دانشگاه آزاد اسلامی واحد الکترونیکی
مجله مدیریت اطلاعات، امنیت و سیستم ها

ارائه روش مقابله با حمله DDOS درشبکه بی‌سیم پهن باند چند رسانه ای

*** مهدی قهرمانی[۱]، محمد مهدی شیر محمدی [۲]**

گروه کامپیوتر،واحد همدان،دانشگاه آزاد اسلامی،همدان،ایران mehdighahremani934@gmail.com[1]

گروه کامپیوتر،واحد همدان،دانشگاه آزاد اسلامی،همدان،ایران Mmshirmohammadi@gmail.com[2]

چکیده

امروزه بسیاری از موسسات و مراکز آموزشی و سازمانها و ادارات موفق جهت معرفی خود و یا با هدف افزایش بهره وری کاری خود، از پیشرفتهای تکنولوژیکی برای ارائه محصولات جدید استفاده می‌کنند. یکی از مهمترین نمودها و محصولات این پیشرفتها، نرم افزارهای چندرسانه‌ای یا مالتی مدیا هستند که روزبه‌روز استفاده از آنها در زمینه های مختلف مانند آموزش و تجارت افزایش می یابد. با رشد سریع برنامه های چندرسانه‌ای از طریق اینترنت، حفظ کیفیت خدمات (QoS) ضروری شده است. ارائه تضمین خدمات معتبر از طریق اینترنت، بزرگترین چالش فعلی برای خدمات مبتنی بر پروتکل اینترنتی است. استفاده از ترافیک چندرسانه ای در ارتباط با رسانه های جریانی مانند: ویدئوکنفرانس با استفاده از شبیه ساز آپنت افزایش یافته است. در این مقاله، عملکرد سیستم های ویدئوکنفرانس را می‌توان بر اساس سناریوهای متفاوت مدل‌سازی کرد. این سناریوها: شامل شرایط سنگین و سبک و بررسی میزان بار و تاخیر شبکه است، همچنین امکان بررسی حملات DDOS که یک نوع حمله سایبری است که به دنبال از کار انداختن و مختل کردن سرویس‌های آنلاین و منابع شبکه‌ای مختلف است. در این حملات، مهاجم از تعداد زیادی دستگاه کامپیوتری (که به طور معمول توسط بدافزار تحت کنترل او درآمده‌اند) برای ارسال درخواست‌های تقلبی و بی‌فایده به سیستم مورد هدف استفاده می‌کند.هدف اصلی چنین حملاتی، اشباع کردن منابع شبکه و سیستمی مانند پهنای باند، پردازنده و حافظه است تا به این ترتیب سرویس‌های آن سیستم را از دسترس خارج و غیرفعال سازد. این موضوع باعث افزایش چشمگیر زمان پاسخ‌دهی و در نهایت فروپاشی کامل سرویس مورد هدف می‌شود.

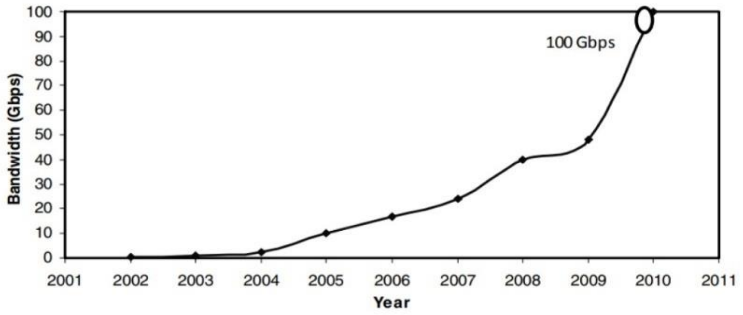
کلمات کلیدی: بار زیاد، بارکم، تاخیر، حمله DDOS، شبکه محلی بی سیم(WLAN)

۲- مقدمه

افزایش تقاضا برای انتقال داده موجب پیشرفت فناوری‌های شبکه‌های کامپیوتری مانند LAN، VLAN و WLAN شده است تا برنامه‌های کاربردی مفیدی را برای مشتریان فراهم کنند. VLAN به مهندسان شبکه اجازه می‌دهد تا به جای شبکه‌های فیزیکی، شبکه‌های منطقی را طراحی کنند و برای جداسازی شبکه به چندین دامنه پخش بدون مشکل تأخیر استفاده شود.[۱].پیشرفت فناوری‌های الکترونیکی موجب افزایش اهمیت ارتباطات بی‌سیم، به‌ویژه کاربردهای چندرسانه‌ای شده است. در شبکه‌های چندخدماتی، تخصیص مناسب و قابل اعتماد پهنای باند برای ارائه کیفیت خدمات تضمین‌شده، یکی از مهم‌ترین مسائل است. [۲]

در دهه اخیر، ارتباطات با استفاده از ابزارهای فناورانه محبوب شده است و بهبود برآورده کردن انتظارات مشتریان را به همراه دارد. ابتکارات جدید در شبکه های سلولی به منظور پاسخگویی به نیازهای کاربران در حال توسعه هستند و تنوع خدمات در دسترس است. بهبود کیفیت خدمات (QoS) می‌تواند برای ارتقاء کیفیت خدمات و رضایت مشتریان مهم باشد. فناوری اینترنت اخیراً روش‌های ارتباطی کاربران را تغییر و استفاده از کاربردهای IP را افزایش داده است. توسعه دسترسی پرسرعت IP و شبکه‌های مبتنی بر آن، توجه زیادی به خدمات تلفن اینترنتی (VoIP) جلب کرده است. برای جذابیت بیشتر VoIP، کیفیت آن باید مشابه با تلفن سنتی باشد.[۳].دسترسی عمومی به جریان‌های چند رسانه‌ای، اکنون اصلی‌ترین انگیزه در طراحی شبکه‌های کامپیوتری و ارتباطی نسل بعدی است. محصولات در حال توسعه هستند تا قابلیت‌های ترافیک چند رسانه‌ای را در تمام اتصالات شبکه افزایش دهند. این تغییر از شبکه تلفن آنالوگ به شبکه‌ای را نشان می‌دهد که از پروتکل داده‌ای اینترنت استفاده می‌کند. تکامل سریع این شبکه‌ها باعث افزایش انتظارات عمومی و فرصت‌های کارآفرینی شده است. پژوهشگران و تولیدکنندگان علاقه‌مند به انتقال جریان‌های چند رسانه‌ای در شبکه‌ها هستند و ما نیاز داریم تا شبکه بتواند همزمان چندین رسانه را پشتیبانی کند. دو نکته مهم در اینجا وجود دارد؛ اول اینکه رسانه‌ها به شکل دیجیتال نمایش داده می‌شوند و شبکه‌های ارتباطات دیجیتال از آنها استفاده می‌کنند. دوم اینکه پایانه‌های کاربر نیز تأثیر زیادی بر ارتباطات چند رسانه‌ای و دسترسی به آنچه در دسترس است، دارند.[۴].

حملات DDoS به تهدیدی رایج برای کسب‌وکارهای آنلاین تبدیل شده‌اند. این حملات به شکل مرئی و پُرهزینه‌ای از جرم‌های سایبری درآمده‌اند و کسب‌وکارهای آنلاین به منظور اجتناب از هزینه‌های ویرانگر تعطیلی مرتبط با DDoS، به صورت پیشگیرانه در این زمینه فعالیت می‌کنند. مطالعات نشان می‌دهد که میزان حملات DDoS افزایش یافته و ترافیک آنها نیز درحال افزایش است. باگذشت زمان، حملات DDoS تکامل یافته‌اند و مهاجمان چندین ماشین آسیب‌پذیر را بر روی قربانی هماهنگ می‌کنند تا اثر انکار سرویس را بیشتر کنند. شکل۱افزایش حملات DDOS را نشان می دهد[۵].



شکل ۱: افزایش حملات DDOS

۲-کارهای مرتبط

در این مقاله[۶] ما درباره مسائل امنیتی مهم و تهدیدات امنیتی مختلف، به‌ویژه ریسک‌های فعال و غیرفعال، در شبکه‌های بی‌سیم پهن‌باند بحث کردیم. حملات سرویس‌انکاری (DoS) شکل شدید حمله فعال به همه انواع شبکه‌های بی‌سیم، به‌ویژه شبکه‌های پهن‌باند هستند و قادرند یک گره‌تکی، قسمتی از شبکه بی‌سیم، کل شبکه بی‌سیم یا منابع شبکه بی‌سیم را هدف قرار دهند. حملات DoS می‌توانند دو ویژگی مهم شبکه‌های بی‌سیم امن، یعنی صحت داده و در دسترسی سرویس را تهدید کنند. شبکه‌های متناسب با ۸۰۲,۱۱ و ۸۰۲,۱۶ در مقابل انواع مختلف حملات DoS، نسبت به WMN به دلیل معماری چند قفسه، پوشش مساحت گسترده و اتصال کاربران ادهاک، آسیب‌پذیرتر هستند. در لایه فیزیکی، تمامی سه شبکه پهن‌باند به‌اندازه یکدیگر در برابر تهدیدات DoS آسیب‌پذیر هستند، در حالی که در لایه پیوند، ۸۰۲,۱۶ نسبت به بقیه نسبتاً امن‌تر است. WMN به دلیل هزینه‌های چند قفسه از نظر لایه شبکه به حملات DoS آسیب‌پذیرتر است نسبت به ۸۰۲,۱۱ و ۸۰۲,۱۶ که هزینه‌های مسیریابی کمتری دارند. با توجه به اهمیت WMN، نیاز به تلاش‌هایی در جهت مبارزه با حملات DoS وجود دارد. طراحی و پیاده‌سازی رادیوی شناور، مکانیزم‌های رمزنگاری و احراز هویت بهبود یافته و مکانیزم‌های تشخیص تجاوز انحصاری، اقدامات مقابله ممکن هستند که باید مورد بررسی قرار گیرند. نیاز به تحقیقات بیشتر در زمینه امنیت شبکه‌های بی‌سیم پهن‌باند وجود دارد. فقط یک شبکه بی‌سیم پهن‌باند امن مورد پذیرش بالا برای استقرار تجاری در سطح گسترده خواهد بود.

- آنتونی تانوری و همکاران از نقشه تفاوت (disparity map) برای جمع‌آوری دید گسترده‌تری از داده‌های چندرسانه‌ای استفاده کردند. این نقشه با استفاده از تجزیه و تحلیل عمق ۳ بعدی، اطلاعات مربوط به عمق اشیا را فراهم می‌کند.

- این روش باعث کاهش زمان محاسبات و ارائه راه‌حل برای پردازش داده‌ها در زمان واقعی می‌شود. حسگرها با مطابقت دادن تصاویر استریو، نقشه تفاوت را ایجاد می‌کنند که باعث کاهش تأثیر ترافیک بر پهنای باند و افزایش طول عمر شبکه حسگر چندرسانه‌ای بی‌سیم (WMSN) می‌شود[۷].

- احمد متین و همکاران در مقاله خود[۸] به مقایسه شبکه‌های حسگر بی‌سیم (WSN) و شبکه‌های حسگر چندرسانه‌ای بی‌سیم (WMSN) پرداخته‌اند. WSN به طور کلی ارزان، مصرف انرژی کم و تعداد زیادی حسگر همراه با ایستگاه‌های پایه دارد. در مقابل، WMSN برای پردازش جریان‌های ویدئویی، صوتی و داده‌های حسگر اسکالار طراحی شده است.

- وائل علی حسین و همکاران در مقاله [۹] طراحی و تحلیل عملکرد پروتکل مسیریابی قابل اطمینان-مطمئن را برای شبکه‌های حسگر چندرسانه‌ای بی‌سیم متحرک انجام داده‌اند. آنها یک پروتکل مسیریابی جدید را طراحی کرده‌اند که بر اساس مسیریابی چند-مسیری با عبور از بهترین گره از نظر نرخ انتقال داده و نزدیکی به مقصد است. این پروتکل را GFTEM Greedy Forwarding with Throughput and Energy Metric نامیده‌اند. عملکرد را با سایر پروتکل‌های مسیریابی موجود مانند: AODV ، DYMO و پروتکل مسیریابی stateless درمحیط شبکه‌های Wi-Fi مقایسه کرده‌اند. نتایج نشان می‌دهد که GFTEM در مقایسه با سایر پروتکل‌ها، تأخیر پایان-به-پایان کمتر، نرخ از دست رفتن بسته‌های کمتر و کارایی انرژی بهتری دارد.

-ناصم عباس و فنگکی یو در مقاله [۱۰] یک الگوریتم کنترل ترافیک ازدحام (TCCA) را برای شبکه‌های حسگر چندرسانه‌ای پیشنهاد داده‌اند: TCCAاز ترکیب دو شاخص ازدحام برای تشخیص ازدحام استفاده می‌کند: اشغال بافر و نرخ تغییر اشغال بافر همچنین یک کنترل کننده نرخ همراه با بازخورد را توسعه داده‌اند تا کیفیت جریان ویدیویی را بهبود بخشند. مکانیزم‌های مختلفی برای بازانتقال بسته‌های از دست رفته ارائه شده است، به طوری که بسته‌های گم شده موقتاً ذخیره و زمانی که ازدحام برطرف شد، بازانتقال می‌شوند. این طرح با استفاده از ۱۴ مبدل Pi مورد آزمایش قرار گرفته است. نتایج نشان می‌دهد که TCCA با کنترل نرخ و کاهش از دست رفتن بسته‌ها، عملکرد بهتری نسبت به روش‌های متداول دارد.

در مقاله [۱۱] مهم‌ترین جنبه چالش‌برانگیز در انتخاب سرور چند رسانه‌ای پویا، نرخ بیت تطبیقی هر جریان چند رسانه‌ای است که با وضعیت شبکه تغییر می‌کند. بنابراین، در این مقاله، ما بر روش تخمین پهنای باند موجود یک پیوند بی‌سیم تمرکز کرده‌ایم.

این روش باید ویژگی‌های زیر را داشته باشد:

(الف) قابل اجرا در برنامه‌های کاربردی بر روی زمان واقعی مانند خدمات پخش چند رسانه‌ای باشد.

(ب) ساده و مؤثر در تخمین پهنای باند موجود باشد.

(ج) بار مصرفی پایینی داشته باشد.

این مقاله [۱۲]چارچوب QoS IEEE 802.16e، IEEE 802.16m و LTE را توضیح می‌دهد و ویژگی‌های QoS آنها را با یکدیگر مقایسه می‌کند.ارائه QoS مورد نیاز برای تحویل تجربه کاربری خوب در اینترنت موبایل بسیار مهم است. مفهوم QoS حتی اهمیت بیشتری پیدا می‌کند، زیرا قابلیت‌های دستگاه‌ها تمایل مصرف‌کنندگان برای استفاده از محتوای رسانه‌ای غنی‌تر مانند ویدئو را نشان داده است. فناوری‌های بی‌سیم نسل چهارم مانند IEEE 802.16e، IEEE 802.16m و LTE برای پشتیبانی از نیازهای QoS کنونی و آینده طراحی شده‌اند. پشتیبانی QoS مبتنی بر جریان-محور و یک‌طرفه در IEEE 802.16e، به انواع مختلف جریان سرویس مانند: UGS و BE امکان ارائه ترافیک زمان‌واقعی و غیرزمان‌واقعی را می‌دهد. مکانیزم درخواست و اعطای پهنای باند صعودی به MSها امکان درخواست و دریافت منابع مورد نیاز برای انتقال داده در جهت صعودی را می‌دهد. ویژگی‌های پیشرفته مانند یک سرویس برنامه‌ریزی جدید، دسترسی سریع و درخواست پهنای باند به تأخیر انداخته شده در IEEE 802.16m، قابلیت‌های ارائه QoS مورد نیاز برای برنامه‌های کاربردی اینترنت موبایل نسل بعدی را بیشتر بهبود می‌دهد. مکانیزم‌های QoS LTE از کنترل QoS آغازشده توسط شبکه بر اساس GBR و غیر-GBR بیننده‌ها پیروی می‌کنندکه یک رفتار انتقال بسته بر اساس کلاس برای ارائه ترافیک زمان‌واقعی و غیرزمان‌واقعی است.

۳-مکانیزم RTS/CTS

در شبکه های بی‌سیم، ایستگاه پایه برای انتقال آماده است و قبل از انتقال هر فریم داده، یک فریم کوتاه درخواست برای ارسال (RTS) می‌فرستد.. تأثیر یک فریم RTS کمتر از تأثیر فریم داده واقعی است زیرا اختلاف اندازه آنها کمتر است. وقتی ایستگاه پایه در گیرنده برای دریافت آماده است، فریم RTS با یک فریم ارسال "مجاز برای ارسال" (CTS) برای فرستنده تأیید می‌شود و بنابراین همه ترافیک از ایستگاه دیگر مسدود می‌شود. علاوه بر این، اگر فرستنده، فریم CTS را دریافت کند، یک فریم داده در صورتی که کانال برای طول انتقال کامل رزرو شده باشد، ارسال می‌شود. در نهایت، فریم تأیید (ACK) توسط گیرنده به فرستنده بر اساس دریافت فریم ارسال می‌شود. بنابراین، ارزیابی کارایی

قابل توجه مکانیزم اختیاری مصافحه RTS/CTS بر عملکرد شبکه های محلی بی‌سیم مبتنی بر IEEE 802.11 اهمیت دارد.کیفیت سرویس (QoS) در شبکه‌های ارتباطی به مجموعه‌ای از ویژگی‌ها اشاره دارد که بیانگر کیفیت و قابلیت اطمینان سرویس ارائه شده توسط آن شبکه است.

برخی از این ویژگی‌ها عبارتند از:

۱. تأخیر (Delay): زمان لازم برای انتقال بسته‌ها از منبع به مقصد برای برنامه‌های زنده مانند صوت و تصویر، تأخیر کم اهمیت دارد.

۲. نوسان تأخیر (Jitter): تغییرات در تأخیر بسته‌ها که می‌تواند باعث قطع و وصل در ارتباطات شود.

۳. نرخ از دست رفتن بسته‌ها (Packet Loss Rate): درصد بسته‌هایی که در طول مسیر از بین می‌روند.

۴. باندای عبوری (Throughput): حداکثر میزان داده‌ای که شبکه می‌تواند با کیفیت مطلوب انتقال دهد.

سرویس‌دهی با QoS مناسب به معنای تضمین این پارامترها در حد مطلوب برای کاربردهای مختلف است. این امر نیازمند مکانیزم‌هایی برای مدیریت ترافیک و منابع شبکه است که متناسب با نیازهای کاربردی تنظیم می‌شود.

۴-پیاده‌سازی و شبیه‌سازی OPNET

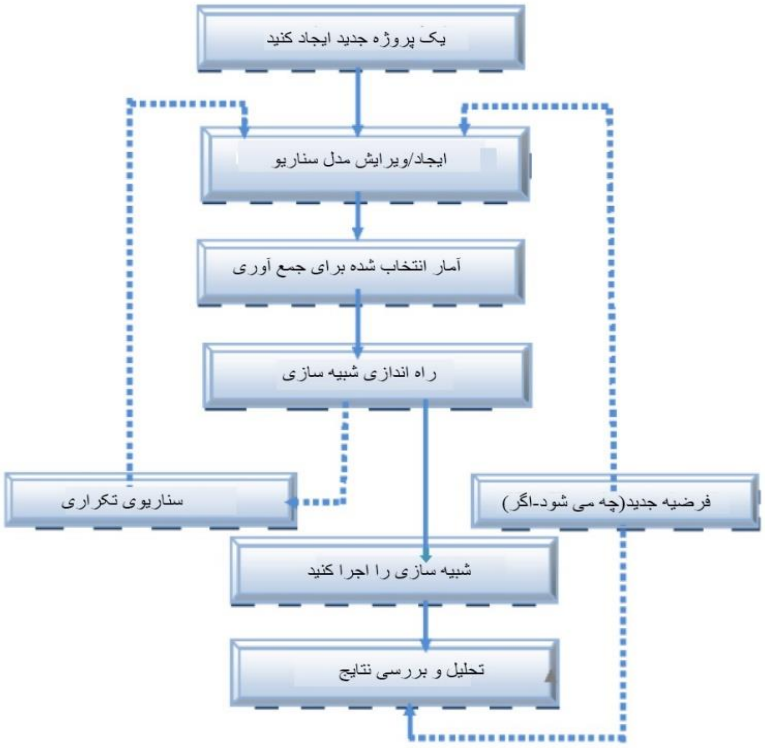
۴-۱.شبیه ساز OPNET

OPNET (Optimized Network Engineering Tool) شرکتی است که در سال ۱۹۸٦ در انستیتوی فناوری ماساچوست (MIT) تأسیس شد. یک سال بعد، در سال ۱۹۸۷، اولین نرم‌افزار شبیه‌سازی عملکرد شبکه‌های تجاری توسط این شرکت منتشر شد که می‌توانست ابزار بهینه‌سازی عملکردهای مهم شبکه را فراهم کند و یک انقلاب در شبیه‌سازی شبکه ایجاد کرد. ایجاد مدیریت عملکردهای تحلیلی شبکه با شبیه‌سازی امکان‌پذیر شد.

علاوه بر مدلر OPNET، توسعه محصولات دیگری مانند: OPNET Development Kit و WDM Guru نیز انجام شده است. شبیه‌سازی به عنوان یک روش فزاینده محبوب برای مطالعه عملکردها و کارکردهای مدل‌های پیشنهادی در سناریوهای مختلف در نظر گرفته می‌شود. شبیه‌سازی یک رویه آزمایشی از یک نمونه طراحی شده در یک پلتفرم است که محیط واقعی را تقلید می‌کند و فرصتی برای مطالعه، ایجاد و اصلاح عملکرد طرح پیشنهاد شده با هدف تقویت و ضعف انتظارات قبل از پیاده‌سازی مدل در محیط واقعی فراهم می‌کند.

۵-مدل پیشنهادی

شبیه‌سازی هر سیستمی با مراحلی که در فرآیند شبیه‌سازی صورت می‌گیرد، آغاز می‌شود. برای هر سناریو، ترافیک شبکه و پیکربندی‌ها اصلاح می‌شوند و شبیه‌سازی اجرا می‌شود. نمودار جریان برای نشان دادن مراحل کلیدی انجام شده برای ارزیابی عملکرد یک شبکه محلی بی‌سیم در شکل ۲ ارائه شده است.



شکل ۲: نمودار جریان برای ارزیابی عملکرد WLAN

این نمودار جریان مراحل اصلی را به شرح زیر نشان می‌دهد:

۱. تعریف سناریوهای شبیه‌سازی

۲. پیکربندی پارامترهای شبکه

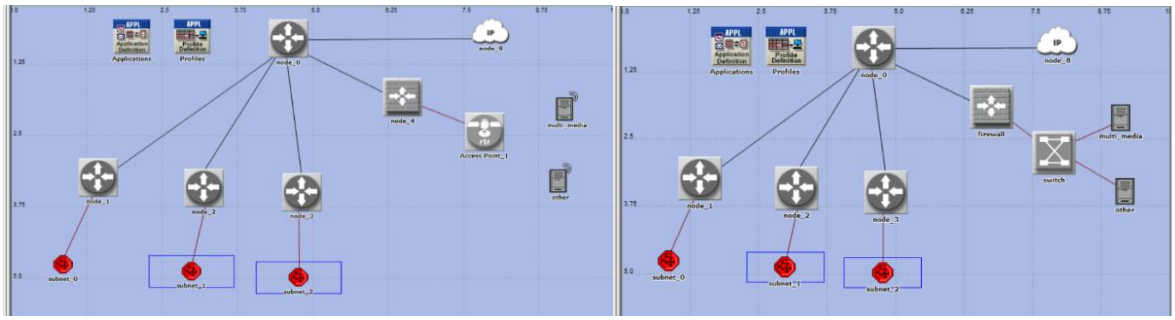
۳. اجرای شبیه‌سازی

۴. جمع‌آوری و تحلیل نتایج

۱-۵. سناریوی پایه

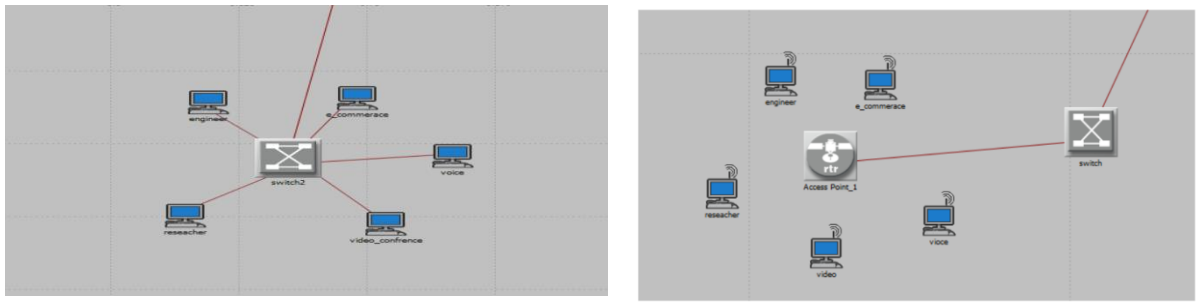
پیکربندی پایه ۸۰۲,۱۱g به عنوان یک سناریوی پایه با استفاده از یک مدل استاندارد از تنظیمات شبکه محلی بی‌سیم OPNET 14.5 ایجاد شده است. در این سناریو، رفتار یک شبکه محلی بی‌سیم ۸۰۲,۱۱g با یک زیرساخت در چارچوب شبکه محلی بی‌سیم سازمان‌یافته برای بهتر نمایش پیکربندی واقعی شبکه، مورد بررسی قرار می‌گیرد.(همانطور که در شکل (الف) نشان داده شده است).

یک ابر پروتکل اینترنتی (IP) می‌تواند برای نشان دادن اتصال اینترنت اصلی به یک لینک سریال نقطه به نقطه (1.544Mbps) T1 استفاده شود. سه زیرشبکه در هر طرف ابر IP از طریق یک دروازه IP که به یک لینک T1 نقطه به نقطه متصل است، قرار گرفته‌اند. همچنین دو سرور از طریق یک سوییچ مرکزی با استفاده از یک لینک BasetT ۱۰۰متصل هستند که در شکل (الف) نشان داده شده و به صورت بی‌سیم در شکل (ب) قابل مشاهده است.



الف- چارچوب‌های سرور سیم‌دار شبیه‌سازی شده ب- چارچوب‌های سرور بی‌سیم شبیه‌سازی شده

یک زیرشبکه اول در سمت راست ابر پروتکل اینترنتی (IP) قرار دارد و سرورهای شبکه ترافیک از طریق اترنت BasetT ۱۰۰ به هم متصل هستند. این سرورها از طریق لینک اترنت Baset ۱۰۰ به دیوار آتش متصل هستند و می‌توانند به عنوان منابع و مقاصد در همه برنامه‌ها مانند ویدیو کنفرانس، پروتکل انتقال فایل (FTP)، پروتکل انتقال فایل (HTTP)، برنامه‌های صوتی، پست الکترونیکی (ایمیل) و شبیه‌سازی پایگاه داده در شبکه کامل که ترافیک مبادله شده با گره‌های موبایل WLAN۸۰۲,۱۱ g را مشخص می‌کند، استفاده شوند (همانطور که در شکل های زیر نشان داده شده است).



شکل الف : زیرشبکه ۲ WLAN ۸۰۲,۱۱ شکل ب : زیرشبکه ۱ WLAN ۸۰۲,۱۱g

زیرشبکه دوم، دفتر شعبه دورکار را نشان می‌دهد که شامل پنج ایستگاه کاری در LAN دفتر است که با لینک BaseT ۱۰۰ به هم متصل هستند. این LAN دفتر از طریق یک سوییچ مرکزی با لینک اترنت Base ۱۰۰ به هم متصل است تا یک موقعیت دفتر واقعی را که از استاندارد LAN اترنت سریع استفاده می‌کند، شبیه‌سازی کند. دروازه IP LAN را به ابر IP متصل می‌کند، این دروازه به LAN دفتر از طریق لینک

اترنت Base T ۱۰۰ متصل است، در حالی که لینک سریال نقطه به نقطه T1 ابر IP را به دروازه IP متصل می‌کند (همانطور که در شکل(ب) نشان داده شده است).

سرانجام، زیرشبکه سوم در سمت دیگر ابر پروتکل اینترنتی قرار دارد. اتصال شبکه بی‌سیم محلی (WLAN) از طریق نقطه دسترسی AP به LAN دفتر از طریق یک سوئیچ مرکزی با استفاده از سیم‌کشی اترنت انجام می‌شود تا محیطی از دفتر واقعی در استانداردهای LAN اترنت سریع را شبیه‌سازی کند که شامل گسترش یک WLAN به یک منطقه از سیم‌کشی دشوار یا زیبایی‌شناسی مورد نیاز مانند یک اتاق رسانه (صوت یا ویدیو) یا کنفرانس است (همانطور که در شکل ۳ نشان داده شده است).

شکل ۳: زیرشبکه ۳ WLAN دفاتر

LAN دفتر به طور مساوی بین پروفایل‌ها تقسیم شده است، به طوری که هر پروفایل یک ایستگاه کاری دارد. در اینجا هدف اصلی تحلیل عملکرد مفید ادراک شده توسط اپراتور مربوط به کاربران WLAN است. یک زیرشبکه WLAN با پنج گره موبایل به پروفایل‌های مختلف اختصاص داده شده است، همانطور که در جدول ۱ نشان داده شده است.

جدول ۱: نمایه‌های تخصیص داده شده به گره‌های موبایل در زیرشبکه WLAN

مشخصات کاربر	گره موبایل
مهندس	ایستگاه۱
محقق	ایستگاه۲
مشتری تجارت الکترونیک	ایستگاه۳
شخص فروش	ایستگاه۴

۵-۲. سناریوهای بار چندرسانه‌ای

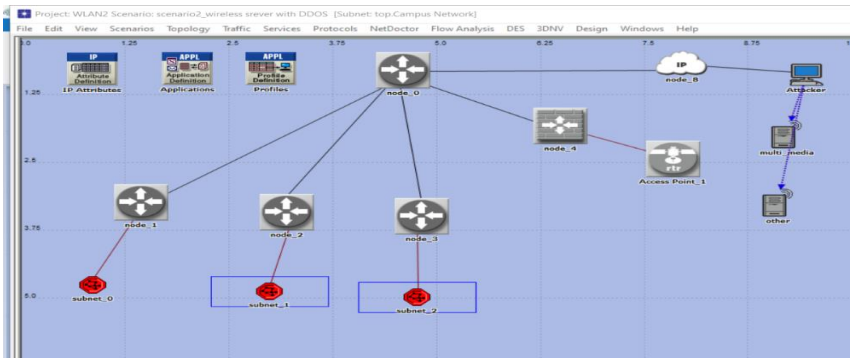
ترافیک چندرسانه‌ای می‌تواند به شکل یک ویدئو کنفرانس در شبکه نمایش داده شود. این شکل از کنفرانس شامل تصاویر، داده و صدا، و نمایش ترافیک چندرسانه‌ای تعریف شده است. در حالی که سرور ویدیو برای کمک به برنامه ویدئو کنفرانس در جزئیات شبکه ارائه شده است.

۵-۳. سناریوی حمله ی DDOS

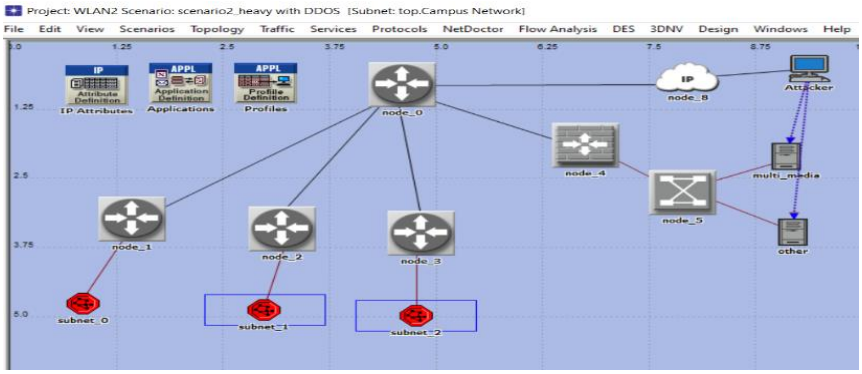
همان طور که مشاهده می‌کنید یک نوع حمله از نوع حمله (DDOS) به آن اضافه می شود و ۳ سناریو :

سناریوی اول :حمله DDOS به وایرلس سرور(با بار کم) شکل ٤

سناریوی دوم و سوم حمله DDOS به سرور با سیم (با بارکم و بار سنگین) شکل ۵



شکل ۴سناریوی اول : حمله DDOS به وایرلس سرور(با بار متوسط)

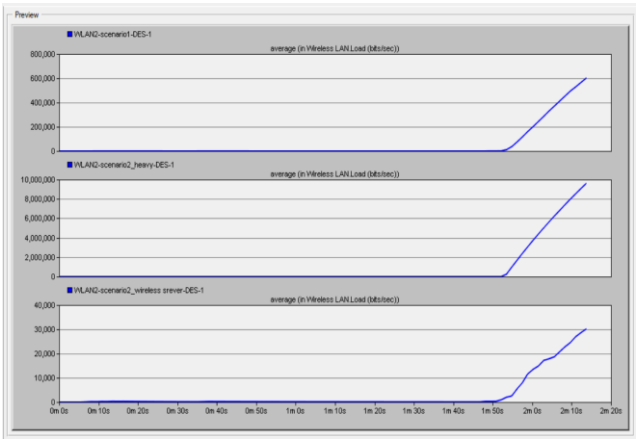


شکل ۵ سناریوی دوم :حمله DDOS به سرور با سیم (بار سنگین و بار کم)

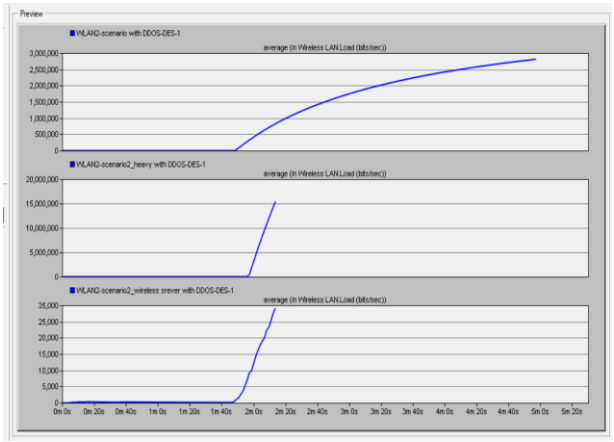
۶. نتایج و بحث شبیه‌سازی

۶,۱. بار

بار اولین پارامتری است که بر کل عملکرد کارایی بی‌سیم تأثیر می‌گذارد. ارزیابی بار مربوط به دریافت داده‌های ارسال شده است، داده‌ها دارای میانگین کلی بار WLAN با مقدار تقریبی (٤٣٠,٧٤٠٧) Kbps در مدت ۵ دقیقه اجرا شده است. شکل ۶ نتایج مربوط به سه سناریو قبل از حمله را نشان می‌دهد وشکل ۷ نتایج حمله DDOS را نشان می دهد.



شکل ۶: قبل از حمله DDOS



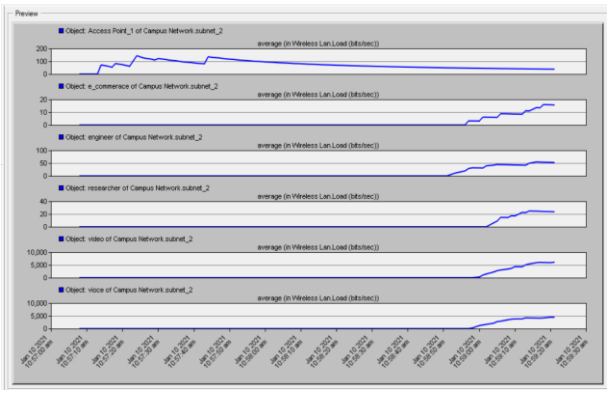
شکل۷: در زمان حملهDDOS

در مقایسه این دو تصویر:

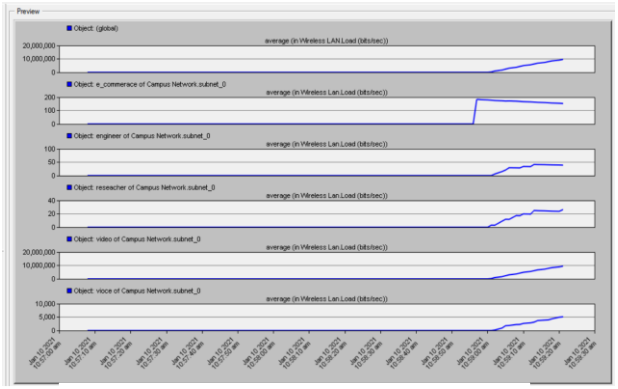
هر ۳ سناریو مقایسه شده است (قبل از حمله و بعد از حمله):

۱. هر دو تصویر نمودارهایی را نمایش می‌دهند که انرژی در (Wireless LAN/Local (M bits/s)) را در طول زمان برای پیکربندی‌های شبکه مختلف نشان می‌دهند.در شکل ۶ سناریوی اول مقدار بار به ۶۰۰/۰۰۰ رسیده است و در سناریوی دوم (با بار زیاد) به مقدار نزدیک ۱۰ /۰۰۰/۰۰۰ و در سناریوی سوم وایرلس سرور(با بار کم) به مقدار :۳۰/۰۰۰ رسیده است. ۲-مشاهده می شود که در شکل ۷ میزان بار بیش تر شده است چون حمله DDOS به شبکه اتفاق افتاده است که در سناریوی اول مقدار بار به ۳/۰۰۰/۰۰۰رسیده است و در سناریوی دوم (با بار زیاد) به مقدار نزدیک ۱۵ /۰۰۰/۰۰۰ و در سناریوی سوم وایرلس سرور(با بار کم) به مقدار :۳۵/۰۰۰ رسیده است. از نظر زمانی هم در شکل ۶ در وایرلس سرور در زمان ۱ دقیقه و ۵۰ ثانیه بوده و بعد از حمله نیز در زمان: ۱ دقیقه و ۵۰ ثانیه اتفاق افتاده است. وقتی یک حمله DDoS به یک شبکه رخ می‌دهد، میزان ترافیک ورودی به آن شبکه به طور شدیدی افزایش می‌یابد. این افزایش بار باعث می‌شود که منابع شبکه مانند باند پهنای اینترنت، ظرفیت سرور و پهنای باند ارتباطی به سرعت تحت فشار قرار گیرند و در نتیجه، دسترسی به سرویس‌های شبکه برای کاربران واقعی

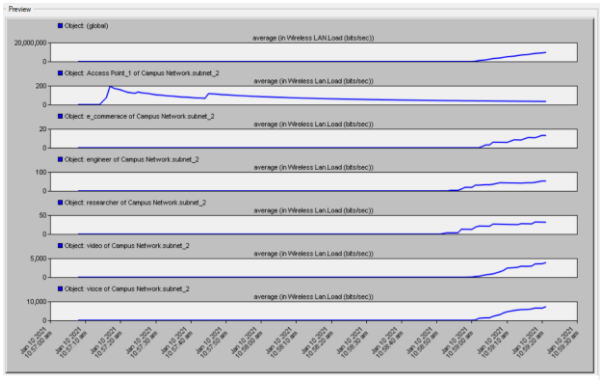
دچار اختلال شود. بنابراین، نمودارهای مربوط به چنین حملاتی معمولاً افزایش چشمگیر در میزان انرژی یا ترافیک شبکه را نشان می‌دهند که ناشی از بار سنگین وارد شده به سیستم است. این افت عملکرد و دسترسی‌پذیری شبکه می‌تواند منجر به اختلال در خدمات و افت رضایت کاربران شود.



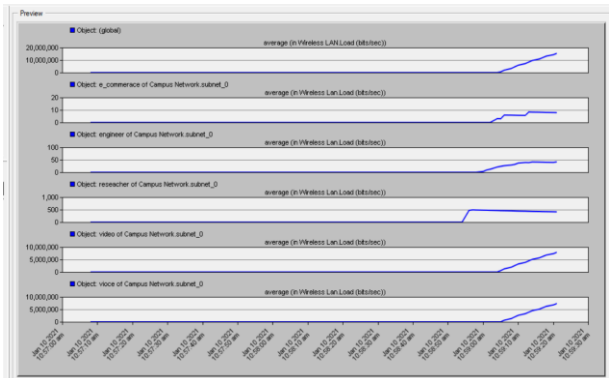
شکل ۹ مقادیر بار فردی با بار زیاد (سابنت ۲)



شکل ۸ مقادیر بار فردی با بار زیاد (سابنت ۰)



شکل ۱۱: مقادیر فردی با بار زیاد بعد از حمله DDOS (سابنت۲)



شکل ۱۰ :مقادیر فردی با بار زیاد بعد از حمله DDOS (سابنت۰)

در این سناریوی شبیه‌سازی، دو حالت مختلف بار شبکه نمایش داده شده است: برای بار زیاد

۱. قبل از حمله DDoS (شکل‌های ۸ و۹):

- در این حالت، مقادیر بار برای subnet=0 و subnet=2 در تاخیر کمتری قرار دارند.

- میزان ترافیک و انرژی استفاده شده در شبکه در این مرحله در محدوده‌ای طبیعی و قابل قبول است.

۲. بعد از حمله DDoS (شکل‌های ۱۱ و۱۰):

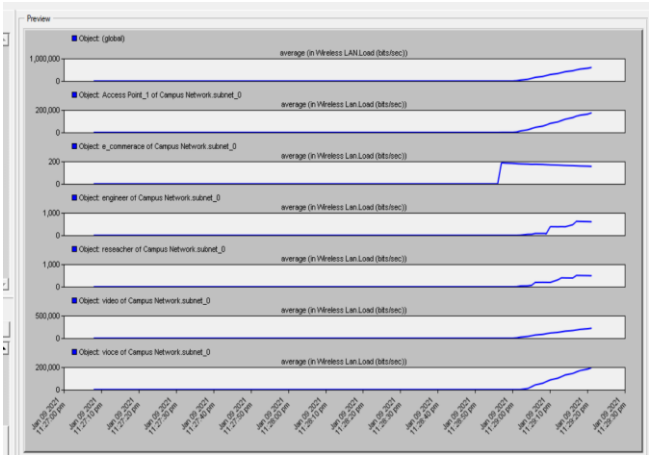
- در این حالت، مقادیر بار برای subnet=0 و subnet=2 افزایش یافته‌اند.

این افزایش بار ناشی از حمله DDoS به سیستم است.

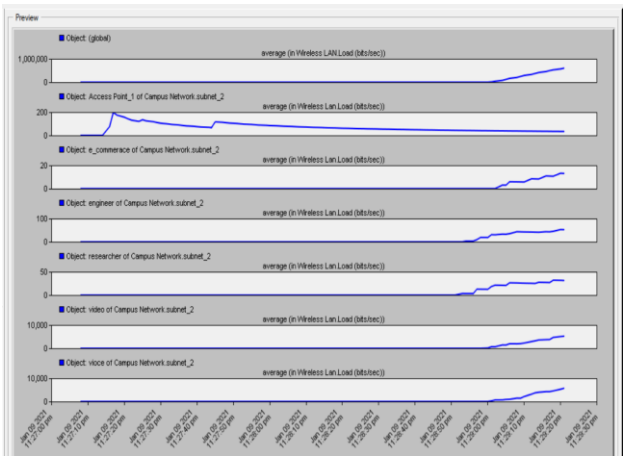
بنابراین، مقادیر بار در حالت بعد از حمله DDoS به طور قابل ملاحظه‌ای بالاتر از حالت قبل از حمله است و این افزایش بار، نشان‌دهنده اثرات مخرب این نوع حملات بر روی زیرساخت‌های شبکه است.

جدول ۲ سناریوی مقادیر بار انفرادی سناریوی ۱ (سبک) و سناریوی ۲ (سنگین)

نوع گره	بار WLAN (kbps)(سنگین) زیر شبکه1	بار WLAN(سنگین) (kbps) زیر شبکه سه	بار WLAN (kbps)(سبک) زیر شبکه یک	بار WLAN (kbps)(سبک) زیر شبکه 3
نقطه دسترسی	(AP2) 42.07	(AP1) 200.2	(AP1) 916124	(AP3) 899128
تجارت الکترونیک	0	188.4	73	146
مشتری				
مهندس	0	0	223	232
محقق	0	0	202	260
ویدئو	0	0	893783	87652
کنفرانس				
صدا	0	0	17878	18201
مقدار فرعی	42.07	388.6	1828285	1794502
جمع کل	430.7407407		3622787.467	



شکل۱۲. مقادیر بار فردی برای سناریوی (با بار کم)



شکل۱۳. مقادیر بار فردی برای سناریوی (با بار کم)

در این حالت نیز سناریوی شبیه‌سازی، دو حالت مختلف بار شبکه نمایش داده شده است: برای بار کم

۱. قبل از حمله DDoS (شکل‌های ۱۳ و ۱۲):

- در این حالت، مقادیر بار برای subnet=0 و subnet=2 در تاخیرخیلی کمتری قرار دارند.

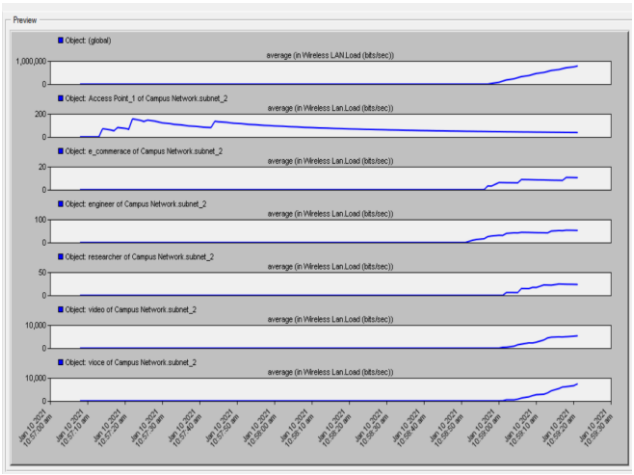
- میزان ترافیک و انرژی استفاده شده در شبکه در این مرحله در محدوده‌ای طبیعی و قابل قبول است.

۲. بعد از حمله DDoS (شکل‌های ۱۵ و ۱۴):

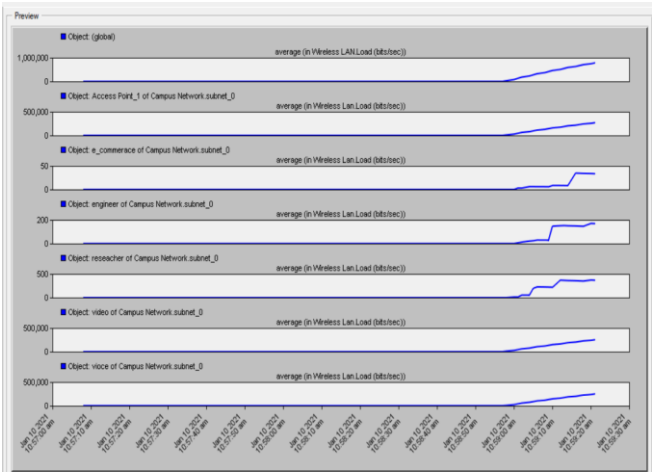
- در این حالت نیز، مقادیر بار برای subnet=0 و subnet=2 افزایش کمی را داشته اند.

- این افزایش بار ناشی از حمله DDoS به سیستم است.

بنابراین، مقادیر بار در حالت بعد از حمله DDoS به طور قابل ملاحظه‌ای بالاتر از حالت قبل از حمله است.



شکل۱۵. مقادیر بار فردی برای سناریوی (با بار کم) بعد از حمله



شکل۱۴. مقادیر بار فردی برای سناریوی (با بار کم) بعد از حمله

۶،۲. تاخیر

تاخیر می‌تواند یک معیار بنیادی برای توصیف کیفیت سرویس (QoS) هر شبکه ای، به ویژه در زمان واقعی باشد. در کاربرد چندرسانه‌ای، تاخیر می‌تواند یک پارامتر مرکزی برای انتخاب عملکرد مؤثر لایه MAC، زمان عملیات آن و مکانیسم Required To Send/ Clear To Send (RTS/CTS) باشد. تاخیر دو نوع اصلی دارد: تاخیر دسترسی به رسانه و آمار تاخیر کلی انتقال بسته. مشاهده می‌شود که تاخیر WLAN که تاخیر پایان تا پایان همه بسته‌های دریافتی توسط MAC های WLAN توسط همه گره‌های شبکه WLAN و سپس هدایت شده به لایه‌های بالاتر را مشخص می‌کند، بسیار بالا است که نشان دهنده تلاش‌های مجدد زیاد است.

در شکل ۱۶، نمودارها مربوط به سه سناریوی مختلف هستند:

WLAN2-scenario2_heavy_with_DDOS-DES-**1**

WLAN2-scenario2_heavy_DES-**1**

WLAN2-scenario1_wireless_server_DES-**1**

هر سناریو با یک رنگ مشخص شده است و روند میانگین تاخیر ترافیک شبکه را در طول زمان نشان می‌دهد. درشکل ۱۶، تاخیر ترافیک شبکه برای سه سناریو نشان داده شده است.

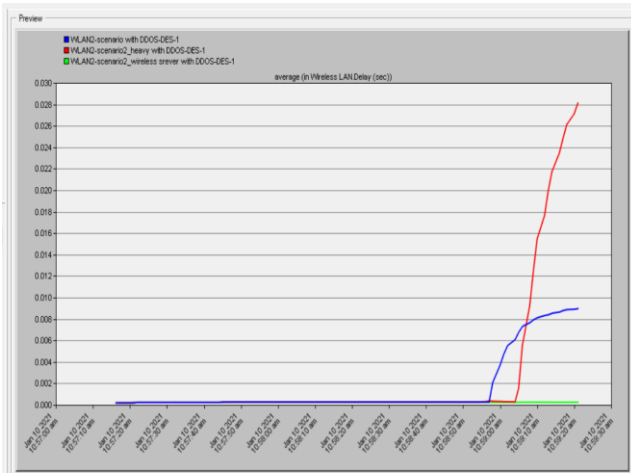
شکل۱۷ نمودارهایی هستند که تاثیر حمله DDOS را بر روی ترافیک شبکه نشان می‌دهند.

WLAN2-scenario_with_DDOS-DES-**1**

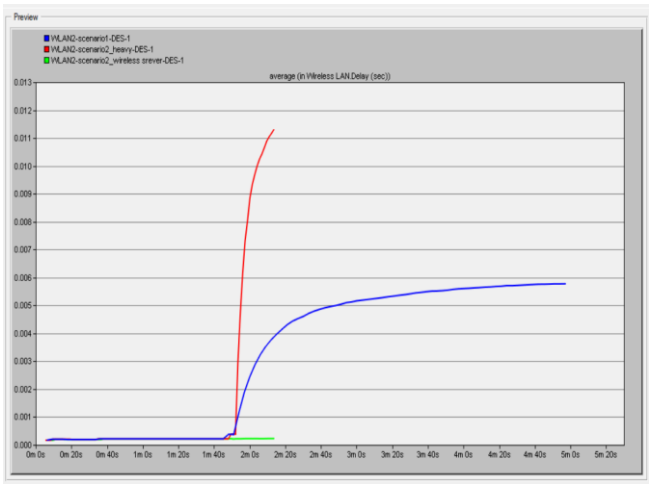
WLAN2-scenario2_heavy_with_DDOS-DES-**1**

WLAN2-scenario2_wireless_server_with_DDOS-DES-**1**

درشکل ۱۷، تاخیر ترافیک شبکه بی‌سیم محلی به صورت واضح تر و با جزئیات بیشتری نشان داده شده است. مقایسه این دو تصویر نشان می‌دهد که حمله DDOS چگونه تاخیر ترافیک شبکه را به شکل قابل توجهی افزایش می‌دهد.



شکل ۱۷ : میزان تاخیر بعد از حمله(به صورت یک نمودار)



شکل ۱۶ میزان تاخیر قبل از جمله(به صورت یک نمودار)

در یک حمله DDoS به شبکه، عامل اصلی افزایش تأخیر در شبکه است:

۱. کاهش پاسخ‌گویی سیستم:

- با اشباع منابع شبکه، سیستم قادر به پردازش و پاسخ‌گویی به همه درخواست‌ها به موقع نخواهد بود.

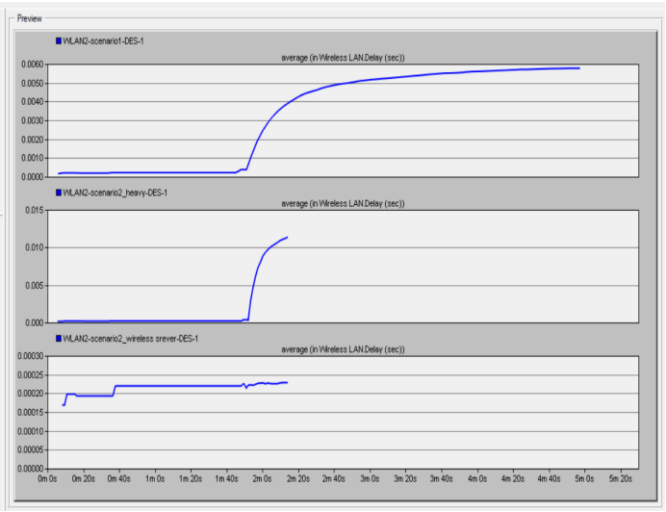
- این موضوع منجر به افزایش چشمگیر در زمان پاسخ‌گویی و تأخیر در ارائه سرویس‌ها به کاربران واقعی می‌شود.

۲. اختلال در مسیریابی و قطع ارتباط:

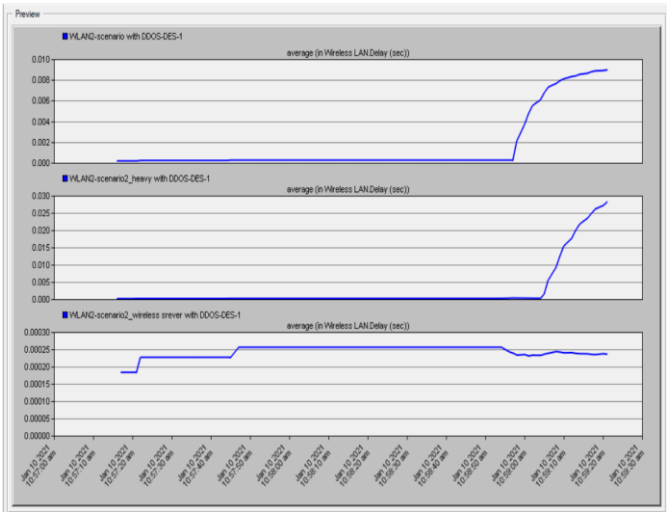
- در شرایط اشباع شبکه، مسیریابی ترافیک و انتقال داده‌ها دچار اختلال می‌شود.

- در نتیجه، بسته‌های داده به درستی مسیریابی نشده و ممکن است ارتباطات قطع شوند.

بنابراین، نمودارهای مربوط به چنین حملاتی معمولاً افزایش چشمگیر در میزان تأخیر در شبکه را نشان می‌دهند. این افزایش تأخیر ناشی از بار سنگین وارد شده به سیستم و ناتوانی آن در پاسخ‌گویی به موقع به همه درخواست‌ها است. این موضوع می‌تواند منجر به قطع ارتباطات و اختلال جدی در خدمات ارائه شده به کاربران نهایی شود. درشکل۱۷ نمودارهای بعد از حمله: سناریوی اول مقدار تاخیر به ۰,۰۱۰ رسیده است و در سناریوی دوم (با بار زیاد) مقدار تاخیر به مقدار نزدیک ۰,۰۲۸ و در سناریوی سوم وایرلس سرور(با بار کم) آن چنان تاخیری نداشته است. در مقابل، شکل های۱۸ و ۱۹ که قبل از حمله و بعد از حمله را به صورت ۳ سناریو و نمودارهای تکی ارائه داده اند، این افزایش تأخیر به خوبی نمایش داده شده است.



شکل ۱۸ : میزان تاخیر قبل از حمله(به صورت نمودارهای جدا از هم



شکل۱۹: میزان تاخیر بعد از حمله (به صورت نمودار های جدا از هم)

۷- نتیجه‌گیری

در این مقاله، عملکرد شبکه‌های WLAN قبل از حمله و بعد از حمله از نظر تأخیر انتهایی به انتهایی، با استفاده از ترافیک چندرسانه‌ای در سناریوی کنفرانس ویدئویی مورد ارزیابی قرار گرفته است. شبیه‌سازی‌ها با استفاده از مدل‌ساز OPNET 14.5 تنظیم شده است. مقاله به استفاده از مکانیزم RTS/CTS (درخواست برای ارسال/واضح برای ارسال) در شبکه‌های بی‌سیم اشاره می‌کند. این یک پروتکل لایه MAC است که در شبکه‌های WLAN IEEE 802.11 برای کمک به هماهنگی دسترسی به رسانه بی‌سیم مشترک و کاهش مشکل گره پنهان استفاده می‌شود. در مجموع، پروتکل کلیدی مورد بحث در این مقاله، پروتکل WLAN IEEE 802.11 است که از مکانیزم RTS/CTS به عنوان بخشی از هماهنگی دسترسی لایه MAC استفاده می‌کند. عملکرد کیفیت سرویس (QoS) در شبکه‌های IP می‌تواند به کارگیری کارآمدترین روش از منابع شبکه موجود را برای به حداقل رساندن تأخیرهای ترافیک شبکه که دارای خدمات چندرسانه‌ای متنوعی از جمله صدا، ویدئو و پایگاه داده است، به کار گیرد. چهار سناریو برای شبکه ایجاد شده است: سناریوی ۱ (بار سنگین)، سناریوی ۲ (بار متوسط تا پایین) و سناریوی ۳ (بار سنگین)سناریوی۴ (حمله DDOS) مقایسه بین آنها انجام شده است و ارزیابی‌های عملکردی هر دو به بار و تأخیر عملکردها مربوط بوده است. در این آزمون‌های عملکرد، نتایج در دو سناریوی قبل از حمله و بعد از حمله مقایسه شده است.

مراجع

[۱] Al-Khaffaf, D.A.J. and M.G. Al-Hamiri, Performance evaluation of campus network involving VLAN and broadband multimedia wireless networks using OPNET modeler. TELKOMNIKA (Telecommunication Computing Electronics and Control), 2021. **19**(5): p. 1490-1497.

[۲] Atmaca, S., et al., A new MAC protocol for broadband wireless communications and its performance evaluation. Telecommunication Systems, 2014. **57**: p. 13-23.

[۳] Lafta, S.A., et al., Quality of service performances of video and voice transmission in universal mobile telecommunications system network based on OPNET. Bulletin of Electrical Engineering and Informatics, ۲۰۲۱. ۱۰(٦): p. ۳۲۰۲-۳۲۱۰.

[٤] Ghazala, M.M.A., M.F. Zaghloul, and M. Zahra, Performance evaluation of multimedia streams over Wireless Computer Networks (WLANs). International Journal of Advanced Science and Technology, 2009. ۱۳: p. ٦۳-۷٦.

[٥] Srivastava, A., et al. A recent survey on DDoS attacks and defense mechanisms. in International Conference on Parallel Distributed Computing Technologies and Applications. 2011. Springer.

[٦] Khan, S., et al., Denial of service attacks and challenges in broadband wireless networks. 8; 7, 2008.

[۷] Tannoury, A., et al. Efficient and accurate monitoring of the depth information in a Wireless Multimedia Sensor Network based surveillance. in 2017 Sensors Networks Smart and Emerging Technologies (SENSET). 2017. IEEE.

[۸] Mateen, A., et al. Comparative analysis of wireless sensor networks with wireless multimedia sensor networks. in 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). 2017. IEEE.

[۹] Hussein, W.A., et al. Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks. in 2017 IEEE 13th Malaysia International Conference on Communications (MICC). 2017. IEEE.

[۱۰] Abbas, N. and F. Yu. A traffic congestion control algorithm for wireless multimedia sensor networks. in 2018 IEEE SENSORS. 2018. IEEE.

[۱۱] Lee, H.K., et al., Bandwidth estimation in wireless lans for multimedia streaming services. Advances in Multimedia, 2007. **2007**(1): p. 070429.

[۱۲] Alasti, M., et al., Quality of service in WiMAX and LTE networks [Topics in Wireless Communications]. IEEE Communications Magazine, 2010. **48**(5): p. 104.۱۱۱-