
بسم الله الرحمن الرحيم

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی هوش مصنوعی

طراحی یک مدل هوشمند امن برای وسایل نقلیه در فضای ابری

نگارنده: سمیرا رجب‌لو

استاد راهنما:

دکتر علی‌اکبر پویان

استاد مشاور:

دکتر محسن رضوانی

بهمن ۹۶

شماره: ۵۸۲ ر/ک
تاریخ: ۹۶/۱۲/۲

باسمه‌تعالی

دانشگاه صنعتی شاهرود

مدیریت تحصیلات تکمیلی

فرم شماره (۳) صورتجلسه نهایی دفاع از پایان نامه دوره کارشناسی ارشد

با نام و یاد خداوند متعال، ارزیابی جلسه دفاع از پایان نامه کارشناسی ارشد خانم **سمیرا رجب‌لو** با شماره دانشجویی **۹۴۳۶۱۳۴** رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیک تحت عنوان **طراحی یک مدل هوشمند امن برای وسایل نقلیه در فضای ابری** که در تاریخ **۹۶/۱۱/۱۱** با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می‌گردد:

قبول (با درجه: عالی) ☑ **مردود** ☐

نوع تحقیق: نظری ■ **عملی** ☐

عضو هیأت داوران	نام ونام خانوادگی	مرتبهٔ علمی	امضاء
۱ـ استاد راهنمای اول	دکتر علی‌اکبر پویان	استادیار	
۳- استاد مشاور	دکتر محسن رضوانی	استادیار	
۴- نماینده تحصیلات تکمیلی	مهندس محسن فرهادی	مربی	
۵- استاد ممتحن اول	دکتر منصور فاتح	استادیار	
۶-ـ استاد ممتحن دوم	دکتر سعیده فردوسی	استادیار	

نام و نام خانوادگی رئیس دانشکده: دکترعلی‌اکبر پویان

تاریخ و امضاء و مهر دانشکده: ۹۶/۱۱/۱۱

تبصره: در صورتی که کسی مردود شود حداکثر یکبار دیگر (در مدت مجاز تحصیل) می تواند از پایان نامه خود دفاع نماید (دفاع مجدد نباید زودتر از ۴ ماه برگزار شود).

تقدیم به

خدای مشرق

خدای مغرب...

خدایی که دیدگان هر بیننده‌ای از دیدنش قاصر و اندیشه هر توصیف کننده‌ای از وصف او عاجز است.

و تقدیم به کسی که بذر عشق را در وجودم پروراند

همسر صبور و مهربانم که نشانه لطف الهی در زندگی من است .

و سپاس از آن خدایی است که در همین حوالی است.. خدایی که عزیزانم را آفرید تا مرا یاری کنند.. عزیزانی چون جان؛ **پدر، مادر و همسر**

پدرم.. واژه‌ای بس سخت و محکم که در تمامی مراحل همچو کوه، استواری را به من آموخت تا در این راه با مشقاتش کنار بیایم.. تو را سپاس گویم.

مادرم.. تمام الطاف و احساسات خداوند در تو نهفته است. چه بسیار از خودگذشتگی‌ها را که به چشم ندیدم و چه بسیار رنج و زحمات را که با وجود خود حس نکردم. مادرم به درستی بهشت در دستان توست.. تو را سپاسگزارم.

همسرم.. در هر مرحله از زندگی‌ام مرا یاری نمود و صبوری را به من آموخت تا غم دوری مانع از رسیدن من به آرزوهای شیرینم نباشد.. خداوند را بابت وجود زیبای تو سپاسگزارم.

به مصداق «**من لم یشکر المخلوق لم یشکر الخالق**» بسی شایسته است از استاد فرهیخته و اندیشمند؛ **جناب آقای دکتر پویان** که با کرامتی چون خورشید، سرزمین دل را روشنی بخشیدند و گلشن سرای علم و دانش را با راهنمایی‌های سازنده خویش بارور ساختند؛

از استاد با کمالات و شایسته **جناب آقای دکتر رضوانی** که بدون شک بدون راهنمایی‌های ایشان این پژوهش به نتیجه نمی‌رسید؛

از اساتید محترم گروه: **جناب آقای دکتر فاتح** که همواره با حسن خلق و فروتنی در عرصه علم بر ما دریغ ننمودند؛ **جناب آقای دکتر زاهدی** که با نکته‌های دلاویز و گفته‌های بلند خویش صحیفه‌های سخن را برایمان علم پرور نمودند؛ **جناب آقای دکتر حسن‌پور** که با قلبی آکنده از دلسوزی ما را با چشمه‌های علم آشنا کردند، کمال تشکر و قدردانی را دارم.

لازم می‌دانم از دوستان گروه هوش مصنوعی و رباتیک خانم‌ها: زکی‌زاده، علی‌پور، آیت و مقدم نژاد که لحظات را برایم زیبا نمودند قدردانی کنم و همچنین از دوست و همکلاسی محترم جناب آقای فرمان‌بر که برادرانه موجبات آلام روحی ایجانب را فراهم نمودند تشکر کنم.

تعهد نامه

اینجانب **سمیرارجب‌لو** دانشجوی دوره کارشناسی ارشد رشته مهندسی کامپیوتر دانشکده کامپیوتر و فناوری اطلاعات دانشگاه صنعتی شاهرود نویسنده پایان‌نامه **طراحی یک مدل هوشمند امن برای وسایل نقلیه در فضای ابری** تحت راهنمائی **دکتر علی‌اکبر پویان** متعهد می شوم :

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ

امضای دانشجو

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود است. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

چکیده

شبکه بین خودرویی امروزه به عنوان طرحی نوین برای برقراری ایمنی، مدیریت ترافیک و کاربردهای رفاهی برای رانندگان و مسافران در جاده مطرح شده است. ارتباطات خودروها در این شبکه به دو صورت خودور به خودرو و خودرو به زیرساخت می‌باشد. در این ارتباطات، پیام‌های حاوی رخدادهای مهم در مورد جاده ارسال می‌گردند. ارتباطات بی‌سیم در این شبکه‌ها منجر به ایجاد چالش‌هایی از جمله اطلاعات نادرست، تغییر و ارسال مجدد پیام‌های منتشرشده در شبکه، جعل هویت و انکار سرویس توزیع شده (DDOS) می‌شود. یکی از تهدیدات امنیتی در شبکه‌های خودرویی، حمله DDOS است و هدف آن، مشغول نمودن واحد کنار جاده و غیرقابل دسترس نمودن آن برای خودروهای مجاز است. از طرفی، شماری از وسایل نقلیه در جاده‌ها دارای منابع محاسباتی هستند و می‌توانند به عنوان یک منبع بهره‌برداری نشده استفاده شوند بنابراین، مفهوم محاسبات ابری برای وسایل نقلیه مطرح شد. برای استفاده از تکنولوژی ابر در شبکه‌های خودرویی نیازمند به کارگیری یک زیرساخت (بستر) به عنوان سرویس می‌باشیم تا مدیریت شبکه را متمرکز و در برابر حملات ایمن سازد.

در این پایان‌نامه، از شبکه‌های مبتنی بر نرم‌افزار (SDN)، جهت طراحی مدل هوشمند امن برای وسایل نقلیه استفاده شده است. یکی از چالش‌های امنیتی شبکه‌های خودرویی مبتنی بر SDN، در دسترس بودن کنترل‌کننده است. در این پایان‌نامه، برای رفع نیاز امنیتی در دسترس بودن کنترل‌کننده، حمله DDOS بررسی شده است. با اعمال ترافیک مجاز و حمله به شبکه‌های خودرویی مبتنی بر SDN و براساس معیار آنتروپی و ویژگی‌های ترافیک، الگوی رفتار شبکه مورد بررسی قرار می‌گیرد. هدف این پژوهش وفقی‌سازی الگوریتم بهبودیافته با رفتار شبکه توسط ویژگی‌های ترافیک، یک مدل پویا برای تشخیص حمله DDOS بدست آمده است که در آن نرخ تشخیص حمله دارای رشد ۶۵/۶۱ ٪ است.

کلمات کلیدی: شبکه‌های بین خودرویی موردی، محاسبات ابری، حمله انکار سرویس (DDOS)، شبکه‌های مبتنی بر نرم‌افزار (SDN)، آنتروپی، ویژگی‌های ترافیک

فهرست مطالب

فصل اول

فصل دوم

فصل سوم

فصل چهارم

فصل پنجم

فهرست اشکال

فهرست جداول

فهرست علائم اختصاری

Vehicle to Vehicle	V2V
Vehicle to Infrastructure or Vehicle to RSU	V2I-V2R
On-Board Units	OBU
Road Side Unit	RSU
Vehicular Ad-Hoc Network	VANET
Mobile Ad-Hoc Network	MANET
Dedicated Short Range Communictaions	DSRC
Trusted Authority	TA
Denial of Service	DOS
Software-defined Network	SDN
Open Networking Foun	ONF
Software-defined VANET	SD VANET
Openflow	OF
Distributed Denial of Service	DDOS

فصل اول

مبانی و مفاهیم نظری

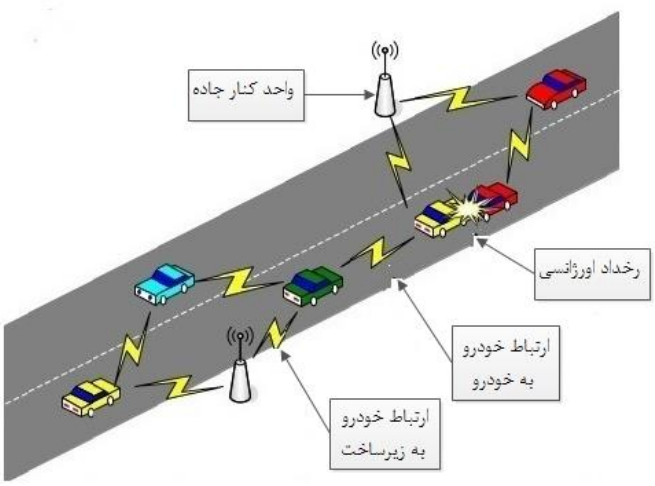
۱-۱- مقدمه

شبکه‌های بین خودرویی هوشمند در ایجاد سامانه حمل ونقل هوشمند بسیار مؤثر هستند که نمونه‌ای از کاربرد هوش مصنوعی در خودروها می‌باشند و باعث بروز رفتار خودمختار هوشمند توسط خودروها در مواقعی مانند تصادف، ناشی بودن راننده و ... می‌شوند. در این فناوری در شبکه‌های بین خودرویی هر خودرو مانند یک گره در شبکه عمل می‌کند. این گره‌ها می‌توانند با یکدیگر همکاری کنند تا کارایی شبکه افزایش یابد. درواقع، شبکه‌های بین خودرویی نوعی از شبکه اقتضایی می‌باشند که زیرساختار ثابت ندارند و به خودروهای شبکه وابسته هستند تا عملیات و توابع شبکه همچون مسیریابی بسته و مدیریت شبکه را انجام دهند. بالطبع این شبکه‌ها ممکن است مورد حمله قرار گیرند که تشخیص حملات و جلوگیری از پیشروی آن‌ها از چالش‌های امنیتی این شبکه‌ها است. باتوجه به نامتمرکز بودن این شبکه‌ها و غیرساختارمند بودن آن‌ها که از معایب این شبکه‌ها است از خصوصیات شبکه‌های مبتنی بر نرم‌افزار برای ارتقای آن‌ها استفاده شده است. شبکه‌های مبتنی بر نرم‌افزار، شبکه‌هایی متمرکز هستند و از منطق کنترل مرکزی برای کنترل شبکه‌ها استفاده می‌کنند. بدین‌ترتیب شبکه‌های خودرویی توسط یک کنترل‌کننده مرکزی که از اجزای شبکه‌های مبتنی بر نرم‌افزار است نظارت و مدیریت می‌شود و این مدیریت قابل برنامه‌نویسی خواهد بود. در این پژوهش سعی شده است با در نظر گرفتن یک حمله (DDOS[1]) در شبکه‌های خودرویی، الگوریتم تشخیص این حمله بهبود داده شود. در این فصل نخست شبکه‌های خودرویی، خصوصیات و چالش‌های امنیتی این شبکه‌ها معرفی شده است و سپس به معرفی و ساختار شبکه‌های مبتنی بر نرم‌افزار پرداخته شده است و در نهایت به تعمیم شبکه‌های خودرویی به شبکه‌های مبتنی بر نرم‌افزار و توپولوژی آن‌ها پرداخته خواهد شد و در انتهای این فصل هدف و رویکرد پژوهش ذکر شده است.

[1] Distributed Denial of Service (DOS)

۱-۲- معرفی شبکه خودرویی

ایده اولیه شبکه‌های بین خودرویی برای نخستین بار در سال ۱۹۹۸ توسط یک گروه مهندسی به نام سیستم‌های الکترونیکی Delpho Deleo با همکاری شرکت BMI، با هدف استفاده در رنج وسیعی از کاربردها مطرح شد[۱]. شبکه خودرویی با استفاده از امواج رادیویی، انواع ارتباطات خودرو به خودرو[۱] و خودرو به زیرساخت[۲] را ایجاد می‌کند. خودروها به صورت کاملا خودمختار با یکدیگر ارتباط برقرار کرده و یک شبکه غیرساختارمند بی‌سیم را ایجاد می‌کنند. (شکل (۱-۱))



شکل (۱-۱): شمایی کلی از شبکه‌های بین خودرویی موردی

برای برقراری ارتباط، هر خودرو باید مجهز به ابزاری باشد که امکان ارتباطات بی‌سیم را فراهم سازد. این ابزار ارتباطی، واحد داخل خودرو[۳] نامیده می‌شود که با نصب این ابزار، هر خودرو قادر به ارتباط با خودروهای دیگر و واحدهای کنار جاده[۴] می‌باشد. واحدهای کنار جاده واحدهایی نصب شده در نقاط شاخص کنار جاده هستند که این نقاط شاخص می‌توانند چراغ‌های راهنمایی رانندگی، علائم ترافیکی و

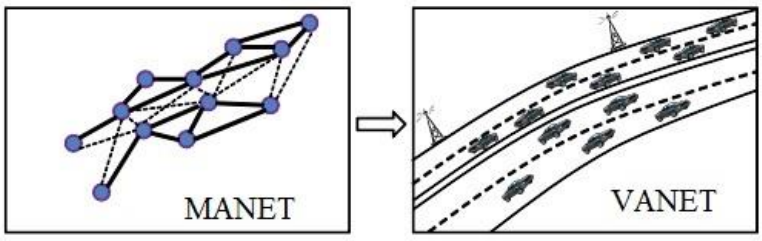
[۱] Vehicle to Vehicle (V2V)
[۲] Vehicle to Infrastructure (V2I) یا Vehicle to RSU (V2R)
[۳] Onboard Units (OBU)
[۴] Road Side Units (RSU)

مسیریاب‌های بی‌سیم باشند که مسیردهی به خودروهای روی جاده را فراهم می‌کنند. واحدهای کنار جاده می‌توانند به ستون فقرات اینترنت وصل شده و سرویس‌های گوناگونی همچون پروتکل‌های کنترل انتقال و کاربردهای زمان واقعی مالتی مدیا را برای کاربران خود فراهم سازند. بدین ترتیب با وجود واحد داخل خودرو و واحدهای کنار جاده، یک شبکه خودسازمان‌یافته می‌تواند ایجاد شود که شبکه‌های بین خودرویی موردی[۱] نامیده می‌شوند.

در حقیقت شبکه‌های خودرویی، یک نوع خاص از شبکه‌های سیار موردی[۲] هستند که نودها در این شبکه خودروها هستند. هر خودرو می‌تواند در هر لحظه خودروهای اطرافش را شناسایی کرده و با اتصال به آن‌ها یک شبکه تشکیل دهد و ارتباطات لازم را برقرار کند. این خودرو کمی بعدتر با خودروهای جدید اطرافش یک شبکه دیگر ایجاد خواهد کرد. مبنای اصلی شبکه‌های خودرویی غیرساختارمند بودن آن‌ها و استفاده از استاندارد ۸۰۲.۱۱p و مجموعه استانداردهای ارتباطات اختصاصی بردکوتاه[۳] [۲] است.

۱-۲-۱- خصوصیات

همانطور که اشاره شد، شبکه بین خودرویی موردی نوع خاصی از شبکه سیار موردی هستند به نحوی که نودهای سیار با خودروهای مجهز به واحد پردازشی داخل خودرو جایگزین شده است (شکل(۱-۱)) که در نتیجه خصوصیاتی دارد که متمایز از خصوصیات شبکه‌های سیار موردی می‌باشد. این خصوصیات شامل موارد زیر می‌باشند[۳-۵].



شکل (۱-۲): ارتباط بین شبکه خودرویی موردی و سیار موردی[۴]

[۱] Vehicular Ad Hoc Network (VANET)
[۲] Mobile Ad Hoc Network (MANET)
[۳] Dedicated Short Range Communications (DSRC)

- تغییر سریع در توپولوژی: خودروها معمولا با سرعت نسبی بالا حرکت می‌نمایند و بنابراین توپولوژی این شبکه‌ها بصورت پویا سریعا در حال تغییر است. برای خودروهایی که در یک جهت حرکت می‌کنند موقعیت‌های آن‌ها نسبت به هم تغییراتش آهسته بوده و برای خودروهایی که از مقابل هم حرکت می‌کنند این تغییرات خیلی سریع است.
- عدم محدودیت توان: برخلاف لب‌تاپ‌ها، دستیار دیجیتال شخصی (PDAها) یا سنسورها، که محدودیت باطری دارند؛ شبکه بین خودرویی بدلیل اتکا بر انرژی نامحدود باطری از این محدودیت معاف است.
- مقیاس وسیع: شبکه‌های بین خودرویی در حالت کلی می‌توانند به بزرگی شبکه جاده‌ای باشند و تعداد زیادی خودروها باعث ایجاد شبکه‌ای در مقیاس وسیع از آن‌ها می‌گردد، به‌گونه‌ای که مرتبه تعداد خودروها در واقعیت در حدود $۱۰^{۷}$ می‌باشد. در نتیجه چالش‌های متفاوتی برای این نوع شبکه‌ها بروز می‌کنند.
- تغییر تراکم خودروها در شبکه: تعداد خودروهایی که در یک ناحیه مشخص از جاده هستند، در طول روز در حال تغییر است. به این معنا که در ساعات خاصی از روز تردد وسائل نقلیه بیشتر است. این امر از این لحاظ قابل تأمل است که شبکه‌های متراکم و کم تراکم در برخی از موارد از جمله کنترل توان، کنترل بار و مسیریابی، تفاوت‌های زیادی با هم دارند. به عنوان مثال در یک شبکه متراکم، گره‌ها سعی می‌کنند با کم کردن توان ارسالی از میزان تداخل‌ها و بار شبکه بکاهند در حالی که در یک شبکه کم تراکم گره‌ها با بالاترین توان خود سعی دارند تا همبندی شبکه را حفظ نمایند.
- تحرک بالا و در عین حال قابل پیش‌بینی: سرعت وسائل نقلیه در شهرها معمولا تا۶۰ کیلومتر بر ساعت است که این سرعت می‌تواند به ۱۲۰ کیلومتر بر ساعت در بزرگراه‌ها برسد. علاوه بر این، تحرک خودروها تصادفی نیست و در نتیجه الگوی تحرک خودروها بر اثر شکل خاص جاده و محدودیت‌های مقرراتی (ازقبیل سرعت)، محدود می‌شود. این امر باعث شده است که عده‌ای

از محققان تلاش کرده‌اند که برای بالابردن دقت شبیه‌سازی‌ها، مدل‌های تحرک ویژه برای این شبکه‌ها بنیان نهاده و تأثیر محدودیت‌های فوق را در آن‌ها لحاظ نمایند[۳].

- توپولوژی شبکه ارتباط زیادی با رفتار راننده دارد: در شبکه خودرویی و به‌خصوص در کاربردهای ایمنی آن، رفتار راننده باید مدنظر قرار بگیرد. این امر در شبکه‌های موردی عمومی موضوعیت ندارد. این رفتار باید به نحوی از طریق سیستم‌های داخل خودرو استخراج شده و به خودورهای همسایه ارسال گردد. خاصیت جالب دیگر این است که محتویات پیام‌ها نیز می‌تواند باعث تغییر توپولوژی گردد. مثلا هنگامی که پیام مبتنی بر وقوع تصادف ارسال می‌گردد، خودروها با کم کردن سرعت، باعث ایجاد ازدحام و در نتیجه به وجود آمدن شبکه‌ای متراکم می‌شوند[۶].

۱-۲-۲- کاربردهای شبکه خودرویی

کاربردهای شبکه خودرویی به دو دسته تقسیم می‌شوند؛ دسته اول کاربردهایی هستند که باعث افزایش ایمنی در جاده‌ها می‌شوند تحت عنوان کاربردهای ایمنی و دسته دوم کاربردهایی هستند که سرویس-های ارزشمندی را برای خودروها فراهم می‌کنند که از جمله این سرویس‌ها می‌توان به سرویس‌های سرگرمی اشاره کرد[۷-۹].

۱-۲-۲-۱- کاربردهای ایمنی

کاربردهای ایمنی همانطور که قبلا اشاره شد، شمار تصادفات را تا حد زیادی می‌توانند کاهش دهند. بر حسب مطالعات انجام شده[۱۰]، در صورتی‌که نیم ثانیه قبل از لحظه برخورد به راننده هشدار داده شود، شش درصد از شمار تصادفات کاهش خواهد یافت. سه سناریوی اصلی در کاربردهای ایمنی وجود دارد که شامل:

۱. تصادفات: زمانی‌که رانندگان با سرعت بالا در جاده‌های اصلی حرکت می‌کنند و خودرویی در جلوی آن‌ها حرکتی ناخواسته و غیرعادی دارد، زمان برای عکس‌العمل نشان دادن توسط راننده خیلی اندک است. همچنین اگر یک تصادف رخ دهد، خودروهای نزدیک به خودروی مورد نظر، اغلب قبل از اینکه توقف کنند به یکدیگر برخورد خواهند کرد. کاربردهای حوزه ایمنی شبکه‌های VANET

در اینجا برای اخطار به رانندگان از وقوع یک تصادف در آینده‌ای نزدیک مورد استفاده قرار می‌گیرند و به این ترتیب از یک تصادف زنجیره‌ای در جاده اجتناب خواهد شد. علاوه بر این با دریافت اخطار توسط راننده از تصادف اول نیز می‌توان جلوگیری کرد و به عنوان نمونه با رسیدن به یک پیچ خطرناک به راننده هشدار داد تا از سرعت خود بکاهد و به این ترتیب از هرگونه تصادفی با شرایط آب و هوایی با جاده‌ای نامناسب تا حد امکان جلوگیری کرد.

۲. تقاطع‌ها: در واقعیت، رانندگی در نزدیکی یا در خود بزرگراه‌ها یکی از چالش‌های پیچیده‌ای است که رانندگان با آن مواجه می‌شوند. زیرا با رسیدن دو یا چند جریان ترافیکی به هم احتمال وقوع تصادف افزایش می‌یابد. در سال ۲۰۰۳ طبق اعلام وزارت حمل و نقل ایالات متحده آمریکا، برخوردهایی که در تقاطع‌ها اتفاق افتاده بیش از ۴۵ درصد از کل برخوردها و ۲۱ درصد از تصادفاتی است که منجر به فوت شده است. تعداد این تصادفات کشنده ۹۲۱۳ تصادف گزارش شده است[۱۱]. در این شرایط اگر یک کاربرد مرتبط با ایمنی VANET برخوردهای قریب‌الوقوع را به راننده اطلاع دهد، اعداد تصادفات کاهش چشمگیری خواهد داشت.

۳. ترافیک جاده‌ای: کاربردهای مرتبط با ایمنی برای تعیین بهترین مسیر برای رانندگان به منظور رسیدن به مقصد می‌توانند مورد استفاده قرار بگیرند. با این کار، ترافیک جاده‌ها کاهش می‌یابد و از ایجاد ازدحام در مناطق خاصی از جاده جلوگیری می‌شود و در نتیجه ظرفیت جاده‌ها افزایش یافته و جریان ترافیکی نرمی در جاده‌ها برقرار می‌شود. علاوه بر این، برقراری این شرایط تأثیر غیرمستقیمی هم بر کاهش تصادفات خواهد داشت زیرا اتلاف وقت رانندگان کمتر شده و در نتیجه رانندگان تمایل بیشتری به رعایت قوانین ترافیکی از خود نشان خواهند داد.

۱-۲-۲-۲- کاربردهای غیرایمنی

کاربردهای غیرایمنی فراهم‌کننده اطلاعات، آگهی‌ها و سرگرمی برای کاربران هستند. نمونه‌هایی از این کاربردها شامل موارد زیر می‌باشند.

۱. اتصال به اینترنت: امروزه دسترسی به اینترنت برای خیلی از افراد به عنوان یک نیاز روزانه مطرح شده است. بدین منظور واحدهای کنار جاده برای دستیابی به اینترنت می‌توانند به عنوان گذرگاه عمل کرده و امکان دسترسی به اینترنت و نیز آپلود یا دانلود mp۳ یا ویدئوهای با سایز کوچک را برای رانندگان خودروها فراهم نمایند. مسافران داخل خودروها نیز می‌توانند از امکانات دریافت و ارسال ایمیل، گشت و گذار در وب‌سایت‌ها و بازی‌های آنلاین استفاده کنند.

۲. کاربردهای نظیر به نظیر: این کاربردها برای رفع خستگی مسافران می‌تواند مفید واقع شوند و امکان به اشتراک‌گذاری موزیک، فیلم و غیره و همچنین چت و بازی با یکدیگر را فراهم می‌کنند.

۳. کاربردهای یاری‌رسان: واحدهای کنار جاده می‌توانند به رانندگان کمک کنند که مکان‌های مورد نظر خود را بیابند. این مکان‌ها از قبیل نزدیک‌ترین رستوران، کافی‌شاپ، منطقه خرید، پمپ‌بنزین و پارکینگ می‌باشند. زمانی‌که خودروها به یک واحد کنار جاده می‌رسند، درخواست‌های خود را به واحد کنار جاده می‌فرستند؛ سپس واحد کنار جاده در بانک اطلاعاتی خود جستجو کرده و پاسخ درخواست‌های آن‌ها را می‌دهد. واحدهای کنار جاده می‌توانند در ورودی پارکینگ‌ها نیز قرار گیرند و بدین طریق خودروها قبل از ورود به پارکینگ از وجود فضای خالی در پارکینگ مطلع گردند و در صورت وجود فضای خالی برای پارک خودرو، واحدهای کنار جاده داخل پارکینگ می‌توانند خودروها را برای ورود به منطقه خالی مورد نظر راهنمایی کنند[۱۲]. در یک نمونه از این کار[۱۳]، با بررسی و یافتن نزدیک‌ترین پارکینگ خالی و راهنمایی خودرو به داخل پارکینگ انجام شده است که علاوه بر این مورد امکان سرقت خودرو پارک شده در پارکینگ را نیز بررسی کرده و در صورت سرقت و خروج از پارکینگ امکان ردگیری را توسط درخواست‌هایی که به طور دوره‌ای توسط خودروهای پارک شده در پارکینگ باید به واحدهای کنار جاده نصب شده در پارکینگ گزارش داده شود فراهم می‌کند و بدین طریق با دریافت این پیام‌ها توسط خودروهای خارج از پارکینگ و واحدهای کنار جاده، خودروی سرقت شده را ردگیری کرد.

۴. کاربردهای تجاری: واحدهای کنار جاده می‌توانند به فروشگاه‌ها کمک کنند که آگهی‌های خود از قبیل پیشنهادهای ویژه آخر هفته، آگهی‌های هفتگی و سهمیه‌های بلیت فیلم را پخش کنند. علاوه بر این رانندگان قادر خواهند بود که در برخی موارد بلیت خود را مستقیما از واحدهای کنار جاده خریداری کنند.

۵. کاربرد در دریافت اطلاعات محیط: VANETها می‌توانند اطلاعات محیطی را از طریق خودروها جمع‌آوری کنند. در این راستا سنسورهای نصب شده بر روی خودروها داده‌هایی چون اطلاعات رطوبت و شرایط آب و هوایی را دریافت کرده و این اطلاعات را به واحدهای کنار جاده می‌فرستند. واحدهای کنار جاده نیز اطلاعات تمام خودروها در رنج خود را برای استفاده‌های آتی جمع‌آوری می‌کنند.

۱-۲-۳- امنیت در شبکه بین خودرویی

۱-۲-۳-۱- رفتارهای امنیتی

از آنجا که هم‌بندی (توپولوژی) شبکه‌های موردی همیشه در حال تغییر و دگرگونی است و هیچ نودی جای ثابت و مشخصی در شبکه نداشته و نودها خود ارتباطات درون شبکه‌ای را مدیریت و سرویس‌دهی می‌کنند در نتیجه مشکلات امنیتی زیادی در این شبکه به وجود می‌آیند. در این‌گونه شبکه‌ها نمی‌توان از هیچ سرویس یا دستگاه سخت‌افزاری برای تأمین امنیت و بالا بردن ضریب اطمینان استفاده کرد و کافی است یک مهاجم برای سرقت اطلاعات، جایی در شبکه را برای اقامت پیدا کند. در این صورت قادر به ارسال مجدد بسته‌ها به منظور اخلال در شبکه، تغییر محتوای بسته‌ها، جعل و تغییر هویت و بدست آوردن اطلاعات خصوصی خودروها همچون مسیر و مکان خودروها خواهد بود. بنابراین قبل از پیاده‌سازی و استفاده از کاربردهای گوناگون شبکه بین خودرویی موردی، دو مسئله مهم امنیت و حفظ حریم خصوصی در این شبکه‌ها باید حل شوند[۱۴-۱۶]. مشکلات امنیتی در شبکه‌های موردی از آن جهت خاص شده و جداگانه مورد بررسی قرار می‌گیرد که در این شبکه‌ها علاوه بر این که تمامی مشکلات

موجود در یک شبکه کابلی یا یک شبکه بی‌سیم وجود دارد؛ مشکلات تازه و بیشتری نیز دیده می‌شود. مثلا از آنجا که تمامی ارتباطات به صورت بی‌سیم انجام می‌شود، می‌توان آن‌ها را شنود کرد و تغییر داد. همچنین از آنجا که خود نودها در عمل مسیریابی شرکت می‌کنند وجود یک نود متخاصم می‌تواند به نابودی شبکه بیانجامد. همچنین در این شبکه‌ها تصور یک واحد توزیع کلید با زیرساخت کلید واحد به صورت عمومی و غیره مشکل است، زیرا این‌گونه شبکه‌ها بیشتر بدون برنامه‌ریزی قبلی ایجاد می‌شوند و برای مدت کوتاهی به برقراری امنیت نیاز دارند. برای جمع‌بندی این بخش باید بگوییم که عمده حملات به شبکه‌های موردی از جانب مسیریابی (Routing) است و حملات جدید براساس آسیب‌پذیری-های پروتکل‌ها و الگوریتم‌های مسیریابی به‌وجود می‌آیند.

پذیرش یک نوع پروتکل IEEE ۸۰۲,۱۱ توسط کارخانه‌های وسایل نقلیه، کار مهاجم را در شبکه‌های VANET راحت‌تر می‌کند. اگر امنیت در این شبکه‌ها در نظر گرفته نشود، این شبکه‌ها مانند یک شمشیر دولبه عمل می‌کنند. بنابراین با لحاظ کردن امنیت در این شبکه‌ها رفتارهای امنیتی در VANET به صورت زیر دسته‌بندی می‌شوند[۴].

۱. پارازیت: یک حمله‌کننده عمدتا تعداد زیادی از پیام‌های جعلی را تولید کرده تا با شلوغ کردن کانال ارتباطی مانع ارتباطات نرمال سایر خودروها شود.
۲. جعل پیام و سندسازی: یک حمله‌کننده با نیات بدخواهانه می‌تواند یک حمله سندسازی را راه بیاندازد که این کار به‌صورت بالقوه باعث بروز تصادفات می‌شود. بنابراین تازگی و صحت پیام‌ها در ارتباطات بین خودروها (V2V) برای اطمینان از عدم جعل پیام‌های دریافت شده مهم هستند.
۳. دستکاری ترافیک در انتقال بسته: در این نوع حمله، یک حمله‌کننده به‌صورت عمدی باعث تأخیر، حذف، خرابی یا تغییر در پیام‌ها می‌شود تا به ارتباطات نرمال V2V در شبکه آسیب بزند.
۴. جعل هویت: در این حمله هدف حمله‌کننده این است که برای پیاده‌سازی اهداف خود دیگران را متقاعد کند که یک وسیله قانونی در شبکه است. مثلا با این کار ادعا می‌کند که یک خودروی اورژانس است و وسایل نقلیه‌ای که در جلویش هستند را برای عبور خود کنار می‌زند.

۵. شکستن حریم خصوصی: در VANETها، جمع‌آوری اطلاعات خصوصی وسیله نقلیه از سربار اطلاعات خودروها کار آسانی است و بنابراین اگر یک حمله‌کننده پیام‌های کافی را بتواند از خودروها جمع‌آوری کند، با استنتاج روی اطلاعات شخصی خودروی موردنظر، حریم شخصی خودرو شکسته شده و اطلاعات خصوصیش فاش خواهد شد.

۶. دستکاری روی خودرو: علاوه بر سوءاستفاده از پروتکل‌های ارتباطی، ممکن است حمله‌کننده داده را در همان مبدأ دستکاری کند. دستکاری داده در مبدأ، هم با دستکاری حسگرهای نصب شده بر روی خودرو می‌تواند باشد و هم با بکارگیری سخت‌افزارهایی خاص. به عنوان نمونه حمله‌کننده می‌تواند سنسوری را از کار بیاندازد یا مقداری یخ در اطراف سنسور بگذارد تا سنسور پیام جعلی هشدار مبنی بر جاده یخی را برای خودروهای دیگر ارسال کند.

۷. انکار سرویس[۱]: این نوع از رفتارهای امنیتی یکی از شایع‌ترین حمله‌ها است. در این مورد مهاجم‌ها به طرق مختلف منابع سیستم را مصرف می‌کنند و منابع را برای کاربران مجاز غیرقابل دسترس می‌کنند. در این پژوهش سعی شده است یک الگوریتم جهت تشخیص این حمله بهبود داده شود.

۱-۲-۳-۲- نیازمندی‌های امنیتی

۱. اعتبارسنجی[۲]: اعتبارسنجی توانایی ثابت کردن این است که یک کاربر همان شخصی است که ادعا می‌کند. اعتبارسنجی پیام یک نیاز حیاتی در VANET است چون این اطمینان را فراهم می‌کند که پیام دریافت شده در شبکه از طرف یک خودروی قانونی و تعیین اعتبار شده در شبکه ارسال شده است.

۲. یکپارچگی[۳]: اطمینان از اینکه پیام‌های مبادله شده بین خودروها در معرض تغییر، اضافه یا حذف قرار نگرفته‌اند. در واقع این ویژگی در صورت برقراری، این اطمینان را فراهم می‌کند که همه پیام‌های فرستاده شده توسط خودروها باید بدون تغییر تحول داده شوند.

---

[۱] Denial Of Service (DOS)
[۲] Authentication
[۳] integrity

۳. عدم انکار[۱]: جلوگیری از اینکه یک وسیله وجود و یا محتوای پیام ارسال شده توسط خود را انکار کند. این ویژگی یک خصوصیت بحرانی در VANET است چون این‌گونه یک مهاجم از انکار حملاتی که خود راه انداخته است خودداری می‌کند.

۴. دسترس‌پذیری[۲]: اطمینان از اینکه سیستم به درستی کار می‌کند و خدمات به کاربران مجاز و زمانی‌که موردنیاز است، ارائه می‌شود. حمله‌کننده ممکن است مانع ارائه خدمات به گره‌های معتبر از طریق شلوغ کردن کانال به وسیله اختلال در پروتکل‌های مسیریابی به وسیله تخلیه باطری و یا غیره شود. به عنوان مثال خدمات ارائه شده توسط تجهیزات کنار جاده (RSU) باید در هر زمان که موردنیاز است در دسترس وسایل نقلیه باشد.

۵. حریم خصوصی[۳]: توانایی حفاظت از اطلاعات خصوصی، از یک گروه تصدیق نشده در شبکه را حریم خصوصی گویند. در VANET شناسه واقعی هر خودروی شخصی تنها برای خودروهای دیگر و واحدهای کنار جاده پنهان است. این شناسه باید برای تصدیق‌کننده قابل اطمینان[۴] یا واحد TA آشکار باشد. علاوه بر شناسه هر خودرو موقعیت و مکان خودرو نیز باید برای خودروهای دیگر مخفی بماند و به این ترتیب مسیر خودرو قابل ردگیری نباشد.

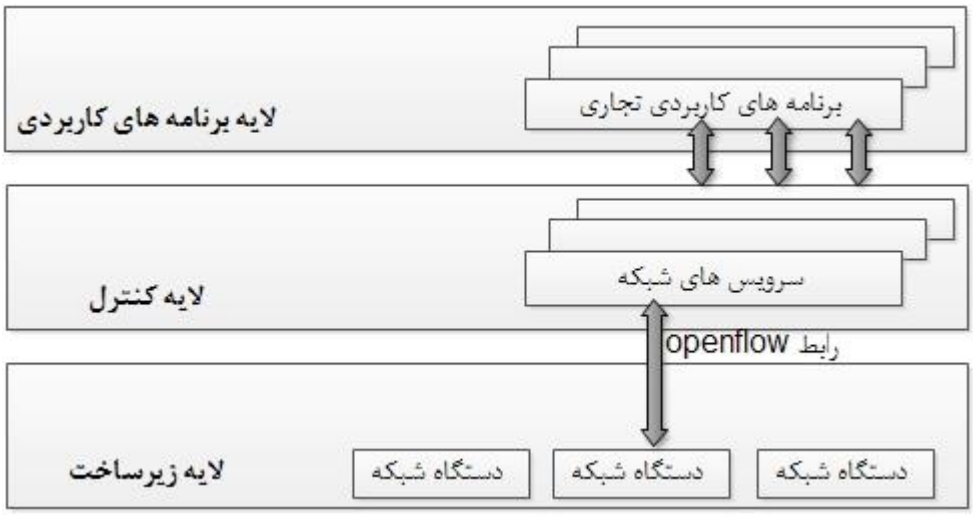
۱-۳- شبکه‌های مبتنی بر نرم‌افزار[۵]

در شبکه‌های مبتنی بر نرم‌افزار، معماری شبکه به گونه‌ای فراهم شده است که در آن بخش داده[۶] و کنترل[۷] از یکدیگر مجزا هستند. بخش داده برای انتقال داده استفاده می‌شود در حالی که بخش کنترل برای کنترل ترافیک شبکه مورد استفاده قرار می‌گیرد. ساختار معماری در شبکه‌های SDN هوشمندتر و کنترل‌پذیرتر شده است. یکی از ایده‌های بارز شبکه‌های مبتنی بر نرم‌افزار این است که دستگاهی به

---

[۱] Non-repudiation
[۲] Availability
[۳] Privacy
[۴] Trusted Authority (TA)
[۵] Software_defined Network (SDN)
[۶] Data plane
[۷] Control plane

نام کنترل‌کننده با همه دستگاه‌های موجود در یک دامنه[1] ارتباط مستقیم داشته باشد، از معماری شبکه آگاه باشد و شبکه را از یک نقطه مرکزی برنامه‌ریزی کند[۱۷]. یک کنترل‌کننده SDN مدل برنامه‌ریزی شبکه را از حالت توزیع‌شده به حالت متمرکز تبدیل می‌کند. برنامه‌ریزی متمرکز شبکه، ویژگی ارزشمندی است که می‌توان به‌وسیله آن انواع سیاست‌گذاری‌های امنیتی را به صورت کلان انجام داد. با استفاده از SDN ، شرکت‌ها و اپراتورهای مخابراتی، از طریق یک کنترل‌کننده مرکزی واحد در کل شبکه می توانند فارغ از سخت‌افزار و شرکت سازنده آن شبکه را کنترل و مدیریت کنند. به این ترتیب، طراحی شبکه و کاربری آن، به طور چشمگیری، ساده‌تر خواهد شد. همچنین SDN، دستگاه‌ها و ماشین‌های به کار گرفته شده در شبکه را نیز ساده‌تر می‌کند، چرا که دیگر نیازی به شناسایی و پردازش هزاران پروتکل نخواهد بود و دستورات فقط از کنترل‌کننده SDN دریافت می‌شود. ساختار شبکه‌های مبتنی بر نرم‌افزار در شکل (۱-۳) نشان داده شده است.



شکل (۱-۳): معماری SDN [۱۸]

همانطور که در شکل (۱-۳) مشاهده می‌شود معماری شبکه‌های SDN دارای سه لایه است که عبارتند از:

[1] Domain

۱. لایه زیرساخت: این بخش به طور مستقیم مسئول ارسال داده‌ها بر اساس جدول‌های برنامه‌ریزی شده توسط کنترل‌کننده‌ها است.

۲. لایه کنترل: در این لایه کنترل‌کننده با همه دستگاه‌های موجود در یک دامنه شبکه ارتباط مستقیم داشته، از توپولوژی شبکه آگاه است و شبکه را از یک نقطه مرکزی برنامه‌ریزی می‌کند.

۳. لایه کاربرد: این برنامه‌ها از طریق واسط شمالی مابین رفتارها و منابع مورد نیاز کنترل‌کننده ارتباط برقرار می‌کند. علاوه بر این، برنامه‌های کاربردی می‌توانند از طریق جمع‌آوری اطلاعات از کنترل‌کننده یک دید انتزاعی از شبکه ایجاد نمایند که برای تصمیم‌گیری مورد استفاده قرار می‌گیرد.

۴. واسط جنوبی[۱]: توسط پروتکل OpenFlow استاندارد شده است. پروتکل OpenFlow امکان دسترسی مستقیم و ایجاد تغییر در برنامه ارسال تجهیزات شبکه نظیر سوئیچ‌ها را، هم به صورت فیزیکی و هم مجازی فراهم می‌کند.

۵. واسط شمالی[۲]: برای برقراری ارتباط میان کنترل‌کننده و سرویس‌ها و برنامه‌های کاربردی در حال اجرای شبکه استفاده می‌شود. این واسط برای تسهیل نوآوری و ارائه سرویس‌های جدید با روشی آسان استفاده می‌شود.

۱-۳-۱- پروتکل OpenFlow

OpenFlow، نخستین واسط ارتباطی استانداردی است که در معماری SDN، بین لایه‌های کنترل و زیرساخت تعریف می شود. بنیاد ONF[۳] در سال ۲۰۱۱ با هدف ترویج شکل جدیدی از شبکه‌های SDN سازگار با پروتکل OpenFlow آغاز به کار کرد. برای این منظور، این بنیاد مسئولیت استانداردسازی پروتکل OpenFlow را عهده‌دار شده است. بنیاد ONF برخلاف بیشتر گروه‌ها یا کنسرسیوم‌های صنعتی استانداردسازی IT، توسط تأمین‌کنندگان فناوری‌های زیر ساختی تاسیس نشد بلکه توسط شرکت‌هایی

[۱] Northbound Interface
[۲] Southbound Interface
[۳] Open Networking Foun

تاسیس شد که به استفاده از این فناوری مشتاق بودند مانند: گوگل، فیسبوک، مایکروسافت، یاهو و ۱۹ شرکت دیگر[۱۹].

OpenFlow امکان دسترسی مستقیم و ایجاد تغییر در برنامه ارسال تجهیزات شبکه نظیر سوئیچ‌ها و مسیریاب‌ها را، هم به صورت فیزیکی و هم مجازی فراهم می‌کند. OpenFlow کنترل شبکه را از سوئیچ‌های شبکه خارج و به کنترل‌کننده مرکزی منطقی هدایت می‌کند. در شبکه‌های SDN کنترل‌کننده تمامی قوانین شبکه را نگهداری و برحسب نیاز، دستورات را از طریق پروتکل OpenFlow صادر می‌کند. در ابتدا، OpenFlow کنترل‌کننده مرکزی را تعریف می‌کند و بعد می‌گوید چگونه این کنترل‌کننده می‌تواند به صورت امن به دستگاه‌های شبکه متصل و آن را کنترل کند. سپس OpenFlow مشخص می‌کند که چگونه باید بسته‌های دریافتی را دستکاری، پردازش و دوباره ارسال کرد. قبل از OpenFlow، هیچ استانداردی برای دستکاری و forwarding جدول مسیریابی شبکه وجود نداشت؛ بنابراین، SDN بدون OpenFlow ناچار بود به صورت انحصاری اجرا شود یا با کاستی‌ها و عیب‌هایی در عملکرد روبرو باشد[۲۰]. نسخه اول پروتکل OpenFlow در دسامبر سال ۲۰۰۹ تعریف و منتشر شد که از سه جزء اصلی کنترل‌کننده، کانال‌های امن و جدول جریان تشکیل شده است. در سال ۲۰۱۱ نسخه جدید نیز عرضه شد که علاوه بر اجزای قبلی شامل دو جزء جدول گروهی و پایپ‌لایان[۱] است. تاکنون شش نسخه پروتکل OpenFlow عرضه شده که هر نسخه شامل قابلیت‌های بیشتری نسبت به نسخه‌های قبلی است[۱۹-۲۱].

۱-۴- شبکه‌های خودرویی مبتنی بر نرم‌افزار[۲]

در این قسمت به منظور گسترش شبکه‌های SDN و مزایای آن به چگونگی ارتقاء شبکه‌های VANET توسط SDN اشاره می‌شود. در [۲۲] یک بررسی جامع در مورد نحوه اجرای SDN در شبکه‌های VANET انجام شده است. آن‌ها معماری و سرویس‌های شبکه‌های SD VANET و ویژگی‌های جدید

[۱] Pipeline
[۲] Software-defined VANET (SD VANET)

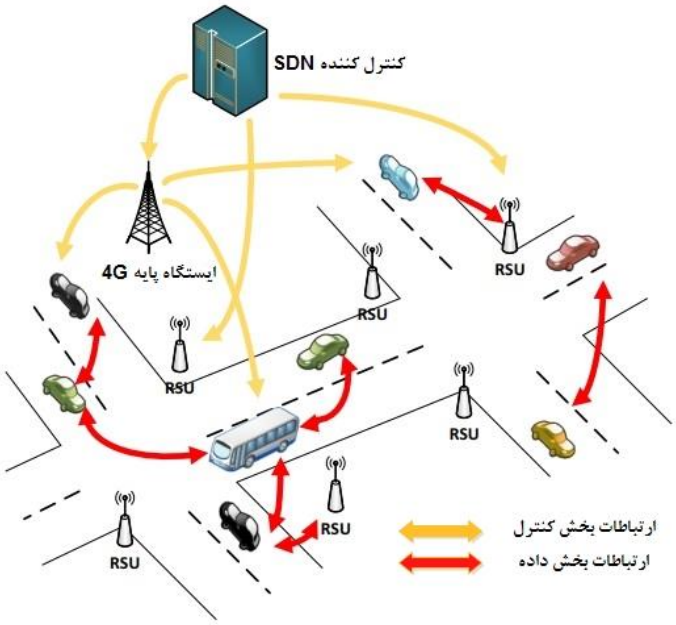
را برای پشتیبانی از آن‌ها ارائه کرده‌اند. با استفاده از جداسازی بخش داده و بخش کنترل در VANETها، اطلاعات شبکه می‌تواند به طور منطقی متمرکز شود. بنابراین می‌توان محیط‌های بسیار انطباق‌پذیر، همه‌کاره، قابل برنامه‌ریزی و مقیاس‌پذیر در VANET داشت. همان‌طور که گفته شد اساس شبکه‌های SDN جداسازی بخش داده از بخش کنترل است. استفاده از SDN در محیط‌هایی مانند VANETها می‌تواند تداخل را کاهش دهد و دارای مزیت‌های استفاده از کانال‌ها و بهبود منابع بی‌سیم و همچنین مسیریابی داده‌ها در سناریوهای چند مسیره[۱] و چند هپ [۲] می‌باشد.

۱-۴-۱- معماری VANET مبتنی بر نرم‌افزار

در [۲۳] معماری پیشنهادی VANET مبتنی بر نرم‌افزار دارای اجزای زیر است:

- کنترل‌کننده SDN: مسئول تعیین کل عملکرد شبکه است.
- گره بی‌سیم SDN: کنترل‌کننده SDN، کنترل عناصر بخش داده را برعهده دارد و در این معماری این عناصر خودروهایی هستند که پیام کنترل را از کنترل‌کننده برای انجام اقدامات دریافت می‌کنند.
- واحد کنار جاده SDN: عناصر بخش داده که توسط کنترل‌کننده SDN کنترل می‌شوند. آن‌ها واحد کنار جاده هستند. شکل (۱-۴) ارتباط بین اجزاء در VANET مبتنی بر نرم‌افزار را نشان می‌دهد.

[۱] Multi-Path
[۲] Multi-hop

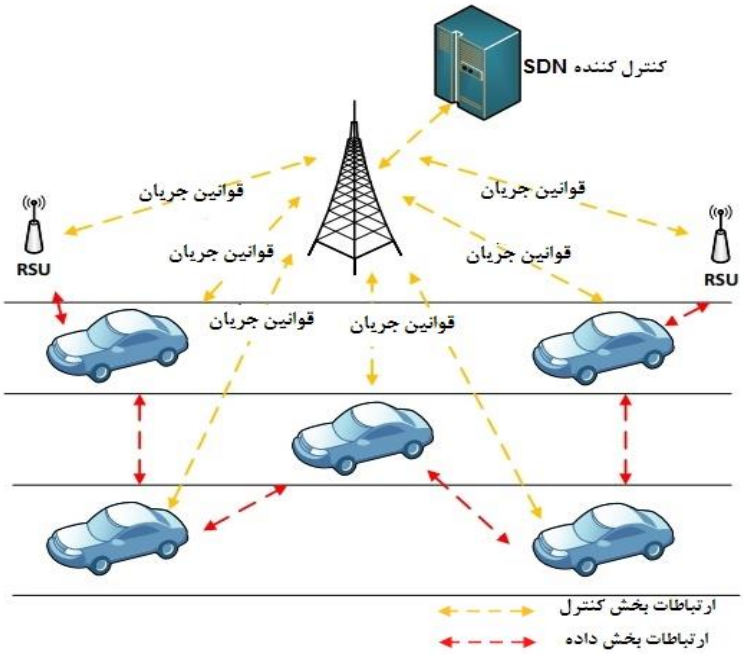


شکل (۱-۴): ارتباطات شبکه‌های VANET مبتنی بر نرم‌افزار[۲۳]

۱-۴-۲- بررسی عملکرد شبکه‌های VANET مبتنی بر نرم‌افزار

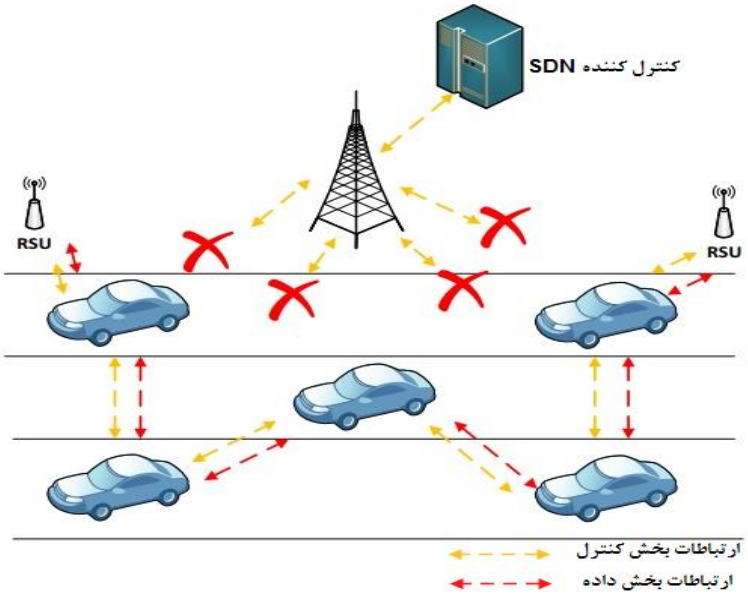
روش‌های متعددی وجود دارد که در آن‌ها VANET مبتنی بر نرم‌افزار می‌تواند براساس درجه کنترل‌کننده SDN تعریف شود. با این وجود ایده اساسی آن‌ها جداسازی بخش داده از بخش کنترل است. طبقه‌بندی این معماری به سه حالت ارائه شده است:

- حالت کنترل مرکزی: در این حالت تمام عملیات پایه گره‌های بی‌سیم SDN و RSU توسط کنترل‌کننده SDN کنترل می‌شود. تمام اقداماتی که عناصر داده SDN انجام می‌دهند به طور خاص توسط کنترل‌کننده تعیین می‌شود. کنترل‌کننده تمام قوانین جریان را در مورد چگونگی مدیریت ترافیک، همانطور که در شکل (۱-۵) نشان داده شده است انجام می‌دهد.
- حالت کنترل توزیع‌شده: در این حالت هنگام تحویل بسته، گره‌های بی‌سیم SDN و RSU بدون هیچگونه دستورالعملی از کنترل‌کننده عمل می‌کنند. در اصل این حالت برای شبکه‌های توزیع‌شده خودسازمانده بسیار رایج است که انتظار دارند عامل محلی در هر گره بی‌سیم SDN، عملکردهای



شکل (۱-۵): حالت کنترل مرکزی[۲۳]

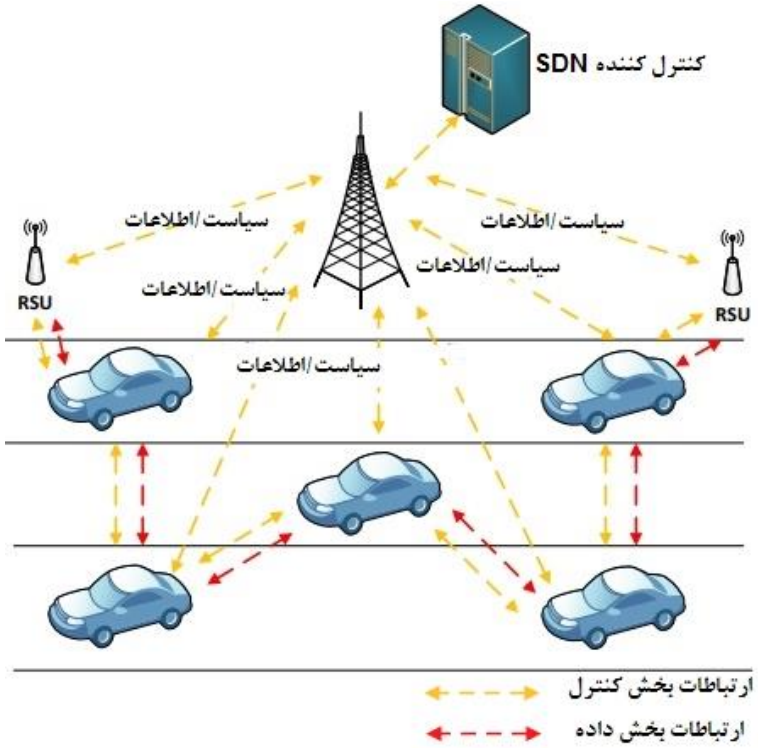
هر گره را کنترل کند. شکل (۱-۶) نشان‌دهنده این حالت است.



شکل (۱-۶): حالت کنترل توزیع‌شده[۲۳]

- حالت کنترل ترکیبی: تمام حالت‌های سیستم که در آن کنترل‌کننده SDN در هر نقطه بین صفر و کامل قرار می‌گیرد در این حالت گنجانده شده است. شکل (۱-۷) یک مثال را نشان می‌دهد که در آن کنترل‌کننده، کنترل را ندارد اما از طرف دیگر می‌تواند جزئیات پردازش بسته به عوامل محلی

را کنترل کند. به همین دلیل ترافیک کنترل بین تمام عناصر SDN منتقل می‌شود. به عنوان مثال به جای ارسال تمام قوانین جریان، کنترل‌کننده به جای آن قوانین خط‌مشی را ارسال می‌کند که رفتار اصلی را تعیین می‌کنند. در حالی که گره‌های بی‌سیم و RSUها از هوش محلی برای انتقال بسته‌ها و پردازش سطح جریان استفاده می‌کنند.



شکل (۱-۷): حالت ترکیبی[۲۳]

۱-۴-۳- مزایای VANET مبتنی بر نرم‌افزار

پیاده‌سازی SDN می‌تواند مزایای متعددی برای شبکه‌های VANET داشته باشد و آن‌ها را می‌توان به سه دسته مختلف تقسیم کرد: انتخاب مسیر، انتخاب فرکانس/کانال و انتخاب قدرت. در ادامه به ماهیت هر یک پرداخته شده است.

۱. انتخاب مسیر: تصمیم‌گیری مسیریابی در شبکه‌های SDN؛ به دلیل وضعیت فعلی شبکه که کنترل‌کننده می‌تواند بلافاصله بدست آورد و بیشتر آگاه است بهتر انجام خواهد شد. در مورد شبکه-های VANET ترافیک داده می‌تواند بی‌نظم شود که یکی از دلایل مهم آن به دلیل مسیریابی کوتاه‌ترین مسیر است که منجر به متمرکز شدن ترافیک بر روی گره‌های انتخاب شده می‌شود.

SDN می‌تواند این مشکلات را شناسایی کند و کنترل‌کننده می‌تواند فرآیند مسیریابی دیگر را انتخاب کند تا موجب کاهش تراکم شود.

۲. انتخاب کانال/فرکانس: در SDN معمولا گره بی‌سیم دارای چندین واسط بی‌سیم قابل تنظیم است [۲۴, ۲۵]که در شبکه‌های مبتنی بر SDN، به بهبود هماهنگی استفاده از کانال/فرکانس کمک می‌کند. ماهیت پویایی کنترل‌کننده این اجازه را می‌دهد که شبکه تصمیم بگیرد کدام نوع از ترافیک از کدام واسط رادیویی یا فرکانس استفاده کند.

۳. انتخاب قدرت: در سیستم‌های VANET مبتنی بر SDN به دلیل وضعیت فعلی شبکه، سیستم می‌تواند انتخاب منطقی در مورد محدوده انتقال در نظر بگیرد. به عنوان مثال، کنترل‌کننده می‌تواند داده‌های همسایه را از گره‌های بی‌سیم جمع‌آوری کند تا گره‌ای را که بیش از حد ناقص است را تخمین بزند. در این حالت می‌توان میزان افزایش قدرت تمام گره‌ها را برای رسیدن به تحویل بسته‌های خوب و کاهش تداخل تعیین کرد.

۱-۴-۴- سرویس‌های شبکه‌های VANET مبتنی بر نرم‌افزار

پیاده‌سازی فناوری‌های SDN در شبکه‌های VANET می‌تواند منجر به ظهور نوع جدیدی از سرویس‌ها و یا ارتقاء آن‌چه که وجود داشته است شود. این پیشرفت‌ها به سه دسته تقسیم می‌شوند: سرویس‌های ایمنی VANET مبتنی بر نرم‌افزار، سرویس انحصاری VANET براساس تقاضا و سرویس‌های مجازی‌سازی شبکه بی‌سیم[۲۳].

- سرویس‌های ایمنی VANET مبتنی بر نرم‌افزار: هدف اصلی استفاده از ارتباطات وسیله نقلیه توسط خودرو، ایمنی جاده‌ها است. در بخش ۱-۴-۳ نشان داده شده که چگونه یک VANET مبتنی بر نرم‌افزار می‌تواند خدمات را نسبت به روش‌های معمول بهبود دهد. ترافیک اضطراری و/یا ویژه می‌تواند توسط SDN از رزرو یا محدودیت فرکانس‌های خاص بهره‌مند شود. وجه تمایز SDN از سایر شبکه‌ها این است که می‌تواند استفاده از این کانال‌ها را افزایش دهد و رزرو را به طور پویا قابل

تنظیم کند. کنترل‌کننده SDN می‌تواند شرایط ترافیکی فعلی و نیازهای برنامه را مشاهده کند و براساس آن اطلاعات می‌تواند جریان‌ها را به کانال‌های رزرو شده اختصاص داده و یا حذف کند. علاوه بر این، با استفاده از سیاست‌های SDN می‌توان سطوح مختلف از سرویس‌ها را با تغییر قوانین جریان در طول دوره زمانی اضطراری ارائه داد. به این ترتیب، ترافیک اضطراری بیش از ترافیک معمول باقی‌مانده اولویت دارد.

- سرویس انحصاری VANET براساس تقاضا: رویکرد SDN می‌تواند برای ارتقاء سرویس دیگری از شبکه VANET، یعنی سرویس نظارت بر وسیله نقلیه اضطراری استفاده شود. روش معمول ارائه این سرویس شامل تقاضا برای داده‌های نظارتی توسط یک درخواست‌کننده (به عنوان مثال، ماشین پلیس) است. در VANET مبتنی بر نرم‌افزار این درخواست توسط کنترل‌کننده انجام می‌شود و می‌تواند قوانین جریان را برای اطلاعات نظارتی وارد کند و به این ترتیب می‌تواند به گره‌های درخواست‌کننده برسد. علاوه بر این، زمانی‌که اطلاعات مشابه توسط چندین خودرو پلیس تقاضا (درخواست) می‌شود، کنترل‌کننده SDN قوانین جریان را وارد می‌کند و به این ترتیب کپی مشابه از داده به بیش از یک مقصد ارسال می‌شود.
- سرویس مجازی‌سازی شبکه بی‌سیم: می‌دانیم که هدف SDN، ارائه شبکه‌های منطقی انتزاعی بیش از منابع شبکه فیزیکی مشترک است و SDN در مراکز داده برای رسیدن به این هدف مورد استفاده قرار گرفته است. همان ایده را می‌توان برای VANET مبتنی بر نرم‌افزار در نظر گرفت. روشی که می‌توان انجام داد این است که جریان‌های مختلف را مجبور به انتخاب رادیو/رابط‌های مختلف با استفاده از فرکانس‌های مختلف کرد. SDN می‌تواند به طور موثر فرکانس‌های مختلف رادیویی را برای هر شبکه جهت ایجاد شبکه‌های بی‌سیم مجازی با ترافیک جداگانه برای یکدیگر ایجاد کند. یک رویکرد می‌تواند گروه‌بندی گره‌های بی‌سیم و RSUها باشد. به این ترتیب هر RSU می‌تواند ترافیک را فقط از یک گروه انتخاب شده از گره‌ها منتقل کند.

۱-۵- هدف و رویکرد پژوهش

هدف از این پژوهش این است که با بررسی ضرورت مسئله امنیت، رخنه‌ها و مشکلات را در برخی مدل‌های امنیتی موجود پیدا کرده و به منظور برطرف نمودن آن‌ها راه‌حلی کارا پیشنهاد و یا ارائه دهد. یکی از مشکلات امنیتی مهمی که در این زمینه مورد بحث و بررسی قرار می‌گیرند شامل: راه‌اندازی حمله (DOS/DDOS) برای افت کارایی شبکه و از بین بردن منابع گره‌ها است.

راه‌اندازی حمله (DOS/DDOS) در شبکه خودرویی، با اهداف مختلفی صورت می‌گیرد. هدف اصلی این حمله جلوگیری کاربر مجاز از دسترسی به خدمات و منابع شبکه است. این حمله از طریق ایجاد اختلال در شبکه (پخش پارازیت) و یا مشغول نگه داشتن سیستم رخ می‌دهد، به طوری که هیچ وسیله نقلیه‌ای قادر به دسترسی به خدمات و منابع شبکه نیست و مهاجم پیام‌های ساختگی را تزریق می‌کند. در [۲۳] جهت افزایش کارایی شبکه‌های VANET آن‌ها را در حوزه شبکه‌های مبتنی بر نرم‌افزار بررسی کرده است. در این الگوریتم مبنا، با در نظر گرفتن ارتباط V2I در توپولوژی موردنظر و با استفاده از معیارهای آماری؛ غیرطبیعی بودن ارتباط در شبکه را مشخص کرده است. با توجه به ناکافی بودن معیار استفاده شده (آنتروپی) سعی شده است الگوریتم توسط ویژگی‌های جداول جریان در سوئیچ‌ها بهبود داده شود.

۱-۶- ساختار پایان‌نامه

در فصل دوم برای فهمیدن نقاط ضعف و فهم کلیت موضوع، به طور خلاصه به بررسی برخی پژوهش‌های انجام شده در این زمینه پرداخته شده است.

در فصل سوم از این پایان‌نامه با استفاده از یک توپولوژی مطرح شده در تحقیق‌های سابق به بهبود الگوریتم تشخیص حمله (DOS/DDOS) پرداخته و روش پیشنهادی ارائه خواهد شد. در فصل چهارم نتایج حاصل از روش پیشنهادی و همینطور ارزیابی آن بررسی می‌شوند. در نهایت در فصل پنجم جمع‌بندی پژوهش انجام شده است و در پایان موضوعاتی برای تحقیق در آینده پیشنهاد می‌گردند.

۱-۷- جمع‌بندی

در ابتدای این فصل به معرفی شبکه‌های بین خودرویی پرداخته شد و خصوصیات آن بیان شد، سپس به چالش‌های امنیتی آن‌ها اشاره شد و نیازمندی‌های امنیتی در خور این چالش‌ها نیز ذکر شد. این شبکه‌ها غیرساختارمند هستند و کنترل ترافیک در این شبکه‌ها به صورت متمرکز نیست بنابراین در تلاش برای متمرکز کردن این شبکه‌ها برآمدند و آن را در شبکه‌های مبتنی بر نرم‌افزار مورد بررسی قرار دادند. در نتیجه در این فصل توضیح اجمالی درباره شبکه‌های مبتنی بر نرم‌افزار داده شد و ساختار این شبکه‌ها مورد بررسی قرار گرفت و در نهایت شبکه‌های بین خودرویی را به شبکه‌های خودرویی مبتنی بر نرم‌افزار تعمیم داده شد و ساختار و توپولوژی آن مورد بحث قرار گرفت.

فصل دوم

ادبیات موضوع و مرور بر کارهای پیشین

۲-۱- مقدمه

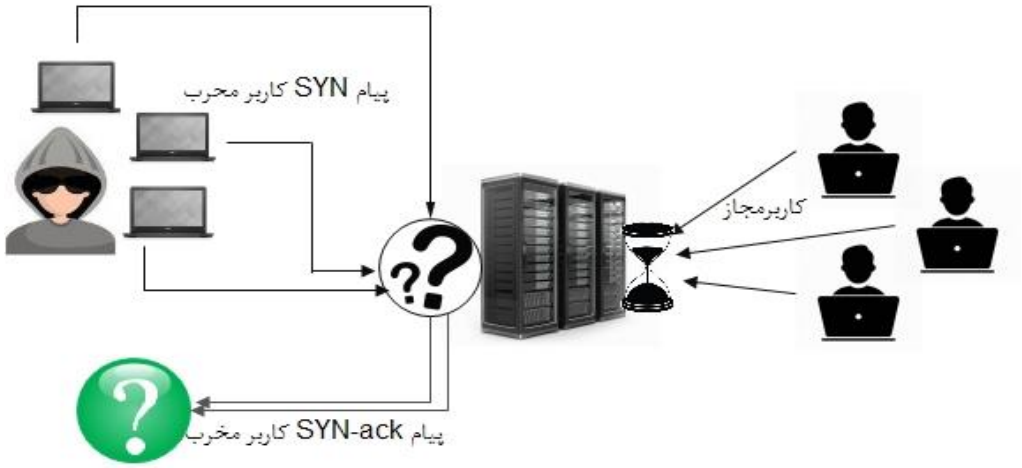
در فضای سایبری، حملات براساس اهداف و مکانیزم‌های مختلفی صورت می‌پذیرند. هدف بسیاری از حملات، ایجاد اختلال و وقفه در سرویس‌دهی یک ماشین در شبکه است. امروزه حملات از کار انداختن سرویس‌ها به صورت توزیع شده بسیار فراگیر شده است. این حملات با ارسال بسته‌ها و درخواست‌های بی‌شماری به سوی چندین قربانی و به وسیله نرم‌افزارهای اتوماتیک، یک سرویس یا سرور را از کار می‌اندازد. این در حالی است که طبق آمارها این حملات بسیار افزایش یافته است و به طور جدی بسیاری از سرویس‌ها، سرورها و تأمین‌کنندگان میزبانی وب را تهدید می‌کنند. در این فصل نخست توضیحاتی درباره حمله انکار سرویس (DOS)، انکار سرویس توزیع شده[۱] و انواع آن‌ها پرداخته می‌شود سپس به دلیل اینکه VANET بر مبنای SDN بنا نهاده شده است، این نوع حملات در شبکه‌های SDN مورد بررسی قرار می‌گیرند و در نهایت مقالاتی که در گذشته برای شناسایی و جلوگیری این نوع حمله انجام شده است بررسی خواهند شد.

۲-۲- تعریف حمله DOS

حمله انکار سرویس (DOS) می‌تواند به عنوان تلاش یک کاربر مخرب برای به خطر انداختن عملکرد منظم شبکه تعریف شود. حملات DOS حملاتی هستند که هدف اصلی آنها ممانعت از دسترسی قربانیان به منابع کامپیوتری، شبکه‌ها و یا اطلاعات است. در این نوع حملات نفوذگر تلاش می‌کند مانع از سرویس‌دهی یک سرویس‌دهنده در شبکه شود. در واقع نفوذگر با ایجاد ترافیک بی‌مورد و بی‌استفاده، حجم زیادی از منابع سرویس‌دهنده و پهنای باند شبکه را مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی‌مورد می‌کند و این تقاضاها تا جایی که دستگاه سرویس‌دهنده را از کار بیندازد، ادامه پیدا می‌کند. متداول‌ترین و مشهودترین نوع حملات DOS، زمانی محقق می‌گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. برای مثال زمانی که کاربر آدرس URL یک وب سایت

[۱] Distributed Denial of Service (DDOS)

را در مرورگر خود تایپ می‌نماید، درخواست آن برای سرویس‌دهنده ارسال می‌گردد. سرویس‌دهنده در هر لحظه قادر به پاسخگویی به حجم محدودی از درخواست‌ها می‌باشد، بنابراین اگر یک مهاجم با ارسال درخواست‌های متعدد و سیلاب‌گونه باعث افزایش حجم عملیات سرویس‌دهنده گردد، قطعا امکان پردازش درخواست کاربر مجاز برای سرویس‌دهنده وجود نخواهد داشت[۲۶].



شکل (۲-۱): یک حمله DOS از نوع سیلاب (flood) [۲۳]

۲-۲-۱- انواع حمله DOS

حملات DOS را می‌توان به دو دسته اصلی تقسیم کرد: حملات لایه کاربردی و حملات لایه شبکه. حمله لایه کاربردی در لایه هفت مدل OSI[۱] کار می‌کند و می‌تواند به عنوان حمله DOS یا DDOS باشد. تلاش‌های کاربر مخرب بر مبنای هدف قرار دادن یک سرور با استفاده از تعداد زیادی از درخواست است. حمله DOS به چندین روش انجام می‌شود که عمده آن‌ها عبارتند از: ۱- مصرف منابع محاسباتی مانند پهنای باند، حافظه فضای دیسک و زمان پردازش. ۲- ایجاد تداخل در اطلاعات پیکربندی مانند اطلاعات مسیریابی. ۳- ایجاد تداخل در تجهیزات فیزیکی شبکه. ۴- مانع ارتباطی بین کاربران مجاز و قربانی تا نتوانند به ارتباط ادامه دهند.

[۱] Open System Interconnection (OSI)

معمولا اندازه این حملات با درخواست در هر ثانیه[۱] اندازه‌گیری می‌شود. برای فلج کردن یک وب‌سایت متوسط بین ۵۰ تا ۱۰۰ درخواست در هر ثانیه موردنیاز است.

حمله لایه شبکه در لایه ۴-۳ از مدل OSI کار می‌کند و در حالت کلی حمله DDOS است. این نوع حملات به دنبال سقوط پایپ‌لاین‌ها[۲] در شبکه است. در این دسته می‌توان حمله‌هایی مانند SYN flood و UDP flood را نام برد. معمولا این نوع حملات به منظور جلوگیری از دسترسی به سرورها مورد استفاده قرار می‌گیرند و منجر به خسارت‌های شدید عملیاتی می‌شوند. به طور معمول اندازه این حملات با اندازه گیگابایت در ثانیه[۳] یا بسته‌ها در ثانیه[۴] اندازه‌گیری می‌شوند زیرا معمولا عمق ترافیک بسیار زیاد است.

۲-۳- تعریف حمله DDOS

اگر تلاش کاربر مخرب برای به خطر انداختن عملکرد منظم شبکه از یک گروه از میزبان‌ها، به جای یک میزبان صورت پذیرد، حمله انکار توزیع شده نامیده می‌شود. این گروه از میزبان‌ها توسط کاربر مخرب خاص هماهنگ شده است. برای راه‌اندازی حملات DDOS، مهاجم از بوت‌نت‌ها[۵] - خوشه‌های بزرگ از دستگاه‌های متصل (مانند تلفن همراه، رایانه‌های شخصی یا مسیریاب‌ها) - استفاده می‌کنند. این دستگاه‌ها با نرم‌افزارهای مخرب آلوده می‌شوند و این اجازه را می‌دهد تا مهاجم کنترل از راه دور بر روی آن‌ها داشته باشد. به این ترتیب هر یک از دستگاه‌های آلوده مقدار بزرگی از بسته‌ها را به سمت قربانی ارسال می‌کند تا منابع‌اش را از بین ببرد و شبکه را از دسترس کاربران مجاز خارج سازد. مهاجم با آدرس‌های IP[۶] جعلی دارای پتانسیل برای ارسال حجم زیادی از بسته‌ها به قربانی می‌باشد.

---

[۱] Request Per Second (RPS)
[۲] Pipeline
[۳] Giga byte per second (Gbps)
[۴] Packet per second (Pps)
[۵] Botnet (Robot Network)
[۶] Internet Protocol (IP) address

۲-۴- حملات DDOS در شبکه‌های SDN

همان طور که اشاره شد شبکه‌های VANET با استفاده ازSDN ارتقا داده شده است بنابراین هدف بررسی حمله DDOS بر روی VANET به بررسی حمله بر روی شبکه‌های مبتنی بر SDN تغییر پیدا می‌کند. SDN می‌تواند مزایای بسیاری داشته باشد اما هنوز رابطه بین آسیب‌پذیری بین SDN و حملات DDOS وجود دارد. خود SDN ممکن است هدف حملات DDOS باشد. قابلیت‌های شبکه مانند بروزرسانی پویای انتقال می‌تواند تشخیص حملات DDOS را آسان نماید اما جداسازی بخش داده از بخش کنترل منجر به ایجاد نوع جدیدی از حملات می‌شود[۲۷]. به عنوان مثال، مهاجم می‌تواند از ویژگی‌های SDN برای راه‌اندازی حملات DDOS علیه لایه‌های آن استفاده کند. اگر مهاجم‌ها از بوت-نت‌ها استفاده کنند تأثیر حملات می‌تواند به شدت افزایش یابد و شبکه قربانی را غارت کنند. گوشی‌های هوشمند، لب‌تاپ‌ها و سایر دستگاه‌های سیار در حال حاضر یک پلت‌فرم قابل حمل برای این نوع حملات هستند و دلیل آن افزایش پهنای باند و قدرت پردازش در این نوع ارتباطات است. مهاجم‌ها می‌توانند از فقدان امنیت در این دستگاه‌های سیار نیز بهره‌مند شوند. در جدول زیر می‌توان برخی ویژگی‌های خوب SDN را در شکست دادن حملات DDOS مشاهده کرد[۲۷]:

جدول (۲-۱) ویژگی‌های خوب SDN در دفاع از حملات DDOS

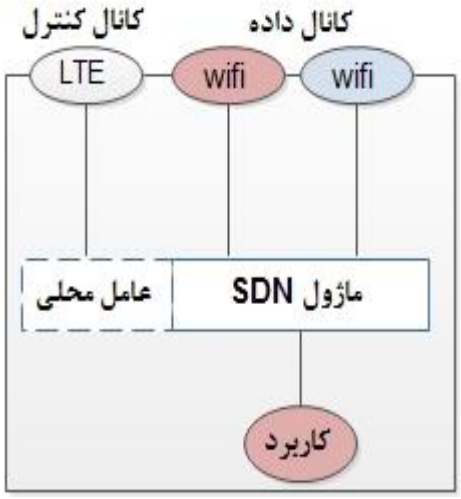
مزایای خوب SDN	مزایای دفاع در برابر حملات DDOS
جداسازی بخش داده از بخش کنترل	می‌تواند به راحتی آزمایش حمله و آزمایشات دفاعی را انجام دهد.
کنترل منطقی و متمرکز و مشاهده شبکه	کمک می‌کند تا پلیس امنیتی مستقل ایجاد شود.
برنامه‌نویسی شبکه توسط برنامه‌های خارجی	از فرآیند جمع‌آوری اطلاعات از IDS[۱]ها و IPS[۲]های موجود پشتیبانی می‌کند.
تجزیه و تحلیل ترافیک مبتنی بر نرم‌افزار	قابلیت‌های یک سوئیچ را با استفاده از هر تکنیک مبتنی بر نرم‌افزار بهبود می‌دهد.
بروزرسانی پویای قوانین forwarding و انتساب جریان	کمک می‌کند تا به سرعت پاسخ دهد.

[۱] Intrusion Detection Systems (IDS)
[۲] Intrusion Prevention Systems (IPS)

طبق جدول (۲-۱) شبکه‌های SDN می‌توانند از سیستم‌های تشخیص نفوذ (IDSها) و سیستم‌های پیشگیری از نفوذ (IPSها) به علت قابلیت برنامه‌ریزی شبکه استفاده کنند[۲۸]. تجزیه و تحلیل ترافیک مبتنی بر نرم‌افزار می‌تواند با استفاده از انواع الگوریتم‌های هوشمند، پایگاه داده‌ها و هر ابزار نرم‌افزاری دیگری انجام شود. این ویژگی به طور چشمگیری باعث ظهور این نوآوری شد. سیاست امنیتی جدید یا بروز شده را می‌توان به عنوان قوانین جریان برای جلوگیری از ترافیک حمله بدون تأخیر زیاد راه‌اندازی کرد که می‌تواند براساس تجزیه و تحلیل ترافیک انجام شود[۲۷].

۲-۵- کارهای پیشین

در [۲۲] یک بررسی جامع در مورد نحوه اجرای SDN در شبکه‌های VANET انجام شده است. آن‌ها معماری و سرویس‌های شبکه SD VANET و ویژگی‌های جدید را برای پشتیبانی از آن‌ها ارائه کرده‌اند. ماهیت شبکه‌های VANET بی‌سیم بودن آن‌هاست. بنابراین گره‌های شبکه‌های SD VANET متفاوت از گره‌های SDN است.

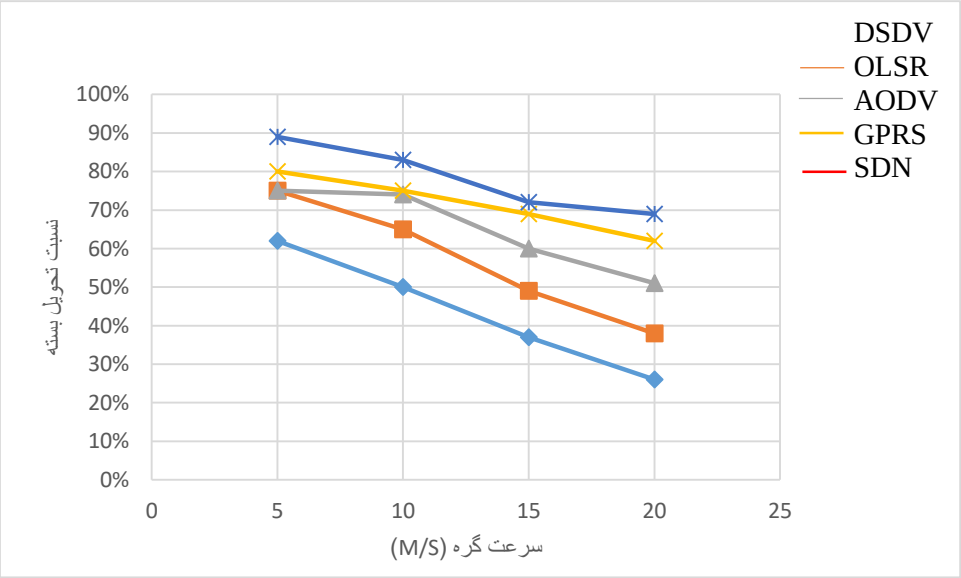


شکل (۲-۲): گره بی‌سیم SDN در شبکه‌های VANET [۲۲]

شکل (۲-۲) اجزای داخلی گره بی‌سیم را نشان می‌دهد. گره‌ها شامل تمام قابلیت‌های یک سوئیچ OF در شبکه‌های OF سنتی و همچنین اطلاعات اضافی برای فعال کردن حالت‌های مختلف عملیات در

محیط‌های VANET می‌باشد. هر گره بی‌سیم SDN یک عامل محلی دارد که قابلیت آن بستگی به ویژگی‌های فعال در گره بی‌سیم SDN دارد. این عامل محلی در زمانی که اتصال به کنترل‌کننده یا اطلاعات اولیه SDN در هنگام دریافت ورودی از کنترل‌کننده از بین برود می‌تواند کنترل‌کننده را پشتیبانی کند. این نوع گره شامل واسط wifi به عنوان کانال داده می‌باشد که برای پشتیبانی موردنیاز است. ماژول SDN ترکیبی از پردازش بسته و رابط است که ورودی را از بخش کنترل جدا می‌کند.

در شبیه‌سازی [۲۲]، قابلیت شبکه خودرویی مبتنی بر نرم‌افزار را با مقایسه مسیریابی مبتنی بر SDN و پروتکل‌های مسیریابی شبکه‌های خودرویی نشان داده‌اند. آن‌ها مسیریابی در شبکه‌های خودرویی مبتنی بر نرم‌افزار را با شبکه‌های خودرویی سنتی توسط پروتکل‌های OLSR, DSDV, AODV, GPSR مقایسه کرده‌اند و نتایج در شکل (۲-۳) نشان داده شده است.

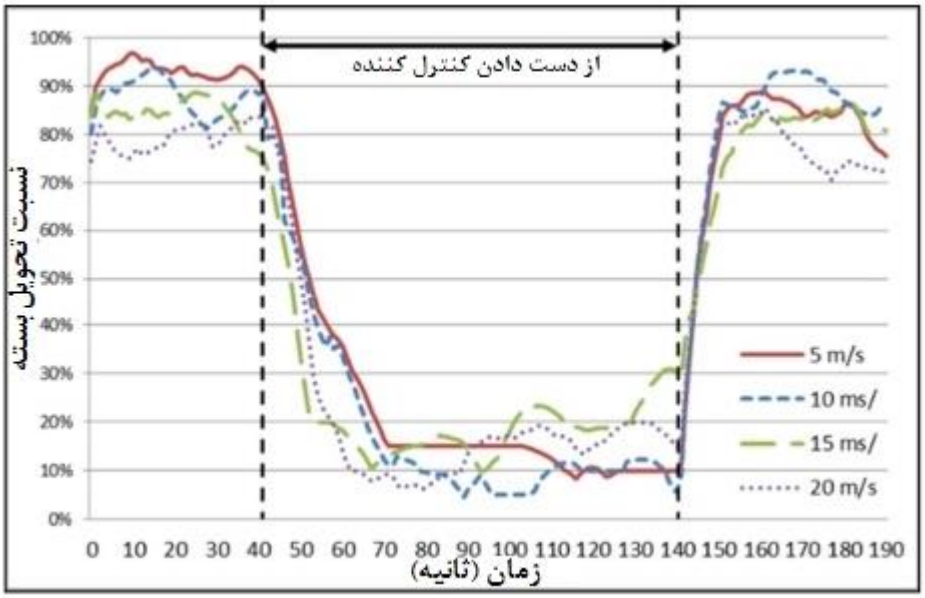


شکل (۲-۳): مقایسه نسبت تحویل بسته: SDN در مقایسه با شبکه خودرویی[۲۲]

همان طور که مشاهده می‌شود مسیریابی مبتنی بر شبکه‌های SDN نسبت به پروتکل‌های مسیریابی شبکه‌های خودرویی سنتی بهتر عمل می‌کند. دانش جمعی که کنترل‌کننده SDN دارد، دلیل اصلی آن است. بنابراین گره‌های بی‌سیم شبکه مبتنی بر نرم‌افزار کنترل‌کننده را در مورد اطلاعات همسایگی بروز می‌کند. کنترل‌کننده بلافاصله تشخیص می‌دهد که تغییر توپولوژی وجود دارد و پیام‌های کنترل را در

صورت نیاز ارسال می‌کند. بنابراین سیستم خودرویی مبتنی بر نرم‌افزار خیلی سریع‌تر به تغییر توپولوژی پاسخ می‌دهد.

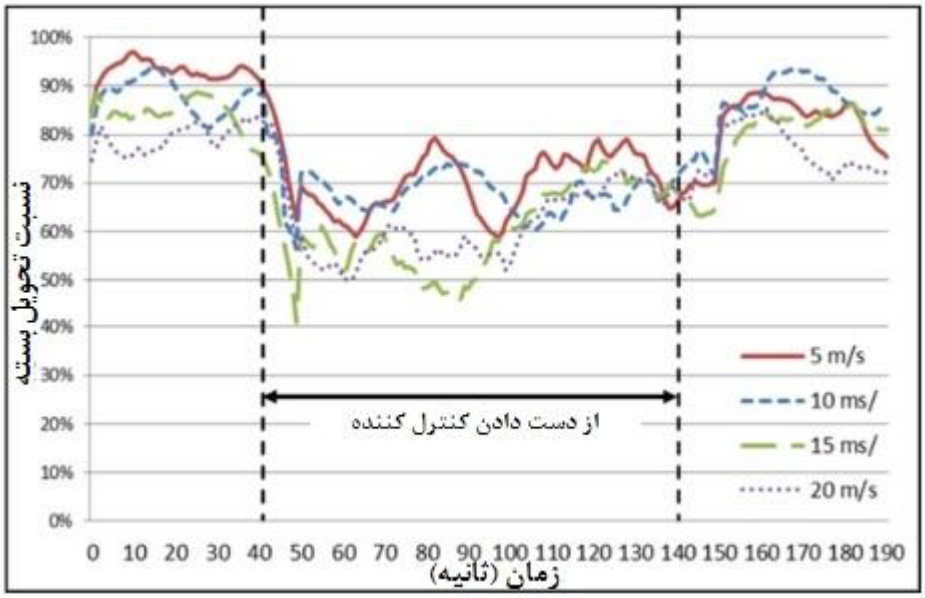
یکی از دلایل برتری شبکه‌های خودرویی مبتنی بر نرم‌افزار نسبت به شبکه‌های خودرویی سنتی جبران از دست دادن کنترل‌کننده SDN است. در این ارزیابی نشانه داده شده است که چگونه مکانیزم‌های پشتیبان‌گیری حتی زمانی که کنترل‌کننده از دست رفته است می‌تواند توسط عامل محلی در گره‌های بی‌سیم شبکه‌های مبتنی برنرم‌افزار تحویل بسته را به خوبی انجام دهد.



شکل (۲-۴): از دست دادن کنترل‌کننده شبکه SDN[۲۲]

شکل (۲-۴) سناریویی را که در آن یک خطای کنترل‌کننده برای ۱۰۰ ثانیه وجود دارد نشان می‌دهد. همان‌طور که مشاهده می‌شود نسبت تحویل بسته به سرعت شروع به کاهش می‌کند. بنابراین کنترل‌کننده دیگر قوانین جدید را برای گره‌های بی‌سیم شبکه مبتنی بر نرم‌افزار وارد نمی‌کند. این

نشان می‌دهد که مدیریت شبکه خودرویی مبتنی بر نرم‌افزار در حالت کنترل مرکزی خطرناک است. ماهیت یک شبکه خودرویی این است که گره‌ها به سرعت حرکت می‌کنند و قوانین قبلی بسیار سریع‌تر نسبت به زمانی که تحرک گره کم است منسوخ می‌شود. بنابراین آن‌ها از مکانیزم عقبگرد[1] مسیریابی GPRS برای زمانی که ارتباط کنترل‌کننده از بین می‌رود استفاده کردند. شکل (۲-۵) نسبت تحویل بسته را در این سناریو نشان می‌دهد.



شکل (۲-۵): استفاده از مکانیزم عقبگرد برای جبران از دست دادن کنترل‌کننده[۲۲]

می‌توان مشاهده نمود که پس از کاهش اولیه (پس از شکست ارتباط با کنترل‌کننده و قبل از اینکه GPRS فعال شود) نسبت تحویل بسته به خوبی بازسازی می‌شود. هنگامی که ارتباط با کنترل‌کننده بازسازی می‌شود، سیستم یک بار دیگر به مسیریابی مبتنی بر نرم‌افزار بازگردانده می‌شود.

[1] Fallback

جنبه مشترک در هر نوع حمله از DDOS، این است که حجم زیادی از ترافیک را به شبکه منتقل می‌کند تا منابع شبکه را از بین ببرد. معمولا در شرایط عادی یک الگویی در فعالیت شبکه را می‌توان تعریف نمود تا نرخ پهنای باند پذیرفته شده را مشخص کرد. برای طبقه‌بندی ترافیک غیرعادی باید افزایش ناگهانی ترافیک، تأخیر، استفاده از CPU یا کاهش ناگهانی در عملکرد هر یک از دارایی‌های شبکه را مورد توجه قرار داد. این تغییرات "آنومالی یا ناهنجاری[۱]" نامیده می‌شود که مربوط به نوع داده‌ها در شبکه می‌باشند[۲۹].

در [۳۰]، به طور عمده تشخیص حمله DDOS را به دو روش مطرح می‌کند: رویکرد مبتنی بر امضا[۲] و رویکرد مبتنی بر آنومالی[۳]. در رویکرد مبتنی بر امضا ویژگی‌های سیستم در برابر یک پایگاه‌داده از امضا یا ویژگی‌هایی از تهدیدات مخرب شناسایی می‌شود. این شبیه به شیوه‌ای است که بیشتر نرم‌افزارهای آنتی‌ویروس، ویروس بدافزار را شناسایی می‌کند. مسأله این است که یک تأخیر بین تهدید جدیدی که کشف شده است و امضای آن برای تشخیص تهدیدی که به پایگاه‌داده اعمال شده وجود دارد. در طی این دوره، تهدیدات جدید ناشناخته خواهد ماند. رویکرد مبتنی بر امضا کارایی زیادی دارد زیرا اجرای آن آسان است اما با توجه به این دیدگاه دارای محدودیت‌هایی است که تأخیر در بروزرسانی و شناسایی حمله یکی از آن‌هاست[۳۱].

در [۳۲]، برای برطرف نمودن محدودیت‌های رویکرد مبتنی بر امضا روشی پیشنهاد شده است که بر مبنای رویکرد انحرافی عمل می‌شود و از روش‌های تجزیه و تحلیل توزیع، داده‌کاوی ، یادگیری ماشین و آماری (مانند تکنیک‌های آنتروپی و Chi_Square) استفاده می‌شود. رویکرد مبتنی بر آنومالی، ترافیک شبکه را نظارت خواهد کرد و آن را در برابر مقادیر ثابتی مقایسه می‌کند. یکی از روش‌های تشخیص آنومالی، آنتروپی است. آنتروپی (شاخص شانون _ وینر[۴]) یک مفهوم ضروری از تئوری اطلاعات است که

---

[۱] Anomaly
[۲] Signature Based Approach (SBA)
[۳] Anomaly Based Approach (ABA)
[۱] Shanon_Wiener

عدم قطعیت یا تصادفی بودن مرتبط با یک متغیر تصادفی یا در اینجا (آدرس IP مقصد) را اندازه‌گیری می‌کند. برای محاسبه آنتروپی و توضیحات در باره پارامترهای آن معادلات زیر را خواهیم داشت که w مجموعه داده‌ای و برابر با n عنصر IP مقصد هستند و x یک رخداد در این مجموعه است (معادله(۲-۱)). احتمال رخداد x در این مجموعه توسط معادله (۲-۲) محاسبه می‌شود[۳۳].

$$w = \{x_1, x_2, \dots, x_n\} \qquad (۱-۲)$$

$$p_i = \frac{x_i}{n} \qquad (۲-۲)$$

برای محاسبه آنتروپی که با H نشان داده می‌شود باید احتمال تمام عناصر در مجموعه و مجموع آن‌ها محاسبه شود که در معادله (۲-۳) نشان داده شده است:

$$H = -\sum_{i=1}^{n} p_i \log p_i \qquad (۳-۲)$$

اگر تمام عناصر دارای احتمال یکسان باشد (عناصر= IP مقصد بسته‌های مشاهده شده در یک پنجره یعنی w ، که این پنجره می‌تواند ۳۰تایی یا۵۰تایی باشد و بستگی به میزان دقت به کار رفته در الگوریتم دارد) بدین معنی است که هر عنصر فقط یک بار در آن پنجره دیده شده باشد آنتروپی حداکثر مقدار خواهد داشت. اگر یک عنصر بیشتر از دیگران ظاهر شود، آنتروپی پایین‌تر خواهد بود. کاربرد آنتروپی در شبکه که هدف موردنظر در اینجا است، در به کارگیری اطلاعات هدر بسته است. بسته‌ها به مجموعه‌های برابر تقسیم می‌شوند که همان پنجره است. در هر پنجره تعداد مشاهده هر عنصر محاسبه می‌شود. به عنوان مثال: اگر پنجره دارای ۶۴ عنصر باشد و همه عناصر یک بار ظاهر شده باشند، آنتروپی برابر با ۱/۱۵ است و اگر یک عنصر ۱۰ بار مشاهده شده باشد آنتروپی برابر با ۱/۰۲ خواهد بود. رویکرد مبتنی بر آنتروپی دارای مزایای قابل توجهی در تشخیص DDOS هستند. هنگامی‌که شبکه نظارت شده به طور عادی اجرا می‌شود، مقادیر آنتروپی نسبتا پایدار است. در غیر این صورت مقادیر آنتروپی با تغییر

یک یا چند ویژگی به طور قابل توجهی تغییر خواهد کرد. استفاده از آنتروپی می‌تواند حساسیت تشخیص را برای شناسایی حوادث غیر طبیعی افزایش دهد با وجود اینکه استفاده از آنتروپی دارای مزایای متعددی است، اما هنوز هم یک الگوریتم کارآمد برای کاهش زمان و استفاده از حافظه در یک شبکه با سرعت بالا نیاز دارد.

یکی از روش‌هایی که برای تشخیص حملات DDOS از آن استفاده می‌کنند یادگیری ماشین است. در [۳۴]، یک روش یادگیری ماشین برای یادگیری عملکرد شبکه ارائه شده است و براساس آن تصمیم می‌گیرد که آیا حمله رخ داده است یا خیر. این روش عمدتا در شبکه‌های غیر SDN مورد استفاده قرار می‌گیرد و زمانی که در این نوع شبکه مورد استفاده قرار می‌گیرد همان روش را دنبال می‌کند. در این روش تشخیص حمله در کنترل‌کننده NOX براساس شبکه خودسازمانده[۱] است. SOM یک شبکه عصبی مصنوعی بدون نظارت است که با ویژگی‌های جریان شبکه که به صورت دوره‌ای از سوئیچ‌ها جمع‌آوری می‌شود آموزش داده می‌شود. ترافیک براساس الگوی SOM به دو دسته طبیعی یا غیرطبیعی طبقه‌بندی می‌شود. این روش تشخیص که در شکل زیر نشان داده شده است، در سه ماژول اجرا می‌شود که به صورت دوره‌ای در یک حلقه در کنترل‌کننده NOX اجرا می‌شود.

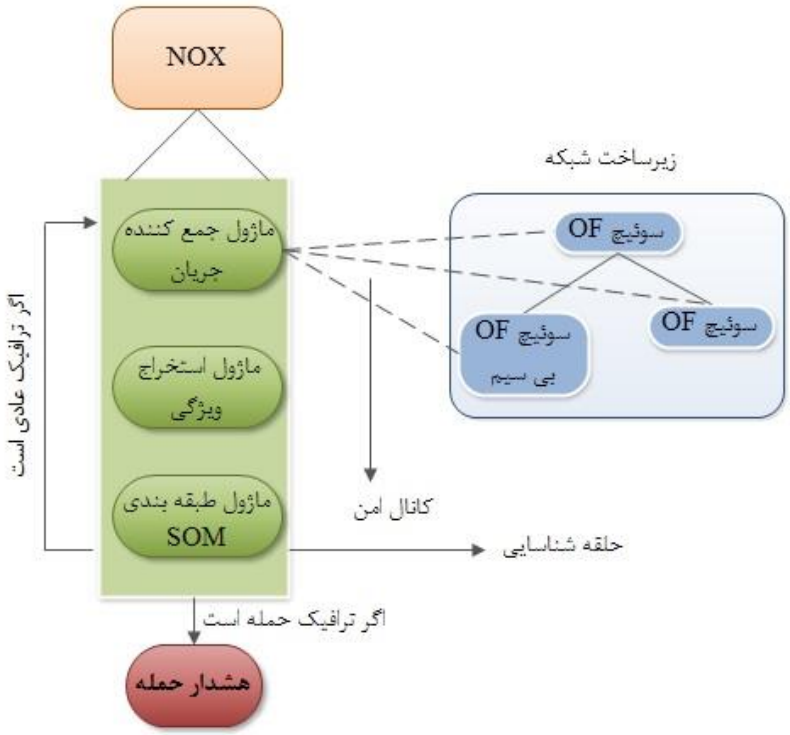
- ماژول جمع‌کننده جریان: جریان سوئیچ‌ها را به صورت دوره‌ای برای جداول جریان خود نمایش می‌دهد.
- ماژول استخراج ویژگی: ویژگی‌های اصلی را که برای تشخیص حمله DDOS مورد مطالعه قرار می‌گیرد را استخراج می‌کند و آن‌ها را در شش تاپل جمع می‌کند. عناصر اصلی که براساس ویژگی‌های جمع‌آوری شده محاسبه می‌شوند و در ماژول بعدی برای طبقه‌بندی ترافیک مورد

[۱] Self-organizing map (SOM)

مطالعه قرار می‌گیرند عبارتند از: میانگین بسته در هر جریان، میانگین بایت در هر جریان، میانگین طول مدت جریان، درصد جریان‌ها جفت، رشد جریان‌های تک و رشد پورت‌های مختلف.

- ماژول طبقه‌بندی: این ماژول باید تجزیه و تحلیل کند و تصمیم بگیرد که آیا داده‌های شش تاپل مربوط به یک حمله DDOS است یا خیر؟

این روش دارای معایبی است که در اینجا به اختصار به آن‌ها پرداخته می‌شود. یکی از معایب این روش این است که این سیستم باید در کنار SDN اجرا شود و باید برای چندین ساعت قبل از اینکه بتواند در شبکه استفاده شود آموزش ببیند. یکی دیگر از اشکالات آن این است که SDN می‌تواند شبکه را مجددا پیکربندی کند. این بدین معنی است که SOM باید برای حفاظت بهتر دوباره آموزش یابد. در نهایت همانطور که شبکه گسترش می‌یابد، نرون‌های الگوریتم SOM افزایش می‌یابد و برای شبکه سنگین می‌شود. از دیگر اشکالات آن می‌توان به پرس‌وجوی سوئیچ‌ها اشاره کرد که این پرس‌وجو به صورت دوره‌ای به خصوص در معماری‌های بزرگ با تعداد زیادی از سوئیچ‌ها سربارهای شدیدی در سیستم قرار داده و در نهایت بر عملکرد کنترل‌کننده تأثیر می‌گذارد و این روش اثر DDOS بر روی کنترل‌کننده را در نظر نمی‌گیرد. پردازش حجم زیاد جریان‌ها در جداول جریان، مسأله دیگری است که باید به خوبی مورد توجه قرار گیرد.



شکل (۲-۲): عملیات شناسایی حمله DDOS[۳۴]

برخی روش‌های انجام شده برای ایمن‌سازی شبکه‌های SDN توسط پروتکل OF صورت پذیرفته است یعنی بر روی این پروتکل متمرکز شده‌اند. در این بخش این روش‌ها به اختصار توضیح داده خواهد شد.

Yuhung و همکارانش در [۳۵]، از کمپانی Chungwa یک طرح دفاعی OF DDOS ارائه می‌دهد که جریان را در یک سوئیچ OF نمایش می‌دهد. اگر تعداد بسته‌های دریافت شده در ۵ثانیه بیشتر از ۳۰۰۰ باشد، تعداد بسته‌ها در مدت زمان دوم بررسی می‌شود. اگر تعداد بسته‌ها در هر ثانیه بیش از ۸۰۰، برای ۵ بار پیوسته باشد یک حمله شناسایی می‌شود و طرح دفاعی شروع به کاهش بسته‌های دریافتی تا زمان انقضای ورودی جریان می‌کند. یکی از ایرادهای این روش می‌توان به نرخ مثبت کاذب[۱] اشاره کرد که شاید در یک بازه زمانی میزان درخواست‌ها افزایش پیدا کند و ترافیک نوعی ترافیک مجاز باشد.

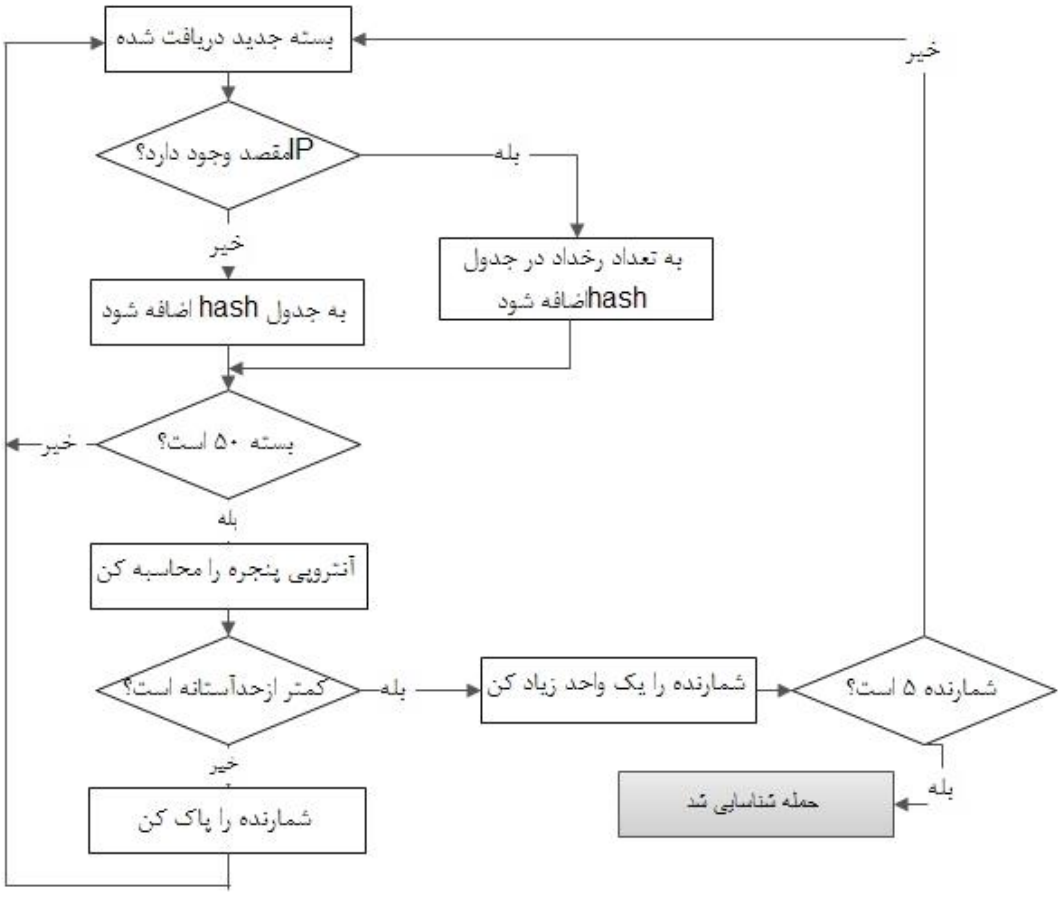
[۱] False Positive (FP)

استفاده از این معیار به تنهایی نمی‌تواند برای سایر حملات DDOS با ویژگی‌های مختلف در تشخیص کمک کند.

نویسندگان در [۳۶]، OF را برای یافتن کوتاه‌ترین مسیر برای سیستم‌های تشخیص نفوذ شبکه (IDS) ارائه می‌کند. این راه‌حل نیاز به اضافه کردن دستگاه‌های IDS در طول لینک‌های شبکه برای نظارت بر ترافیک برای فعالیت مشکوک است. آنتروپی این محدودیت‌ها را ندارد و در راه‌حل پیشنهادی ما از کنترل‌کننده برای شناسایی حمله استفاده می‌شود.

در این قسمت، روش‌های مختلف آنتروپی را که برای تشخیص DDOS مورد استفاده قرار گرفته است ارائه می‌شود تا متوجه شویم که چه کارهایی در شبکه‌های SDN و VANET انجام شده است. آنتروپی از طریق راه‌های مختلفی برای تشخیص حملات DDOS در شبکه استفاده شده است اما به بهترین وجه از اطلاعات موردنظر، در شبکه‌های VANET مبتنی بر نرم‌افزار انجام نشده است.

در [۳۳]، تغییر آنتروپی از آدرس IP مقصد به عنوان یک روش زودهنگام در کنترل‌کننده POX استفاده کرده است. آنتروپی به عنوان اندازه‌گیری تصادفی شناخته می‌شود. حداکثر آنتروپی زمانی اتفاق می‌افتد که هر بسته ورودی برای میزبان‌های متمایز ارسال شود و حداقل آنتروپی زمانی اتفاق می‌افتد که همه بسته‌ها به یک آدرس مقصد هدایت شود. همان‌طور که قبلا توضیح داده شد، مشخصه حمله DDOS حجم زیادی از بسته‌ها را به یک مقصد ارسال می‌کند. در این روش پیشنهادی IP مقصد برای محاسبه آنتروپی استفاده می‌شود. الگوریتم در شکل (۲-۶) نشان داده شده است. پنجره‌ای از بسته‌ها مورد مطالعه قرار گرفته و آنتروپی برای آدرس‌های IP مقصد آن‌ها محاسبه می‌شود. اگر آنتروپی محاسبه شده برای یک تعداد پیوسته کمتر از حدآستانه باشد یک حمله گزارش خواهد شد.



شکل (۲-۶): فلوچارت تشخیص حمله DDOS با استفاده از روش تغییر آنتروپی[۳۳]

اندازه پنجره‌ای که در این روش مورد استفاده قرار گرفته برابر با ۵۰ است. طبق الگوریتم در هر پنجره از بسته‌ها احتمال رخداد هر IP مقصد محاسبه می‌شود و بعد از آن مقدار آنتروپی محاسبه می‌شود. سپس مقدار آنتروپی محاسبه شده با مقدار آنتروپی ترافیک مجاز در فاز یادگیری شبکه مقایسه می‌شود که اگر برای ۵ پنجره متوالی کمتر از حدآستانه باشد یک حمله گزارش خواهد شد.

تعدادی محدودیت برای این روش وجود دارد. هنگامی که تعداد میزبان تحت حمله در شبکه افزایش یابد یا زمانی که کل شبکه تحت حمله قرار گیرد، شناسایی آنتروپی شکست خواهد خورد زیرا زمانی‌که حمله بر روی چندین میزبان توزیع می‌شود آنتروپی تغییر (کاهش) به خصوصی نخواهد داشت و در مقایسه با حدآستانه تفاوت چندانی نخواهد داشت. این را می‌توان از روی نتایج به دست آمده توسط روش پیشنهادی مشاهده نمود. بعد از به دست آوردن آنتروپی در ترافیک مجاز، حملات با نرخ‌های ترافیکی مختلف بر روی شبکه انجام می‌شود و با تجزیه و تحلیل بر روی حداقل و حداکثر تغییرات

آنتروپی، حدآستانه را برابر با ۰/۷۶ در نظر می‌گیرد. زمانی که سناریوی حمله به یک میزبان را اجرا می‌کند میانگین تغییرات آنتروپی برابر با ۰/۵۴ است و کمتر از حدآستانه است، بنابراین طبق الگوریتم شمارنده مربوط به مشاهده یک رخداد مشکوک افزایش می‌یابد.

اما در زمانی که ۶ میزبان متصل به یک سوئیچ را مورد حمله قرار می‌دهد میانگین تغییرات آنتروپی برابر با ۰/۸۸ است که بسیار نزدیک به آنتروپی در حالت ترافیک مجاز است و تنها ۰/۰۷کمتر از آنتروپی در ترافیک مجاز است و چون در شرط برقراری مقایسه با حدآستانه شکست خوده است الگوریتم تشخیص می‌دهد که حمله‌ای وجود ندارد. در روش پیشنهادی این پایان‌نامه، با وفقی‌سازی حدآستانه آنتروپی طبق الگوی رفتار شبکه سعی شده است که تشخیص این‌گونه حمله‌ها آسان شود و نرخ مثبت کاذب و منفی کاذب[۱] کاهش یابد.

Ra و همکارانش در [۳۷]، روش سریع‌تر برای محاسبه آنتروپی را با استفاده ازمحاسبات بر روی نوع بسته و حجم بسته‌ها پیشنهاد می‌کند. این الگوریتم همچنین از پنجره زمانی استفاده می‌کند. در این روش برای یافتن حدآستانه قابل اجرا، مجموعه داده‌های مختلفی را در نظر می‌گیرند و آن را چند برابر انحراف استاندارد مقادیر آنتروپی در نظر می‌گیرند. با استفاده از این روش نرخ FN نسبت به روش‌های دیگر بیشتر شده و FP را کاهش می‌دهد. در این روش هیچ اشاره‌ای برای محاسبات سریع و همچنین عدم قطعیت دقت[۲] وجود ندارد.

Qin و همکارانش در [۳۸]، الگوریتم با پنجره زمانی و سه حدآستانه از آنتروپی پیشنهاد می‌کنند. این روش به منظور اجتناب از نرخ FP و FN در شبکه صورت پذیرفته است. یکی از مشکلات این روش می‌توان به وقت‌گیر بودن آن اشاره کرد و اینکه از منابع زیادی استفاده می‌کند.

Oshima و همکارانش در [۳۹]، یک روش تشخیص "آماری کوتاه مدت[۳]" براساس آنتروپی پیشنهاد کرده‌اند. دلیل استفاده از اصطلاح کوتاه مدت، محاسبه آنتروپی در اندازه پنجره کوچک یعنی ۵۰ بسته

[۱] False Negative (FN)
[۲] Percentage of accuracy
[۱] Short_term statistics

است. آن‌ها اندازه پنجره‌های مختلف را آزمایش کرده‌اند تا بهترین روش برای اندازه‌گیری آنتروپی مطلوب را پیدا کنند. جدول (۲-۲) نتایج این آزمایش‌ها را نشان می‌دهد.

جدول (۲-۲): محاسبه آنتروپی اندازه پنجره‌های مختلف [۳۹]

w	H_N	H_A	$\lvert H_N - H_A \rvert$	S_N	S_A	Z
۵	۱/۳۶	۱/۹۸	۰/۶۲	۰/۷۹	۰/۴۸	۱/۲۹
۱۰	۱/۸۹	۲/۷۲	۰/۸۳	۰/۹۸	۰/۵۶	۱/۴۹
۵۰	۳/۱۱	۴/۲۲	۱/۱۱	۱/۳۵	۰/۶۵	۱/۷
۱۰۰	۳/۵۹	۴/۷۳	۱/۱۵	۱/۳۹	۱/۶۴	۱/۸
۵۰۰	۴/۵۴	۵/۵۱	۰/۹۶	۱/۰۵	۰/۴	۲/۴
۱۰۰۰	۴/۸۸	۵/۶۷	۰/۷۹	۰/۷۸	۰/۳۲	۴/۴۸
۵۰۰۰	۵/۵	۵/۹۷	۰/۴۲	۰/۳۱	۰/۱۳	۳/۲۵

که در آن:

$\boldsymbol{w}$ اندازه پنجره (براساس تعداد بسته‌ها) است. H_N آنتروپی شبکه در ترافیک مجاز، H_A آنتروپی در طول ترافیک حمله، S_A و S_N انحراف استاندارد آنتروپی برای شرایط ترافیکی مجاز و حمله است و Z آزمون اهمیت است و نشان‌دهنده اعتبار فرضیه بین دو میانگین از جمعیت‌های مختلف است. هنگامی که ارزش بیش از ۱/۶۴ باشد، فرضیه را می‌توان معتبر دانست. در جدول (۲-۲) می‌توان دید که برای یک پنجره با اندازه ۵۰، Z برابر با ۱/۷۰ است. Z توسط معادله (۲-۴) زیر محاسبه می‌شود.

$$Z = \frac{\overline{H_N} - \overline{H_A}}{\sqrt{\frac{\sigma_n^2}{n}} - \sqrt{\frac{\sigma_r^2}{r}}} \qquad (۴-۲)$$

که در آن:

σ_n و σ_r مشابه S_A و S_N است، n همان تعداد کل بسته‌های تولیدی در شبکه است (جمعیت بسته‌های ترافیک مجاز) و r برابر با ۲۵ در نظر گرفته شده است.

برای آزمون فرضیه، آزمون یک طرفه با فاصله اطمینان ۵ ٪ مورد استفاده قرار گرفته است که به جای این کار در روش پیشنهادی این پایان‌نامه، حملات مختلف برای انتخاب یک حدآستانه برای مقایسه آنتروپی در نظر گرفته شده است. طبق جدول، آنتروپی حمله بیشتر از وضعیت مجاز است. در این روش آنتروپی براساس پورت مقصد و آدرس IP منبع است و به همین دلیل بالاتر است (بسته‌های حمله دارای آدرس‌های مختلف IP و جعلی هستند).

در [۲۳]، روشی ارائه شده است که تقریبا به روش پیشنهادی در[۳۳] متکی است. در این روش محاسبه آنتروپی را به توپولوژی‌های ارائه شده در شبکه‌های VANET مبتنی بر نرم‌افزار تعمیم داده است که مبنای شروع کار این پایان‌نامه را تشکیل می‌دهد. در این روش دو توپولوژی برای یک جریان V2I پیشنهاد شده است. تنها تفاوت این روش با روش [۳۳] در تعمیم شبکه‌های SDN به شبکه‌های VANET است که ایده‌ای بسیار کارآمد است و در فصل اول به اجمال به توضیح مزایای این ایده پرداخته شده است. اما این روش که معیار تشخیص حمله را آنتروپی قرار داده است دارای محدودیت است و باعث افزایش نرخ FP و FN می‌شود. شبکه در زمانی که یک زیرشبکه مورد حمله قرار گیرد آنتروپی دچار تغییرات قابل توجهی نمی‌شود و موجب تشخیص منفی کاذب می‌شود. همچنین اگر در یک بازه زمانی خاصی ترافیک شبکه بیش از حد معمول نسبت به زمان‌های دیگر شود به اشتباه تشخیص می‌دهد که حمله رخ داده است. برای بهبود این روش معیار نرخ شروع جریان و خصوصیات آن مورد بررسی قرار داده خواهد شد تا میزان تشخیص بیشتر شود.

۲-۶ جمع‌بندی

در ابتدای این فصل به تعاریف حمله DOS و DDOS و انواع آن‌ها پرداخته شد. در ادامه این فصل به مزیت‌های شبکه‌های SDN در طرح‌های دفاعی در برابر حمله DDOS اشاره شد و در ادامه به تعمیم شبکه‌های خودرویی به شبکه‌های مبتنی بر نرم‌افزار و بررسی برخی از روش‌های تشخیص حمله DDOS پرداخته شد.

پس از تعمیم شبکه‌های خودرویی به شبکه‌های خودرویی مبتنی بر نرم‌افزار، مسأله طراحی یک مدل هوشمند امن برای وسایل نقلیه به مسأله طراحی یک مدل امن برای شبکه‌های مبتنی بر نرم‌افزار تغییر پیدا می‌کند. در این پژوهش یک توپولوژی ارتباطی در شبکه‌های خودرویی مبتنی بر نرم‌افزار که شامل ارتباط V2I است در نظر گرفته می‌شود. روش پیشنهادی مبتنی بر آنومالی با معیار آنتروپی و همچنین خصوصیات جریان در شبکه‌های SDN برای تشخیص حمله DDOS ارائه می‌شود. این روش پیشنهادی با ایجاد ترافیک مجاز و حملات DDOS بین گره‌ها و وقفی‌سازی شروط تشخیص حمله از غیرحمله قدرت شبکه را در تشخیص بالا می‌برد. در فصل بعدی به معرفی بیشتر روش پیشنهادی پرداخته خواهد شد.

فصل سوم

روش پیشنهادی

۳-۱- مقدمه

در این فصل یک مدل بهبود یافته برای شناسایی حمله DDOS براساس یک روش آماری با استفاده از آنتروپی و خصوصیات نرخ جریان و پرس‌وجو از سوئیچ‌ها ارائه خواهد شد. همان طور که اشاره شد حمله DDOS در شبکه‌های خودرویی به شناسایی این حمله در شبکه‌های مبتنی بر نرم‌افزار تعمیم داده شد. بنابراین بدین گونه می‌توان یک مدل امن برای شبکه‌های خودرویی طراحی کرد. سناریوی مورد بحث براساس معماری توپولوژی ارتباطات V2I در شبکه‌های VANET مبتنی بر نرم‌افزار است. در این پایان-نامه شبکه در دو فاز یادگیری و تست اجرا خواهد شد و پارامترها تنظیم می‌شوند. سپس ترافیک حمله DDOS در شبکه اجرا و نتایج ارائه می‌شود. سپس تشخیص ناهنجاری، با استفاده از پارامترهای آنتروپی و خصوصیات نرخ جریان و پرس‌وجو از سوئیچ‌ها با کاهش نرخ FP و FN انجام می‌شود. بدین منظور یک ماژول شناسایی حمله در کنترل‌کننده معماری SDN برنامه‌نویسی می‌شود.

۳-۲- انواع تکنیک‌های تشخیص ناهنجاری

جنبه مشترک در هر نوع حمله DDOS، این است که حجم زیادی از ترافیک را به شبکه منتقل می‌کند تا منابع شبکه را از بین ببرد. معمولا در شرایط عادی یک الگویی در فعالیت شبکه را می‌توان تعریف کرد تا نرخ پهنای باند پذیرفته شده را مشخص کند. برای طبقه‌بندی ترافیک مجاز و حمله، باید افزایش ناگهانی ترافیک، تأخیر، استفاده از CPU یا کاهش ناگهانی در عملکرد هر یک از دارایی‌های شبکه را مورد توجه قرار داد. در مورد کلی، ناهنجاری‌ها مربوط به نوع داده‌ها در شبکه‌می‌باشند[۲۹].

شناخت ماهیت اطلاعات منتقل شده و ویژگی‌های آن در شبکه اولین گام اصلی برای تشخیص اختلال است. برخی از این ویژگی‌ها می‌توانند اطلاعات هدر بسته‌ها، تأخیر، اندازه بسته‌ها، نوع پروتکل و غیره باشد. می‌توان نتیجه گرفت که ویژگی‌های شبکه، نوع نفوذ را تعریف می‌کنند. اگر شبکه به یک تهدید خاص آسیب‌پذیر باشد پس تلاش‌ها باید بر تشخیص و مقابله با این نوع تهدید متمرکز شود.

هر شبکه پهنای باند و توان پردازش خاصی را برای انتقال ترافیک دارد. اگر این ویژگی‌ها به تجزیه و تحلیل‌های آماری داده شود می‌توان الگویی برای هر ویژگی شبکه تعریف کرد. قابلیت اطمینان الگو به زمان بستگی دارد و هر چه زمان طولانی‌تر شود الگوی شبکه پایدارتر خواهد بود و این زمانی درست است که ترافیک ثابت باشد. جمع‌آوری، فیلتر و پردازش داده روش‌های شناخته شده‌ای برای تشخیص حمله DDOS هستند[۳۷, ۳۸, ۴۰]. همانطور که در فصل قبل گفته شد تجزیه و تحلیل آماری مانند تکنیک‌های آنتروپی و Chi_Square) و یادگیری ماشین دو روش معمول از تشخیص ناهنجاری هستند.

آنتروپی نشان‌دهنده هدر بسته‌ها به عنوان نمادهای داده مستقل با احتمال وقوع یکتا است. این یک روش معمول برای تشخیص حمله DDOS است. اگر یک پنجره از یک عدد را برای مثال ۱۰۰۰۰ انتخاب شود و پنجره رو به جلو حرکت داده شود می‌توان یک الگویی با احتمالات مختلف برای هر نوع هدر پیدا کرد. اگر تغییرات به طور چشمگیر باشد سیستم هشدار ناهنجاری می‌دهد. از این تکنیک به صورت بالقوه در معماری‌های SDN مورد استفاده قرار می‌گیرد. اگر نوع نفوذ و نوع هدر بسته شناخته شده باشد، بهتر است از مدل Chi-Square استفاده شود. برای مثال، اگر سیلاب TCP SYN حمله‌ای است که می‌تواند اتفاق بیافتد، سپس نمونه‌برداری از داده‌ها و شمارش تعداد هدرهای TCP SYN، یک الگوی میانگین تعداد هدرها را نشان می‌دهد. بنابراین برای تشخیص ناهنجاری هر واریانس فراتر از محدودیت‌های برآورد شده غیر طبیعی است.

۳-۲-۱- تعریف آنتروپی

آنتروپی یک مفهوم مهم در نظریه اطلاعات است[۴۱]. آنتروپی اندازه‌گیری عدم قطعیت یا تصادفی مرتبط با یک متغیر تصادفی است که در مسأله مورد بحث این پژوهش آدرس IP مقصد است. هرچه تصادف بیشتر باشد آنتروپی افزایش می‌یابد. در واقع مقدار آنتروپی در تعداد آدرس‌هایIP مقصد نهفته است. مقدار آنتروپی زمانی حداقل است که تمام ترافیک شبکه در یک مقصد قرار گیرد. از سوی دیگر، مقدار آنتروپی زمانی حداکثر است که ترافیک به طور مساوی برای همه مقاصد ممکن توزیع شود. قبل

از بحث درباره الگوریتم بهبودیافته پیشنهادی، به طور خلاصه توضیح داده خواهد شد که آنتروپی روش مناسبی برای اندازه‌گیری آمار در شبکه‌های مبتنی بر SDN است. همان طور که در گذشته اشاره شد، دلیل اصلی انتخاب آنتروپی توانایی آن در اندازه‌گیری تصادفی در یک شبکه است و همچنین می‌توان ادعا داشت که وضعیت فعلی شبکه می‌تواند به کنترل‌کننده کمک کند تا تصمیم بگیرد که آیا حمله رخ داده است یا خیر.

در شبکه‌های OF[1] کنترل‌کننده، سیستم عامل است و از دست دادن آن به معنای از دست دادن مزایای کنترل گسترده SDN است. دلیل این که بسته‌ها به کنترل‌کننده می‌آیند این است که آدرس IP منبع، جدید است. نمونه‌ای از آنها در جدول سوئیچ وجود نداشته است، بنابراین آن‌ها به کنترل‌کننده منتقل می‌شوند. برای هر اتصال ورودی جدید کنترل‌کننده یک جریان را در سوئیچ نصب می‌کند تا بقیه بسته‌های دریافتی بدون پردازش بیشتر به مقصد منتقل شوند. همچنین برای هر بسته جدید در کنترل‌کننده میزبان مقصد در شبکه کنترل مشخص است. شبکه شامل سوئیچ ها (آنها RSU ها و ایستگاه‌های پایه در بحث موردنظر VANET هستند) و میزبان‌ها (برای توپولوژی به کار رفته در این پژوهش وسایل نقلیه هستند) است که به سوئیچ‌ها متصل است. با استفاده از این دانش (بسته در کنترل‌کننده همیشه جدید است و مقصد در شبکه است) میزان تصادفی را می‌توان با محاسبه آنتروپی بر اساس اندازه پنجره اندازه‌گیری کرد.

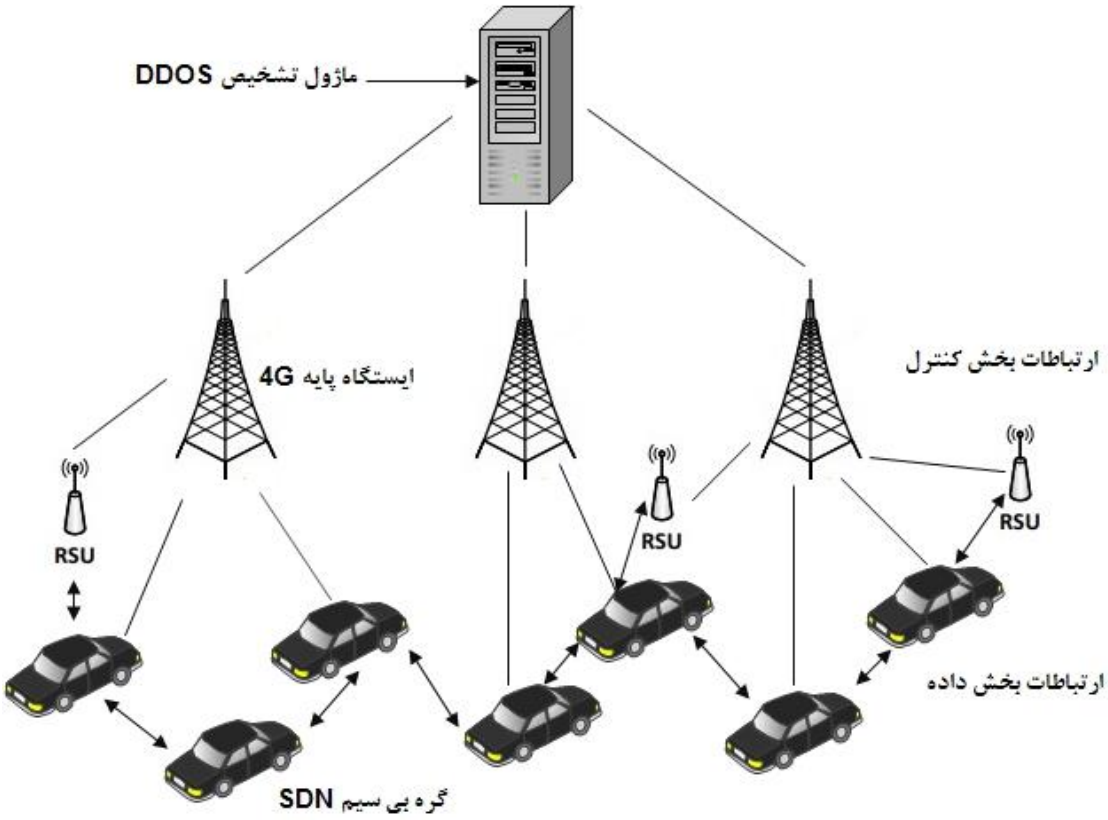
۳-۳- توپولوژی پیشنهادی

راه حل پیشنهادی در این پایان‌نامه تقریبا به روش پیشنهادی در [۲۳] متکی است. هدف از این پژوهش ایجاد برنامه تشخیص DDOS با استفاده از آنتروپی و خصوصیات جریان می‌باشد. علاوه بر این، به کارگیری ماهیت این راه حل برای شبکه‌های VANET مبتنی بر SDN یکی از ایده‌های [۲۳] می‌باشد. بنابراین، با توجه به استانداردهای VANET و محدودیت‌های آن پارامترهای شبکه باید به دقت بررسی

[1] شبکه‌هایی که از پروتکل openflow (OF) استفاده می‌کنند.

شود. بنابراین در این پژوهش راه حل موجود در [۲۳]، برای ارائه بهبود روش تشخیص DDOS در شبکه‌های خودرویی مبتنی بر SDN اصلاح می‌شود. هدف اصلی این پژوهش بررسی موارد حمله DDOS با استفاده از بسته های UDP است که نیازهای سرویس‌ها در زمان واقعی مانند پیشگیری از حوادث، هشدار ترافیک یا ارتباطات را برآورده می‌کند. در [۷]، یک جریان V2I برای ساخت یک شبکه V2I پیشنهاد شده است. در ادامه عملکرد الگوریتم تشخیص حمله DDOS مورد بررسی قرار خواهد گرفت.

همان طور که در بخش‌های بعدی توضیح داده خواهد شد، در این پایان‌نامه، اندازه پنجره‌های بسته کوچک در نظر گرفته شده است. بنابراین فرض شده است که توپولوژی را می‌توان به عنوان استاتیک مورد بررسی قرار داد و ویژگی‌های ترافیک مورد مطالعه قرار می‌گیرند. ارتباط خودرو به خودرو (V2V) ارتباطات بخش داده‌ای است و این بخشی از علاقه پایان‌نامه به این کار نیست؛ بنابراین در این پژوهش ارتباط دیگری در نظر گرفته شده است - ارتباط میان وسایل نقلیه، ایستگاه های پایه و کنترل کننده. همانطور که واضح است، RSU ها و وسایل نقلیه می‌توانند همزمان مانند سوئیچ‌ها و میزبان‌ها عمل کنند. به همین دلیل در [۲۳]، سناریو را با دو توپولوژی ارائه کرده است. در توپولوژی‌های ارائه شده RSU ها را هم به عنوان سوئیچ و هم به عنوان میزبان در نظر گرفته است. در روش پیشنهادی این پایان‌نامه، یک توپولوژی که در آن RSU ها به عنوان سوئیچ هستند مورد بحث واقع شده است و عملکرد الگوریتم با استفاده از جداول جریان مورد ارزیابی قرار می‌گیرد.



شکل (۳-۱): توپولوژی استفده شده راه‌حل پیشنهادی [۲۳]

۳-۴- الگوریتم بهبودیافته پیشنهادی

الگوریتم تشخیص بر مبنای سه مفهوم اصلی شامل تنوع آنتروپی آدرس IP مقصد، نرخ شروع جریان و بررسی مشخصات جریان [۳۴] طراحی شده است. الگوریتم تشخیص پیشنهادی را می توان به هفت مرحله تقسیم کرد.

۱- جمع‌آوری داده‌ها

۲- محاسبه و مقایسه آنتروپی

۳- محاسبه و مقایسه مقدار شروع جریان

۴- پیدا کردن مسیر حمله که ممکن است در مراحل ۲ یا ۳ مشکوک باشد، در غیر این صورت بازگشت به مرحله ۱

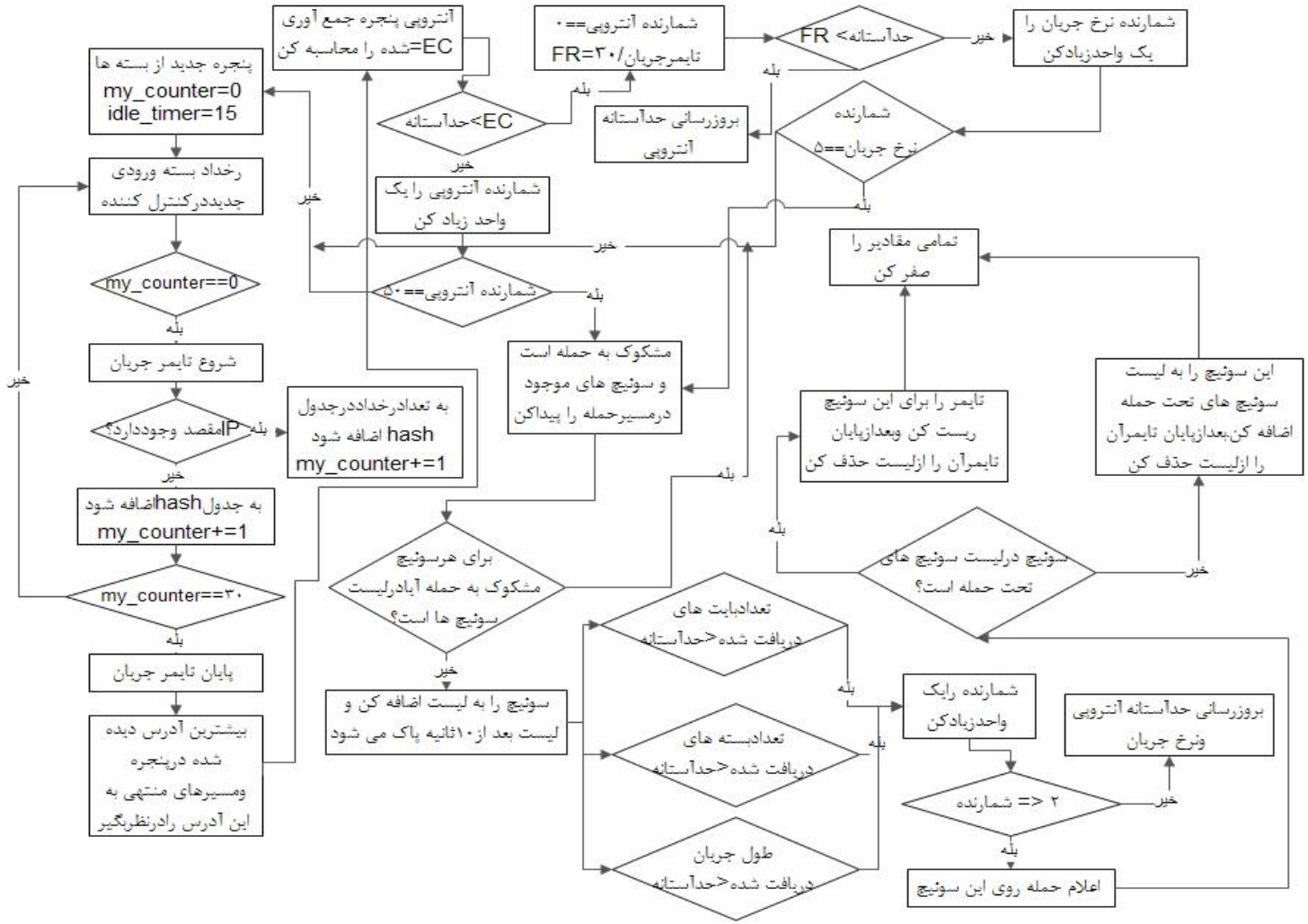
۵- بررسی سوئیچ‌های موجود در مسیر حمله برای آمار جریان و نتایج به دست آمده از سوئیچ‌ها برای تایید یا لغو یک حمله[۳۴]

۶- به روزرسانی حدآستانه‌ها با توجه به نتیجه تشخیص در مرحله ۵

پس از اینکه حمله شناسایی شد، یک روش کاهش برای جلوگیری از درهم شکستن شبکه و ایجاد زمان کافی برای مدیریت شبکه جهت انجام اقدامات لازم مورد استفاده قرار می‌گیرد. رویکرد کاهش، idle_timer جریان را به یک مقدار کوچک برای جریان‌های جدید تنظیم می‌کند. تمام مراحل فوق با اضافه کردن مجموعه‌ای از برنامه‌نویسی به کنترل‌کننده انجام می‌شود. فلوچارت الگوریتم پیشنهادی در شکل (۳-۲) نشان داده شده است.

۳-۴-۱- تغییر آنتروپی برای تشخیص حمله DDOS

الگوریتم تشخیص مبتنی بر آنتروپی به کار گرفته شده در این پایان‌نامه، مشابه الگوریتم در [۲۳] است. در روش پیشنهادی برای جمع آوری بسته‌ها برای تحلیل آنتروپی، از یک پنجره اندازه ثابت استفاده شده است. استفاده از پنجره اندازه ثابت، پیچیدگی محاسبات آنتروپی را ساده می‌کند. اندازه پنجره می‌تواند با توجه به زمان سپری شده یا تعداد بسته‌های دریافت شده ثابت باشد. از آنجایی‌که در زمان بارگیری ترافیک سبک، در یک پنجره ثابت زمانی ممکن است دقت محاسبات آنتروپی کاهش یابد به جای استفاده از پنجره زمانی، الگوریتم از پنجره‌ای استفاده می کند که توسط n تعداد بسته‌ها اندازه-گیری می‌شود، که n اندازه پنجره است. برای هر پنجره، بسته‌ها بر اساس آدرس‌های IP مقصد خود گروه‌بندی می‌شوند. تمام بسته ها در هر گروه آدرس مقصد یکسانی دارند، اما ممکن است آدرس منبع متمایز داشته باشند. آدرس IP مقصد به عنوان شاخص متریک مورد استفاده قرار می‌گیرد و فرکانس هر آدرس IP مقصد مشخص در پنجره به عنوان یک اندازه‌گیری تصادفی در نظر گرفته می‌شود. معادلات مربوط به چگونگی محاسبه آنتروپی در بخش ۲-۵ آورده شده است.



شکل (۳-۲): فلوچارت روش پیشنهادی

کاهش در آنتروپی یک زنگ هشدار برای شبکه جهت محافظت از یک حمله احتمالی است. در شبکه های SDN، این امر حیاتی است که یک روش تشخیص سریع در مراحل اولیه خود داشته باشد. شبکه های SDN در برابر حملات DDOS آسیب‌پذیرتر از شبکه‌های سنتی هستند. اگر زمان تشخیص بیش از حد طولانی شود، مهاجم می‌تواند سوئیچ‌ها و یا کنترل‌کننده را شکست دهد. بنابراین تشخیص زود هنگام بسیار مهم است. برای تشخیص زود هنگام پنجره نباید خیلی بزرگ باشد. از طرف دیگر یک پنجره کوچک به سربار محاسباتی اضافه می‌شود. در این پایان‌نامه از اندازه پنجره ۳۰ تایی به منظور تعادل دو نگرانی استفاده شده است.

یک ماژول برای محاسبات آنتروپی به کنترل‌کننده POX اضافه شده است. برای هر ۳۰ بسته‌ای که وارد کنترل‌کننده می‌شود، فرکانس‌ها محاسبه می‌شوند. آنتروپی محاسبه شده با مقدار حدآستانه مقایسه می‌شود. اگر آنتروپی محاسبه شده کمتر از حدآستانه برای پنج تکرار متوالی باشد، مشکوک به حمله است و تجزیه و تحلیل بیشتر برای تعیین اینکه آیا حمله واقعی است یا خیر انجام خواهد شد.

در مرحله اول، یک پنجره از ۳۰ بسته بر روی کنترل‌کننده جمع‌آوری می‌شود. این بسته‌ها یک پنجره از ۳۰ درخواست شروع جریان است که توسط سوئیچ‌ها به کنترل‌کننده ارسال می‌شود. یک تایمر مدت زمان لازم برای این پنجره از ۳۰ بسته جمع‌آوری شده را محاسبه می‌کند. این تایمر در مرحله بعدی تشخیص که براساس میزان شروع جریان می‌باشد، استفاده می‌شود.کنترل‌کننده با استفاده از نوع یادگیری که برای آن تعیین می‌شود کوتاه‌ترین مسیر (با استفاده از یادگیری L2_multi) را برای هر جریان محاسبه و جریان‌ها را در مسیر نصب می‌کند. به طور پیش‌فرض کنترل‌کننده مسیرهای محاسبه شده را حفظ نمی‌کند. با این حال جهت یافتن مسیر حمله در مراحل بعدی از تشخیص الگوریتم، یک ماژول برای ثبت مسیرهای محاسبه شده اضافه می‌شود. پس از رسیدن به یک پنجره از ۳۰ بسته جمع‌آوری شده، آدرس IP مقصد برای هر بسته بررسی می‌شود تا تعیین شود که تعداد تکرار هر یک از آدرس‌های IP در پنجره چقدر است؟ آدرس IP مقصد که بیشترین تعداد بار تکرار شده است و

مسیرهایی که برای رسیدن به این آدرس IP مورد استفاده قرار گرفته‌اند برای پردازش‌های بعدی ذخیره می‌شوند. سپس تابع آنتروپی فراخوانده می‌شود. این تابع آدرس IP مقصد و تعداد دفعاتی که آن‌ها به عنوان ورودی تکرار می‌شود را می‌گیرد و فرکانس هر آدرس IP مقصد را محاسبه می‌کند. فرکانس‌های محاسبه شده برای محاسبه آنتروپی طبق معادله (۲-۳) مورد استفاده قرار می‌گیرند. هنگامی که یک مهاجم یک میزبان را در شبکه هدف قرار می‌دهد، تعداد جریان‌های جدیدی که برای آدرس خاص تعیین شده، به طور چشمگیری افزایش می‌یابد. بر این اساس آنتروپی شروع به کاهش می‌کند. در ابتدای الگوریتم یک حدآستانه برای مقایسه آنتروپی در نظر گرفته شده است که این حدآستانه با اعمال ترافیک مجاز در فاز یادگیری به شبکه به دست آمده است. آنتروپی محاسبه شده با این حدآستانه مقایسه می‌شود اگر برای ۵ تکرار متوالی آنتروپی محاسبه شده کمتر از حدآستانه حمله باشد، مشکوک است و سوئیچ‌ها در مسیر حمله احتمالی شناسایی می‌شوند و آمارها و جدوال جریان آن‌ها مورد تجزیه و تحلیل قرار می‌گیرند.

اگر پس از بررسی جداول جریان و سوئیچ‌ها، یک آشکارسازی حمله شناسایی نشود، حدآستانه آنتروپی به آنتروپی محاسبه شده کنونی به منظور جلوگیری از FP، بروزرسانی خواهد شد. این رویکرد، الگوریتم را قادر می‌سازد خود را به صورت پویا با الگوی جریان ترافیک فعلی تنظیم کند. علاوه بر این اگر یک حمله تأیید شود، حدآستانه آنتروپی به مقدار پیش‌فرض بر می‌گردد تا سطح حساسیت و آگاهی در فرآیند تشخیص را افزایش دهد. از آنجا که تغییرات ساده در الگوی ترافیک می‌تواند آنتروپی را در زمان کوتاه‌مدت تغییر دهد[۲۳]، به همین دلیل الگوریتم تشخیص، احتمال حمله ممکن را تنها در صورتی که آنتروپی محاسبه شده کمتر از حدآستانه برای ۵ تکرار متوالی باشد، تأیید می‌کند.

اگر چه که آنتروپی ثابت کرده است که یک روش تشخیص موفق است، اما استفاده از آنتروپی به تنهایی نمی‌تواند بسیاری از سناریوهای حمله را شناسایی کند. برای مثال در زمان‌هایی که تقاضا برای یک مقصد خاص شبکه مانند سرور وب یا ایمیل رشد می‌کند (افزایش ناگهانی ترافیک مجاز رخ می‌دهد)

روش تشخیص مبتنی بر آنتروپی می‌تواند به طور مداوم هشدارهای FP گزارش کند. از سوی دیگر هنگامی که مهاجم حمله را در میان بسیاری از قربانیان (میزبان‌های هدف) توزیع می‌کند، آنتروپی ممکن است میزان قابل توجهی را نشان ندهد و بنابراین هشدارهای FN را به همراه خواهیم داشت. برای غلبه بر محدودیت‌های ذکر شده از تشخیص آنتروپی، روش تشخیص پیشنهاد شده در این پژوهش الگوریتم‌های تشخیص دیگر را همچنین شامل می‌شود.

۳-۴-۲- نرخ شروع جریان

همان طور که در بخش‌های قبلی ذکر شد، آنتروپی یک رویکرد مورد استفاده در سیستم‌های مورد حمله DDOS است و یک عنصر موثر در تشخیص حمله DDOS به یک قربانی (میزبان) است. اما با توجه به محدودیت‌های روش آنتروپی، به ویژه در حملات به چندین قربانی، نمی‌توان آن را یک برنامه مستقل و موثر برای تشخیص حمله DDOS دانست. زیرا در ترافیک حمله به چندین قربانی، بسیاری از مقصدهای مختلف را هدف قرار می‌دهد که تغییرات ناچیزی در آنتروپی ایجاد می‌کند. الگوریتم تشخیص کارآمد در این مورد براساس نرخ شروع جریان خواهد بود. جداول جریان در هر سوئیچ برای مدیریت جریان شبکه قرار دارند. جریان در SDN به عنوان مجموعه‌ای از بسته‌های با مقادیر مشابه برای برخی از فیلدهای هدر تعریف شده است. این جداول جریان شامل قوانین جریان است که توسط کنترل-کننده براساس برنامه‌های شبکه اجرا می‌شود.

هنگامی که یک حمله DDOS در حال انجام است، مهاجم حجم زیادی از بسته‌ها را از طریق عوامل خود به مقصد (های) مورد هدف ارسال می‌کند. نتایج حاصل از [۳۴]، نشان می‌دهد که شروع جریان دارای رشد خطی در طول حمله DDOS است.

نرخ شروع جریان هر پنجره از ۳۰ بسته با استفاده از معادله (۳-۱) محاسبه می‌شود:

$$FlowRate(FR) = \frac{n}{T_W} \qquad (۱-۳)$$

که در آن:

n سایز پنجره و T_W طول پنجره (زمانی که طول می‌کشد تا یک پنجره از بسته‌ها جمع‌آوری شود). اگر مقدار شروع جریان محاسبه شده بالاتر از حدآستانه باشد شبکه به حمله مشکوک است و باید بررسی بیشتر انجام شود. اگر میزان محاسبه شده کمتر از حدآستانه باشد، سیستم در حالت ایمن است. در مواقعی ممکن است آنتروپی کمتر از حدآستانه نباشد اما حمله وجود داشته باشد، بنابراین نرخ جریان می‌تواند معیار خوبی برای تشخیص حمله باشد.

در الگوریتم پیشنهاد شده، حدآستانه اولیه ثابت است که باید مطمئن بود این یک ترافیک قابل قبول برای شبکه است و با چنین میزانی شبکه قادر خواهد بود ایمن عمل کند. حدآستانه را می‌توان در یک فاز یادگیری اولیه در حالی که ترافیک مجاز در حال اجرا است با بررسی کنترل‌کننده محاسبه کرد. با این حال حدآستانه باید با ترافیک شبکه تطبیق داده شود تا منعکس‌کننده الگوی جریان ترافیکی فعلی باشد.

هنگامی که نرخ شروع جریان شروع به افزایش می‌کند از حد آستانه عبور می‌کند. اگر این رفتار برای ۵ تکرار متوالی ادامه پیدا کند، به عنوان نشانه‌ای از حمله مورد بررسی قرار می‌گیرد. در چنین مواردی، آمار ترافیک شبکه باید بیشتر مورد بررسی قرار گیرد تا تأیید حمله انجام شود. اگر بررسی‌های بیشتر در مورد آمار جریان نشان‌دهنده یک حمله نیست، پس باید حدآستانه به میزان محاسبه شده فعلی بروزرسانی شود تا گزارش‌های FP در سیستم رخ ندهد. هنگامی که بار ترافیک شبکه کاهش می‌یابد و نرخ جریان شروع به کاهش می‌کند حدآستانه باید دوباره به مقدار پیش‌فرض برای اجتناب از هر سناریو FN بروزرسانی شود. در صورت تأیید حمله، شبکه به وضعیت هشدار درآمده و حدآستانه به مقدار پیش‌فرض اولیه کاهش می‌یابد تا حساسیت الگوریتم تشخیص را افزایش دهد.

همان طور که ذکر شد استفاده از ۵ پنجره متوالی برای شناسایی یک حمله مشکوک، به کاهش احتمال تشخیص‌های FP کمک می‌کند. مقدار حدآستانه نرخ شروع جریان باید با نرخ شروع جریان از ترافیک

مجاز شبکه مطابقت داشته باشد. حدآستانه پیش‌فرض به یک مقداری تنظیم می‌شود که شبکه قادر به اداره ترافیک در آن نرخ باشد.

مقدار حدآستانه به طور مداوم با توجه به بار ترافیک فعلی شبکه به روزرسانی می‌شود. هنگام استفاده از نرخ شروع جریان به عنوان یک روش تشخیص، باید همیشه در نظر داشت که حجم بالای شروع جریان ممکن است ناشی از افزایش ناگهانی ترافیک مجاز باشد. با تکیه بر تنها نرخ شروع جریان برای گزارش حمله ممکن است احتمال بالقوه FP افزایش یابد. بنابراین در الگوریتم پیشنهادی، نظارت بر نرخ شروع جریان، تنها به عنوان یک وسیله برای تشخیص علامت حمله است اما تأیید حمله نیست. اگر حمله‌ای مشکوک باشد، آمار جریان از جداول جریان سوئیچ‌هایی که مشکوک به مسیر حمله هستند، برای تأیید حمله مورد تجزیه و تحلیل قرار می‌گیرد.

۳-۴-۳- بررسی مشخصات جریان

در این قسمت از فرآیند تشخیص، کنترل‌کننده آمار جریان سوئیچ‌هایی را که در مسیرهای ترافیک حمله مشکوک هستند را مورد بررسی قرار می‌دهد. با استفاده از پروتکل openflow، کنترل‌کننده قادر خواهد بود هر یک از سوئیچ‌ها را برای جدول جریان و آمار جریان مورد بررسی قرار دهد. سه آمار جریان برای تشخیص حمله تحلیل می‌شود.

۱. بسته‌های دریافتی در هر جریان
۲. بایت‌های دریافتی در هر جریان
۳. طول جریان[۱]

حال به بررسی ویژگی‌های این سه آمار مرتبط با جریان‌های مخرب پرداخته خواهد شد. برای به حداکثر رساندن حمله به کنترل‌کننده و سوئیچ‌ها تحت یک بار ترافیکی حمله، مهاجم سعی خواهد کرد که

[۱] Flow Duration

حداکثر جریان حمله را ایجاد کند. به عنوان مثال مهاجم می‌تواند در کل ترافیک حمله ۱۰۰ مگابایت در ثانیه تولید کند و حداقل اندازه بسته ۱۰۰ بایت باشد. حداکثر جریان (و حداکثر آسیب) تولید شده توسط مهاجم در هر ثانیه ۱۲۵۰۰۰ است. در این مورد، هر جریان تنها شامل یک بسته با کوچکترین اندازه بسته می‌باشد، اما کنترل‌کننده نیاز به رسیدگی ۱۲۵۰۰۰ درخواست جریان در ثانیه دارد و یک سوئیچ ممکن است مجبور به تنظیم این ۱۲۵۰۰۰ جریان باشد.

براساس استدلال فوق، می‌توان نتیجه گرفت که ترافیک حملات معمولا دارای ویژگی‌های اندازه کوچک بسته، تعداد کمی بسته در جریان و مدت زمان کوتاه مدت است. بنابراین حجم زیادی از جریان با تعداد کمی از بسته‌ها (جریان‌های کوتاه) و بارهای کوچک ممکن است به یک حمله DDOS اشاره کند.

تعدادی از بررسی‌های قبلی در مورد تشخیص حمله DDOS وجود دارد که بر مبنای بررسی آمار مورد نظر از سوئیچ‌های شبکه متکی است. اما از آنجایی که سنجش سوئیچ‌ها و پردازش جداول جریان نسبتا بزرگشان، تعداد زیادی از پهنای باند و منابع را مصرف می‌کند، در نتیجه الگوریتم‌های تشخیص که تنها براساس تجزیه و تحلیل آمار جدول جریان می‌باشد توصیه نمی‌شود زیرا ممکن است منجر به شکست کنترل‌کننده، سوئیچ یا هر دو شود. در الگوریتم پیشنهاد شده، بررسی جداول جریان تنها به عنوان یک مکانیزم برای تضمین نهایی یک حمله است و این کار پس از آنکه حمله براساس تجزیه و تحلیل آنتروپی و نرخ شروع جریان، مشکوک باشد انجام می‌شود. علاوه بر این، الگوریتم پیشنهادی آمار جدول جریان را از همه سوئیچ‌ها بررسی نمی‌کند. به جای این کار آمار جدول جریان برخی از سوئیچ‌هایی که تحت حمله هستند مورد بررسی قرار می‌گیرد.

۳-۴-۳-۱- پیاده‌سازی بررسی خصوصیات جریان

مسیر حمله با یافتن آدرس‌های IP مقصد با بالاترین فرکانس موجود در بسته‌های پردازش شده توسط کنترل‌کننده تعیین می‌شود. در DDOS دو نوع حمله اصلی وجود دارد. در نوع اول مهاجم به یک میزبان خاص حمله می‌کند و در نوع دوم مهاجم ممکن است ترافیک حمله را به طور مساوی بر روی شبکه

توزیع کند. همان طور که مهاجمان خارجی می‌توانند تعداد محدودی از آدرس‌های IP را که برایشان شناخته شده است، حمله کنند احتمالا این حمله تنها می‌تواند محدود به لیستی از آدرس‌ها (مجموعه محدودی از میزبان‌ها) شود. در هر دو مورد کنترل‌کننده باید بتواند میزبان‌هایی را که تحت حمله هستند، با بررسی فرکانس آدرس IP مقصد محاسبه شده طبق معادله (۲-۲) تعیین کند. الگوریتم پیشنهادی میزبان‌های هدف را به صورت زیر تعریف می‌کند:

۱. میزبان با بالاترین فرکانس را پیدا کن (F_h) و آن را در لیست میزبان‌های هدف قرار بده.

۲. همچنین تمام میزبان‌هایی که فرکانس آن‌ها بالاتر از ۰/۵*F_h است را در لیست میزبان‌های هدف قرار بده.

بعد از تشکیل لیست میزبان، الگوریتم مجموعه‌ای از سوئیچ‌هایی را که مشکوک به حمله هستند را تعیین می‌کند.

m تعداد کل مسیرهای منتهی به میزبان‌های موجود در لیست میزبان است. به عبارتی m تعداد کل مسیرهایی است که مقصد (ها) مشکوک به حمله هستند. P_i مجموعه‌ای از سوئیچ‌ها است که در i امین مسیر قرار دارند.

$$P_i = \{S_{i1}, S_{i2}, \dots, S_{in}\} \qquad (۲-۳)$$

$$SA = P_1 \cup P_2 \cup \dots \cup P_m \qquad (۳-۳)$$

که در آن:

S_{ij}: j امین سوئیچ از مسیر i، n طول مسیر از نظر تعداد سوئیچ‌ها است و SA مجموعه‌ای از سوئیچ‌ها که تحت حمله هستند.

پس از پیدا کردن مجموعه SA، الگوریتم یک درخواست برای دانلود جداول جریان از همه سوئیچ‌ها در مجموعه ارسال می‌کند. برای جلوگیری از ایجاد جدول جریان بیش از حد، درخواست حداکثر یک بار در هر ۱۰ ثانیه محدود می‌شود. هر سوئیچی که برای جداول جریان از کنترل‌کننده درخواست شده است به یک لیست اضافه می‌شود. کنترل‌کننده یک درخواست دانلود جدول جریان را به سوئیچ‌هایی که در این لیست هستند ایجاد می‌کند. سوئیچ‌ها قبل از حذف شدن به مدت ۱۰ ثانیه در این لیست باقی می‌ماند.

پردازش جداول جریان یک سربار برای کنترل‌کننده و شبکه قرار می‌دهد. دلیل آن این است که الگوریتم پیشنهاد شده به عنوان برخی از روش‌های تشخیص دیگر به صورت دوره‌ای این بررسی را انجام نمی‌دهد. این الگوریتم سوئیچ‌ها را فقط هنگامی که به یک حمله مشکوک است سوئیچ می‌کند و همان سوئیچ بیش از یک بار در یک فاصله زمانی ۱۰ ثانیه مورد سوال قرار نمی‌گیرد. با استفاده از یک تابع، جدول جریان دریافتی از سوئیچ درخواست‌کننده مورد تجزیه و تحلیل قرار می‌گیرد. داشتن چندین جریان کوتاه یا جریان با تعداد کمی از بایت‌ها یا بسته‌ها به عنوان نشانه‌هایی از حمله است. برای هر جریان جدول جریان دریافتی، این سه ویژگی بررسی و یک شمارنده برای آن درنظر گرفته می‌شود. زمانی که یک جریان با دو مورد از سه شرایط زیر روبرو شود این شمارنده یک واحد افزایش می‌یابد.

۱. آیا تعداد شمارش بایت‌ها از جریان، کمتر از تعداد بایت‌های حدآستانه است؟

۲. آیا تعداد بسته‌های رسیده از جریان، کمتر از تعداد بسته‌های حدآستانه است؟

۳. آیا طول جریان کمتر از طول جریان حدآستانه است؟

باید توجه داشت که مقادیر حدآستانه براساس میانگین‌های گزارش شده توسط الگوریتم در جریان ترافیک مجاز در مرحله یادگیری انتخاب شده‌اند.

هنگامی‌که همه جریان‌ها در جدول جریان مورد بررسی قرار گرفت یک نرخ حمله (A_{rate}) محاسبه می‌شود تا احتمال اینکه سوئیچ تحت حمله است یا خیر را نشان‌دهد. این نرخ به صورت زیر محاسبه می‌شود[۳۴]:

$$A_{rate} = \frac{\text{شمارنده}}{number\_flows} \qquad (۴-۳)$$

که در آن: نرخ حمله برابر با نسبت شمارنده به تعداد جریان‌های موجود است. در نهایت، در روش تشخیص پیشنهادی اگر نرخ حمله بزرگ‌تر از نرخ حدآستانه باشد اعلام می‌کند که حمله رخ داده است.

۳-۴-۴- سناریوی کاهش حمله

اگر یک سوئیچ تحت حمله قرار گیرد، الگوریتم باید سعی کند حمله را کاهش دهد. برخی از روش‌های کاهش احتمال حمله ممکن است شامل نصب جریان‌ها در مسیرهای حمله برای رهاسازی بسته‌ها تا زمانی که حمله متوقف شود باشد، یا مسدود کردن پورت‌های ورودی که در آن ترافیک حمله وارد می‌شود. اگر چه تمام این روش ها موجب کاهش حمله می‌شوند و زمان را برای اپراتورهای شبکه جهت یافتن منابع حمله قبل از شکست کنترل‌کننده یا سوئیچ‌ها فراهم می‌سازد، اما اتخاذ این روش ها نیز به همان اندازه که بر روی ترافیک حمله تأثیر می‌گذارد بر روی ترافیک مجاز هم تأثیر می‌گذارد و سرویس‌های شبکه غیر قابل دسترس می‌شوند و به کندی به ترافیک مجاز شبکه پاسخ می‌دهد.

کنترل کننده معمولا با ظرفیت های بالا طراحی شده است و به آسانی دچار سقوط نمی‌شود. از طرفی سوئیچ‌ها منابع محدودی دارند و در برابر حملات بسیار قوی نیستند. در این پژوهش هنگامی که یک حمله در حال انجام است، جدول جریان روی سوئیچ‌ها با تعداد زیادی جریان کوتاه پر می‌شود که سرانجام موجب قطعی سوئیچ می‌شود. در الگوریتم کاهش‌یافته پیشنهاد شده، برای جلوگیری از سقوط سوئیچ‌ها، idle_timer جریان از مقدار پیش فرض به مقدار کاهش یافته تغییر می‌کند. مقدار کاهش‌یافته کمتر از مقدار پیش فرض است. در نتیجه، جریان‌های مخرب کوتاه به سرعت از جداول جریان سوئیچ

حذف می‌شوند. انتظار می‌رود جریان‌های ترافیک مجاز از طرف دیگر انتظار ارتباط بیشتری با تعداد بیشتری از بسته‌ها داشته باشند. اگر مقدار کاهش‌یافته به درستی انتخاب شود، بر روی ورودی‌های جریان مجاز تاثیر قابل‌توجهی نمی‌گذارد و جریان‌های مخرب را سریع پاک می‌کند.

باید به انتخاب مقدار کاهش‌یافته توجه زیادی داشت. اگر مقدار کاهش‌یافته کوتاه‌تر از زمان تعیین شده برای لیست سوئیچ‌های درخواست‌کننده باشد، الگوریتم نوسان خواهد داشت. بنابراین باید همیشه اطمینان داشت که:

ارزش کاهش‌یافته idle_timer بیشتر از تنظیم تایمر برای لیست سوئیچ‌های درخواست‌کننده (در این پژوهش برابر ۱۰ثانیه است) است.

بعد از ارائه الگوریتم پیشنهادی می‌توان آن را به مبحث محاسبات ابری تعمیم داد.

۳-۵- محاسبات ابری وسایل نقلیه

روش محاسبات ابری، بهره‌وری از قدرت محاسباتی مازاد را فراهم کرده است. شمار وسیعی از وسایل نقلیه در خیابان‌ها، جاده‌ها و پارکینگ‌ها به عنوان منابع محاسباتی قرار گرفته‌اند که می‌توانند برای ارائه خدمات عمومی استفاده شوند. همه روزه بسیاری از وسایل نقلیه ساعت‌ها در پارکینگ‌ها و یا جلوی خانه بلااستفاده هستند. وسایل نقلیه پارک شده، یک منبع بهره‌برداری نشده وسیع هستند که در حال حاضر به هدر رفته‌اند. این ویژگی‌ها وسایل نقلیه را کاندیدای خوبی برای گره‌ها در یک شبکه محاسبات ابری می‌سازد. برخی از مسافرانی که با هواپیما به سفر می‌روند خودروهای خود را در پارکینگ‌های فرودگاه‌ها رها می‌کنند. فرودگاه می‌تواند اجازه دسترسی به این منابع محاسباتی (مرکز داده‌ای پارکینگ) را طبق تقاضا صادر کند. به طور مشابه رانندگانی که در ترافیک هستند می‌توانند منابع محاسباتی خود را در اختیار مسوولین ترافیکی شهر قرار دهند تا آن‌ها به منظور حذف ترافیک، شبیه‌سازی پیچیده را از طریق برنامه‌ریزی مجدد چراغ‌های ترافیکی به اجرا درآورند. اخیرا [۴۲] مفهوم ابر وسایل نقلیه[۱] را

[۱] Vehicle Cloud (VC)

مطرح کردند که با منابع در خودروها سروکار دارد. برخی از خودروها که زمان زیادی را بدون استفاده می‌گذرانند می‌توانند به عنوان مشاوران محلی برای حل ترافیک به موقع کمک کنند که این امر به دلیل فقدان منابع محاسباتی کافی برای شهرداری و مراکز مدیریت ترافیک به تنهایی مقدور نیست. این خودروها با اشتراک‌گذاری منابع محاسباتی و ذخیره‌سازی خود می‌توانند بسیاری از مشکلات ایمنی جاده‌ها و ترافیکی را حل کنند که این امر با تشکیل ابر میسر خواهد بود.

یکی از سرویس‌های محاسبات ابری زیرساخت (بستر) به عنوان سرویس است. برای برآورده کردن این زیرساخت نیاز به مجازی‌سازی شبکه می‌باشد. برای تحقق این امر می‌توان از شبکه‌های مبتنی بر نرم‌افزار به عنوان شبکه‌سازی سیستم استفاده نمود تا خودروها به صورت متمرکز از منابع سایر خودروها بهره‌مند شوند.

۳-۶- شبکه های مبتنی بر نرم‌افزار در محاسبات ابری

در واقع SDN یک پلت فرم مورد توجه شبکه های مجازی است و برنامه‌ها می‌توانند خارج از بخش سخت افزاری به ویژه برای آدرس دادن به IP و برای مکانیزم‌های وابسته به شبکه اجرا شوند. هم چنین ممکن است برنامه‌ها احتیاج به دوباره‌نویسی و پیکربندی قبل از استقرار در ابر برای آدرس‌دهی به چندین شبکه مرتبط داشته باشند. تجهیزات شبکه‌ای به صورت استاتیک به شبکه پیکربندی شده متصل هستند که به طور غیر مستقیم یک مکان بدون محدودیت و وابستگی را ایجاد می‌کند. گاهی اوقات برای یک خودرو موقعیتی به وجود می‌آید که باید قادر به کار با چند ارائه‌دهنده ابر با توجه به محل دسترسی ،انتقالات و ادغام باشد. شرکت ابر باید یک ارائه واضحی از حجم کاری بین ابرها دهد. یکی از بسترهایی که برای ارتباطات در ابر از آن استفاده می‌کنند شبکه‌های SDN است. انگیزه اصلی استفاده از این معماری در استفاده از ابر، وجود توپولوژی مرکز داده‌ای و امکانات ارسال بسته از میان کوتاه‌ترین مسیر بین سرورها برای کاهش زمان تاخیر به نسبت مسیرهای اصلی است. مزیت جداسازی

بخش داده از بخش کنترل در شبکه‌های مبتنی بر نرم‌افزارکه قبلا به عنوان سخت‌افزاری در شبکه مورد استفاده قرار می‌گرفت، به منابع محاسباتی دردسترس این امکان را می دهد که زیر ساخت هایی برای برنامه‌ها و سرویس‌های شبکه انتزاعی داشته باشند. مزایای زیادی برای شرکت‌هایی که شبکه‌های SDN را به عنوان یک زیر ساخت ارتباطی برای اتصال به ابر خصوصی در نظر می‌گیرند وجود دارد که از جمله آنها می‌توان ارائه یک منطق متمرکز شده در سطح کنترل SDN، یک دید جامع از منابع ابر و قابل دسترس بودن را نام برد.

از جمله مزایای این روش می توان به موارد زیر اشاره داشت :

- OpenFlowرا قادر می‌سازد که گره‌های سازنده و اصلی را به شرکت و مراکز ارائه‌دهنده ابر متصل کند.

- OpenFlow را قادر می‌سازد که ترافیک بین گره‌های اصلی را سوئیچ کند.

- OpenFlow و یا شبکه مبتنی بر نرم‌افزار را قادر به پیکربندی جدول‌های جریان درون گره‌های اصلی ابر و فراهم آوردن یک برنامه مجازی شبکه wan می‌کند.

- این روش در شبکه‌های موردی باعث دسترسی اتوماتیک به پهنای باند برای انتقال به موقع حجم کاری مرکز داده و پردازش خواهد شد.

فصل چهارم

جزئیات پیکربندی و ارزیابی روش پیشنهادی

۴-۱- مقدمه

در این فصل سعی شده است با در نظر گرفتن معیارهای آنتروپی، نرخ شروع جریان و خصوصیات جریان الگوریتم تشخیص حمله DDOS در شبکه‌های SDN در [۲۳] بهبود داده شود. همان طور که اشاره شد معیار آنتروپی به تنهایی نمی‌تواند در شناسایی حمله به چندین قربانی موثر باشد. بنابراین نتایج حاصل از این معیار برای تشخیص در این فصل ذکر شده است. سپس با مطرح نمودن ابزار شبیه‌سازی و پیاده‌سازی شبکه با پارامترهای مختلف در ترافیک مجاز و حمله نتایجی به دست آمده است که در ادامه شرح داده شده‌اند. همچنین این نتایج مورد تجزیه و تحلیل قرار می‌گیرند تا از عملکرد الگوریتم بهبودیافته اطمینان حاصل شود.

۴-۲- شبیه‌سازی و نتایج

شبیه‌سازی و آزمایش روش پیشنهادی برای تشخیص حمله DDOS به قسمت‌های زیر تقسیم شده است. الگوریتم با کنترل‌کننده POX مبتنی بر زبان برنامه‌نویسی پایتون در محیط شبکه مجازی Mininet پیاده‌سازی می‌شود. اسکریپت‌های scapy برای تولید ترافیک‌های مجاز و حمله روی میزبان‌های شبکه در طول شبیه‌سازی مورد استفاده قرار می‌گیرد. در واقع scapy اجازه کار با بسته‌های تحت شبکه و دسترسی کامل به فیلدهای هر لایه را می‌دهد.

۴-۲-۱- Mininet

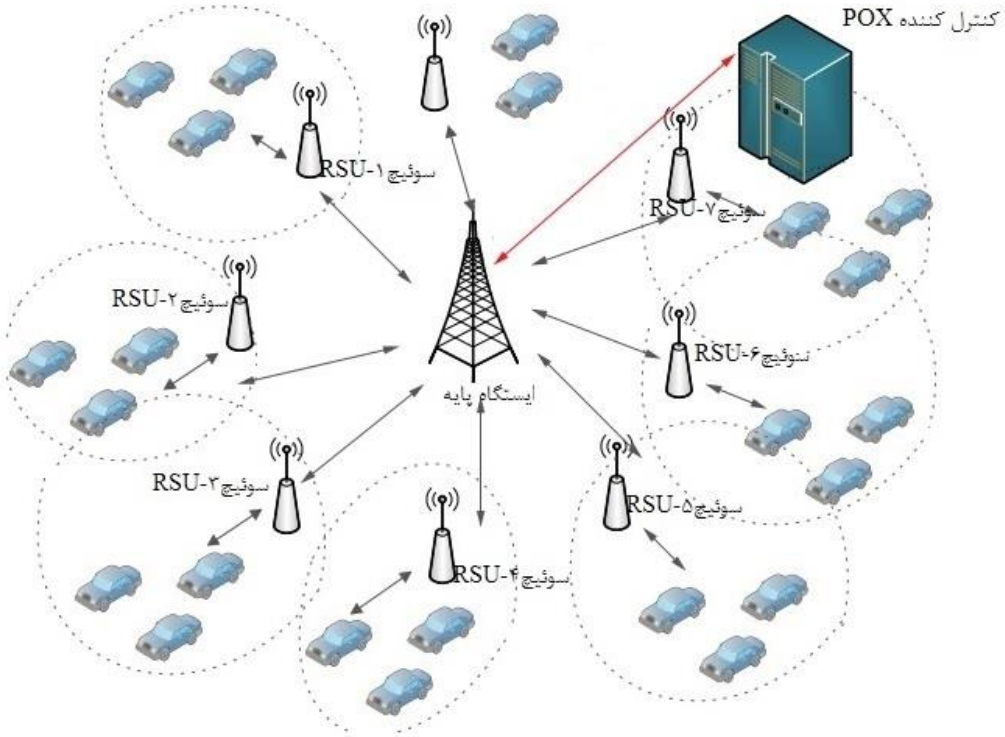
ابزاری برای شبیه‌سازی شبکه‌های SDN است. این ابزار اجازه می‌دهد تا توپولوژی‌های شبکه به صورت پارامتریک مشخص شود.

۴-۲-۲- تولید ترافیک

ابزار مورد استفاده در این پژوهش برای تولید هر دو ترافیک مجاز و حمله، scapy است. scapy یک برنامه دستکاری بسته است. این ابزار می‌تواند بسته‌های فراوانی از پروتکل‌ها را جعل یا رمزگشایی کند، آن‌ها را در شبکه ارسال کند، حملات را شبیه‌سازی کند، درخواست‌ها و پاسخ‌ها را تطابق دهد.

۴-۲-۳- سناریوهای شبیه‌سازی و نتایج

شبیه‌سازی بر روی لب‌تاپ hp با مشخصات Intel (R) Core (TM) i5-6200U CPU , 2.30 GHz , 8.00 GB RAM انجام شده است و ساختار شبکه برای شبیه‌سازی فعلی یک شبکه از نوع درخت با عمق دو، fanout برابر با ۸ که ایجاد ۶۴ میزبان می‌کند. ساختار درختی بر این اساس انتخاب شده است که ساختار شبکه به طور گسترده در مراکز داده، این‌گونه مورد استفاده قرار می‌گیرند. سوئیچ‌های استفاده شده در شبکه، سوئیچ‌های Open Virtual[۱] است.



شکل (۴-۱): توپولوژی مورد بحث در روش پیشنهادی

در مرحله اول نتایج برای ناکافی بودن معیار آنتروپی جهت تشخیص حمله DDOS شرح می‌داده می‌شود. معیار آنتروپی برای زمانی که حمله به یک میزبان در نظر گرفته می‌شود دارای تغییر چشمگیری است. اما زمانی‌که حمله به چندین میزبان در نظر گرفته می‌شود میزان آنتروپی دچار تغییر چشمگیری

[۱] Open Virtual Switch (OVS)

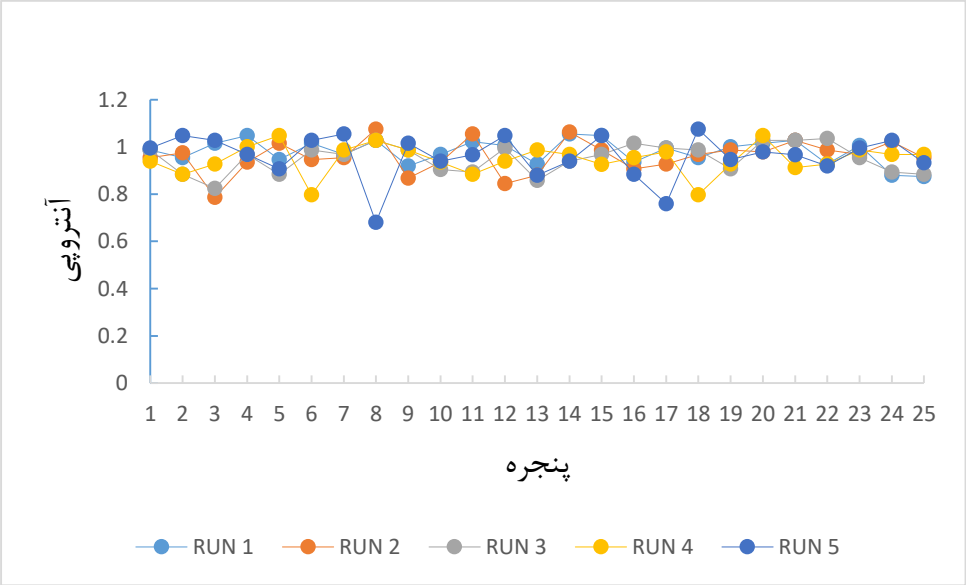
نمی‌شود زیرا ارسال بسته‌ها بین چندین میزبان توزیع می‌شود و قاعدتا میزان آنتروپی کاهش زیادی نخواهد داشت و بسیار مشابه آنتروپی در ترافیک مجاز است. جهت اثبات نمودن ناکافی بودن معیار آنتروپی، ترافیک مجاز و حمله به یک میزبان و چندین (در اینجا ۶) میزبان را در کل شبکه بین میزبان‌ها و سوئیچ‌ها راه‌اندازی می‌شود تا بتوان یک حدآستانه قابل قبول به دست آورد. برای این کار ۵ اجرا انجام شده است، هر یک از آنها شامل ۷۵۰ بسته در اندازه پنجره برابر با ۳۰ است. فاصله ترافیکی مجاز شبکه ۰/۱ ثانیه است. این آزمایش، مشاهده ۳۷۵۰ بسته را پوشش می دهد.

طبق جدول میانگین کل آنتروپی برای ترافیک مجاز برابر با ۰/۹۶ است و محدوده تغییر آنتروپی در این ۵ اجرا بین ۰/۶۸ و ۱/۰۷ است.

جدول (۴-۱): میانگین آنتروپی برای ترافیک مجاز با فاصله ترافیکی ۰/۱ ثانیه

آنتروپی	RUN ۱	RUN ۲	RUN ۳	RUN ۴	RUN ۵
پنجره شماره۱	۰/۹۸۷۵	۰/۹۵۴۹	۰/۹۸۷۵	۰/۹۳۹۷	۰/۹۹۵۰
پنجره شماره۲	۰/۹۵۴۹	۰/۹۷۵۰	۰/۸۸۴۵	۰/۸۸۴۵	۱/۰۴۷۷
پنجره شماره۳	۱/۰۱۵۱	۰/۷۸۶۸	۰/۸۲۴۳	۰/۹۲۷۳	۱/۰۲۷۶
پنجره شماره۴	۱/۰۴۷۷	۰/۹۳۴۸	۰/۹۶۷۴	۱	۰/۹۶۷۴
پنجره شماره۵	۰/۹۴۶۳	۱/۰۱۵۱	۰/۸۸۴۵	۱/۰۴۷۷	۰/۹۰۷۲
پنجره شماره۶	۱/۰۱۵۱	۰/۹۴۶۳	۰/۹۸۷۵	۰/۷۹۶۶	۱/۰۲۷۶
پنجره شماره۷	۰/۹۶۷۴	۰/۹۵۴۹	۰/۹۶۷۴	۰/۹۸۷۵	۱/۰۵۵۲
پنجره شماره۸	۱/۰۲۷۶	۱/۰۷۵۳	۱/۰۲۷۶	۱/۰۲۷۶	۰/۶۸۱۱
پنجره شماره۹	۰/۹۱۸۷	۰/۸۶۷۰	۰/۹۸۷۵	۰/۹۸۷۵	۱/۰۱۵۱
پنجره شماره۱۰	۰/۹۶۷۴	۰/۹۳۴۸	۰/۹۰۴۵	۰/۹۳۴۸	۰/۹۳۷۹
پنجره شماره۱۱	۱/۰۲۲۷	۱/۰۵۵۲	۰/۸۹۳۳	۰/۸۸۴۵	۰/۹۶۶۴
پنجره شماره۱۲	۱/۰۰۶۵	۰/۸۴۴۳	۰/۹۹۵۰	۰/۹۳۷۹	۱/۰۴۷۷
پنجره شماره۱۳	۰/۹۲۷۳	۰/۸۷۹۵	۰/۸۵۸۵	۰/۹۸۷۵	۰/۸۷۹۵
پنجره شماره۱۴	۱/۰۵۵۲	۱/۰۶۲۸	۰/۹۳۷۹	۰/۹۶۷۴	۰/۹۳۷۹
پنجره شماره۱۵	۱/۰۴۷۷	۰/۹۸۷۵	۰/۹۶۷۴	۰/۹۲۶۲	۱/۰۴۷۷
پنجره شماره۱۶	۰/۹۳۴۸	۰/۹۰۷۲	۱/۰۱۵۱	۰/۹۵۴۹	۰/۸۸۴۵
پنجره شماره۱۷	۰/۹۹۵۰	۰/۹۲۷۳	۰/۹۹۵۰	۰/۹۷۸۹	۰/۷۵۹۱

پنجره شماره۱۸	۰/۹۵۴۹	۰/۹۶۷۴	۰/۹۸۷۵	۰/۷۹۶۶	۱/۰۷۵۳
پنجره شماره۱۹	۱	۰/۹۸۷۵	۰/۹۰۷۲	۰/۹۲۷۳	۰/۹۴۶۳
پنجره شماره۲۰	۱/۰۱۵۱	۰/۹۷۸۹	۱/۰۲۷۶	۱/۰۴۷۷	۰/۹۷۸۹
پنجره شماره۲۱	۱/۰۲۷۶	۱/۰۲۷۶	۱/۰۲۷۶	۰/۹۱۲۱	۰/۹۶۶۴
پنجره شماره۲۲	۰/۹۲۷۳	۰/۹۸۷۵	۱/۰۳۵۲	۰/۹۲۷۳	۰/۹۱۸۷
پنجره شماره۲۳	۱/۰۰۶۵	۰/۹۶۷۴	۰/۹۵۴۹	۰/۹۸۷۵	۰/۹۹۵۰
پنجره شماره۲۴	۰/۸۷۹۵	۱/۰۲۲۷	۰/۸۹۳۳	۰/۹۶۷۴	۱/۰۲۷۶
پنجره شماره۲۵	۰/۸۷۴۶	۰/۹۵۴۵	۰/۸۸۳۵	۰/۹۶۷۴	۰/۹۳۲۲
میانگین	۰/۹۸۰۹	۰/۹۵۴۹	۰/۹۵۲۱	۰/۹۴۸۲	۰/۹۶۱۱
میانگین کل			۰/۹۶۰۵		

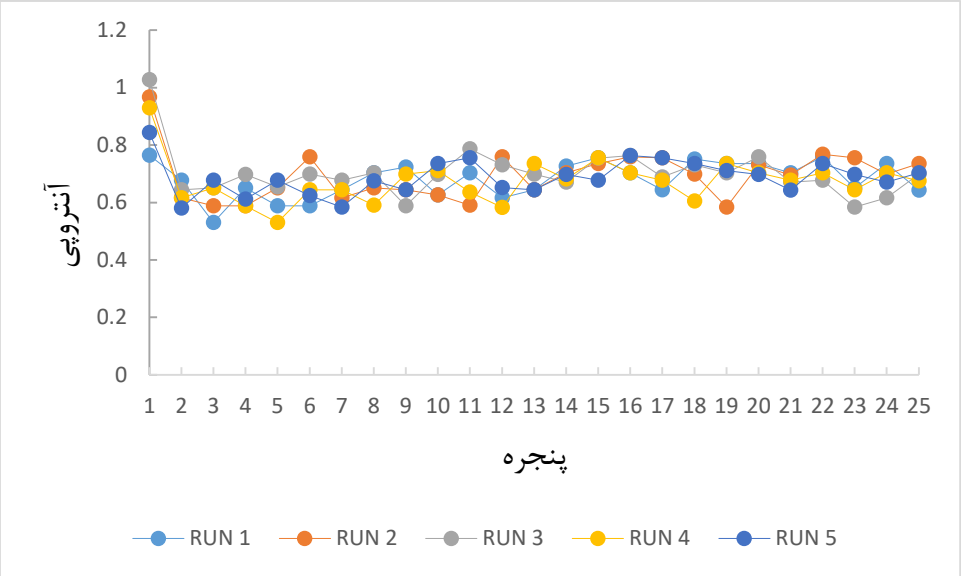


شکل (۴-۲) میانگین آنتروپی برای ترافیک مجاز با فاصله ترافیکی ۰/۱ ثانیه

جدول (۴-۱) نتایج حاصل از محاسبه آنتروپی در ترافیک مجاز با فاصله ترافیکی ۰/۱ ثانیه است. جهت بررسی تغییرات آنتروپی، یک میزبان در شبکه مورد حمله قرار می‌گیرد. چون فواصل ترافیک حمله کوتاه است بنابراین تغییرات آنتروپی با فاصله ترافیکی ۰/۰۳ و ۰/۰۵ ثانیه به ترتیب برابر با جداول (۴-۲) و (۴-۳) و شکل‌های (۴-۳) و (۴-۴) است.

جدول (۴-۲): میانگین آنتروپی برای ترافیک حمله به یک میزبان با فاصله ترافیکی ۰/۰۳ ثانیه

آنتروپی	RUN ۱	RUN ۲	RUN ۳	RUN ۴	RUN ۵
پنجره شماره۱	۰/۷۶۴۷	۰/۹۶۷۴	۱/۰۲۷۶	۰/۹۲۹۹	۰/۸۴۴۳
پنجره شماره۲	۰/۶۷۸۱	۰/۶۱۶۶	۰/۶۴۴۰	۰/۶۱۶۶	۰/۵۸۰۸
پنجره شماره۳	۰/۵۳۰۱	۰/۵۸۹۰	۰/۶۵۰۵	۰/۶۵۰۵	۰/۶۷۸۱
پنجره شماره۴	۰/۶۵۰۵	۰/۵۸۹۰	۰/۶۹۸۲	۰/۵۸۹۰	۰/۶۱۱۵
پنجره شماره۵	۰/۵۸۹۰	۰/۶۵۰۵	۰/۶۵۴۵	۰/۵۳۰۱	۰/۶۷۸۱
پنجره شماره۶	۰/۵۸۹۰	۰/۷۵۹۱	۰/۶۹۷۸	۰/۶۴۴۰	۰/۶۲۴۰
پنجره شماره۷	۰/۶۴۴۰	۰/۶۱۶۶	۰/۶۷۸۱	۰/۶۴۴۰	۰/۵۸۳۸
پنجره شماره۸	۰/۷۰۳۷	۰/۶۵۰۵	۰/۷۰۳۷	۰/۵۹۰۳	۰/۶۷۵۵
پنجره شماره۹	۰/۷۲۳۲	۰/۶۴۴۰	۰/۵۸۹۰	۰/۶۹۸۹	۰/۶۴۴۰
پنجره شماره۱۰	۰/۶۲۶۸	۰/۶۲۶۸	۰/۶۹۸۲	۰/۷۱۱۲	۰/۷۳۵۷
پنجره شماره۱۱	۰/۷۰۳۷	۰/۵۹۰۳	۰/۷۸۶۸	۰/۶۳۶۷	۰/۷۵۵۸
پنجره شماره۱۲	۰/۶۱۶۶	۰/۷۵۹۱	۰/۷۳۱۳	۰/۵۸۳۲	۰/۶۵۱۶
پنجره شماره۱۳	۰/۶۴۴۳	۰/۶۴۴۰	۰/۶۹۸۹	۰/۷۳۵۷	۰/۶۴۴۰
پنجره شماره۱۴	۰/۷۲۶۶	۰/۷۰۳۷	۰/۶۷۱۱	۰/۶۸۲۶	۰/۶۹۸۲
پنجره شماره۱۵	۰/۷۵۵۸	۰/۷۳۵۷	۰/۷۵۴۲	۰/۷۵۵۸	۰/۶۷۸۱
پنجره شماره۱۶	۰/۷۰۳۷	۰/۷۵۹۱	۰/۷۶۳۴	۰/۷۰۳۷	۰/۷۶۳۴
پنجره شماره۱۷	۰/۶۴۴۰	۰/۷۵۵۸	۰/۶۸۸۵	۰/۶۷۸۱	۰/۷۵۵۸
پنجره شماره۱۸	۰/۷۵۱۴	۰/۶۹۸۹	۰/۷۳۱۳	۰/۶۰۵۴	۰/۷۳۵۷
پنجره شماره۱۹	۰/۷۳۵۷	۰/۵۸۳۸	۰/۷۰۳۷	۰/۷۳۵۷	۰/۷۱۱۲
پنجره شماره۲۰	۰/۷۳۵۷	۰/۷۳۱۳	۰/۷۵۹۱	۰/۷۰۳۷	۰/۶۹۸۲
پنجره شماره۲۱	۰/۷۰۳۲	۰/۶۹۵۶	۰/۶۷۱۱	۰/۶۷۸۱	۰/۶۴۳۴
پنجره شماره۲۲	۰/۷۵۹۱	۰/۷۶۷۸	۰/۶۷۸۱	۰/۷۰۳۷	۰/۷۳۵۷
پنجره شماره۲۳	۰/۶۵۰۵	۰/۷۵۵۸	۰/۵۸۳۸	۰/۶۴۴۰	۰/۶۹۸۲
پنجره شماره۲۴	۰/۷۳۵۷	۰/۶۹۸۹	۰/۶۱۶۶	۰/۷۰۳۷	۰/۶۷۱۱
پنجره شماره۲۵	۰/۶۴۳۴	۰/۷۳۵۷	۰/۶۹۸۹	۰/۶۷۵۵	۰/۷۰۳۷
میانگین	۰/۶۸۰۴	۰/۶۹۳۰	۰/۷۰۳۲	۰/۶۷۳۲	۰/۶۸۸۰
میانگین کل			۰/۶۸۷۵		



شکل (۴-۳): میانگین آنتروپی برای ترافیک حمله به یک میزبان با فاصله ترافیکی ۰/۰۳ ثانیه

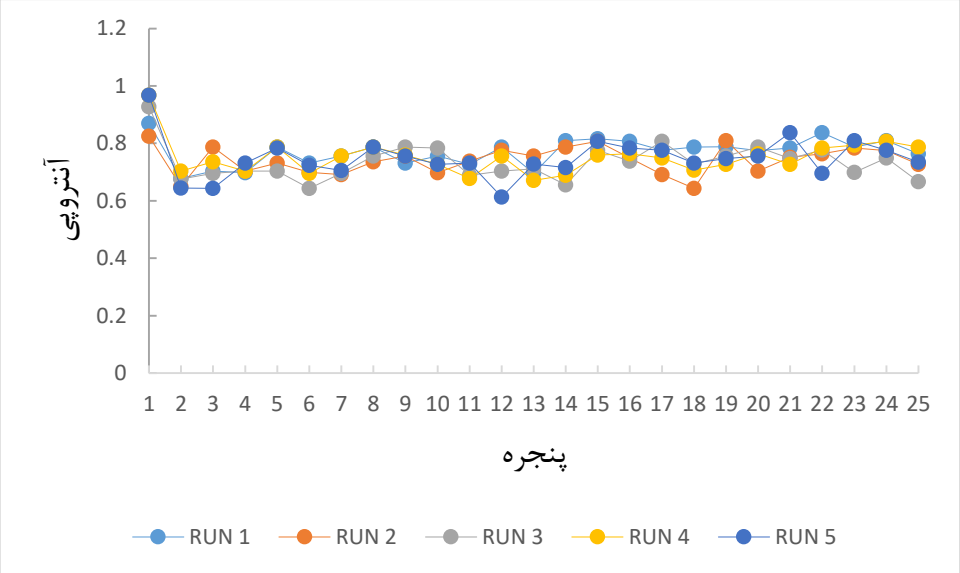
همان طور که مشاهده می‌شود محدوده تغییر آنتروپی در ۵ اجرا زمانی که یک میزبان با فاصله ترافیکی ۰/۰۳ثانیه مورد حمله قرار می‌گیرد بین ۰/۵۳ تا ۰/۷۸ است و میانگین کل آنتروپی برابر با ۰/۶۸ می‌باشد و با کاهش آنتروپی مواجه شده است.

زمانی که یک میزبان با فاصله ترافیکی ۰/۰۵ ثانیه مورد حمله قرار می‌گیرد نتایج برابر با جدول (۴-۲) خواهد بود.

جدول (۴-۳): میانگین آنتروپی برای ترافیک حمله به یک میزبان با فاصله ترافیکی ۰/۰۵ ثانیه

آنتروپی	RUN ۱	RUN ۲	RUN ۳	RUN ۴	RUN ۵
پنجره شماره۱	۰/۸۶۹۷	۰/۸۲۵۵	۰/۹۲۷۳	۰/۹۶۷۴	۰/۹۶۷۴
پنجره شماره۲	۰/۶۷۸۱	۰/۶۵۰۵	۰/۶۷۵۵	۰/۷۰۳۷	۰/۶۴۰
پنجره شماره۳	۰/۷۰۳۷	۰/۷۸۶۸	۰/۶۹۵۶	۰/۷۳۵۷	۰/۶۴۳۴
پنجره شماره۴	۰/۶۹۸۲	۰/۷۰۳۷	۰/۷۰۳۷	۰/۷۰۳۷	۰/۷۳۱۳
پنجره شماره۵	۰/۷۸۶۸	۰/۷۳۱۳	۰/۷۰۳۷	۰/۷۸۶۸	۰/۷۸۳۴
پنجره شماره۶	۰/۷۳۱۳	۰/۶۹۸۷	۰/۶۴۳۶	۰/۶۹۵۶	۰/۷۲۳۲
پنجره شماره۷	۰/۷۵۵۸	۰/۶۹۱۷	۰/۶۹۵۶	۰/۷۵۵۸	۰/۷۰۵۸
پنجره شماره۸	۰/۷۸۶۸	۰/۷۳۵۷	۰/۷۵۵۸	۰/۷۸۶۸	۰/۷۸۶۸
پنجره شماره۹	۰/۷۳۱۳	۰/۷۵۵۸	۰/۷۸۶۸	۰/۷۵۹۱	۰/۷۵۵۸
پنجره شماره۱۰	۰/۷۵۵۸	۰/۶۹۸۲	۰/۷۸۳۴	۰/۷۲۶۶	۰/۷۲۶۶

پنجره شماره۱۱	۰/۷۲۶۶	۰/۷۳۸۱	۰/۶۸۸۵	۰/۶۷۸۱	۰/۷۳۱۳
پنجره شماره۱۲	۰/۷۸۶۸	۰/۷۷۶۴	۰/۷۰۳۷	۰/۷۵۵۸	۰/۶۱۲۷
پنجره شماره۱۳	۰/۶۹۵۶	۰/۷۵۵۸	۰/۷۱۱۲	۰/۶۷۱۱	۰/۷۲۵۸
پنجره شماره۱۴	۰/۸۰۹۰	۰/۷۸۶۸	۰/۶۵۶۰	۰/۶۸۸۵	۰/۷۱۶۸
پنجره شماره۱۵	۰/۸۱۶۵	۰/۸۰۶۸	۰/۷۷۶۴	۰/۷۵۹۱	۰/۸۰۶۸
پنجره شماره۱۶	۰/۸۰۶۸	۰/۸۴۸۷	۰/۷۳۸۱	۰/۷۶۳۴	۰/۷۸۳۴
پنجره شماره۱۷	۰/۷۷۶۴	۰/۶۹۱۲	۰/۸۰۶۸	۰/۷۴۸۷	۰/۷۷۶۴
پنجره شماره۱۸	۰/۷۸۶۸	۰/۶۴۳۴	۰/۷۲۸۵	۰/۷۰۷۲	۰/۷۳۱۳
پنجره شماره۱۹	۰/۷۸۸۷	۰/۸۰۹۰	۰/۷۵۵۸	۰/۷۲۶۴	۰/۷۴۶۶
پنجره شماره۲۰	۰/۷۷۴۳	۰/۷۰۳۲	۰/۷۸۶۸	۰/۷۶۳۴	۰/۷۵۵۵
پنجره شماره۲۱	۰/۷۸۳۴	۰/۷۵۱۴	۰/۷۴۶۶	۰/۷۲۶۶	۰/۸۳۷۴
پنجره شماره۲۲	۰/۸۳۷۴	۰/۷۶۳۴	۰/۷۷۷۲	۰/۷۸۳۴	۰/۶۹۵۶
پنجره شماره۲۳	۰/۷۸۶۸	۰/۷۸۳۴	۰/۶۹۸۹	۰/۷۹۴۳	۰/۸۰۹۰
پنجره شماره۲۴	۰/۸۰۹۰	۰/۷۷۴۳	۰/۷۴۸۷	۰/۸۰۶۸	۰/۷۷۶۴
پنجره شماره۲۵	۰/۷۶۳۴	۰/۷۲۶۶	۰/۶۶۶۴	۰/۷۸۶۸	۰/۷۳۴۷
میانگین	۰/۷۶۹۸	۰/۷۴۱۴	۰/۷۳۴۴	۰/۷۵۱۲	۰/۷۴۸۴
میانگین کل			۰/۷۴۹۱		



شکل (۴-۴): میانگین آنتروپی برای ترافیک حمله به یک میزبان با فاصله ترافیکی ۰/۰۵ ثانیه

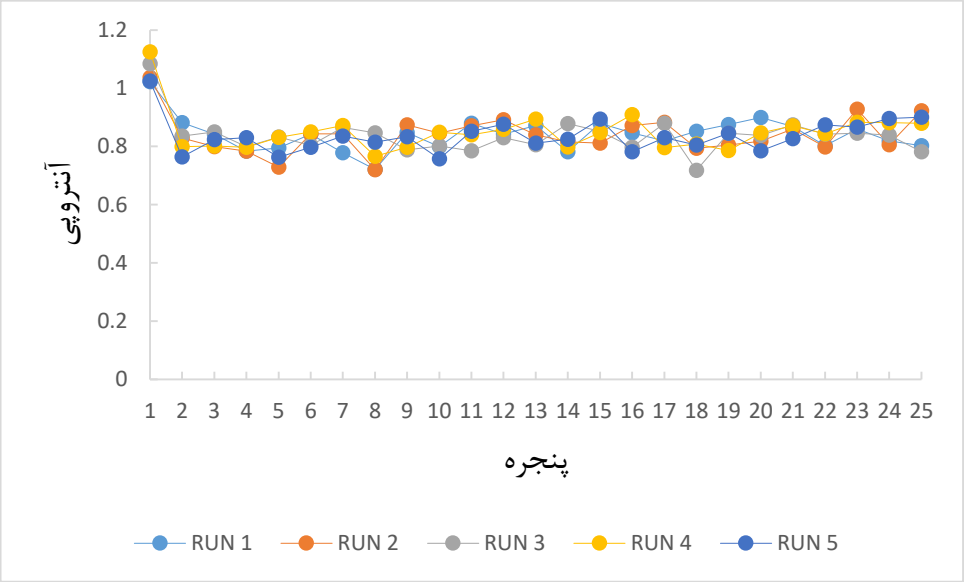
با توجه به جدول (۴-۳) و شکل (۴-۴) محدوده تغییر آنتروپی در ۵ اجرا، زمانی که یک میزبان با فاصله ترافیکی ۰/۰۵ ثانیه مورد حمله قرار می‌گیرد بین ۰/۶۱ تا ۰/۸۴ می‌باشد و میانگین کل آنتروپی برابر با ۰/۷۴ است و با کاهش آنتروپی مواجه شده است.

برای بررسی نقطه ضعف معیار آنتروپی، حمله را بر روی ۶ میزبان متصل به یک سوئیچ در نظر گرفته می‌شود. زمانی که ۶ میزبان مورد حمله قرار می‌گیرد، تغییرات آنتروپی با فاصله ترافیکی ۰/۰۵ ثانیه برابر با جدول (۴-۴) و شکل (۴-۵) خواهد بود.

جدول (۴-۴): میانگین آنتروپی برای ترافیک حمله به ۶ میزبان با فاصله ترافیکی ۰/۰۵ ثانیه

آنتروپی	RUN ۱	RUN ۲	RUN ۳	RUN ۴	RUN ۵
پنجره شماره۱	۱/۰۲۲۹	۱/۰۳۶۸	۱/۰۸۴۵	۱/۱۲۴۷	۱/۰۲۵۳
پنجره شماره۲	۰/۸۸۲۲	۰/۸۲۹۶	۰/۸۳۶۱	۰/۷۹۹۱	۰/۷۶۴۴
پنجره شماره۳	۰/۸۴۲۷	۰/۷۹۹۱	۰/۸۵۰۱	۰/۸۰۲۰	۰/۸۲۳۵
پنجره شماره۴	۰/۷۸۴۳	۰/۷۸۴۱	۰/۷۹۹۹	۰/۷۹۷۳	۰/۷۲۹۸
پنجره شماره۵	۰/۷۹۴۶	۰/۷۲۹۳	۰/۸۳۲۱	۰/۸۳۱۶	۰/۷۶۲۹
پنجره شماره۶	۰/۸۴۲۷	۰/۸۴۳۵	۰/۸۰۳۶	۰/۸۵۰۱	۰/۷۹۶۸
پنجره شماره۷	۰/۷۷۸۴	۰/۸۴۳۵	۰/۸۶۵۹	۰/۸۷۱۶	۰/۸۳۵۷
پنجره شماره۸	۰/۷۲۱۵	۰/۷۲۰۲	۰/۸۴۷۲	۰/۷۶۶۹	۰/۸۱۴۸
پنجره شماره۹	۰/۸۴۸۲	۰/۸۷۴۴	۰/۷۸۸۴	۰/۷۹۷۰	۰/۸۳۳۵
پنجره شماره۱۰	۰/۷۹۹۱	۰/۸۴۶۰	۰/۷۰۱۹	۰/۸۴۸۶	۰/۷۵۸۱
پنجره شماره۱۱	۰/۸۷۹۸	۰/۸۷۱۲	۰/۷۸۵۳	۰/۸۴۰۶	۰/۸۵۲۱
پنجره شماره۱۲	۰/۸۴۲۳	۰/۸۹۱۷	۰/۸۲۹۸	۰/۸۵۸۴	۰/۸۷۶۵
پنجره شماره۱۳	۰/۸۷۲۴	۰/۸۴۰۶	۰/۸۰۵۶	۰/۸۹۳۵	۰/۸۱۱۸
پنجره شماره۱۴	۰/۷۸۱۸	۰/۸۱۵۶	۰/۸۷۸۹	۰/۷۹۸۷	۰/۸۲۴۶
پنجره شماره۱۵	۰/۸۷۹۸	۰/۸۱۲۰	۰/۸۵۲۵	۰/۸۴۸۲	۰/۸۹۳۷
پنجره شماره۱۶	۰/۸۴۷۲	۰/۸۷۲۴	۰/۷۹۷۷	۰/۹۰۹۸	۰/۷۸۱۹
پنجره شماره۱۷	۰/۸۱۹۰	۰/۸۸۲۷	۰/۸۷۹۸	۰/۷۹۵۶	۰/۸۳۰۴
پنجره شماره۱۸	۰/۸۵۲۵	۰/۷۹۳۶	۰/۷۱۸۶	۰/۸۰۸۵	۰/۸۰۴۴
پنجره شماره۱۹	۰/۸۷۵۳	۰/۸۰۴۴	۰/۸۴۶۰	۰/۷۸۶۴	۰/۸۴۶۰
پنجره شماره۲۰	۰/۹۰۰۰	۰/۸۱۸۳	۰/۸۳۸۲	۰/۸۴۷۲	۰/۷۸۵۲

پنجره شماره۲۱	۰/۸۶۸۳	۰/۸۵۹۵	۰/۸۷۴۴	۰/۸۷۰۸	۰/۸۲۶۷
پنجره شماره۲۲	۰/۸۰۲۲	۰/۷۹۸۵	۰/۸۴۲۳	۰/۸۴۳۵	۰/۸۷۴۴
پنجره شماره۲۳	۰/۸۵۹۷	۰/۹۲۷۹	۰/۸۴۵۶	۰/۸۸۲۷	۰/۸۶۶۳
پنجره شماره۲۴	۰/۸۱۹۷	۰/۸۰۵۶	۰/۸۳۱۹	۰/۸۸۱۸	۰/۸۹۶۱
پنجره شماره۲۵	۰/۸۰۲۳	۰/۹۲۲۶	۰/۷۸۱۲	۰/۸۷۹۸	۰/۹۰۰۱
میانگین	۰/۸۶۲۴	۰/۸۷۰۹	۰/۸۶۷۰	۰/۸۷۵۲	۰/۸۶۶۲
میانگین کل			۰/۸۸۷۴		



شکل (۴-۵): میانگین آنتروپی برای ترافیک حمله به ۶ میزبان با فاصله ترافیکی ۰/۰۵ ثانیه

با توجه به جدول (۴-۴) و شکل (۴-۵) محدوده تغییر آنتروپی در زمانی که ۶ میزبان با فاصله ترافیکی ۰/۰۵ ثانیه مورد حمله قرار می‌گیرد بین ۰/۷۲ تا ۱/۱۲ و میانگین کل آنتروپی برابر با ۰/۸۸ می‌باشد.

میانگین آنتروپی به دست آمده برای ۶ میزبان مورد حمله برابر با ۰/۸۸ است که این مقدار فقط ۰/۰۷ کمتر از آنتروپی در ترافیک مجاز است. بنابراین زمانی که یک زیرشبکه مورد حمله قرار می‌گیرد تشخیص حمله بسیار سخت است. برای اجتناب از این امر که هدف و نوآوری این پژوهش است؛ نرخ شروع جریان و خصوصیات جریان مورد تجزیه و تحلیل قرار می‌گیرند.

در بخش ۴-۲-۴، نگاهی کلی به رفتار الگوریتم در تشخیص حملات تحت انواع الگوهای ترافیکی مجاز دارد. جهت بهبود الگوریتم تشخیص، سه الگوی ترافیکی برای ترافیک مجاز مورد آزمایش قرار می‌گیردو رفتارهای الگوریتم تحت بارهای ترافیکی مختلف مشاهده می‌شود. در بخش ۴-۲-۵، تجزیه و تحلیل دقیق‌تر درباره چگونگی اثبات الگوریتم در شناسایی دقیق مسیرهای حمله انجام می‌شود. در بخش ۴-۲-۶، یک بررسی و ارزیابی بر روی عملکرد تشخیص الگوریتم با انواع جریان‌های مجاز و حمله انجام می‌شود.

۴-۲-۴- تشخیص‌های FP و FN حمله

در این بخش الگوریتم تحت سه الگوی ترافیک متفاوت اجرا می‌شود و در هر مورد، میزان تشخیص FP و FN محاسبه می‌شود. سه ترافیک متفاوت تحت دو نوع حمله قرار می‌گیرند: حمله به یک میزبان (قربانی) و حمله به چندین میزبان. ویژگی‌های هر ترافیک به شرح زیر است:

الگوی ترافیکی A:

در این الگوی ترافیکی، مشخصه‌های پارامترهای ترافیکی مجاز و حمله وجود دارد. ترافیک‌های مجاز به عنوان ترافیک با جریان‌های طولانی مدت، تعداد زیادی از بسته‌ها و بایت‌ها تعریف می‌شود. در حالی که ترافیک حمله با جریان‌های کوتاه مدت و تعداد کمی از بسته‌ها و بدون payload است. جدول (۴-۵) مشخصات ترافیکی را در هر سناریوی ترافیک مجاز و حمله را بیان می‌کند.

جدول (۴-۵): مشخصات ترافیک مجاز

نوع بسته	UDP
بسته Payload	۲۶ Bytes
تعداد بسته‌های فرستاده شده	۸
فاصله ترافیکی	۰/۲ ثانیه
نرخ ترافیک	۵ بسته/ثانیه
نرخ جریان	۰/۶ جریان/ثانیه

جدول (۴-۶): مشخصات ترافیک حمله به یک میزبان

نوع بسته	UDP
Payload بسته	-
تعداد بسته‌های فرستاده شده	۲
فاصله ترافیکی	۰/۰۸ ثانیه
نرخ ترافیک	۱۲/۵ بسته/ثانیه
نرخ جریان	۶/۲۵ جریان/ثانیه

جدول (۴-۷): مشخصات ترافیک حمله به چندین میزبان

نوع بسته	UDP
Payload بسته	-
تعداد بسته‌های فرستاده شده	۲
فاصله ترافیکی	۰/۰۳ ثانیه
نرخ ترافیک	۳۳/۳ بسته/ثانیه
نرخ جریان	۱۶/۶۵جریان/ثانیه

برای اندازه‌گیری میزان حمله وارده به شبکه، نسبت ترافیک حمله این گونه تعریف می‌شود: نسبت نرخ ترافیک حمله به نرخ ترافیک کل شبکه است. از آنجایی که بررسی نتایج حاصل از ۶۴ گره زمان‌بر است، منابع مورد بحث ۲۵ در نظر گرفته می‌شود که قابل تعمیم به ۶۴ گره است.

تعداد کل منابع ترافیکی در این شبیه‌سازی روی ۲۵ تنظیم شده است و با n مهاجم. بنابراین تعداد منابع ترافیکی مجاز برابر با n -۲۵ است. در حمله به یک میزبان زمانی که یک میزبان ترافیک حمله را با نرخ ترافیک ۱۲/۵ بسته/ثانیه ارسال می‌کند، ۲۴ میزبان دیگر در حال ارسال ترافیک مجاز با نرخ ترافیکی ۵ بسته/ثانیه است که منتج به نسبت ترافیکی حمله ۹/۴ ٪ می‌شود. اگر حمله با دو میزبان رخ دهد نسبت ترافیک حمله برابر با ۱۷ ٪ است و با سه میزبان برابر با ۲۵ ٪ و با چهار میزبان برابر با ۳۲ ٪ است.

در سناریوی حمله به چندین میزبان با فاصله ترافیکی ۰/۰۳، اگر یک میزبان با ارسال حدود ۳۳/۳ بسته در هر ثانیه ترافیک حمله و ۲۴ میزبان دیگر با ارسال ۵ بسته/ثانیه ترافیک مجاز تولید کند (تعداد میزبان‌های مورد حمله در اینجا ۴ مقصد مختلف می‌باشد) نسبت ترافیک حمله ۲۱ ٪ و اگر دو میزبان به ۸ میزبان دیگر با ارسال ۳۳/۳ بسته در هر ثانیه ترافیک حمله تولید کند، نسبت ترافیک حمله برابر با ۳۶ ٪ و اگر سه میزبان به ۱۲ میزبان مختلف باشد نسبت ترافیک حمله برابر با ۴۷/۵ ٪ است.

الگوی ترافیکی B:

در این الگوی ترافیکی، تفاوت مشخصه‌های پارامترهای ترافیکی حمله و مجاز کمتر است. ترافیک مجاز در این الگو نسبت به الگوی ترافیکی A به عنوان ترافیک با نرخ جریان بیشتر، تعداد بسته‌های کمتر اما حجم زیاد تعریف می‌شود. در حالی که ترافیک حمله دارای طول جریان کوتاه با تعداد بسته‌های کوچک و بدون payload تعریف می‌شود.

جدول (۴-۸): مشخصات ترافیک مجاز

نوع بسته	UDP
بسته Payload	۲۶ Bytes
تعداد بسته‌های فرستاده شده	۵
فاصله ترافیکی	۰/۱ ثانیه
نرخ ترافیک	۱۰ بسته/ثانیه
نرخ جریان	۲ جریان/ثانیه

جدول (۴-۹): مشخصات ترافیک حمله به یک میزبان

نوع بسته	UDP
بسته Payload	-
تعداد بسته‌های فرستاده شده	۲
فاصله ترافیکی	۰/۰۸ ثانیه
نرخ ترافیک	۱۲/۵ بسته/ثانیه
نرخ جریان	۶/۲۵ جریان/ثانیه

جدول (۴-۱۰): مشخصات ترافیک حمله به چندین میزبان

نوع بسته	UDP
بسته Payload	-
تعداد بسته‌های فرستاده شده	۲
فاصله ترافیکی	۰/۰۳ ثانیه
نرخ ترافیک	۳۳/۳ بسته/ثانیه
نرخ جریان	۱۶/۶۵جریان/ثانیه

الگوی ترافیکی C:

این الگوی ترافیکی ترکیبی از الگوهای ترافیکی A و B است. نیمی از میزبان‌ها با ترافیک مجاز با الگوی A ارسال می‌کند و نیمی دیگر ترافیک را براساس الگوی B ارسال می‌کنند. این الگوی ترافیک، ترکیبی از انواع مختلف جریان را تولید می‌کند و ترافیک حمله بدون تغییر خواهد ماند.

شبیه‌سازی شامل دو نوع حمله است: حمله به یک میزبان و حمله به چندین میزبان. در حمله به یک میزبان ۲۰ اجرای شبیه‌سازی شامل ۴ سناریوی حمله با یک میزبان، دو میزبان، سه میزبان و چهار میزبان در حال حمله به یک هدف با IP، ۱۰.۰.۰.۱۵ است. در حمله به چندین میزبان ۲۰ اجرای شبیه‌سازی انجام شده است که هر اجرای شبیه‌سازی شامل ۴ سناریوی حمله است. در این موارد مهاجم حملات را در میان یک گروه از ۴، ۸، ۱۲و ۱۶ هدف (قربانی) توزیع می‌کند در حالی که ارسال ترافیک حمله از یک، دو، سه یا چهار میزبان است.

۴-۲-۴-۱- حملات به یک میزبان

در شبیه‌سازی حملات به یک میزبان، ترافیک مجاز بر روی ۲۵ میزبان برای حداقل یک دقیقه اجرا می‌شود تا شبکه را تثبیت کند و الگوریتم برای ارزیابی مقادیر مناسب حدآستانه‌های مختلف قبل از انجام حملات انجام شود. این دوره همچنین به عنوان فاز یادگیری اولیه برای الگوریتم در نظر گرفته می‌شود. بنابراین حدآستانه را می‌توان در فاز یادگیری اولیه در حالی که ترافیک مجاز در حال اجرا است

با بررسی کنترل‌کننده محاسبه کرد. با این حال حدآستانه باید با ترافیک شبکه تطبیق داده شود تا منعکس‌کننده الگوی جریان ترافیکی فعلی باشد.

هر اجرا شامل چهار سناریو از حملات می‌باشد. در حالی که شبیه‌سازی در حال اجرا است اگر حمله مشکوک یا به دلیل تغییرات آنتروپی و یا تغییر در میزان ترافیک رخ دهد در یک فایل log می‌شود و زمان را هم نشان می‌دهد. سوئیچ‌هایی که مشکوک به بودن در مسیر حمله هستند نیز شناسایی می‌شود و لیستی از این سوئیچ‌ها به فایل log شده همراه با زمان رخداد تایپ می‌شود.

جدول (۴-۱۱) تعداد FP و FN را در حالی که الگوهای ترافیکی A و B و C در حال تست هستند را نشان می‌دهد.

جدول (۴-۱۱): گزارش‌های FP و FN تحت الگوهای ترافیکی مختلف در حملات به یک میزبان

	الگوی ترافیکی A		**الگوی ترافیکی B**		**الگوی ترافیکی C**	
تعداد کل حملات بر روی سیستم	۸۰		۸۰		۸۰	
	خطای شمارش	احتمال خطا	خطای شمارش	احتمال خطا	خطای شمارش	احتمال خطا
FP	۰	٪ ۰	۲	٪ ۳	۶	٪ ۷/۵
FN	۰	٪ ۰	۰	٪ ۰	۴	٪۵
نرخ تشخیص الگوریتم	٪ ۱۰۰		٪ ۹۷		٪۸۷/۵	
نرخ شکست الگوریتم	٪ ۰		٪ ۲/۲۵		٪ ۱۲/۵	

همان طور که در جدول (۴-۱۱) نشان داده شده است هنگامی که ترافیک حمله و مجاز دارای ویژگی‌های متمایزی هستند (الگوی ترافیکی A) الگوریتم قادر به تشخیص ۱۰۰ ٪ است. الگوریتم در الگوی ترافیکی B بسیار خوب عمل می‌کند. این نرخ بالای تشخیص به دلیل بروزرسانی پویای مقادیر حدآستانه است. الگوی ترافیکی C نقطه‌ای است که اگر چه نرخ تشخیص بالای ۸۵ ٪ است اما شروع به نشان دادن افزایش در هر دو تشخیص FP و FN می‌کند. در الگوی ترافیکی C فرض می‌شود که ترافیک

مجاز ترکیبی از جریان‌های کوتاه و بلند است. جریان‌های کوتاه در این الگوریتم ترافیکی مشابه جریان-های تولید شده توسط ترافیک حمله هستند. در این مورد یافتن حدآستانه مناسب بسیار دشوار است.

۴-۲-۴-۲- حملات به چندین میزبان

در این قسمت از شبیه‌سازی ۲۰ اجرای مختلف انجام می‌شود. هر اجرا شامل ۴ سناریو است. در سناریوی اول ۲۴ میزبان در حال تولید ترافیک مجاز و یک میزبان در حال تولید ترافیک حمله به ۴ مقصد مختلف تحت الگوهای ترافیکی مختلف است . نسبت ترافیکی حمله ۲۱ ٪ است. در سناریوی دوم، دو میزبان ترافیک حمله را با نسبت حمله ۳۶ ٪ تحت الگوهای ترافیکی مختلف به ۸ میزبان دیگر ارسال می‌کند و ۲۳ میزبان دیگر در حال تولید ترافیک مجاز هستند. در سناریوی سوم، سه میزبان ترافیک حمله را با نسبت حمله ۴۷/۵ ٪ تحت الگوهای ترافیکی مختلف به ۱۲ میزبان دیگر ارسال می‌کند و ۲۲ میزبان دیگر در حال تولید ترافیک مجاز می‌باشد. در سناریوی چهارم، چهار میزبان ترافیک حمله را به ۱۶ میزبان دیگر ارسال می‌کند و ۱۶ میزبان دیگر در حال تولید ترافیک مجاز است.

جدول (۴-۱۲): گزارش‌های FP و FN تحت الگوهای ترافیکی مختلف در حملات به چندین میزبان

	الگوی ترافیکی A		**الگوی ترافیکی B**		**الگوی ترافیکی C**	
تعداد کل حملات بر روی سیستم	۸۰		۸۰		۸۰	
	خطای شمارش	احتمال خطا	خطای شمارش	احتمال خطا	خطای شمارش	احتمال خطا
FP	۰	٪ ۰	۲	٪ ۳	۵	٪ ۶/۳
FN	۰	٪ ۰	۳	٪ ۳/۷۵	۵	٪ ۶/۳
نرخ تشخیص الگوریتم	٪ ۱۰۰		٪ ۹۵/۲۵		٪ ۸۷/۴	
نرخ شکست الگوریتم	٪ ۰		٪ ۴/۷۵		٪ ۱۲/۶	

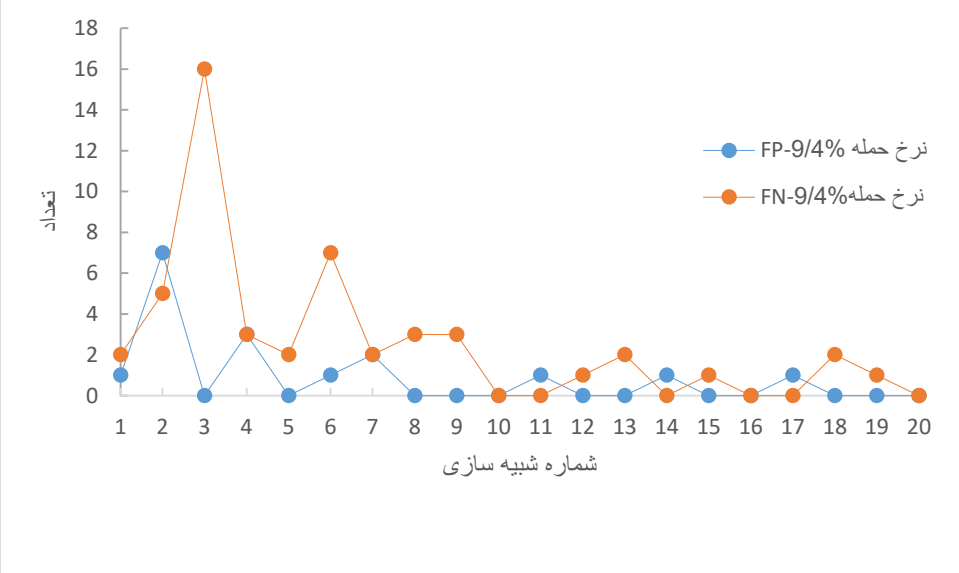
همان طور که مشاهده می‌شود نتایج به دست آمده در حملات به چندین میزبان نرخ بالایی از تشخیص را برای هر سه الگوی ترافیکی نشان می‌دهد. هنگامی‌که حملات بین میزبان‌های بیشتری توزیع می‌شود

عمل شناسایی انجام نمی‌شود. FN به عنوان ترافیک حمله بین مقاصد مختلف توزیع می‌شود و تأثیر حمله ممکن است به مقادیر حدآستانه نرسد. همان طور که در جدول (۴-۱۲) مشاهده می‌شود میزان تشخیص در الگوی ترافیکی C به میزان ۸۸/۷۵ ٪کاهش می‌یابد. الگوی ترافیکی C موردی پیچیده است که در آن یافتن حدآستانه مناسب بسیار دشوار است.

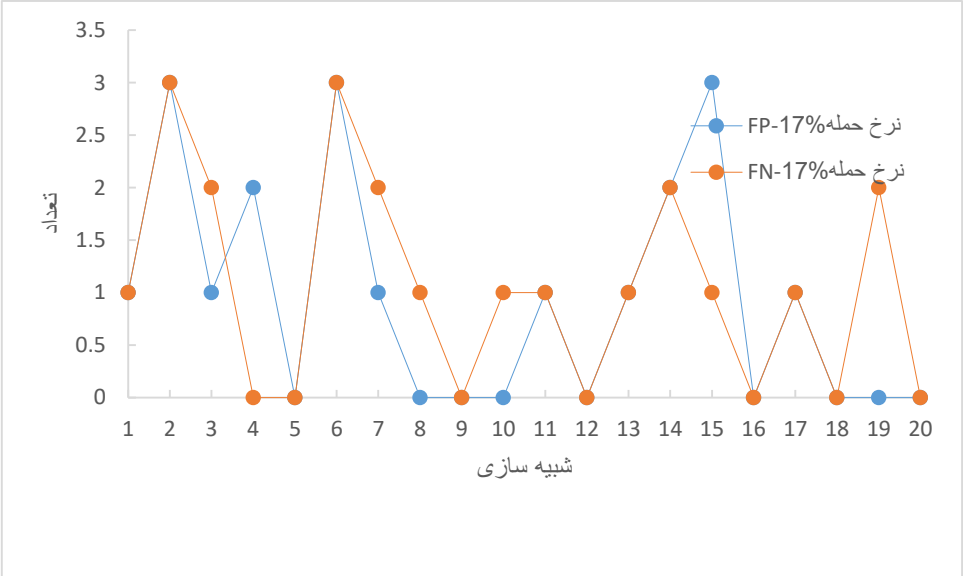
۴-۲-۵- تجزیه و تحلیل دقیق تشخیص مسیر حمله

- حمله به یک میزبان

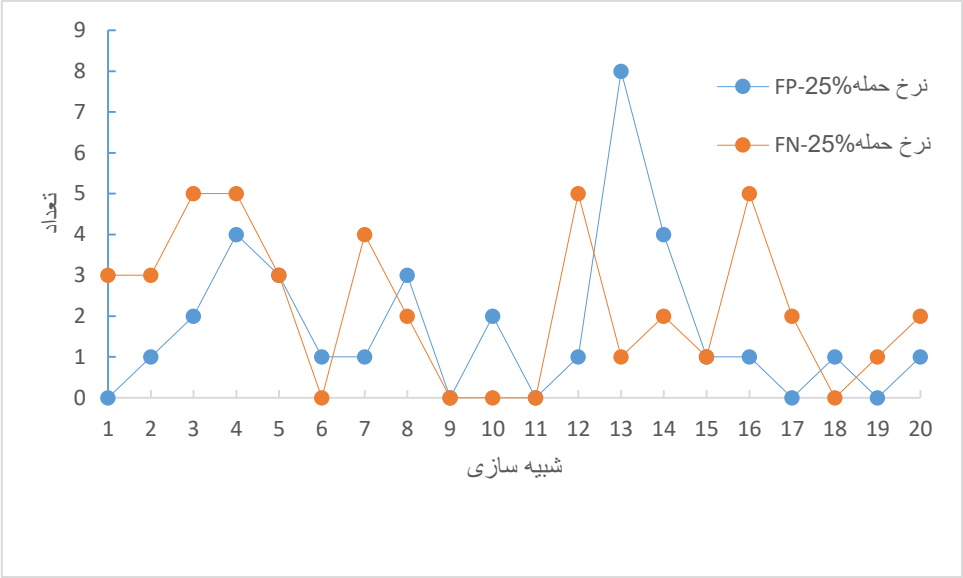
در این بخش، کارایی روش پیشنهادی برای شناسایی سوئیچ‌هایی که تحت حمله قرار دارند را بررسی می‌شود. اگر یک سوئیچ در مسیر حمله نیست اما گزارش شده که تحت حمله است آن را به عنوان نمونه گزارش FP و اگر سوئیچی در مسیر حمله است اما گزارش نشده که تحت حمله است به عنوان نمونه‌ای از گزارش FN در نظر گرفته می‌شود.



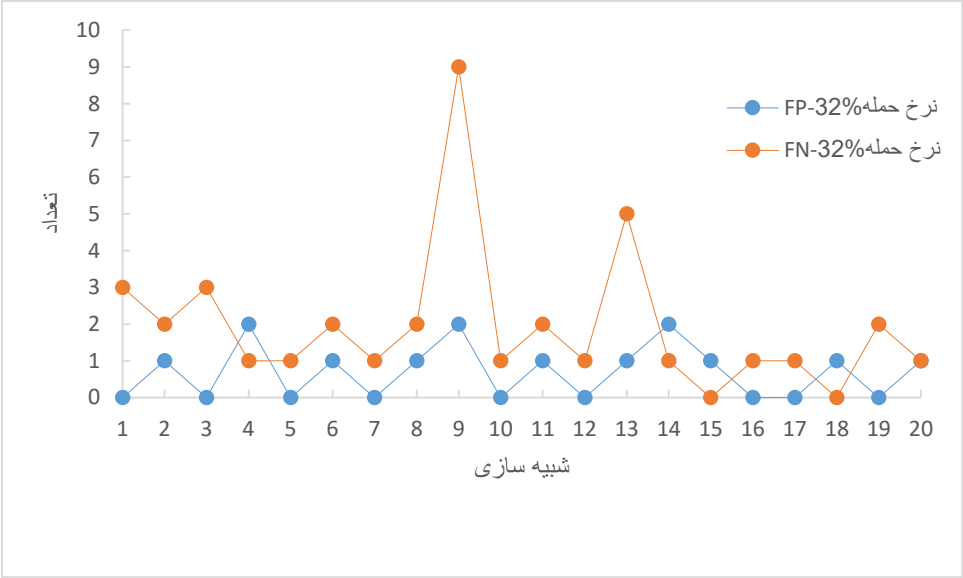
شکل (۴-۶): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۹/۴ ٪



شکل (۴-۷): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۱۷ ٪



شکل (۴-۸): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۲۵ ٪

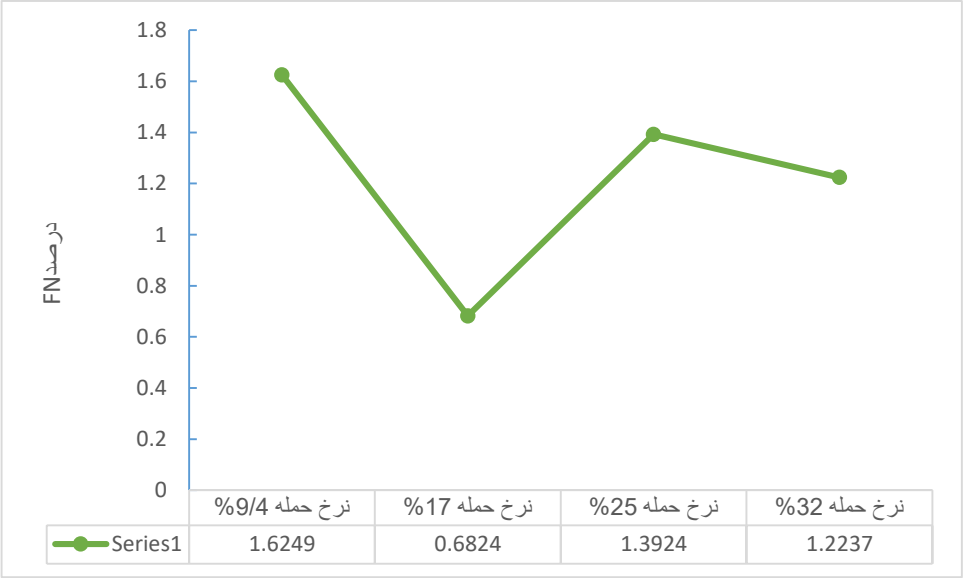


شکل (۴-۹): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۳۲ ٪

همان طور که در ارقام مشاهده می‌شود بیشترین میزان FN در حالی که ترافیک حمله در کمترین نسبت است گزارش شده است. در نسبت حمله ۹/۴٪ در اجرای سوم گزارش‌های FN به نقطه اوج خود یعنی ۱۶ می‌رسد. بنابراین انتظار می‌رود برای ترافیک با نسبت پایین‌تر گزراش FN افزایش یابد. جدول (۴-۱۳) میانگین گزارش‌های FN را در مقادیر مختلف حمله نشان می‌دهد. گرچه بالاترین نرخ FN متعلق به کمترین میزان حمله است، اما همان طور که می‌توان در شکل (۴-۹) مشاهده کرد، نرخ FN از یک رفتار خطی پیروی نمی‌کند. از لحاظ آماری، نتایج نشان می‌دهد که نرخ FN در تمام دامنه‌های حملات بسیار کم است. همچنین نوسانات کم گزارش FN دلیل دیگری بر عملکرد خوب الگوریتم پیشنهادی است. این نوسان کمتر از ۱ ٪ است.

جدول (۴-۱۳): گزارش‌های FN برای حمله به یک میزبان تحت الگوی ترافیکی A

	نرخ حمله ۹/۴ ٪	**نرخ حمله ۱۷ ٪**	**نرخ حمله ۲۵ ٪**	**نرخ حمله ۳۲ ٪**
تعداد گزارش‌های کل	۳۰۷۷	۳۰۷۷	۳۱۶۰	۳۱۸۷
FN	۵۰	۲۱	۴۴	۳۹
٪	٪ ۱/۶۲۴۹	٪ ۰/۶۸۲۴	٪ ۱/۳۹۲۴	٪ ۱/۲۲۳۷

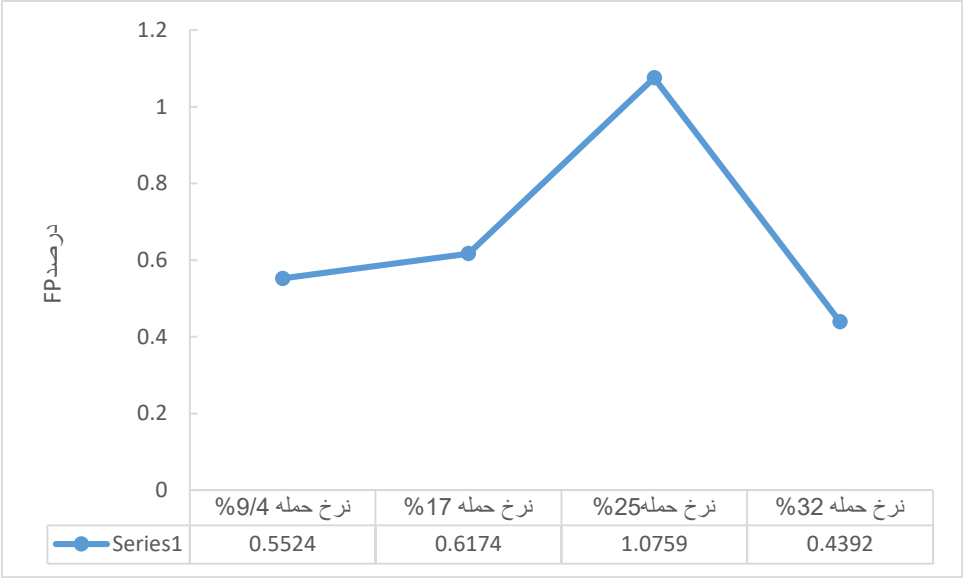


شکل (۴-۱۰): رفتار گزارش‌های FN در حمله به یک میزبان تحت الگوی ترافیکی A

در جدول (۴-۱۴) گزارش‌های FP با نرخ‌های مختلف حمله نشان داده شده است. برای سه نرخ ترافیک حمله تعداد گزارش‌های FP، با افزایش نرخ حمله شروع به افزایش می‌کند. نوسانات گزارش FP کمتر از ۰/۶۳ ٪ است.

جدول (۴-۱۴): گزارش‌های FP برای حمله به یک میزبان تحت الگوی ترافیکی A

	نرخ حمله ۹/۴ ٪	**نرخ حمله ۱۷ ٪**	**نرخ حمله ۲۵ ٪**	**نرخ حمله ۳۲ ٪**
تعداد گزارش‌های کل	۳۰۷۷	۳۰۷۷	۳۱۶۰	۳۱۸۷
FP	۱۷	۱۹	۳۴	۱۴
٪	٪ ۰/۵۵۲۴	٪ ۰/۶۱۷۴	٪ ۱/۰۷۵۹	٪ ۰/۴۳۹۲

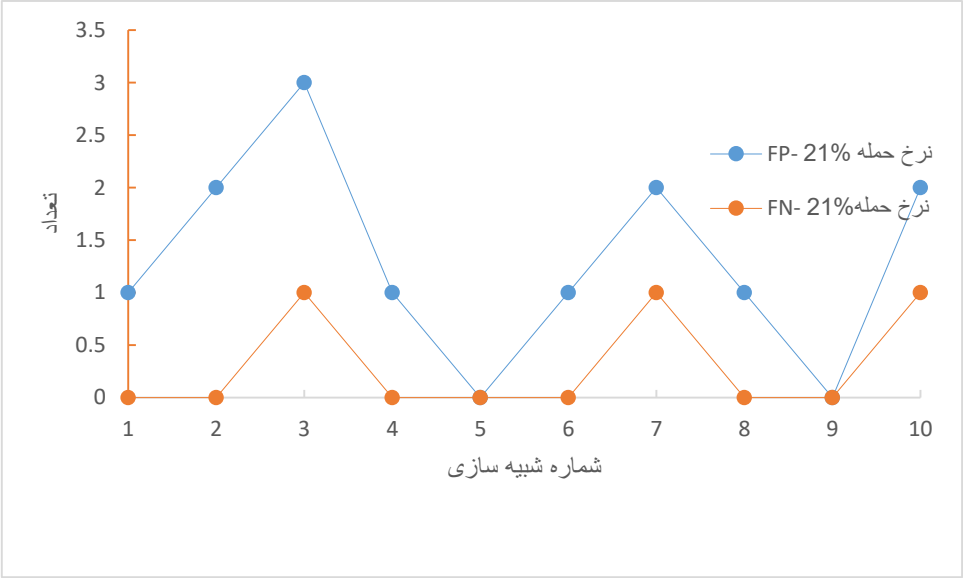


شکل (۴-۱۱): رفتار گزارش‌های FP در حمله به یک میزبان تحت الگوی ترافیکی A

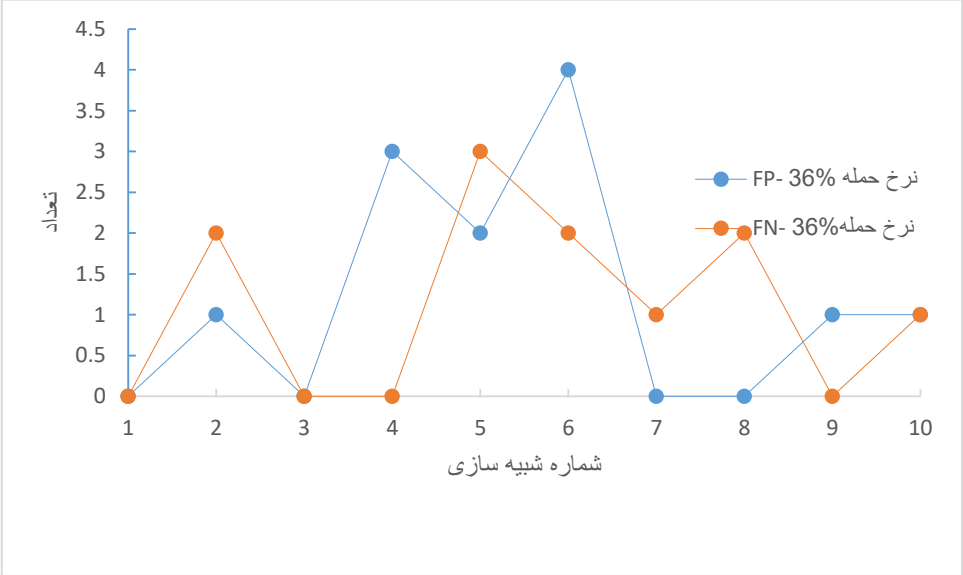
نه تنها خطای احتمالی گزارش FP و FN بسیار کم است بلکه می‌تواند به راحتی با تغییرات کوچک در الگوریتم کاهش یابد.

- حمله به چندین میزبان

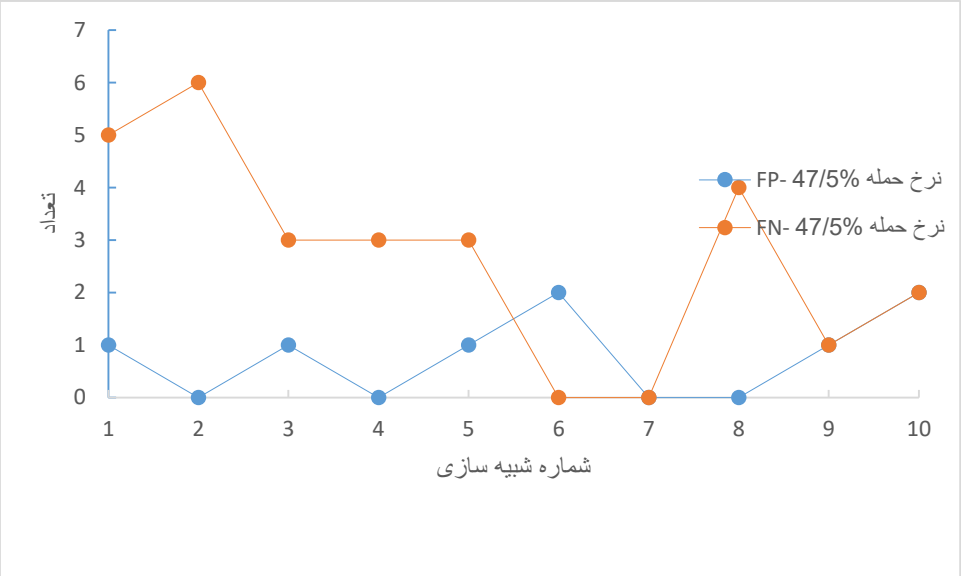
همان طور که در بخش‌های قبلی مشاهده شد در حالی که شبیه‌سازی با الگوی ترافیکی A در حال اجرا است در مرحله تشخیص حمله به یک میزبان هیچ گزارش FP و FN مشاهده نشد. اما در پیدا کردن مسیر دقیق حمله و گزارش سوئیچ‌هایی که در معرض حمله قرار دارند، مواردی وجود دارد که الگوریتم گزارش FP یا FN را گزارش می‌دهد. هنگام بررسی گزارش‌های FN در حمله به چندین میزبان، گزارش‌ها تنها در مورد سوئیچ‌های پایانی (سوئیچ‌هایی که به میزبان متصل هستند) در نظر گرفته می‌شود. این امر برای جلوگیری از پرس و جو از تعداد زیاد سوئیچ‌ها است که می‌تواند بار زیادی را در شبکه و کنترل‌کننده ایجاد کند. شکل‌های (۴-۱۱)، (۴-۱۲) و (۴-۱۳) گزارش‌های FP و FN را تحت نرخ‌های حمله ۲۱ ٪ ، ۳۶ ٪، ۴۷/۵ ٪ نشان می‌دهد.



شکل (۴-۱۲): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۲۱ ٪



شکل (۴-۱۳): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۳۶ ٪



شکل (۴-۱۴): گزارش‌های FP و FN در الگوی ترافیکی A برای حمله به یک میزبان با نسبت حمله ۴۷/۵ ٪

همان طور که مشاهده می‌شود به دلیل افزایش نرخ حمله، احتمال گزارش‌های FN نیز وجود دارد. این رفتار را می‌توان به شرح زیر توضیح داد. در آزمایش‌هایی که نسبت ترافیک حمله افزایش می‌یابد و در نتیجه تعداد سوئیچ‌های گزارش شده به عنوان اینکه تحت حمله هستند نیز افزایش می‌یابد. از آنجا که ترافیک حمله به چندین میزبان توزیع می‌شود، همه سوئیچ‌ها حجم زیادی از جریان‌های حمله را دریافت نمی‌کنند و تعداد گزارش‌های FN شروع به افزایش می‌کنند. نوسان گزارش‌های FN کمتر از ۱/۳ ٪ است که یک نرخ خطای کم و قابل قبول است.

جدول (۴-۱۵): گزارش‌های FN برای حمله به چندین میزبان تحت الگوی ترافیکی A

	نرخ حمله ۲۱ ٪	**نرخ حمله۳۶ ٪**	**نرخ حمله ۴۷/۵ ٪**
تعداد گزارش‌های کل	۱۷۵۹	۲۰۲۱	۱۸۹۱
FN	۳	۱۱	۲۷
٪	٪ ۰/۱۷۰۵	٪ ۰/۵۴۴۲	٪ ۱/۴۲۷۸

در جدول (۴-۱۶) گزارش‌های FP با نرخ‌های مختلف حمله به چندین میزبان نشان داده شده است. برای سه نرخ ترافیک حمله، درصد گزارش‌های FP یک رفتار پایدار نسبی را با کاهش اندک در افزایش ترافیک حملات را نشان می‌دهد. نوسانات گزارش FP فقط ۰/۳ ٪ است.

جدول (۴-۱۶): گزارش‌های FP برای حمله به چندین میزبان تحت الگوی ترافیکی A

	نرخ حمله ۲۱ ٪	**نرخ حمله ۳۶ ٪**	**نرخ حمله ۴۷/۵ ٪**
تعداد گزارش‌های کل	۱۷۵۹	۲۰۲۱	۱۸۹۱
FP	۱۳	۱۲	۸
٪	٪ ۰/۷۳۹۰	٪ ۰/۵۹۳۷	٪ ۰/۴۲۳۰

۴-۲-۶ ارزیابی عملکرد روش پیشنهادی

همان طور که در فصل قبل بحث شد، روش تشخیص حمله در الگوریتم پیشنهادی براساس دو معیار است: تغییرات آنتروپی و تغییرات ناگهانی در نرخ شروع جریان. لازم است یک بررسی درباره اینکه کدام بخش از الگوریتم در تشخیص حملات موثر است انجام شود. جدول (۴-۱۷) احتمال تشخیص حمله به یک میزبان را از طریق دو تکنیک تشخیص نشان می‌دهد. در ابتدای این فصل ذکر شد معیار آنتروپی به تنهایی برای تشخیص حمله DDOS کافی نیست و ممکن است در یک دوره زمانی بار ترافیک مجاز بیش از حد معمول باشد و معیار آنتروپی دچار کاهش شود و موجب گزارش FP شود و یا در زمانی که حمله به چندین میزبان در شبکه باشد آنتروپی دچار کاهش چشمگیری نشود و در مقایسه با حدآستانه تشخیص داده نشود. بنابراین الگوریتم پیشنهادی در زمان حمله به یک میزبان با روش [۲۳] مقایسه می‌شود. نتایج حاصل از این مقایسه در جدول (۴-۱۷) بیان شده است.

جدول (۴-۱۷): مقایسه اثر آنتروپی و نرخ شروع جریان در تشخیص حملات تحت الگوی ترافیکی A برای حمله به یک میزبان

	نرخ حمله ٪ ۹/۴	٪	نرخ حمله ٪ ۱۷	٪	نرخ حمله ٪ ۲۵	٪	نرخ‌حمله ٪ ۳۲	٪
گزارش حمله	۳۵۰		۳۵۲		۲۹۰		۳۷۰	
شناسایی حمله از طریق تغییرات آنتروپی	۳۴۱	۹۷/۴۲	۳۴۵	۹۸/۰۱	۲۸۷	۹۸/۹۶	۳۶۵	۹۸/۶۴
شناسایی حمله از طریق تغییرات نرخ شروع جریان	۹	۲/۵۷	۷	۱/۹۹	۳	۱/۰۴	۵	۱/۳۶

با توجه به جدول (۴-۱۷) مشاهده می‌شود که درصد تشخیص حمله به یک میزبان از طریق معیار آنتروپی بسیار بالاتر از تغییرات نرخ جریان است. با احتمال تشخیص بین ۹۹-۹۷ درصد می‌توان گفت که تنوع آنتروپی موثرترین روش شناسایی حملات است که تعداد محدودی از مقصدها را در شبکه مورد هدف قرار می‌دهد. این به این دلیل است که در چنین حملاتی بیشترین ترافیک حمله به یک مقصد مشخص است و آنتروپی به میزان قابل توجهی کاهش پیدا می‌کند. بنابراین شانس تشخیص حملات به یک میزبان از طریق تغییرات آنتروپی بسیار بالاتر از تغییرات نرخ جریان است.

حال تشخیص برای حملات به چندین میزبان مورد بررسی قرار می‌گیرد و با روش [۲۳] مقایسه می‌شود. احتمال تشخیص حملات به چندین میزبان از طریق روش‌های شناسایی تغییرات آنتروپی و نرخ جریان مطابق با جدول (۴-۱۸) است.

جدول (۴-۱۸): مقایسه اثر آنتروپی و نرخ شروع جریان در تشخیص حملات تحت الگوی ترافیکی A برای حمله به چندین میزبان

	نرخ حمله ٪ ۲۱	٪	نرخ حمله ٪ ۳۶	٪	نرخ حمله ٪ ۴۷/۵	٪
گزارش حمله	۲۰۱		۲۳۵		۲۸۱	
شناسایی حمله از طریق تغییرات آنتروپی	۱۰۰	۴۹/۷۵	۹۶	۴۰/۸۵	۱۰۲	۳۶/۲۹
شناسایی حمله از طریق تغییرات نرخ شروع جریان	۱۰۱	۵۰/۲۴	۱۳۹	۵۹/۱۴	۱۷۹	۶۳/۷۱

همان طور که در جدول (۴-۱۸) اشاره شد، در حمله به چندین میزبان تکنیک آنتروپی به اندازه حمله به یک میزبان موثر نیست. در واقع درصد تشخیص حمله به چندین میزبان از طریق تغییرات نرخ شروع جریان بیشتر از تغییرات آنتروپی است. مقایسه این الگوریتم با الگوریتم [۲۳] که معیار فقط آنتروپی است، به طور میانگین نشان می‌دهد که ۶۵/۶۱ ٪ موثرتر است. این درصد تشخیص که بر مبنای تغییرات نرخ شروع جریان است، نشان می‌دهد تکنیک تغییر آنتروپی نمی‌تواند به عنوان یک روش تشخیص مستقل برای حمله به چندین میزبان مورد توجه قرار گیرد.

۴-۳- جمع‌بندی

در این فصل با ارائه یک توپولوژی از ارتباطات وسایل نقلیه در شبکه‌های SDN، سعی شد یک الگوریتم تشخیص حمله DDOS بهبود داده شود. بر این اساس یک الگوریتم را که از معیار آنتروپی برای تشخیص حمله استفاده کرده بود به عنوان شروع کار در نظر گرفته شد. در این فصل نخست نشان داده شد که این معیار به تنهایی در تشخیص حمله کارا نیست. زیرا اگر در یک دوره زمانی بار ترافیک مجاز شبکه بیش از حد معمول شود آنتروپی کاهش یافته و موجب ایجاد گزارش FP می‌شود و یا اگر حمله به چندین میزبان رخ دهد موجب ایجاد گزارش FN می‌شود. بنابراین با در نظر گرفتن نرخ شروع جریان و خصوصیات آن، قدم در بهبود الگوریتم تشخیص نهاده شد. با تطبیق دادن رفتار شبکه طبق سه الگوی

ترافیکی با مقادیر مختلف از پارامتر جریان نشان داده شد که در مواقعی که چند میزبان از سیستم تحت حمله قرار می‌گیرند معیار آنتروپی به تنهایی قادر به تشخیص حمله نیست. یکی از مزیت‌های روش پیشنهادی تغییر پویای حدآستانه‌ها مطابق با الگوی رفتار شبکه است که این امر موجب کاهش نرخ FP و FN می‌شود. درصد تشخیص حمله DDOS در روش پیشنهادی دارای رشد ۶۵/۶۱ ٪ است که این میزان نسبت به زمانی که آنتروپی به تنهایی معیار تشخیص قرار می‌گیرد بهبود قابل قبولی است.

فصل پنجم

جمع‌بندی و پیشنهادهایی برای ادامه کار

۵-۱- جمع‌بندی

از آنجا که امنیت در شبکه، می تواند به عنوان یک نگرانی عمده درنظر گرفته شود، حفاظت از سیستم عامل معماری VANET مبتنی بر SDN با شناسایی حمله DDoS هدف این پژوهش بود. برای شبکه‌های VANET که شامل برنامه هایی است با اطلاعات حیاتی، امنیت حائز اهمیت است.

نخست با شرح مبانی و مفاهیم نظری از شبکه‌های VANET، SDN و همچنین شبکه‌های خودرویی مبتنی بر نرم‌افزار زمینه برای فهم موضوع پژوهش فراهم شد؛ سپس، روش‌های تشخیص حمله DDOS در بخش کارهای پیشین مورد بررسی قرار گرفتند و مشخص شد که هر کدام از آنها متفاوت عمل می‌کنند. در این پژوهش بعد از ارائه توپولوژی‌های مختلف برای شبکه‌های خودرویی مبتنی بر نرم‌افزار، با استفاده از ویژگی‌های رفتار شبکه یک الگوریتم برای تشخیص حمله در نظر گرفته شد تا مبنای یک راه حل برای تشخیص حمله DDOS در محیط‌های پویا باشد. آزمایش‌ها برای دو سناریوی حمله به یک میزبان و چندین میزبان با نسبت‌های حمله مختلف در نظر گرفته شد. این آزمایش‌ها شامل راه‌اندازی ترافیک مجاز و حمله با آدرس IP های منبع جعلی است. بر اساس ویژگی‌های ترافیکی، مانند آدرس های IP مقصد، دنباله‌ای از پنجره‌های ۳۰ بسته‌ایی، نرخ شروع جریان و خصوصیات جریان، برای تشخیص حمله DDOS توسط کنترل کننده SDN صورت پذیرفت. این پژوهش با محاسبه آنتروپی، نرخ شروع جریان و خصوصیات جریان و پس از تعریف مناسب از حدآستانه برای هر مورد، قادر به تشخیص حمله به یک میزبان یا زیر شبکه‌ای از ۶ میزبان و یا هنگامی که حمله توسط چندین میزبان راه‌اندازی می‌شود، می‌باشد. حدآستانه‌ها در فاز یادگیری شبکه تحت الگوی ترافیکی مجاز به دست می‌آیند و نتایج الگوریتم با توجه به بروزرسانی پویای حدآستانه‌ها در هر مرحله از تشخیص، یک مدل پویا برای تعمیم به شبکه‌های خودرویی فراهم می‌شود.

۵-۲- پیشنهادهایی برای ادامه کار

آزمایش و پیاده‌سازی الگوریتم تشخیص برای توپولوژی‌های بزرگتر و پویا برای دیدن عملکرد آن، مسیر دیگری برای تحقیقات آینده است. از آنجا که هدف این پژوهش بر روی ارتباطات بخش کنترل متمرکز بود، به عنوان مثال در این مورد، ارتباط بین وسایل نقلیه و RSU ها وکنترل کننده؛ بنابراین بررسی ازتباطات بخش داده یعنی ارتباطات خودرو به خودرو هدف بالقوه‌ای برای کار آینده خواهد بود.

همانطور که اشاره شده است هنگامی که جریان‌های ترافیکی مجاز در حال اجرا در شبکه دارای ویژگی‌های مختلف هستند، استفاده از یک حدآستانه می‌تواند شانس گزارشات FP و FN را افزایش دهد. از این رو پیشنهاد می‌شود که سیستمی ایجاد شود تا از طیف وسیعی از حدآستانه‌ها و متناسب با هر نوع جریان استفاده شود.

استفاده از SDN در شبکه‌های خودرویی به طور گسترده نیازمند چندین کنترل‌کننده است. استفاده از یک کنترل‌کننده برای مکان‌هایی از جاده که دارای برد وسیعی از پوشش و تردد خودرو با سرعت‌های مختلف است دشوار است و نیاز به پروتکل‌های زیادی دارد. بنابراین به عنوان یکی از کارهای آینده می‌توان استفاده از چندین کنترل‌کننده به همراه پروتکل‌های ارتباطی بین آن‌ها پیشنهاد کرد تا شبکه در وسعت بیشتری مورد بررسی قرار گیرد و در برابر حملات ایمن شود.

منابع و ماخذ:

[۱] R. Lind, R. Schumacher, R. Reger, R. Olney, H. Yen, M. Laur, *et al.*, "The Network Vehicle-a glimpse into the future of mobile multi-media," *IEEE Aerospace and Electronic Systems Magazine*, vol. 14, pp. 27-32, 1999.

[۲] I. W. Group, "Standard specification for telecommunications and information exchange between roadside and vehicle systems-5 GHz band dedicated short range communications (dsrc) medium access control (mac) and physical layer (phy) specifications," *ASTM DSR STD E2313-02*, 2002.

[۳] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic analysis, control, optimization and applications*, ed: Springer, 1999, pp. 547-566.

[۴] R. Lu, "Security and privacy preservation in vehicular social networks," 2012.

[۵] C. Zhang, "On Achieving Secure Message Authentication for Vehicular Communications," 2010.

[۶] C. Lochert, A. Barthels, A. Cervantes, M. Mauve, and M. Caliskan, "Multiple simulator interlinking environment for IVC," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005, pp. 87-88.

[۷] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE communications surveys & tutorials*, vol. 10, 2008.

[۸] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, vol. 16, 2009.

[۹] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE communications magazine*, vol. 46, 2008.

[۱۰] J. T. Blasius, "Short-Range Wireless Communications for Vehicular Ad hoc Networking," *2014 NCUR*, 2014.

[۱۱] "https://safety.fhwa.dot.gov"./

[۱۲] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications magazine*, vol. 46, 2008.

[۱۳] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2772-2785, 2010.

[۱۴] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, pp. 39-68, 2007.

[۱۵] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, *et al.*, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, 2008.

[۱۶] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, "Fast exclusion of errant devices from vehicular networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on*, 2008, pp. 135-143.

[۱۷] w. t. c. OpenFlow Tutorial: Next-Gen Networking Has Much To Prove, Oct 17, 2011.

[۱۸] S.-D. N. T. N. N. f. N. White paper, Open Networking Foundation, and R. A. April 13, 2013.

[۱۹] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, *et al.*, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, pp. 69-74, 2008.

[۲۰] T. N .Subedi, K. K. Nguyen, and M. Cheriet, "OpenFlow-based in-network Layer-2 adaptive multipath aggregation in data centers," *Computer Communications*, vol. 61, pp. 58-69, 2015.

[۲۱] M. Kobayashi, S. Seetharaman, G. Parulkar, G. Appenzeller, J. Little, J. Van Reijendam, *et al.*, "Maturing of OpenFlow and software-defined networking through deployments," *Computer Networks*, vol. 61, pp. 151-175, 2014.

[۲۲] I. Ku, Y. Lu, M. Gerla, F. Ongaro, R. L. Gomes, and E. Cerqueira, "Towards software-defined VANET: Architecture and services," in *Ad Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean*, 2014, pp. 103-110.

[۲۳] M. S. Todorova and S. T. Todorova, "DDoS Attack Detection in SDN-based VANET Architectures," 2016.

[۲۴] P. Pawelczak, R. V. Prasad, L .Xia, and I. G. Niemegeers, "Cognitive radio emergency networks-requirements and design," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, 2005, pp. 601-606.

[۲۵] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *AD hoc networks*, vol. 7, pp. 810-836, 2009.

[۲۶] غ. ا. آ. ب. ت. س. ن. ا. و. ش. ج. س. ا. شبکه.

[۲۷] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Communications Magazine*, vol. 53, pp. 52-59, 2015.

[۲۸] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For*, 2013, pp. 1-7.

[۲۹] M. Thottan" ,Chuanyi Ji—Anomaly Detection in IP Networks‖ IEEE TRANSACTIONS ON SIGNAL PROCESSING VOL. 51," ed, 2003.

[۳۰] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, 2003, pp. 303-314.

[۳۱] P. A. “Software-defined networking: The new norm for networks, CA, USA, White Paper, Apr. 2012. [Online]. Available: and https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdnnewnorm.pdf.

[۳۲] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 27-51, 2015.

[٣٣] S. M. Mousavi, "Early detection of DDoS attacks in software defined networks controller," *PhD diss., Carleton University Ottawa,* 2014.

[٣٤] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on* ,٢٠١٠ ,pp. 408-415.

[٣٥] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, 2010, pp. 385-388.

[٣٦] S .Shin and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," in *Network Protocols (ICNP), 2012 20th IEEE International Conference on*, 2012, pp. 1-6.

[٣٧] G. No and I. Ra, "An efficient and reliable DDoS attack detection using a fast entropy computation method," in *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, 2009, pp. 1223-1228.

[٣٨] J. Zhang, Z. Qin, L .Ou, P. Jiang, J. Liu, and A. X. Liu, "An advanced entropy-based DDOS detection scheme," in *Information Networking and Automation (ICINA), 2010 International Conference on*, 2010, pp. V2-67-V2-71.

[٣٩] S. Oshima, T. Nakashima, and T. Sueyoshi, "Early DoS/DDoS detection method using short-term statistics," in *Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on*, 2010, pp. 168-173.

[٤٠] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *IEEE Communications Letters,* vol. 18, pp. 114-117, 2014.

[٤١] X. Zhang, G. Li, and F. Qiao, "A speech endpoint detection algorithm based on entropy and RBF neural network," in *Granular Computing, 2007. GRC 2007. IEEE International Conference on*, 2007, pp. 506-506.

[٤٢] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *International Conference on Ad Hoc Networks*, 2010, pp. 1-16.

Abstract

Vehicle ad hoc network (VANET) has been proposed as a new plane to provide road safety, traffic management and convenience applications for drivers and passengers on the road. In this network, communications are in two ways: vehicle to vehicle and vehicle to infrastructure. Different messages containing events warning about road are exchanges in these communications. In these networks, wireless communications leads to many challenges such as: injecting false information, modifying and replaying the disseminated messages in the network, impersonation and distributed denial of service (DDOS). One of the security threats in VANETs is the DDOS attack which aims to busy and unavailable the Road Side Unit for legitimate vehicles. On the other hand, a number of vehicles on the roads have computational resources and can be used as an unexploited resource. Therefor. The concept of cloud computing for vehicles was introduced. To use cloud technology in VANET, we need to use an infrastructure as a service to centralize network management and secure attacks.

In this thesis, the software-defined network (SDN) have been used to design an intelligent secure schema for vehicles. One of the security challenges of SDN based VANETs is availability of the controller. In this thesis, DDOS attack has been investigated to address the security needs of the controller's availability. By launching legitimate and attack traffic to SDN based VANETs based on the entropy criterion and traffic characteristics, the network behavior pattern is investigated. Then by adaptive an improved algorithm with network behavior by traffic characteristics, a dynamic schema was obtained to detect DDOS attack, which the attack detection rate achieved 65/61%.

Keywords: vehicle ad hoc network, cloud computing, distributed denial of service attack, software-defined network, entropy, traffic characteristics

Shahrood University of Technology

Faculty of Computer Engineering

M.Sc. Thesis in Artificial Intelligence Engineering

Designing a Secure Intelligent Model Vehicular Ad Hoc Network (VANET) In a Cloud Environment

By:

Samira Rajabloo

Supervisor:

Dr. Ali Akbar Pouyan

Advisor:

Dr. Mohsen Rezvani

January 2018

۱۰۱