برقرار بوده، حس‌گر نیز آن را درست (وجود خدمت‌رسانی) تشخیص داده است. به همین ترتیب FT مربوط به تعداد نتایج خروجی حس‌گر در حالتی است که سرویس برقرار نبوده، حس‌گر به اشتباه، وجود سرویس را تشخیص داده است و TF نیز عکس آن می‌باشد. در ادامه GFF مربوط به تعداد نتایج خروجی حس‌گر است که وقتی سرویس برقرار نبوده، به‌دلیل خرابی حس‌گر، بطوراتفاقی درست یعنی عدم سرویس را تشخیص داده است، همچنین GTT مربوط به تعداد نتایج خروجی حس‌گر است که وقتی سرویس برقرار بوده، به‌دلیل خرابی حس‌گر، به‌طور اتفاقی درست (وجود سرویس) تشخیص داده است. در شکل (۵- الف و ب) به ترتیب جدول و نمودار دقت تشخیص صحیح مدل نشان داده شده است. همان‌گونه که در شکل (۵-الف) ملاحظه می‌شود میزان دقت تشخیص حس‌گر با افزایش فیلترینگ و میزان خرابی، کاهش می‌یابد؛ به‌گونه‌ای که در ۵٪ فیلترینگ، با افزایش خرابی حس‌گر از صفر تا ۵۰٪، دقت اندازه‌گیری از ۹۷٪ به ۷۳٪ کاهش می‌یابد، همچنین با افزایش فیلترینگ مشاهده می‌شود که تأثیرگذاری خرابی حس‌گر، کاهش می‌یابد؛ به‌گونه‌ای که اثرگذاری در ۱۰۰٪ فیلترینگ، دقت اندازه‌گیری در ۴۹٪ ثابت مانده است.

شکل ۵. میزان دقت تشخیص صحیح مدل

%(TT+FF)	حداکثر درصد خرابی حس‌گر					
	0	5	10	20	40	50
حداکثر درصد اعمال فیلترینگ 100	49	49	49	49	49	49
75	62	61	61	59	57	56
50	74	73	72	69	64	62
20	90	88	86	82	73	69
5	97	95	92	88	78	73
0	100	97	94	90	79	74

الف- جدول نگاشت میزان دقت تشخیص صحیح مدل



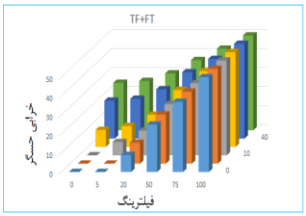
ب- میزان دقت تشخیص صحیح مدل

مشاهده می‌شود که با هر درصد از خرابی حس‌گر با افزایش فیلترینگ، دقت اندازه‌گیری به سمت ۴۹٪ کاهش و به آن همگرا می‌شود؛ این به آن معناست که میزان تغییرات فیلترینگ نسبت به تغییرات خرابی حسگر تأثیر بیشتری دارد، همچنین این نتایج نشان می‌دهد در شرایط فیلترینگ ظهور عدم قطعیت بیشتر مشهود می‌گردد؛ زیرا دقت تشخیص ۵۰ درصد بیانگر اوج نامعلومی تشخیص است. شکل (۶-الف و ب) نیز به ترتیب بیانگر جدول و نمودار میزان تشخیص نادرست حس‌گر (خطای تشخیص) در مواجه با شرایط فیلترینگ و خرابی حس‌گر است.

شکل ۶. میزان خطای تشخیص حس گر

%(TF+FT)	حداکثر درصد اعمال فیلترینگ					
	0	5	20	50	75	100
حداکثر درصد خرابی حسگر 0	0	2	9	25	37	50
5	2	4	11	26	38	50
10	5	7	13	27	38	50
20	9	11	17	30	40	50
40	20	21	26	35	42	50
50	25	26	30	37	43	50

الف- جدول نگاشت میزان خطای تشخیص حسگر



ب- نمودار میله ای سه بعدی میزان تشخیص غلط

همان‌گونه که ملاحظه می‌شود با افزایش فیلترینگ، میزان تغییرات تأثیرگذاری خرابی حس‌گر کاهش می‌یابد؛ به‌گونه‌ای که در ۵٪ فیلترینگ، عامل خرابی حس‌گر، موجب افزایش دقت تشخیص نادرست از ۲٪ به ۲۶٪ می‌شود، درحالی‌که همین تغییرات اثرگذاری، در ۱۰۰٪ فیلترینگ در ۵۰٪ ثابت مانده است، همچنین مشاهده می‌شود که با هر درصد از خرابی حس‌گر، دقت تشخیص نادرست به سمت ۵۰٪ افزایش‌یافته و به این مقدار همگرا می‌گردد. این نتایج نشان می‌دهد در شرایط فیلترینگ ظهور عدم قطعیت بیشتر مشهود می‌گردد؛ زیرا خطای تشخیص ۵۰ درصد بیانگر اوج نامعلومی تشخیص نادرست است. می‌توان میزان دقت

و خطاهای یک حس‌گر در شرایط مختلف (خرابی حس‌گر و فیلترینگ‌های گوناگون) را اندازه‌گیری و محاسبه نمود. نتایج در جدول (۱) (سمت راست) آمده است که عوامل آن به شرح زیر است:

دقت تشخیص صحیح وجود سرویس[1] (ATS): این دقت مربوط به اندازه‌گیری صحیح وجود سرویس توسط حس‌گر است، بنابراین در آزمایش انجام‌گرفته میزان تشخیص‌های درست TT نسبت به‌کل تشخیص (درست یا غلط)هایی که به وجود سرویس ختم شده است (TT, FT) محاسبه می‌گردد که دقت تشخیص صحیح وجود سرویس را تعیین می‌کند.

دقت تشخیص صحیح عدم سرویس[2] (ATnS): این دقت مربوط به اندازه‌گیری صحیح عدم سرویس توسط حس‌گر است، بنابراین در آزمایش انجام‌گرفته میزان تشخیص‌های درست FF نسبت به‌کل تشخیص‌هایی که به عدم سرویس ختم شده است (FF+TF) محاسبه می‌گردد که دقت تشخیص صحیح عدم سرویس را تعیین می‌کند.

$$ATS = \frac{TT}{TT+FT} \qquad \textit{معادله (۱)}$$

$$ATnS = \frac{FF}{FF+TF} \qquad \textit{معادله (۲)}$$

میزان خطای تشخیص غلط وجود سرویس[3] AES: این خطا مربوط به اندازه‌گیری غلط وجود سرویس توسط حس‌گر است، بنابراین در آزمایش انجام‌گرفته میزان تشخیص‌های غلط (FT) نسبت به‌کل تشخیص‌هایی که به وجود سرویس ختم شده است (FT+TT) محاسبه می‌گردد که خطای تشخیص غلط وجود سرویس را تعیین می‌کند.

میزان خطای تشخیص غلط عدم سرویس[4] AEnS: این خطا مربوط به اندازه‌گیری غلط عدم سرویس توسط حس گر است، بنابراین در آزمایش انجام‌گرفته میزان تشخیص‌های غلط (TF) نسبت به‌کل تشخیص‌هایی که به عدم سرویس ختم شده است (TF+FF) محاسبه می‌گردد که خطای تشخیص غلط عدم سرویس را تعیین می‌کند.

$$AES = \frac{FT}{TT+FT} \qquad \textit{معادله (۳)}$$

$$AEnS = \frac{TF}{FF+TF} \qquad \textit{معادله (۴)}$$

دقت کل[5] TotalA: دقت کل از مجموع تشخیص صحیح سرویس TT و تشخیص صحیح عدم سرویس FF نسبت به‌کل تشخیص‌ها است.

خطای کل[6] ETotal: خطای کل از مجموع تشخیص غلط وجود سرویس (FT) و تشخیص غلط عدم سرویس (TF) نسبت به‌کل تشخیص‌ها حاصل می‌شود (David, et.al, 2011:37-63).

$$TotalA = \frac{TT+FF}{TT+FF+TF+FT} \qquad \textit{معادله (۵)}$$

$$ETotal = \frac{FT+TF}{TT+FF+TF+FT} \qquad \textit{معادله (۶)}$$

1. Accuracy True detection for exist Service
2. Accuracy True Detection for not Exist Service
3. Accuracy Error Detection for Exist Service
4. Accuracy Error Detection for not Exist Service
5. Total Accuracy
6. Total Error

جدول ۲. میزان همبستگی داده‌ها نسبت به یکدیگر

r(GFF, DFF)	r(GTT,DTT)	r(GTT,GFF)	r(TT-FF, TF-FT)	r(FF,FT)	r(TT, DTT)	r(TT,TF)
-۰/۹۹۸۶۴۰۱۲۳	۰/۱۳۴۰۷۱۳۷۸	۰/۹۹۹۹۷۱۵۸۵	-۰/۹۹۹۹۳۸۹۵۳	-۱	۰/۹۹۹۶۰۶۳۹۹	-۱

با استفاده از جدول (۲) می‌توان به میزان همبستگی داده‌ها نسبت به یکدیگر پی برد که نتایج در جدول (۵) آمده است. با توجه به مقادیر به‌دست‌آمده از جدول (۲) می‌توان نتایج را به شرح زیر مورد تحلیل قرار داد:

r(GFF, DFF): ضریب همبستگی ۰.۹۹- بیانگر این است که این دو عامل، ارتباط معکوس و تقریباً کاملی با یکدیگر دارند؛ به عبارتی افزایش GFF به همان نسبت باعث کاهش DFF خواهد بود و بالعکس.

r(TT-FF, TF-FT): ضریب همبستگی ۰.۹۹- بیانگر این است که این دو عامل ارتباط معکوس و تقریباً کاملی با یکدیگر دارند؛ به عبارتی افزایش TT-FF به همان نسبت باعث کاهش TF-FT خواهد بود و بالعکس.

۲-۲-۳. خطایابی و اصلاح تشخیص

اگر در نظر باشد خطاهای ناشی از فیلترینگ و خرابی حس‌گر کشف و تصحیح شود، می‌توان از روش‌های گوناگونی مبادرت به انجام این کار کرد. در اینجا نشان داده می‌شود که با استفاده از ویژگی رفتار دنباله داده‌ها می‌توان دقت تشخیص را افزایش داد. در این خصوص می‌توان از روش‌های متداولی همچون گراف کاوی[1]، درخت تصمیم[2] و تحلیل اِن-گرام[3] (Kang, et.al, 2016) استفاده کرد، بنابراین در این تحقیق به علت سادگی روش تحلیل اِن-گرام (نسبت به سایر روش‌ها) می‌توان آن را جهت خطایابی و اصلاح تشخیص مورد استفاده قرار داد.

در این تحلیل وقتی حس‌گر، وضعیتی را تشخیص می‌دهد، به n گام تشخیص پیشین خود نیز نگاه می‌کند و الگوی دنباله کنونی را از دنباله‌های گذشته (که آموزش دیده‌اند) جست‌وجو کرده و میزان تخمین را از نزدیک‌ترین شباهت‌های آموزش دیده، استنتاج می‌کند و برآوردی جدید از تشخیص ارائه می‌گردد. برای این منظور، آزمایشی از مانیتورینگ یک قربانی بر روی ۱۰۰۰ داده انجام شده است، از این‌رو در ابتدا رفتار دنباله‌وار این مجموعه داده، با دنباله‌های ۲، ۳ و ٤ تایی محاسبه و ثبت می‌شود. باتوجه به طول دنباله‌ها می‌توان انتظار داشت که 2^n حالت در نتایج هر دنباله ظاهر شود. حال فرآوانی هر یک از دنباله‌ها محاسبه شده و به‌عنوان رفتار آموزشی یک خدمت‌رسان (خاص) ثبت می‌گردد. پس از انجام مرحلهٔ یادگیری با داده آموزشی، می‌توان داده‌های تشخیص حس‌گر را با آن اعتبارسنجی کرد.

گفتنی است داده‌هایی که حس‌گر، آنها را به‌عنوان صفر تشخیص می‌دهد ممکن است دارای ابهام باشد؛ بنابراین نیاز است تصحیح خطا فقط بر روی این داده‌ها انجام شود، از این‌رو در سطر چهارم از دنباله‌های عدد فرد که بیانگر تشخیص وجود سرویس (یک) توسط حس‌گر است، دیگر نیازی به تصحیح خطا ندارد. در مرحلهٔ آخر، همان داده‌های آموزشی به‌عنوان داده آزمایشی به سامانهٔ اعمال شد که نتایج

1. Graph Mining
2. Decision Tree
3. N-gram

جالبی حاصل گردید که در جدول (۳) نشان داده شده است.

همان‌گونه که ملاحظه می‌شود میزان تشخیص یک‌ها توسط حس‌گر، ۲٤٦ مورد از ٤۹۰ مورد در کل می‌باشد که پس از تشخیص و تصحیح خطا در هر یک از N-gram ها به ترتیب به ۳۸۳ و ۳۰۲ و ۳۰۲ مورد از ٤۹۰ مورد، بهبود یافته است؛ به عبارتی در دنباله ۲ تایی نسبت به سایر دنباله‌های ۳ و ٤ تایی نتیجهٔ بهتری حاصل شده است، بنابراین نتایج این آزمایش‌ها نشان داد که استفاده از روش تحلیل N-gram می‌تواند در رفع ابهام مؤثر باشد و نیز ملاحظه شد که با تغییر طول دنباله‌ها نتایج متفاوتی حاصل می‌شود، بنابراین مناسب است با استفاده از داده‌های واقعی، آزمایش‌های مختلفی را انجام داد و به طول دنباله بهینه رسید که دارای بیشترین دقت برای برآورد باشد.

به نظر می‌رسد مجموع داده‌های آموزشی هم برای انواع سرویس‌دهنده‌ها (قوی یا ضعیف) متفاوت باشد که لازم است مورد بررسی دقیق قرار بگیرد. ممکن است بتوان از روش‌های دیگری (مانند مارکوف) نیز دقت تشخیص را بیشتر کرد، ولی به خاطر استمرار زیاد در وجود فیلترینگ و یا خرابی حس‌گر، کار تشخیص مختل می‌گردد و درنتیجه نمی‌توان وضعیت قربانی را رصد کرد و شرایط عدم قطعیت برای ادامه کار افزایش می‌یابد؛ بنابراین ضرورت پیدا می‌کند برای بالا بردن قابلیت اطمینان از روش‌های دیگری استفاده شود که در این‌جا استفاده از حس‌گرهای اضافی[1] یا زاپاس که لازم است در اقصی نقاط شبکه (اینترنت) مستقر گردند، پیشنهاد می‌گردد که تحت عنوان شبکه حس‌گری به آن پرداخته شود.

۳-۳. مدل‌سازی شبکهٔ حس‌گری (تلفیق حس‌گرها[2])

در بخش پیش رفتار یک دیدبان (حس‌گر) حملات دی‌داس مورد ارزیابی قرار گرفت و نشان داده شد که میزان دقت تشخیص وضعیت خدمت‌رسان با عامل‌های احتمال اعمال فیلترینگ و خرابی حس‌گر موجب افزایش عدم قطعیت و کاهش آگاهی وضعیتی فرماندهی و کنترل می‌گردد. یکی از راه‌کارهای افزایش آگاهی وضعیتی، افزایش تعداد دیدبان‌ها است که در اقصی نقاط فضای سایبری مستقر و به‌کارگیری شوند.

1. Redundancy

2. Data Fusion

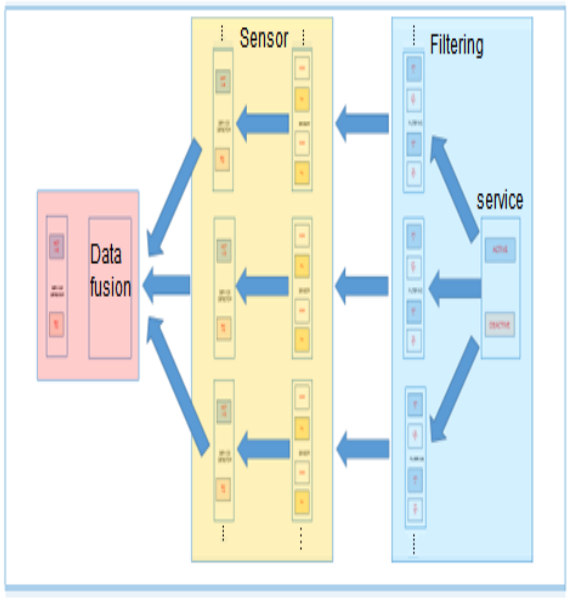
جدول ۳. تصحیح تشخیص N-gram

	تعداد وجودسرویس در وضعیت	تشخیص حس گر	2-G تصحیح تشخیص	3-G تصحیح تشخیص	4-G تصحیح تشخیص	تصحیح تشخیص G-۴ (افراطانه)
۱	۴۹۰	۲۴۶	۳۸۳	۳۰۲	۳۰۲	۴۰۵
۰	۵۱۰	۷۵۴	۶۲۱	۷۰۲	۷۰۲	۵۹۵
خطا در ۱	۰	٪۵۰	٪۷۸	٪۶۱	٪۶۱	٪۸۳

در ادامه، با استفاده از شبکهٔ دیدبانی حملات دی‌داس را مورد تجزیه‌وتحلیل قرار می‌دهیم. برای این منظور در ابتدا آن را مدل کرده و سپس با شبیه‌سازی یک محیط عملیات دیدبانی سایبری و انواع سناریوهای متصور، رفتار شبکه بررسی می‌گردد. در ادامه میزان عدم قطعیت را بررسی نموده و برای کاهش آن پیشنهاد ارائه می‌شود، ازاین‌رو دوباره لازم است با استفاده از چند سناریو طرح‌های پیشنهادی مورد ارزیابی قرار گیرد.

عناصر مدل شامل یک خدمت‌رسان (قربانی) و سازوکار امنیتی فیلترینگ در محدوده‌های جغرافیایی و شبکهٔ حس‌گر دیدبانی که در اقصی نقاط شبکه مستقر شده‌اند (البته ارزش اعتبار هر یک از دیدبان‌ها می‌تواند متفاوت باشد و در بخش ادغام مورد استفاده قرار گیرد) و درنهایت ادغام اطلاعات است که نقش هر یک از عناصر به شرح زیر است. نمای کلی مدل‌سازی شبکهٔ حس‌گری در شرایط احتمالی فیلترینگ و خرابی حس‌گر در شکل (۷) نشان داده شده است.

شکل ۷. مدل‌سازی شبکهٔ حس‌گری دیدبانی از خدمت‌رسان (قربانی) در حملات دی‌داس در شرایط احتمالی فیلترینگ و خرابی حس‌گر



نکتهٔ قابل توجه اینکه هیچ مجموعه داده‌ای در حوزهٔ ارزیابی اثربخشی حمله‌های منع خدمات را نمی‌توان یافت (Peng, et.al, 2011:139-149) و در صورت موجود بودن نیز با شاخص‌های ارزیابی به‌کار رفته در این تحقیق هم‌خوانی ندارند، بنابراین داده‌های موردنیاز این پژوهش را می‌توان با استفاده از تجارب تأثیر حمله‌های منع خدمات گذشته، در قالب سناریوها تولید کرد.

٤-٣. شبیه‌سازی و ارزیابی مدل شبکهٔ حس‌گری

به‌منظور درست‌یابی و ارزیابی مدل آن را با استفاده از شبیه‌سازی، با همان شرایط آزمایش پیشین، مورد پیاده‌سازی قرار می‌گیرد. در این شبیه‌سازی برای ۵۰ حس‌گر دیدبان مستقل، میزان احتمال فیلترینگ و خرابی حس‌گر در سناریوهای مختلف برای ۱۰۰۰ بار (به نیت ۱۰۰۰ دقیقه) اجرا گردید و نتایج آن استخراج شد، بنابراین ۳٦ بار (معادل ۳٦۰۰۰ دقیقه) شبیه‌سازی انجام می‌شود که قسمتی از آن در جدول (٤) نشان داده شده است.

جدول ٤. بخشی از نتایج شبیه‌سازی تشخیص وضعیت قربانی با ۵۰ حس‌گر دیدبان

D.T(ms)	ST	s1	s2	s3	s4	s5	s6	s7	s8	s9	10	11	12	13	14	15	38	39	40	41	42	43	44	45	46	47	48	49	50
9383	1	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	0	1	1
5661	1	1	1	0	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0
13542	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13970	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3163	1	0	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	1	0	0	0	1	1	1	0	0	0	0
7483	1	1	0	0	1	1	0	1	0	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	0	1
2591	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0	0
1655	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	1	0	0	0	0

ستون اول از سمت چپ مربوط به تأخیر پاسخ زمانی[1] واقعی خدمت‌رسانی است که قرار است دیدبان‌ها آن را تشخیص دهند.

این میزان تأخیر با تابع تصادفی از مقدار یک تا ۳۰۰۰۰ (میلی‌ثانیه) توسط شبیه‌ساز تولید می‌گردد. در ستون دوم (ST) با فرض تأخیر کمتر از ۱۵ ثانیه، وجود سرویس قربانی (برای عدد یک) و با فرض تأخیر بیشتر از ۱۵ ثانیه، عدم سرویس واقعی (برای عدد صفر) شکل می‌گیرد. از ستون سوم تا ستون آخر مربوط به تشخیص وضعیت قربانی توسط هر دیدبان است که اندازه‌گیری و اعلام می‌گردد.

بخشی از نتایج آزمایش که وضعیت‌های مختلف قربانی (احتمال‌ها مشخص درصد خرابی حس‌گر و حداکثر فیلترینگ) در آن لحاظ گردیده، به‌صورت جدول (۵) جمع‌بندی شد؛ به این ترتیب که به ازای هر تعداد حس‌گر بینا، می‌توان فراوانی هر یک از انواع فیلترینگ را ملاحظه کرد که در کل، وجود سرویس را تشخیص می‌دهند.

در جدول (۵) سطر اول بیانگر تعداد حس‌گرهای بینا است و سطرهای بعدی به ترتیب فراوانی‌های (مشاهده شده) در انواع فیلترینگ ۰-۲۰-٤۰-٦۰-۸۰ را نشان می‌دهد؛ برای مثال اگر تعداد حس‌گرهای بینا ۳۰ عدد باشد، با احتمال (٦۸/۲۹۵) در شرایط بدون فیلتر و با احتمال‌های (۱۱۰/۲۹۵) و (۱۱۷/۲۹۵) به ترتیب با شرایط فیلترینگ ۲۰ و ٤۰ است، همچنین شکل (۸) جدول بالا را به تصویر کشیده است؛ به‌گونه‌ای که محورهای افقی و عمودی به ترتیب بیانگر تعداد حس‌گر بینا و فراوانی می‌باشند که به نظر می‌رسد نمودارهای بالا از تابع توزیع نرمال تبعیت می‌کنند.

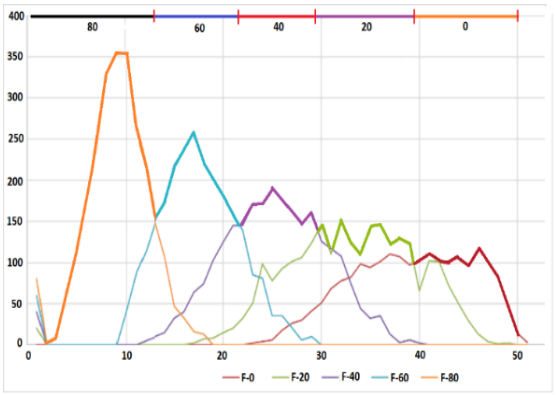
1. Delay Time Response

جدول ۵. تعداد حس‌گرهای مشارکت کننده در تشخیص وضعیت قربانی در شرایط مختلف فیلترینگ و خرابی حس گر

۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰	
۱۸	۶	۴	۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۹۳	۷۸	۹۸	۵۱	۳۲	۲۰	۱۵	۸	۷	۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۲۰
۱۷۷	۱۹۰	۱۷۲	۱۷۰	۱۴۵	۱۴۵	۱۲۵	۱۰۳	۷۴	۶۴	۴۰	۳۲	۱۵	۱۰	۵	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۴۰
۳۵	۳۵	۸۱	۸۵	۱۳۹	۱۵۷	۱۸۱	۲۰۰	۲۲۲	۲۵۹	۲۳۶	۲۱۹	۱۷۴	۱۵۴	۱۱۵	۸۸	۴۳	۰	۰	۰	۰	۰	۰	۰	۰	۰	۶۰
۰	۰	۰	۰	۰	۰	۰	۰	۱۳	۱۶	۳۳	۴۷	۱۰۷	۱۴۹	۲۱۷	۲۶۷	۳۵۴	۳۵۳	۳۳۱	۲۴۵	۱۷۸	۱۱۴	۶۵	۱۰	۳	۰	۸۰
۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۶	۱۵	۶۰	۲۵۸	۶۳۵	۱۵۲۸	۱۰۰
۴۰					۶۰									۸۰									۱۰۰			

۵۰	۴۹	۴۸	۴۷	۴۶	۴۵	۴۴	۴۳	۴۲	۴۱	۴۰	۳۹	۳۸	۳۷	۳۶	۳۵	۳۴	۳۳	۳۲	۳۱	۳۰	۲۹	۲۸	۲۷	۲۶	
۳	۱۴	۵۱	۸۲	۱۰۲	۱۱۷	۹۷	۱۰۶	۱۰۰	۱۰۳	۱۱۰	۱۰۱	۹۷	۱۰۷	۱۱۰	۱۰۱	۹۴	۹۸	۸۲	۷۸	۶۸	۵۱	۴۱	۳۰	۲۶	۰
۰	۰	۲	۱	۴	۱۳	۲۹	۵۰	۷۲	۱۰۱	۱۰۲	۶۶	۱۲۴	۱۲۹	۱۲۳	۱۴۷	۱۴۳	۱۱۱	۱۲۶	۱۵۳	۱۱۰	۱۴۶	۱۲۴	۱۰۶	۱۰۱	۲۰
۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۲	۶	۳	۱۳	۳۵	۳۲	۴۴	۷۵	۱۰۸	۱۱۷	۱۲۶	۱۶۱	۱۴۶	۱۶۲	۴۰
۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱۰	۶	۲۱	۶۰
۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۸۰
۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱۰۰
۰																						۴۰			

شکل ۸. تابع توزیع نرمال هر یک از حس‌گرهای بینا در شرایط انواع فیلترینگ



در ادامه باید به رابطه‌ای دست یافت که بتوان با در دست داشتن تعداد حس‌گرهای بینا، به میزان احتمال فیلترینگ پی برد. از این‌رو با توجه به هم‌پوشانی‌هایی که نمودارها نسبت به هم دارند، تصمیم بر آن شد حداکثر فراوانی‌ها ملاک این نگاشت قرار گیرد که می‌توان نتایج این تدبیر را در محور افقی بالای نمودار شکل (۸) ملاحظه نمود. این نگاشت در سطر آخر جدول (۵) نشان داده شده است، بنابراین می‌توان این نگاشت را با رابطه filtering = f(sensors) به شکل معادلهٔ (۷) بیان کرد:

معادلهٔ (۱)

$$\text{Filtering} = f(\text{sensors}) = \begin{cases} 100 & \text{sen} \le 3 \\ 80 & 4 \le \text{sen} \le 11 \\ 60 & 12 \le \text{sen} \le 20 \\ 40 & 21 \le \text{sen} \le 28 \\ 20 & 29 \le \text{sen} \le 38 \\ 0 & 39 \le \text{sen} \le 50 \end{cases}$$

به منظور راست‌آزمایی این نگاشت، آزمایشی با ۳۵۰ داده تصادفی (از مجموعه داده ۳۶۰۰۰ تایی) انجام شد تا میزان دقت و خطای تخمین اندازه‌گیری شود که نتایج آن را می‌توان در جدول (٦) ملاحظه نمود. نتایج نشان داد که در شرایطی که ممکن است انواع خرابی حس‌گر و فیلترینگ وجود داشته باشد، می‌توان دقت اندازه‌گیری را با تولرانس ۱۰٪ حدود ۸۱ درصد در نظر گرفت.

جدول ٦. دقت تخمین فیلترینگ با استفاده از حس‌گر بینا

	دقت تخمین فیلترینگ		
	درصد	درصد خطای	فراوانی
با خرابی حس‌گر	40%	0	140
	41%	20	143
	9%	40	30
	5%	60	17
	6%	80	20
بدون خرابی	71%	0	24
	29%	20	10

اگر احتمال خرابی حس‌گر صفر در نظر گرفته شود، (با فرض تشخیص و اصلاح خرابی) می‌توان دقت اندازه‌گیری را با تولرانس ۱۰٪ حدود ۱۰۰ درصد در نظر گرفت، بنابراین از این تخمین در بخش بعدی استفاده می‌گردد. همان‌گونه که در جدول (۵) ملاحظه می‌شود، در شرایط فیلترینگ ۱۰۰ درصد، حداکثر حس‌گرهایی که ممکن است تشخیص اشتباه داشته باشند (حس‌گرهای نابینا) به عدد ۵۰ (صفر حس‌گر بینا) می‌رسند که فراوانی آن ۱۵۲۷ است، بنابراین شبکهٔ حس‌گرهای دیدبان در شرایط عدم قطعیت قرار می‌گیرند، بنابراین در ادامه کار باید مدل‌های ادغام اطلاعات پیشنهاد گردد و صحت آن مورد ارزیابی قرار گیرد.

۱-٤-۳. پیشنهاد روش‌های تلفیق داده‌های شبکهٔ حس‌گری و ارزیابی آنها

در این مرحله چند روش تلفیق اطلاعات پیشنهاد داده می‌شود و میزان دقت و خطای هر یک از آنها اندازه‌گیری کرده و سپس نتایج نسبت به یکدیگر مورد مقایسه قرار می‌گیرد.

میانگین‌گیری: ساده‌ترین تلفیق داده، معدل گرفتن از نتایج است، بنابراین می‌توان مقدار معدل تأخیر زمانی بیش از صفر را وجود سرویس و مقدار صفر را عدم سرویس تلقی کرد.

رأی‌گیری: در این روش تعداد حس‌گرهای که وجود سرویس (عدم سرویس) را تأیید می‌کنند، مورد شمارش قرار می‌گیرند و اگر هر کدام از دیگری بزرگ‌تر بود یا حد آستانه‌ای را دارا بود، به‌عنوان نتیجهٔ تلفیق اعلام می‌شود.

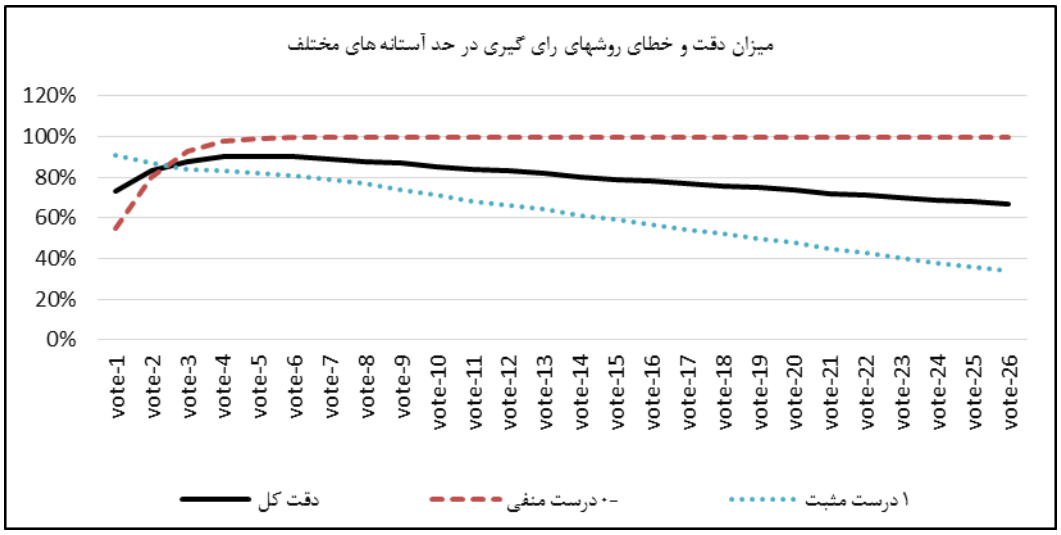
مجموع داده ۳٦۰۰۰ تایی با استفاده از روش‌های تلفیق میانگین‌گیری و انواع رأی‌گیری با حد آستانه‌های یک تا ۲٦ حس‌گر مورد پردازش قرار گرفت که مقادیر درست مثبت، درست منفی، غلط مثبت و غلط منفی محاسبه گردید که در جدول (۷) به‌صورت عددی و درصدی و در شکل (۹) به‌صورت نموداری نشان داده شده است. همان‌گونه که در جدول (۷) ملاحظه می‌شود در روش رأی‌گیری حد آستانه‌های ٦ تا ۲٦ حس‌گر دارای دقت ۱۰۰٪ در وضعیت عدم سرویس‌دهی (صفر) هستند، ولی در وضعیت وجود سرویس دارای نتایجی مناسبی نیستند و بهترین آنها در رأی‌گیری در حد آستانه ٦ حس‌گر برابر ۸۰٪ است که می‌توان نقطهٔ بهینه را در رأی‌گیری در حد آستانه ٤ با دقت ۹۰٪ مشاهده کرد، همچنین در روش رأی‌گیری حد آستانه یک حس‌گر (vote-1)، دقت در وضعیت سرویس‌دهی به ۹۱٪ می‌رسد و دارای خطای ۹٪ دارد، ولی در وضعیت عدم سرویس‌دهی، دقت آن به ۵۵٪ کاهش می‌یابد و خطای ٤۵٪ دارد. با بررسی انجام شده در داده‌های خطای ۹ درصدی مشخص شد که فقط علت آن وجود فیلترینگ بوده است و در خطای ٤۵٪ فقط علت آن وجود خرابی بوده است.

نکتهٔ مهم این است که سامانه دیدبانی می‌تواند در انتخاب حس‌گرهای خود اختیار داشته باشد و با روش‌هایی خرابی را تشخیص داده و اثر آن را در دقت اندازه‌گیری کاهش دهد ولی در عوض در مورد فیلترینگ اختیاری ندارد، بنابراین اگر تلاش شود خرابی حس‌گر به صفر تنزل پیدا کند، می‌توان انتظار داشت دقت تشخیص به ۹۶ درصد افزایش یابد.

جدول ۷. نتایج تشخیص دقت و خطای روش‌های تلفیق انواع رأی‌گیری با حد آستانه‌های مختلف

	میزان دقت و خطا				Total A	فراوانی دقت و خطا			
	(%50.2) [1]		(%49.8) [0]			18072[1] مثبت		17928[0] منفی	
تشخیص	TT	TF	FT	FF		TT	TF	FT	FF
	1- درست مثبت	0- غلط مثبت	1- غلط منفی	0- درست منفی	دقت	1- درست مثبت	0- غلط مثبت	1- غلط منفی	0- درست منفی	تشخیص
vote-1	٪۹۱	٪۹	٪۴۵	٪۵۵	٪۷۳	۱۶۴۲۲	۱۶۵۰	۸۱۳۷	۹۷۹۳	vote-1
vote-2	٪۸۷	٪۱۳	٪۲۰	٪۸۰	٪۸۳	۱۵۶۰۶	۲۴۶۶	۳۶۳۶	۱۴۲۹۲	vote-2
vote-3	٪۸۴	٪۱۶	٪۷	٪۹۳	٪۸۸	۱۵۲۰۰	۲۸۷۲	۱۲۹۶	۱۶۶۳۳	vote-3
vote-4	٪۸۳	٪۱۷	٪۲	٪۹۸	٪۹۰	۱۴۹۶۸	۳۱۰۴	۳۷۳	۱۷۵۵۷	vote-4
vote-5	٪۸۲	٪۱۸	٪۱	٪۹۹	٪۹۰	۱۴۷۷۲	۳۳۰۰	۱۳۸	۱۷۷۹۱	vote-5
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
vote-25	٪۳۶	٪۶۴	٪۰	٪۱۰۰	٪۶۸	۶۴۴۵	۱۱۶۲۷	۰	۱۷۹۲۸	vote-25
vote-26	٪۳۴	٪۶۶	٪۰	٪۱۰۰	٪۶۷	۶۰۵۲	۱۲۰۲۰	۰	۱۷۹۲۸	vote-26

شکل ۹. میزان دقت و خطای روش‌های رأی‌گیری در حد آستانه‌های مختلف



در این مرحله می‌توان یک مقایسه اولیه بین دقت تک دیدبان (تک حس‌گر) و دیدبانی شبکهٔ حس‌گری را انجام داد. نتایج نشان می‌دهد در شبکهٔ حس‌گری (بدون ابهام‌یابی) دقت تشخیص ۹۰٪ و در تک حس‌گر

دقت تشخیص (بدون ابهام‌یابی) به ۵۰٪ کاهش می‌یابد. اگر قرار باشد تمامی دیدبان‌ها از یک محدود جغرافیایی بخواهند کار رصد را انجام دهند، با مسدود شدن مسیر فیلترینگ، همهٔ دیدبان‌ها نابینا شده و کار تشخیص در هاله‌ای از ابهام باقی می‌ماند.

۲-٤-۳. پیشنهادهای رفع ابهام در شبکه حس گری

در این قسمت در نظر است خطایابی در شبکهٔ حس‌گری با دو ویژگی مشاهده رفتار روند فیلترینگ و رفتار دنباله‌های خدمت‌رسانی ماشین خدمات‌دهنده (قربانی) مورد بررسی و تجزیه‌وتحلیل قرار گیرد. نظر به اینکه اگر مشاهده تمامی حس‌گرها برابر با عدم سرویس‌دهی باشد، می‌توان اثر هر یک از سامانه‌های تصحیح خطا را مورد بررسی قرار داد در آزمایش‌ها ملاحظه شد که تعدادی از تشخیص‌های نادرست حس‌گر، اصلاح می‌شود و نتیجه را بهبود می‌دهد، ولی در برخی موارد، تشخیص‌های درست، عدم سرویس را تحت تأثیر قرار داده و به اشتباه، آن را وجود سرویس تخمین زده است (کاذب مثبت) که این عملکرد نادرست (با اینکه در مقایسه با تعداد بهبودیافته‌ها کمتر است) می‌تواند در پردازش‌های بعدی اثر نامطلوب بگذارد.

۳-٤-۳. تأثیر n-gram

با بهره‌مندی از مجموعه داده پیشین و با استفاده از روش n گرام، فراوانی توالی‌های ۲ و ۳ و ٤ تایی مورد آزمایش قرار گرفت و احصا گردید و سپس با استفاده از همین داده، گام‌های بعدی حس‌گرها تخمین زده شد و نتایج نشان داد:

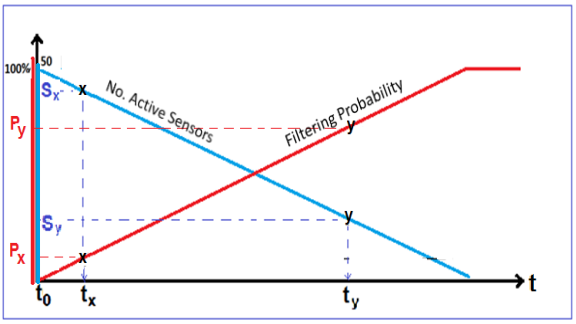
- اگر در شرایطی که وجود سرویس برقرار باشد، برای اعمال رابطه n-gram مشکلی وجود نخواهد داشت.
- اگر در شرایطی که عدم سرویس به‌طور مستمر برقرار باشد، با توجه به ماهیت رابطهٔ n-gram، همگرایی رخ‌داده و موجب می‌شود تصحیح تشخیص به آنچه حس‌گر تشخیص می‌دهد (عدم سرویس) میل کرده و دوباره نقطهٔ ابهام شکل بگیرد. برای کاهش محدود این ابهام به نظر می‌رسد، تعیین اندازه مناسب گام‌های رابطهٔ n-gram، میسر باشد.

٤-٤-۳. تأثیر ویژگی تغییرات (رشد یا کاهش) فیلتر شدن مسیرها

در ابتدا نقش شبکهٔ حس‌گری در مواجه با فیلترینگ مرور می‌شود. فرض می‌شود حس‌گرهای دیدبان نیز از گسترهٔ وسیع خدمت‌گیرندگان باشند. حال می‌توان این حس‌گرها را به‌عنوان نمونه‌ای از جامعهٔ آماری خدمت‌گیرندگان تلقی کرد. در این مرحله که قرار است وضعیت ماشین خدمت‌رسان تعیین گردد، وجود فیلترینگ، تشخیص این کار را در هاله‌ای از ابهام قرار می‌دهد. حال باوجود قرائن و شواهد تغییرات فیلترینگ، می‌توان به میزان احتمال وجود فیلترینگ به‌شرط timeOut دست یافت و متعاقب آن به میزان احتمال ازکارافتادن سرویس به‌شرط TimeOut پی برد. این ویژگی به‌دنبال کشف سیر صعودی یا نزولی اعمال فیلترینگ ماشین خدمت‌رسان است؛ بنابراین لازم است وجود فیلترینگ هر یک از حس‌گرها در بازهٔ زمانی معین ثبت و مورد ارزیابی قرار گیرد. به این ترتیب می‌توان پیش از شرایط عدم قطعیت (ازکارافتادن سرویس یا فیلترینگ) این سیر رفتار را کشف نمود. این

رفتار را می‌توان در شکل (۱۰) ملاحظه کرد، به‌گونه‌ای که فرض شده حس‌گرها سیر نزولی وجود سرویس را رصد می‌کنند و در زمان‌های tx یا ty به بعد، هیچ‌گونه سرویسی را تشخیص نمی‌دهند که با حروف x, y بر روی منحنی مشهود است. حال اگر عدم‌تشخیص سرویس به احتمال وجود فیلترینگ سنجش شود، می‌توان آن را در منحنی صعودی ملاحظه نمود.

شکل ۱۰. تأثیر فیلترینگ بر حس‌گرهای بینا



در نقاط x و y می‌توان به برآوردهای احتمال Px و Py دست یافت؛ به‌عبارتی اگر مقدار تغییرات اعمال فیلترینگ (x) کوتاه باشد و TimeOut رخ داده باشد، به‌احتمال کم (Px) فیلترینگ اتفاق افتاده و محتمل خدمت‌رسانی قربانی از کار افتاده است و اگر مقدار تغییرات اعمال فیلترینگ (y) زیاد باشد و TimeOut رخ داده باشد، به‌احتمال زیاد (Py) فیلترینگ اتفاق افتاده و محتمل خدمت‌رسانی قربانی ازکار نیفتاده است.

با توجه به اینکه حس‌گرهای دیدبان محدود می‌باشند (برای مثال ۵۰)، بنابراین هنگامی‌که تمامی حس‌گرها قادر به تشخیص سرویس نباشند، نمی‌تواند بیانگر از کار افتادن سرویس باشد، بلکه فیلترینگ بر تمامی حس‌گرها غلبه کرده و حتی این فیلترینگ می‌تواند در حال افزایش باشد که دیگر حس‌گرها قادر به تشخیص آن نیستند، بنابراین به‌منظور تحقق این روش می‌توان به این گونه تحلیل نمود که در هر برش زمانی، وضعیت حس‌گرهایی که عدم خدمت‌رسانی قربانی را اعلام می‌کنند، توسط سایر حس‌گرها تعیین وضعیت شوند؛ به‌بیانی حس‌گر در معرض فیلترینگ است (حس‌گر نابینا) یا نه؟ برای این منظور اگر یک یا چند حس‌گر وجود سرویس‌دهی قربانی را مشاهده کنند، بیانگر این مطلب است که سایر حس‌گرها (حس‌گرهای نابینا) در معرض فیلترینگ می‌باشند و می‌توان این برچسب را به آنها زد؛ بنابراین می‌توان در هرلحظه که ممکن است TimeOut اتفاق بیفتد، این احتمال را با استفاده از تغییر تعداد برچسب‌ها به دست آورد. برای این منظور در هر دورهٔ زمانی تعداد حس‌گرهای برچسب خورده محاسبه و ثبت می‌گردد که روند رشد یا کاهش این تعداد، ملاک محاسبهٔ این احتمال‌هاست. در اینجا تغییرات می‌تواند با شیب‌های مختلفی رخ دهد. اگر بتوان تغییرات فاصلهٔ جاری را با یک یا دو مرحلهٔ پیش محاسبه کرد، می‌توان شیب‌های تند را به‌خوبی ملاحظه کرد، ولی در شیب‌های کُند مطلوب نیست. اگر تغییرات فاصلهٔ جاری با نقطهٔ شروع محاسبه شود، این بار شیب‌های تند خوب رؤیت نمی‌شود، ولی شیب‌های کُند، محسوس می‌باشند، به همین دلیل پیشنهاد شده که تغییرات نسبت به نقطهٔ وسط داده‌های گذشته در نظر گرفته شود. به این منظور برای به دست آوردن نقطهٔ وسط، از مقدار میانگین استفاده می‌شود، ازاین‌رو برای تحقق این امر، در ابتدا میانگین جاری (از لحظهٔ صفرتا زمان جاری) را از معادلهٔ (۸) محاسبه کرده و سپس با کمک معادلهٔ (۷)، می‌توان تغییرات فیلترینگ را با محاسبهٔ اختلاف فیلترینگ حاصل از میانگین جاری و تعداد حس‌گرهای (بینا) جاری، به دست آورد.

معادله (۷)

$$\text{میانگین جاری} = \frac{1}{n}\sum_{t=0}^{n} \text{Sum}\,(\text{sensors}(\text{بینا}))_t$$

معادله (۸)

$$\text{تغییرات فیلترینگ} = f(\text{میانگین جاری}) - f\left(\text{Sum}\left(\text{sensors}\left(\text{بینا}\right)\right)_t\right)$$

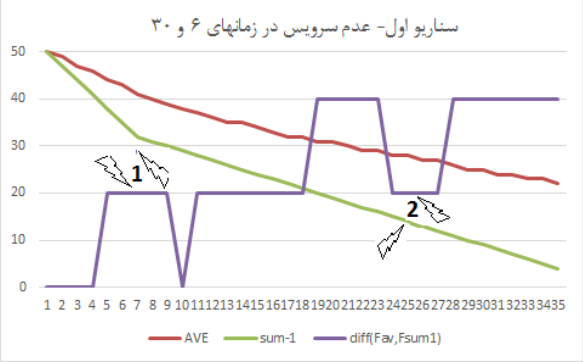
در معادلهٔ (۹) اگر تغییرات فیلترینگ مثبت باشد، به معنی کاهش مجموع حس‌گرهای بینا و درنتیجه افزایش فیلترینگ بوده و اگر تغییرات فیلترینگ منفی باشد، به معنی کاهش فیلترینگ است. به‌منظور تحقق و ارزیابی تأثیر ویژگی تغییرات فیلتر شدن مسیرها، آزمایش‌هایی در محیط شبیه‌سازی با چند سناریو و با استفاده از چند مجموعه داده[1] (۵۰ حس‌گر دیدبان از یک سرویس‌دهنده) انجام شده است.

سناریوی اول

در سناریوی اول، ۵۰ حس‌گر شروع به رصدگری کرده و از ابتدا با فیلترینگ مواجه می‌شود و تا هفت واحد زمانی با یک شیب مناسبی زیاد می‌شود و حس‌گرهای بینا به حدود ۲۵ عدد می‌رسد و در ادامه فیلترینگ با شیب کمتری تا انتهای زمان سناریو ادامه می‌یابد و تعداد حس‌گرهای بینا به ٤ عدد می‌رسد.

همان‌گونه که در شکل (۱۱) ملاحظه می‌شود هنگامی‌که عدم سرویس در زمان ٦ رخ می‌دهد، طبق معادلهٔ (۹)، احتمال رخداد فیلترینگ را حدود ۲۰ درصد تخمین می‌زند، همچنین اگر عدم سرویس در زمان ۲۵ رخ دهد، مقدار تغییرات طبق معادلهٔ (۹)، احتمال رخداد فیلترینگ را هم حدود ۲۰ درصد تخمین می‌زند.

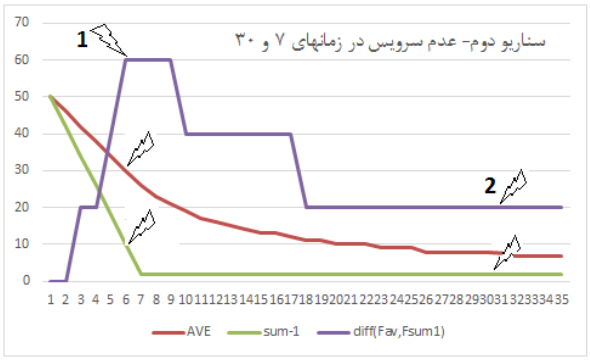
شکل ۱۱. نمودارهای سناریوی اول در دو حالت رخداد عدم سرویس در زمان‌های ۵ و ۳۰



سناریو دوم

در سناریوی دوم رشد فیلترینگ تا ۷ واحد زمان اول، با شیب زیاد تغییر می‌کند و سپس فیلترینگ متوقف‌شده و تا انتهای زمان، شیبی ندارد و تعداد حس‌گرها ثابت باقی می‌ماند. همان‌گونه که در شکل (۱۲) ملاحظه می‌شود، هنگامی‌که عدم سرویس در زمان ۷ رخ می‌دهد، زمانی است که تعداد حس‌گرها در فاصلهٔ زمانی صفرتا هفت با شیب زیاد کاهش پیدا می‌کنند، ازاین‌رو مقدار رابطهٔ (۹)، (احتمال) رخداد فیلترینگ را حدود ٦۰ درصد تخمین می‌زند.

شکل ۱۲. نمودارهای سناریوی دوم در دو حالت رخداد عدم سرویس در زمان‌های ۷ و ۳۰



اگر عدم سرویس در زمان ۳۰ رخ دهد، زمانی است که تعداد حس‌گرها در فاصلهٔ زمانی ۷ تا ۳۰ با شیب

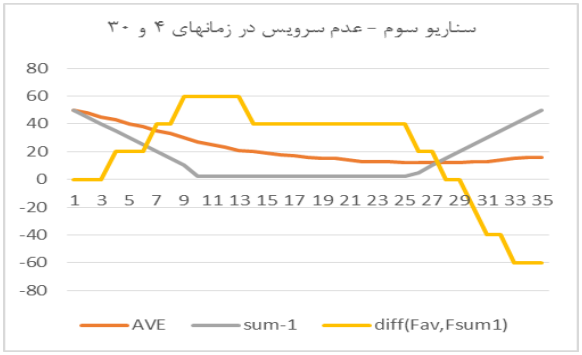
1. Dataset (delta filtering.xlsx)

صفر ثابت می‌ماند، ازاین‌رو مقدار تغییرات طبق رابطهٔ (۹)، احتمال رخداد فیلترینگ را حدود ۲۰ درصد تخمین می‌زند.

سناریو سوم

در سناریوی سوم، رشد فیلترینگ تا ۱۰ واحد زمانی اول، با شیب زیاد تغییر می‌کند و سپس فیلترینگ متوقف‌شده و تا زمان ۲۵ شیبی ندارد و دوباره حس‌گرها با شیب زیاد از وضعیت فیلترینگ خارج می‌شوند و شیب، مثبت می‌گردد.

شکل ۱۳. نمودارهای سناریوی سوم در دو حالت رخداد عدم سرویس در زمان‌های ٤ و ۲۵



همان‌گونه که در شکل (۱۳) ملاحظه می‌شود هنگامی‌که عدم سرویس در زمان ٤ رخ می‌دهد، زمانی است که تعداد حس‌گرها در فاصله زمانی صفرتا ٤ با شیب زیاد کاهش پیدا می‌کند، ازاین‌رو مقدار رابطهٔ (۹)، احتمال رخداد فیلترینگ را حدود ۲۰ درصد تخمین می‌زند. اگر عدم سرویس در زمان ۲۵ رخ دهد، زمانی است که تعداد حس‌گرها در فاصلهٔ زمانی ٤ تا ۲۰ با شیب صفر و سپس با شیب مثبت افزایش و به سمت بینایی تمام حس‌گرها میل می‌کند، ازاین‌رو مقدار تغییرات طبق رابطهٔ (۹)، (احتمال) رخداد فیلترینگ را حدود منفی ٦۰ درصد تخمین می‌زند؛ به عبارتی منفی شدن این تخمین، به این معناست که فیلترینگ رو به کاهش است و بعید به نظر می‌رسد که TimeOut به دلیل فیلترینگ باشد و درنتیجه به‌احتمال زیاد، سرویس از کار افتاده است.

۵-٤-۳. تغییر رشد یا کاهش پاسخ تأخیر

این ایده به دنبال بهره‌مندی از ویژگی تغییرات تأخیر پاسخ به سرویس است، به‌گونه‌ای که اگر در روند رصد از قربانی با رشد تأخیر در پاسخ‌دهی رؤیت گردید، بتوان انتظار داشت در آیندهٔ نزدیک این وضعیت ادامه پیدا کند تا جایی که سرور از کار بیفتد و دیگر پاسخ‌گو نباشد. این ایده برخلاف ایدهٔ ویژگی تغییرات فیلترینگ است، به‌گونه‌ای که بیشتر به‌دنبال تخمین ازکارافتادن سرویس است تا اینکه فیلترینگ را برآورد کند.

۵-۳. چارچوب آگاهی وضعیتی سرور قربانی با استفاده از شبکهٔ حس‌گری

در بخش اول برای ارزیابی صحنهٔ نبرد حملات منع‌خدمت، چارچوب در قالب شکل (۱) ارائه گردید. در این مرحله می‌توان ارزیابی صحنهٔ نبرد قربانی (مدافع) را در شکل (١٤) پیشنهاد کرد. در این چارچوب، در ابتدا از شبکهٔ رصدگری (قربانی) گردآوری داده انجام می‌شود و سپس با پاک‌سازی داده‌ها (از داده‌های مربوط به حس‌گر خراب و داده‌های ناقص یا پرت) شرایط برای تلفیق اطلاعات مهیا می‌شود و در مرحلهٔ اول ادغام اطلاعات داده‌هایی که خدمت‌رسانی قربانی را مسدود می‌بینند را مورد بازبینی قرار داده و با استفاده از روش‌های تصحیح خطا، آنها را اصلاح می‌کنند و سپس تمامی داده حس‌گرها را با استفاده از روش رأی‌گیری، تلفیق و چکیده‌سازی

می‌کنند. در این مرحله می‌توان وضعیت برخی از موجودیت‌های سرویس قربانی را تخمین زد. مرحلهٔ دوم ادغام اطلاعات، زمانی آغاز می‌گردد که وضعیت قربانی به عدم سرویس، تخمین زده شده است و این در حالی است که این عدم سرویس به دلیل وجود فیلترینگ باشد؛ بنابراین با استفاده از دنبال کردن روند فیلترینگ و روند زمان پاسخ می‌توان تخمین در شرایط عدم قطعیت را به دست آورد. در مرحلهٔ سوم با استفاده از وضعیت‌های کنونی و گذشته و روش‌های پیشگویی (مانند مارکوف) وضعیت‌های (کمیت و کیفیت خدمت‌رسانی) آتی قربانی را تخمین زد. این فرایند با چارچوب مدل آگاهی وضعیتی اندسلی و نیز مدل ادغام اطلاعات JDL دارای سازگاری است که در شکل (١٤) نشان داده شده است.

۳-۷. ارزیابی (مدل)

ارزیابی طرح پیشنهادی را می‌توان در چارچوب شکل (١٤) مورد بررسی قرار داد؛ به‌گونه‌ای که با اجرای ۳ سناریو بتوان نشان داد که طرح فوق دارای کارایی مطلوب است. در سناریوی اول فرض بر این است که سرور تحت حمله، با اعمال فیلترینگ ٦٠ درصد از خود مقاومت نشان داده و خدمت‌رسانی نماید. در سناریوی دوم فرض بر این است که سرور تحت حمله از فیلترینگ ۳۰ درصد بهره‌مند بوده و اصرار بر خدمت‌رسانی دارد و رفته‌رفته با گذشت زمان، پاسخ تأخیر خدمت‌رسانی زیاد شده تا اینکه سرویس از کار بیفتد. در سناریوی سوم، سرور تحت حمله ترجیح می‌دهد با اعمال فیلترینگ گسترده، خود را حفظ نماید. بدیهی است که طرح پیشنهادی باید بتواند هر یک از وضعیت سناریوها را تشخیص دهد (در متن تحقیق اثبات شد).

۴. نتیجه‌گیری

در این بخش به دستاوردها، پاسخ به پرسش‌های تحقیق و کارهای آتی پرداخته می‌شود. دستاوردهای تحقیق شامل موارد زیر است:

(۱) یک چارچوب برای ارزیابی صحنهٔ نبرد حملات منع خدمت توزیع‌شده، مطابق شکل (۱) که با مدل‌های اندس‌لی و JDL سازگاری دارد، ارائه گردیده است.

(۲) یک چارچوب آگاهی وضعیتی سرور قربانی با استفاده از شبکهٔ حس‌گری، مطابق شکل (١٤) ارائه گردید که با مدل‌های اندس‌لی و JDL سازگاری دارد. امکان تخمین کمیت و کیفیت خدمت‌رسانی قربانی در حین حمله را با دقت بیش از ۹۵٪ میسر می‌کند.

(۳) نتایج تخمین پیشنهادی نسبت به گزارش‌های وبگاه‌های رصدگری (در روش‌های موجود) واقعی و قابل‌اطمینان‌تر است.

پرسش‌های تحقیق نیز به این شکل پاسخ داده می‌شود:

پرسش اصلی: رصد سرویس‌دهی قربانی تحت حملهٔ منع خدمت توزیع شده چگونه است؟

با استفاده از یک شبکهٔ حسگری می‌توان از اقصی نقاط شبکه مبادرت به دیدبانی قربانی نمود. این دیدبانی می‌تواند در سطوح مختلف انجام گیرد که در این تحقیق رصد در سطح بسته‌های شبکه انجام شده است.

پرسش فرعی یکم: چالش‌ها و موانع شبکهٔ حس‌گری سایبری در مواجه با دسترس‌پذیری به ماشین‌های تحت حملهٔ منع خدمت چیست؟

تخمین کمیت و کیفیت خدمت‌رسانی قربانی در حین حمله برای تشخیص وضعیت قربانی همواره یک چالش اساسی بوده و طرح‌های کنونی، برای شرایط عدم قطعیت (تمهیدات مدافع اعم از فیلترینگ و غیره) پاسخ‌گو نیست که طرح پیشنهادی درصدد رفع این چالش بوده است.

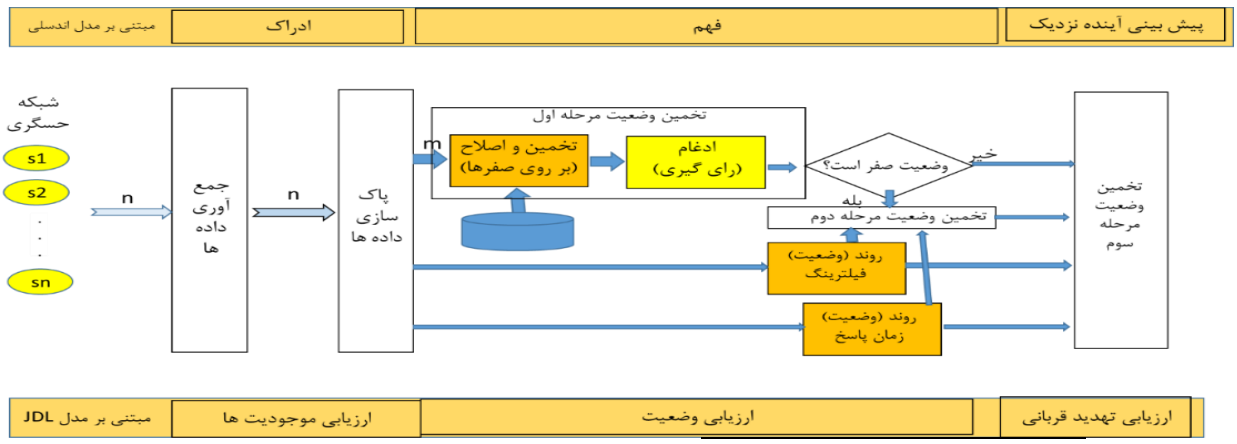
پرسش فرعی دوم: چگونه می‌توان عوامل عدم قطعیت در شبکهٔ حس‌گری را کاهش داد؟

مدل پیشنهادی شبکهٔ حس‌گری نشان داد که می‌توان تخمین مناسبی از کمیت و کیفیت خدمت‌رسانی قربانی به دست آورد.

با توجه به آزمایش‌های مختلف (اعمال انواع فیلترینگ و خرابی حس‌گر) نشان داده شد که با استفاده از روش رأی‌گیری (٤ تایی) در مرحلهٔ تلفیق داده‌ها می‌توان به بیش از ٩٦٪ درجه اطمینان دست یافت. در شرایط عدم قطعیت نشان داده شد که می‌توان با استفاده از دنبال کردن روند فیلترینگ و روند پاسخ تأخیر در خدمت‌رسانی، ابهام‌ها را در تعیین وضعیت قربانی کاهش داد.

برای ادامهٔ کار و تحقیقات بعدی استفاده از روش‌های بیزین[1] و مارکوف در رفع ابهام‌ها پیشنهاد می‌گردد.

شکل ١٤. چارچوب آگاهی وضعیتی سرور قربانی با استفاده از شبکهٔ حس‌گری



1. Bayesian

فهرست منابع

1. Bannwart, C (August 2012), ***Predicting the Impact of Denial of Service Attacks***, Master thesis MA-2012-03, Institute fur Technische Informattik und Kommunikations Netze (TIK), ETH zurich.
2. Barth, W (October 2008), ***Nagios, System and Network Monitoring***, Munich, Open Source Press GmbH.
3. Charalampos, Patrikakis and Olga, Zouraraki (2004), "Distributed Denial of Service Attacks", ***The Internet Protocol Journal***, Vol 7, No 4.
4. David, M. and Powers, W (2011), "Evaluation: From Precision, Recall and F-Measure to Roc, Informedness, Markedness & Correlation", ***Journal of Machine Learning Technologies***, Vol 1.
5. Endsley Mica, R (March 2015), "Final Reflections: Situation Awareness Models and Measures", ***Journal of Cognitive Engineering and Decision Making***.
6. Hohlfeld, Oliver and Feldmann Anja and Thomas Krenc (July 2014), "An Internet Census Taken by an Illegal Botnet –A Qualitative Assessment of Published Measurements", in: ACM SIGCOMM ***Computer Communication Review***, Vol. 44, No. 3.
7. Kang, B. and Yerima Suleiman, Y. and Sezer, Kieran (2016), N-gram Opcode Analysis for Android Malware Detection, ***International Journal on Cyber Situational Awareness***, Vol. 1, No. 1
8. Kanich, Savage Chris and Levchenko, Kirill and Enright, Brandon and Geoffrey, M and Stefan, Voelker (2008), ***The Heisenbot Uncertainty Problem: Challenges in Separating Bots from Chaff***, San Diego, University of California.
9. Peng, Z. and Zhao, W. and Long, J (July 2011), Grey Synthetic Clustering Method for DoS attack Effectiveness Evaluation, ***International Conference on Modeling Decisions for Artificial Intelligence*** (pp:139-149). Springer Berlin Heidelberg
10. Petersen, L. A. and Singh, H. and Thomas, E. J (Jun 2006), Understanding Diagnostic Errors in Medicine: a Lesson from Aviation, ***Qual Saf Health Care***, 15(3).
11. Rizvi, S. and Malik, S (February 2014), Ontology Design and Development Using Ontology editors along with Semantic Search Patterns towards Intelligent Retrieval of Information on Web, ***Journal International Journal of Autonomic Computing Archive***, Vol. 2, Issue 1.
12. Shen, D, Chen, G and Cruz, Jr and Haynes, L and Kruger, M and Blasch, E (April 2007), "A Markov Game Theoretic Data Fusion Approach for Cyber Situational Awareness", ***Defense and Security Symposium*** (pp. 65710F-65710F), International Society for Optics and Photonics.
13. Trauner Radwar, Daniel and Ziv Gadot and Deborah. Manor and Ronen. Kenig (2013), "DDoS Survival Hand Book, The Ultimate Guide to Everything You Need to Know about DDoS Attacks", available at: ***https:// www.security.radware.com***.
14. Waichal, Saili and Meshram, B (June 2013), Router Attacks-Detection and Defense Mechanisms, ***International Journal of Scientific & Technology Research***, Vol 2, Issue 6.
15. Welzel, Arne and Rossow, Christian and Bos, Herbert (April 2014), On Measuring the Impact of DDoS Botnets, ***EuroSec***, 14.
16. Yuan, F. S (June 2015), Data Fusion-based Resilient Control System under DoS Attacks: A Game Theoretic Approach, ***International Journal of Control Automation and Systems,*** 13 (3).
17. Zhang, L.J. and Cao, Y and Wang, Q.X (2010), "A DoS Attack Effect Evaluation Method Based on Multi-source Data Fusion", ***Communications and Mobile Computing***, Vol. 1, IEEE.