مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۴، زمستان ۱۳۹۵، ص ۲۴-۱۱

شبکه فرماندهی و کنترل بات مبتنی بر کانال‌های پوششی زمانبندی‌دار

حسین گرزین[۱]، مهدی دهقانی*[۲]، محمود صالح اصفهانی[۳]

۱- دانشجوی کارشناسی ارشد، ۲ و ۳- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۴/۰۷/۲۷، پذیرش: ۹۵/۰۲/۱۴)

چکیده

محرمانگی و گریز از کشف به‌وسیله سامانه‌های امنیتی دو ویژگی مهم شبکه بات می‌باشند که ساختار ارتباطی در این شبکه‌ها به صورت مستقیم بر روی آنها تأثیرگذار است. در این مقاله، پروتکل ارتباط پوششی مبتنی بر کانال پوششی زمانبندی‌دار برای شبکه فرماندهی و کنترل بات ارائه می‌شود و از قابلیت‌های این نوع کانال جهت ارتقاء این ویژگی‌ها استفاده می‌گردد. پروتکل پیشنهادی با ساختاری لایه‌ای و پیمانه‌ای طراحی و دارای توسعه‌پذیری و انعطاف‌پذیری مناسبی است. در این طرح، علاوه بر توسعه کاربرد این کانال‌ها در شبکه‌های بات، تأثیر متقابل معیارهای ارزیابی دو حوزه به صورت واقعی مورد بررسی قرار می‌گیرد. با توجه به تنوع شرایط ترافیکی برای سامانه‌های عضو شبکه بات از ابزار مقلد شبکه برای پیاده‌سازی محیط آزمایشی مطابق با شرایط واقعی استفاده شده و معیارهای ظرفیت، استحکام و نامحسوسی کانال ارزیابی می‌شوند. نتایج نشان می‌دهد که در بهترین شرایط ترافیکی میانگین زمانی معادل ۴۸،۰۷ بیت بر ثانیه همراه با ضریب استحکام ۹۹ درصد و در بدترین شرایط ترافیکی با وجود انواع خطاها، ظرفیتی معادل ۱۱،۰۱ بیت بر ثانیه همراه با ضریب استحکام ۸۵ درصد برای پروتکل پیشنهادی میسر است. آزمون آنتروپی شرطی نیز نامحسوسی ارتباطات در این پروتکل را نشان می‌دهد. نتایج حاصل نشان‌دهنده قابلیت مناسب کانال پوششی زمانبندی‌دار جهت تأمین زیرساخت ارتباطی در شبکه بات است.

واژه‌های کلیدی: شبکه بات، کانال پوششی زمانبندی دار، شبکه فرماندهی و کنترل بات، ابزار مقلد شبکه

۱- مقدمه

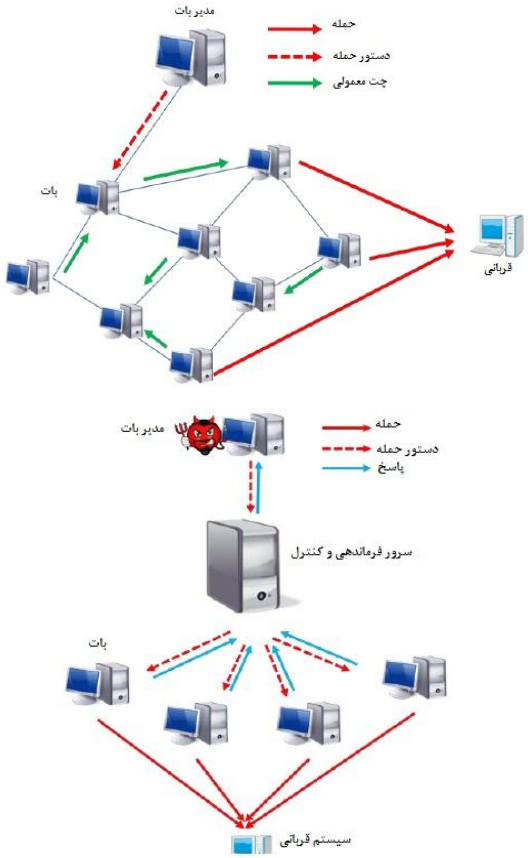
شبکه بات[۱] متشکل از تعداد زیادی سامانه‌های آلوده متصل به اینترنت می‌باشد که تحت کنترل و دستورپذیری یک مرکز فرماندهی و کنترل[۲] قرار داشته که برای انجام فعالیت‌های توزیع شده مورد استفاده قرار می‌گیرد [۱]. و دارای معماری، اجزاء و مولفه‌های مختلفی است. شبکه فرماندهی و کنترل به عنوان زیرساخت ارتباطی شبکه بات است که کلیه ارتباطات و فرآیندهای کنترلی از طریق این شبکه صورت می‌گیرد. به عبارتی دیگر مدیر بات از این طریق بر کل شبکه بات نظارت دارد. این شبکه واسط بین مدیر و سامانه‌های بات بوده تا از خطر کشف و ردیابی مدیر بات کاسته شود. با توجه به اهمیت این بخش، بسیاری از معیارهای ارزیابی شبکه بات براساس ساختار و ویژگی‌های زیرساخت فرماندهی و کنترل آن سنجیده می‌شود و ارتقای معیارهایی همچون محرمانگی داده و ارتباطات جهت بهبود قابلیت گریز از کشف در شبکه بات بر روی این بخش متمرکز است. از لحاظ ساختاری، شبکه فرماندهی و کنترل بر اساس همبندی[۳] و پروتکل‌های مختلف طراحی می‌شوند. در شکل (۱) همبندی متمرکز و نظیر به نظیر در شبکه بات نشان داده شده است [۲].

زیرساخت مهم دیگری که زیرمجموعه مبحث گسترده‌تری با عنوان پنهان‌سازی اطلاعات می‌باشد [۳]، کانال پوششی[۴] است که در پنهان‌سازی همزمان داده و ارتباط کاربرد دارد و با توجه به فنون و بستر مورد استفاده، تقسیم‌بندی‌های متعددی دارد [۵-۴]. دسته‌بندی اصلی این کانال‌ها شامل دو دسته کانال‌های ذخیره‌ای[۵] و زمانبندی‌دار[۶] می‌باشند[۷-۶]. در کانال‌های زمانبندی‌دار، اطلاعات پنهان بر روی زمان ارسال بسته‌ها سوار شده و مبادله می‌شوند، یعنی با دست‌کاری و تغییر زمان ارسال بسته، اطلاعات پوششی کدگذاری شده و گیرنده نیز با تحلیل زمانبندی دریافت بسته‌ها، اطلاعات را کدگشایی می‌نماید. در

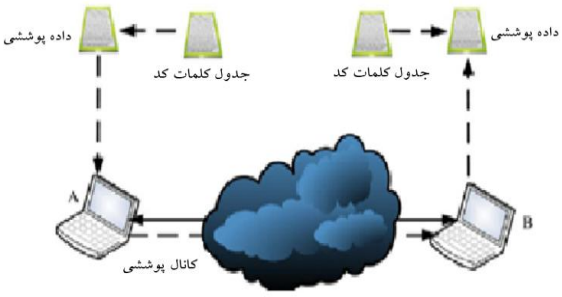
* رایانامه نویسنده مسئول: mdehghany@ihu.ac.ir

1-Botnet
2-Command and Control (C&C)
3-Topology
4-Covert channel
5-Storage
6-Timing

شکل (۲) نمای کلی کانال پوششی زمانبندی‌دار نشان داده شده است.



شکل (۱). ساختار بات‌نت با همبندی متمرکز و نظیر به نظیر[۲]



شکل (۲). نمای کلی کانال پوششی زمانبندی‌دار [۸]

این نوع کانال به علت استفاده از ترافیک مجاز دارای نامحسوسی بالاتری است. بر این اساس، توسعه کاربرد کانال‌های پوششی زمانبندی‌دار در زیرساخت ارتباطی شبکه بات مدنظر قرار گرفت تا با استفاده از قابلیت‌های این کانال‌ها کارآیی این شبکه‌ها بهبود یابد. ویژگی پنهان بودن ارتباط و پیام در کانال پوششی به عنوان ویژگی کاربردی در ارتقاء محرمانگی ارتباطات در شبکه فرماندهی و کنترل بات مطرح است. بنابراین چارچوبی مبتنی بر این نوع کانال در قالب پروتکل ارتباطی پوششی برای شبکه بات ارائه می‌شود که فرآیند طراحی، معماری و ارزیابی این پروتکل براساس ساختار و ویژگی‌های دو حوزه انجام می‌شود.

در ادامه در بخش دو کارهای مرتبط در حوزه‌های کانال‌های پوششی زمانبندی‌دار و شبکه‌های بات مرور می‌شوند. در بخش سه، معیارهای ارزیابی کارآیی و اهداف مشترک در دو حوزه بررسی شده و معیارهای متناظر استخراج می‌شوند. سپس در بخش چهار فرآیند طراحی و معماری شبکه فرماندهی و کنترل تشریح شده و پروتکل پیشنهادی ارائه می‌گردد. در بخش پنج با استفاده از ابزار مقلد شبکه و ایجاد آزمایشگاهی منطبق بر محیط واقعی، معیارهای استحکام، نامحسوسی و ظرفیت کانال در ساختار بخش فرماندهی و کنترل شبکه بات مورد ارزیابی قرار می‌گیرند.

۲- کارهای مرتبط

در بررسی صورت گرفته در خصوص استفاده از کانال‌های پوششی زمانبندی‌دار در ساختار شبکه فرماندهی و کنترل بات، تنها می‌توان رساله آقای واین را مدنظر قرار داد که چارچوبی جهت پنهان‌سازی و انتقال اطلاعات بر روی پروتکل IRC با عنوان VANISH[1] را ارائه کرده است [۹]. در این چارچوب جهت کاهش خطر کشف و ارتقاء نامحسوسی از کانال پوششی زمانبندی‌دار در ارتباطات IRC استفاده شده است. اما تکنیک‌های مورد استفاده در شبکه فرماندهی و کنترل برای رسیدن به محرمانگی بیشتر و افزایش احتمال گریز از کشف به وسیله سامانه‌های امنیتی، حائز اهمیت است. ساختار فرماندهی و کنترل از انواع متمرکز به غیرمتمرکز و شبکه‌های مبتنی بر لایه کاربرد تغییر می‌یابد تا جایی که در نسل جدید شبکه‌های بات از شبکه‌های اجتماعی مانند توئیتر[2] برای توسعه زیرساخت فرماندهی و کنترل و ارتقاء محرمانگی شبکه‌های بات استفاده می‌شود [۱۰]. در این راستا روش‌های دیگری برای ارتقاء محرمانگی ارتباطات در شبکه فرماندهی و کنترل بات ارائه شده است. آقای متئو و همکارش استفاده از شبکه تور[3] در این شبکه را بررسی کرده‌اند که با وجود ارتقاء قابلیت گریز از کشف با به‌کارگیری تور در شبکه‌های بات P2P، همچنان برخی آسیب‌پذیری‌های امنیتی برای شبکه بات وجود دارد [۱۱]. آقای دیاگو و همکارش زیرساخت جدیدی را با هدف افزایش استحکام و نامحسوسی در شبکه فرماندهی و کنترل بات ارائه کرده‌اند [۱۲]. در این زیرساخت، سامانه‌های بات، دستورات را به‌وسیله سامانه‌های خارج از شبکه دریافت کرده و کنترل می‌شوند و به دلیل اینکه فاقد هر گونه اطلاعی در

1- Variable Advanced Network IRC Stealth Handler
2- Twitter
3- Tor

خصوص مکانیزم‌های ارتباطی در شبکه فرماندهی و کنترل هستند، احتمال خطر کشف شبکه کاهش می‌یابد. آقای ناپا و همکارانش طرحی مبتنی بر شبکه اسکایپ[1] ارائه کرده‌اند و از ویژگی‌های این شبکه برای افزایش محرمانگی و احتمال گریز از کشف در شبکه بات بهره‌برداری کردند [۱۳]. در این شبکه ارتباطات بین سامانه‌های بات از طریق نودهای متناظر و ارتباطات موجود در شبکه اسکایپ صورت گرفته و به این صورت کشف مدیر بات و شبکه فرماندهی و کنترل بسیار سخت می‌شود.

در نظر گرفتن معیارهای سنجش و کشف شبکه بات توسط ابزارها و چارچوب‌های ارائه شده از عوامل دیگری که بر روی طراحی زیرساخت فرماندهی و کنترل نامحسوس تأثیرگذار است. روش‌های مبتنی بر تحلیل رفتاری، اغلب به صورت مستقل از پروتکل و با بررسی ویژگی جریان‌های موجود و به‌کارگیری تحلیل آماری و داده‌کاوی بر روی ترافیک شبکه بات عمل می‌کنند. آقای آکیاما روشی را مبتنی بر تحلیل زمان پاسخ برای کشف شبکه بات ارائه کرده است [۱۴]. در طرح آقای حسین روحانی دو معیار متوسط تعداد بایت در واحد زمان و متوسط تعداد بایت در هر بسته برای کشف جریان‌های هر سیستم بات عضو شبکه در نظر گرفته شده است [۱۵]. در روش مبتنی بر تحلیل رفتاری توسط آقای کانان، مشخصات بسته‌های مختلف در ترافیک، براساس روش داده‌کاوی درخت تصمیم دسته‌بندی شده و مبنای تشخیص شبکه بات قرار می‌گیرد [۱۶]. طرح آقای بیلج بر روی استخراج خصوصیات جریان شبکه و محاسبه اندازه جریان متمرکز است [۱۷]. فرآیند کلی در چارچوب BotMiner شامل مانیتور کردن جریان و رفتار سامانه‌ها و سپس دسته‌بندی و کشف بات‌ها می‌باشد [۱۸]. در طرح آقای برگر نیز نرخ انتقال داده در کانال ارتباطی، استفاده از خواص و ویژگی‌های ترافیک مجاز و ایجاد بار پردازشی پایین بر روی سامانه به عنوان عوامل مؤثر در مقابله با روش‌های کشف، مورد توجه قرار گرفته‌اند [۱۹].

جمع‌بندی طرح‌های مرور شده، نشان‌دهنده به‌کارگیری پروتکل‌ها و ساختارهای نرمال به عنوان زیرساخت شبکه‌های بات بوده و از این طریق، قابلیت‌های محرمانگی و گریز از کشف در این شبکه‌ها ارتقاء می‌یابند. از طرفی اغلب معیارهای کشف شبکه بات، متمرکز بر خصوصیات ترافیکی می‌باشند. بر این اساس در طرح مورد نظر از کانال‌های پوششی زمانبندی‌دار در ساختار شبکه فرماندهی و کنترل بات استفاده می‌شود تا از قابلیت‌های استحکام[2]، ظرفیت[3] و نامحسوسی[4] این نوع کانال در تأمین نیاز ارتباط پوششی و استفاده از خصوصیات ترافیک مجاز شبکه جهت کاهش احتمال خطر کشف در شبکه بات بهره‌برداری شود.

۳- معیارهای ارزیابی مشترک بین کانال پوششی و شبکه بات

اغلب معیارهای ارزیابی شبکه بات بر روی بخش فرماندهی و کنترل متمرکز می‌باشند. علاوه بر معیارهای سنجش امنیت که در بخش قبل مرور شد، معیارهای دیگری بر روی ارزیابی کارآیی این شبکه‌ها مطرح می‌باشند. در طرح آقای برگر، حداقلی تأخیر بین زمان ارسال و اجرای دستور در سامانه بات، سادگی و حجم پایین کد به عنوان معیارهای تأثیرگذار بر کارآیی شبکه ارائه شده‌اند و پایداری و مقیاس‌پذیری شبکه نیز مورد توجه قرار گرفته است [۱۹]. آقای بیگن در طراحی شبکه بات، قابلیت‌هایی از قبیل یک یا دو طرفه بودن کانال ارتباطی، انواع حملات قابل اجراء به وسیله شبکه، سکوی اجرایی، پروتکل‌های مورد استفاده و ویژگی‌های کد و سبک‌سازی آن را در نظر گرفته است [۲۰]. آقای کونزتی معیارهای منطقی شامل دسترس‌پذیری و مدیریت خطا، تأثیر معماری شبکه و همچنین تأیید اعتبار و رمزنگاری را عنوان کرده است [۲۱]. معیارهای نظم‌پذیری از قبیل تنوع حملات، سطح همزمانی، مدت زمان لازم جهت آماده‌سازی شبکه، نرخ حمله و اندازه شبکه بات در بخشی از تحقیق آقای استینسون و همکارش تشریح شده‌اند [۲۲]. در مطالعه آقای ماهاتی مقیاس‌پذیری، قابلیت اطمینان و تراکم ترافیک در شبکه و از نظر امنیتی گمنامی، صحت و درستی، سطح دسترسی و محرمانگی کانال در شبکه بات مبتنی بر پروتکل IRC مورد بررسی قرار گرفته‌اند [۲۳]. با جمع‌بندی معیارهای ارزیابی شبکه بات در مطالعات مذکور که بر روی ساختار ارتباطی متمرکز بوده‌اند، می‌توان این معیارها را به سه دسته کارآیی، امنیتی و قابلیت‌های عملیاتی تقسیم نمود.

معیارهای ارزیابی کانال‌های پوششی شامل ظرفیت، استحکام و نامحسوسی می‌باشند. حداکثر نرخ انتقال داده به‌وسیله کانال، ظرفیت یا پهنای باند آن می‌باشد که براساس میزان انتقال داده بر واحد زمان[5] و یا میزان انتقال داده در هر بسته انتقالی[6] در کانال آشکار مورد ارزیابی قرار می‌گیرد [۲۴]. میزان مقاومت کانال در برابر انواع خطاها در شبکه بیانگر استحکام کانال است که این خطاها ممکن است باعث حذف کانال و یا محدود کردن

1- Skype
2- Robustness
3- Capacity
4- Stealthy
5- bit/s
6- bit/packet

ظرفیت آن شود[۲۴]. معمولاً برای سنجش استحکام کانال میزان رخداد خطا را در نظر می‌گیرند، یعنی نرخ وقوع خطای بیتی[1]، میزان دشواری در برابر انواع روش‌های تشخیص کانال نیز نامحسوسی کانال است [۲۴].

ویژگی قابل ملاحظه در بررسی معیارهای ارزیابی کانال‌های پوششی و شبکه‌های بات، تطبیق و تناظر معیارها در دو حوزه می‌باشد. به عبارت دیگر در صورت به‌کارگیری کانال پوششی در شبکه بات، سه معیار ظرفیت، استحکام و نامحسوسی کانال پوششی زمانبندی‌دار بر معیارهای ارزیابی شبکه به صورت مستقیم و یا غیرمستقیم تأثیرگذار بوده یا منطبق هستند. جمع‌بندی تأثیرات در نمودار شکل (۳) نشان داده شده است. ارتقاء نامحسوسی در کانال پوششی، تأثیر مستقیم بر روی معیارهای امنیتی شبکه بات خواهد داشت و هر چه میزان استحکام کانال پوششی بیشتر باشد، میزان وقوع خطا پایین‌تر و قابلیت اطمینان در شبکه بالاتر خواهد بود و احتمال درستی و صحت پیام‌ها نیز افزایش می‌یابد. نتیجه افزایش ظرفیت در کانال ارتباطی نیز موجب بهبود در معیارهای کارآیی شبکه می‌شود.

شکل (۳). تناظر معیارهای ارزیابی شبکه‌های بات و کانال‌های پوششی زمانبندی‌دار

۴- طرح پیشنهادی: شبکه فرماندهی و کنترل بات مبتنی بر کانال‌های پوششی زمانبندی‌دار

مؤلفه‌های اساسی در شبکه فرماندهی و کنترل شامل برنامه سمت سرور، برنامه مقیم در سیستم بات و کانال ارتباطی بین دو برنامه جهت تبادل دستورات و داده می‌باشند. در این طرح به عنوان نمونه اولیه، ساختار شبکه براساس همبندی متمرکز در نظر گرفته شده است. در این بخش مراحل و جزئیات طراحی و معماری این مؤلفه‌ها و زیرساخت ارتباطی تشریح می‌شود.

۴-۱- طراحی کانال ارتباطی

در طرح پیشنهادی، ساختار ارتباطی در شبکه فرماندهی و کنترل مبتنی بر کانال‌های پوششی زمانبندی‌دار است و از سه نوع کانال استفاده می‌شود. تنوع انواع کانال در شبکه به تغییر رفتار ترافیکی کمک کرده و باعث افزایش نامحسوسی ارتباطات و در نتیجه محرمانگی بیشتر شبکه می‌شود. از طرفی با توجه به لزوم پایداری ساختار ارتباطی و به‌کارگیری کانال‌هایی با ظرفیت و استحکام مناسب از سه نوع کانال مبتنی بر فواصل زمانی، بازترتیبی و کانال ترکیبی استفاده می‌شود.

در کانال بازترتیبی از پدیده بازترتیب بسته‌ها[2] به عنوان مبنای کدگذاری در کانال استفاده می‌شود که هم از بخش داده بسته‌ها مستقل است و هم نسبت به لغزش زمانی بین بسته‌ها حساس نیست. ساختار این نوع کانال، مبتنی بر طرح آقای آتاوی است [۲۵]. مسئله مهمی که در این کانال باید به آن توجه داشت نرخ بازترتیبی است. یک کانال TCP با نرخ بالایی از درهم ریختگی، در صورت کنترل، مشکوک به نظر می‌رسد و نامحسوسی کانال کاهش می‌یابد. عوامل مؤثر بر روی این نرخ، عمق بازترتیبی و حجم بازترتیبی هستند که البته به وسیله پارامترهای چگالی بازترتیبی[3] و چگالی اشغال بافر بازترتیبی[4] که توسط آقای پیراتلا مشخص شده‌اند [۲۶] نیز در نظر گرفته می‌شوند. به طور مثال، محدود کردن اندازه بلاک به مقدار کمتر از ۵ و بازترتیبی کمتر از ۳ بسته در یک بلاک برای هر کلمه کد، می‌تواند سطح نامحسوسی مناسبی را برای کانال تأمین کند [۲۵].

در روش دوم از کانال مبتنی بر فاصله زمانی بین بسته‌ها و از مدل ۱ بیت به n بسته خانم سلکه استفاده می‌شود [۲۷]. مبنای اصلی در این روش، کدگذاری ۱ بیت داده بر روی دنباله‌ای متشکل از n فاصله زمانی بین بسته‌ای است. کدگذاری و کدگشایی پیام براساس جدول کلمات کد انجام می‌شود که دارای دو بعد شامل رشته بیت و فاصله‌های زمانی متناظر با هر رشته است. پارامترهای اصلی در تشکیل این جدول شامل کمترین مقدار تفاوت بین فواصل زمانی (δ) و حداقل مقدار فاصله زمانی بین بسته‌ها (Δ) است که پارامتر اول جهت جلوگیری از تداخل فاصله‌های بین بسته‌های ارسالی و پارامتر دوم جهت جلوگیری از ازدحام در ترافیک در نظر گرفته شده‌اند.

در کانال ترکیبی[5]، از تلفیق دو تکنیک فاصله زمانی و بازترتیبی بسته‌ها برای کدگذاری استفاده شد و از قابلیت‌های هر یک جهت ارتقاء معیارهای نامحسوسی، ظرفیت و استحکام کانال

1- Bit Error Rate (BER)

2- Packet-Reordering CTC (PR-CTC)
3- Reorder Density (RD)
4- Reorder Buffer-occupancy Density (RBD)
5 -Inter packets & Packet reordering covert timing channels

نهایی به صورت مناسبی بهره‌برداری گردید. در این روش برای ارتقاء ظرفیت کانال از ترکیب دو تکنیک مذکور و برای ارتقاء نامحسوسی در کانال نیز از ایده‌های کم‌پشت و مدولاسیون استفاده شده است [۲۸].

۴-۱-۱- عوامل موثر بر کارآیی کانال

پارامترهای متعددی بر عملکرد کانال پوششی تأثیرگذار است و تنظیم مقادیر نامناسب آنها کارآیی کانال را کاهش خواهد داد. عوامل مهمی که در تنظیم پارامترهای کانال باید به آنها توجه داشت، عبارتند از:

- **الگوی ترافیک شبکه:** کانال مورد نظر در این طرح، از نوع فعال می‌باشد و از یک تولیدکننده بسته استفاده می‌شود، به همین دلیل باید مدل تولید و ارسال بسته‌ها در کانال منطبق بر شبکه میزبان باشد، تا رفتار کانال همانند رفتار ترافیک نرمال باشد و نامحسوسی کانال تا حد ممکن تأمین شود. براساس آزمون نکوئی برازش آقای جیانوچیو بر روی فاصله زمانی بین بسته‌های ترافیک HTTP در سمت فرستنده، مدل توزیع احتمال ویبول بیشترین تطبیق را با رفتار واقعی شبکه دارد [۲۹].
- **فاصله متوسط بین بسته‌ها:** فاصله ارسال بسته‌های متوالی باید به صورتی باشد که موجب وقوع خطا در قسمت گیرنده نگردد. یعنی حداقل فاصله زمانی لازم بین دو بسته متوالی به طوری که باعث ایجاد خطای گم شدن، حذف و بازترتیبی بسته‌ها نگردد. آقای ژیائوچاو این فاصله را به‌عنوان فاصله متوسط معمول[1] در نظر گرفته است [۳۰]. این فاصله در کانال‌های مبتنی بر فاصله زمانی و ترکیبی با پارامتر Δ در نظر گرفته شده است [۳۱].
- **متوسط لغزش زمانی:** لغزش زمانی یا جیتر باعث می‌شود بین فاصله‌های زمانی ارسال دو بسته متوالی از مبدأ کانال و فاصله متناظر دریافت آنها در سمت مقصد، خطایی زمانی ایجاد گردد. عدم پیش‌بینی مقدار لغزش زمانی در کدگذاری کانال باعث ایجاد خطا خواهد شد. ژیائوچاو لغزش زمانی را به عنوان محدوده انحراف[2] در نظر گرفته است [۳۰]. اما در روش‌های مبتنی بر فاصله زمانی و ترکیبی حداکثر لغزش زمانی ممکن را به عنوان ε_{max} در نظر گرفته و جهت جلوگیری از وقوع خطا در کانال، پارامتر δ با شرط $\delta > 4\,\varepsilon_{max}$ برای محاسبه فواصل زمانی در کانال استفاده می‌شود [۳۱].
- **فاصله بازترتیبی:** در کانال بازترتیبی، فاصله بازترتیبی بسته‌ها به عنوان مهمترین عامل مطرح است. آتاوی در طرح خود، بیشترین احتمال بازترتیبی بسته‌ها را مربوط به بسته‌های مجاور هم دانسته است [۲۵]. از این مسئله در کانال ترکیبی برای ارتقاء نامحسوسی کانال استفاده شده است و از بلاک‌هایی برای کدگذاری در کانال استفاده می‌شود که از فاصله بازترتیبی کمتری برخوردار هستند.

۴-۲- طراحی و معماری پروتکل ارتباط پوششی

علاوه بر کانال ارتباطی باید برنامه‌های دو طرف سرور و سیستم بات با تمرکز بر فرآیندهای شبکه فرماندهی و کنترل و تبادل پیام بر بستر کانال پوششی زمانبندی‌دار طراحی و پیاده‌سازی شوند. طراحی برنامه‌ها با در نظر گرفتن معماری پایه، مدل‌سازی نیازمندی‌ها[3]، فرآیندها[4] و مدل ساختار[5] برنامه انجام می‌شود. در برخی از چارچوب‌های پیاده‌سازی برنامه‌های کدگذار و کدگشای کانال، ساختار به صورت چندسطحی در نظر گرفته شده است [۳۲] و در برخی دیگر به صورت مؤلفه‌هایی مجزا در نظر گرفته شدند که به صورت سری، فرآیندهای مورد نیاز در ایجاد ارتباط و ارسال داده را تکمیل می‌کنند [۲۹ و ۳۳]. در طرح مورد نظر، علاوه بر در نظر گرفتن ساختارهای مذکور، معماری چندلایه‌ای[6] به عنوان مدل پایه در طراحی ساختار ارتباطی شبکه فرماندهی و کنترل در نظر گرفته شده است. ایده اصلی در این معماری براساس ساختار موجود در مدل‌های مرجع شبکه از قبیل OSI یا TCP/IP شکل گرفته است. در این مدل‌ها، کلیه فرآیندها در قالب وظایف مجزا در لایه‌های مختلف اجراء می‌شوند. در طرح حاضر نیز با توجه به نیازمندی‌ها، لایه‌های مختلفی با تطبیق و تناظر با ساختار مدل‌های مرجع در نظر گرفته شده و فرآیندهای ارتباطی و وظایف مختلف در دو طرف سیستم بات و سرور فرماندهی و کنترل در این لایه‌ها تعریف می‌شوند.

۴-۲-۱- مدل‌سازی نیازمندی‌ها

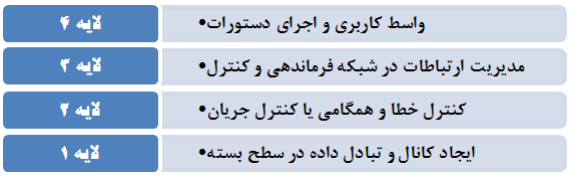
نیازمندی‌های اساسی در شبکه فرماندهی و کنترل شامل تراکنش‌هایی است که جهت عملکرد پیش‌فرض شبکه بات اجراء می‌شوند و شامل امکان برقراری مداوم ارتباط بین سیستم بات و سرور مرکزی، کدگذاری و ارسال پیام با استفاده از زیرساخت

1- Original Mean Interval
2- Deviation Rate

3- Requirement Modeling
4- Process Modeling
5- Enterprise Architecture Model (EAM)
6- N-Layer

ارتباطی و حفظ صحت آن، کنترل خطا و امنیت پیام و وضعیت‌های مختلف سیستم بات از قبیل حمله، بیکاری، به‌روزرسانی و یا ارسال گزارش می‌باشند. وضعیت دیگری که در این طرح با توجه به ویژگی‌های کانال پوششی زمانبندی‌دار اضافه شده است، همگامی نام دارد که در اولین اتصال سیستم به شبکه فرماندهی و کنترل رخ می‌دهد. با توجه به الگوی لایه‌ها در مدل OSI، این نیازمندی‌های پایه در قالب چهار لایه مجزا و منطبق بر لایه‌های فیزیکی، پیوند داده، شبکه و کاربرد در نظر گرفته شده‌اند. شرح وظایف کلی لایه‌ها در شکل (۴) ذکر شده است.

- **لایه اول:** در این لایه، ارتباط در پایین‌ترین سطح یعنی بسته برقرار می‌شود و اطلاعات پنهان با ایجاد کانال پوششی زمانبندی‌دار کدگذاری و ارسال می‌شوند. بستر ارسال داده و کلیه تراکنش‌های ارتباطی در این لایه در سطح سوکت انجام می‌شود.
- **لایه دوم:** با توجه به وجود نویز و احتمال رخداد انواع خطاها در کانال، مکانیزم کشف و تصحیح خطا در شبکه فرماندهی و کنترل پیش‌بینی و از کدهای کنترل خطا از قبیل بیت توازن[1] استفاده شد که به افزایش کارآیی و پایداری کانال و شبکه کمک خواهد کرد. مسئله مهم دیگر در کانال، همزمانی بین سرور و سامانه بات است که در قالب توافق بر روی تنظیم پارامترهای کانال اجراء می‌شود.
- **لایه سوم:** مدیریت برقراری ارتباط سامانه‌های متعدد بات با سرور فرماندهی و کنترل در این لایه اجراء می‌شود. مکانیزم موجود در شبکه به این صورت است که سامانه‌های عضو جهت دریافت دستورات جدید به صورت مداوم و با فواصل معین، درخواست برقراری ارتباط به سرور ارسال می‌کنند. مدیریت این درخواست‌ها و تعیین این که به کدام یک از درخواست‌ها پاسخ مثبت داده شود، در لایه سوم مشخص می‌شود.
- **لایه چهارم:** در این لایه وظایف متناظر با لایه آخر مدل OSI یعنی لایه کاربرد در نظر گرفته شده است. برنامه واسط کاربر و دستورات در این لایه اجراء می‌شوند.



شکل (۴). لایه‌های شبکه فرماندهی و کنترل و وظایف هر لایه

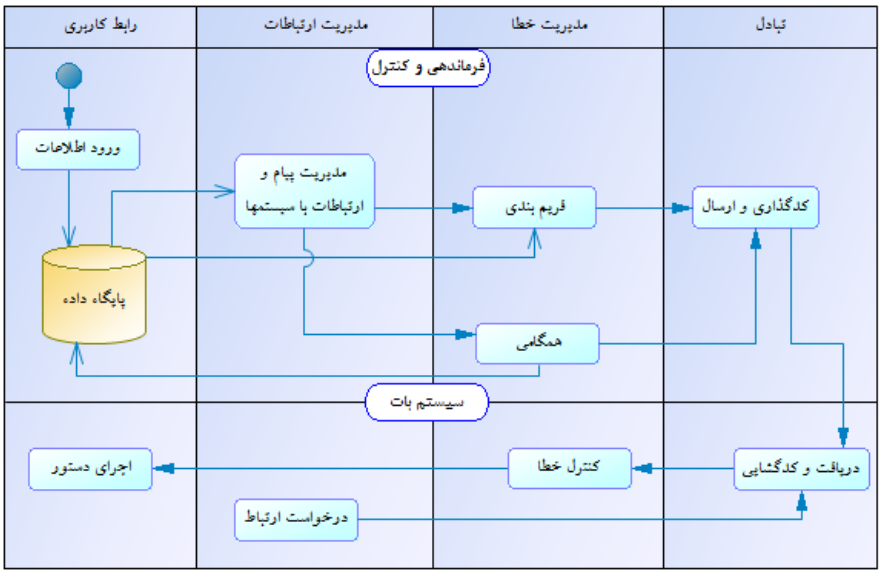
۴-۲-۲- مدل‌سازی فرآیندها و ساختار طرح

براساس مدل نیازمندی‌ها، فرآیندهای اصلی و جریان داده بین آنها مشخص می‌شوند. فرآیندهای سمت سرور شامل ورود دستورات، مدیریت ارتباطات، اجرای مکانیزم‌های کنترل خطا همانند فریم‌بندی داده، کدگذاری و ارسال پیام و همگامی می‌باشند. فرآیندها در سامانه بات شامل ثبت زمان و ترتیب بسته‌ها، کدگشایی، کنترل و کشف خطا و در نهایت اجرای دستورات هستند. مدل این فرآیندها در دو بخش فرماندهی و کنترل و برنامه بات در شکل (۵) ارائه شده است.

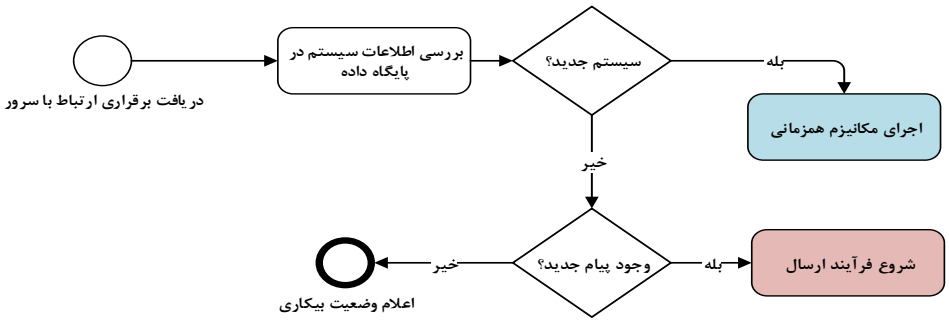
همزمانی بین سرور و سامانه بات، فرآیند مهمی است که در لایه دوم اجراء می‌شود. سامانه‌های عضو شبکه بات دارای شرایط ترافیکی و قابلیت‌های پردازشی متفاوت می‌باشند، بنابراین در نظر گرفتن کانال ارتباطی با پارامترهای ثابت برای تمامی سامانه‌های عضو شبکه مناسب نخواهد بود و از کارایی کانال کاسته می‌شود. بنابراین مکانیزم اجرای همزمانی برای هوشمندسازی و مقداردهی پارامترها متناسب با شرایط ترافیکی بین سیستم بات با سرور فرماندهی و کنترل پیش‌بینی شده است. اجرای این روال باعث جلوگیری از وقوع خطا در مواقع به‌کارگیری سامانه‌های بات، کاهش تأخیر در زمان آماده‌سازی شبکه، افزایش کارایی، انعطاف‌پذیری در شرایط مختلف ترافیکی در شبکه می‌شود. فرآیند مهم دیگر، مدیریت ارتباط و وضعیت سامانه‌ها است که در لایه سوم اجراء می‌شود. در این لایه، وضعیت بعدی سامانه‌های بات متقاضی ارتباط با سرور مشخص می‌شود. روال کلی طبق نمودار جریان شکل (۶) صورت می‌گیرد.

در اولین اتصال یک سیستم جدید به شبکه، فرآیند همزمانی و تنظیم مقادیر پارامترهای مناسب کانال(δ ,Δ) برای آن سامانه اجراء می‌شود به این صورت که ابتدا سرور با مقادیر پیش‌فرض، کانال را ایجاد و یک پیام مشخص را به دفعات معین ارسال می‌کند. اگر تعداد پیام‌های صحیح دریافت شده در حد مجاز باشد، یعنی مقادیر جاری برای این سامانه مناسب بوده و ذخیره می‌شوند ولی اگر پیام‌های همراه با خطا زیاد باشد، مقادیر پارامترها افزایش می‌یابد و دوباره این فرآیند تکرار می‌شود تا جائی که سرور به حالت مناسب تبادل صحیح پیام‌ها دست یابد. روال‌ها و فرآیندهای دو طرف مرکز فرماندهی و کنترل و سیستم بات در نمودار شکل (۷) جمع‌بندی شده است.

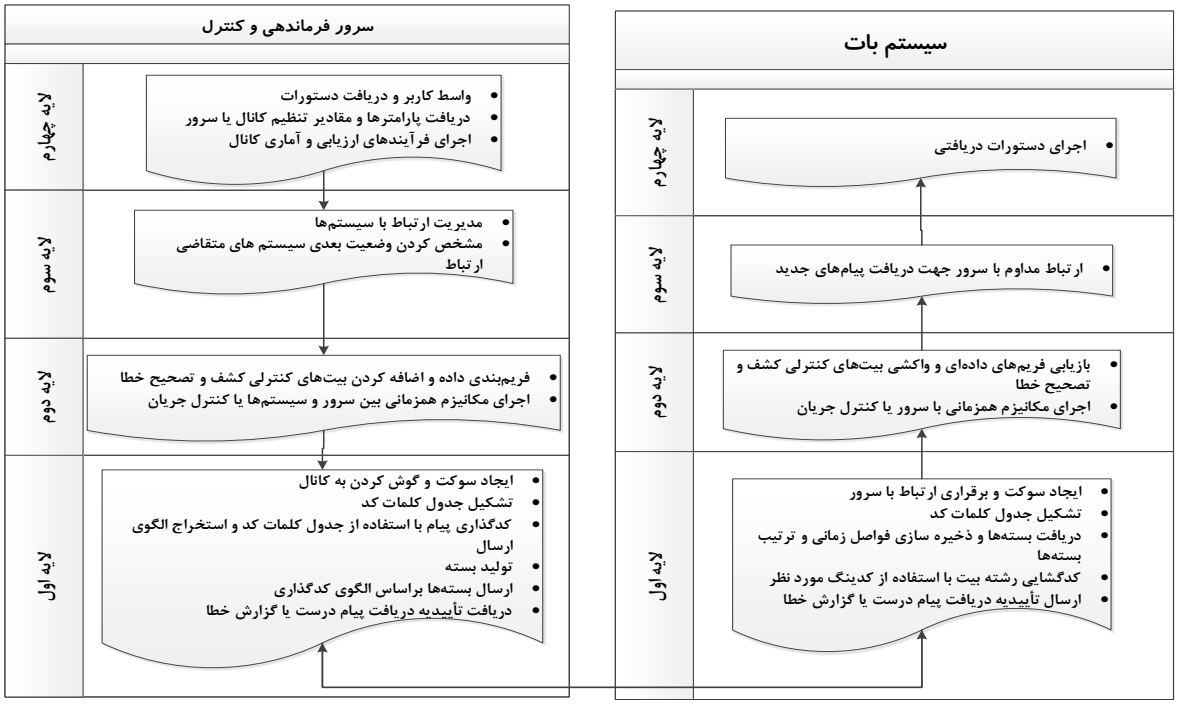
1 -Parity bit



شکل (۵). مدل فرآیند در سرور فرماندهی و کنترل و برنامه بات

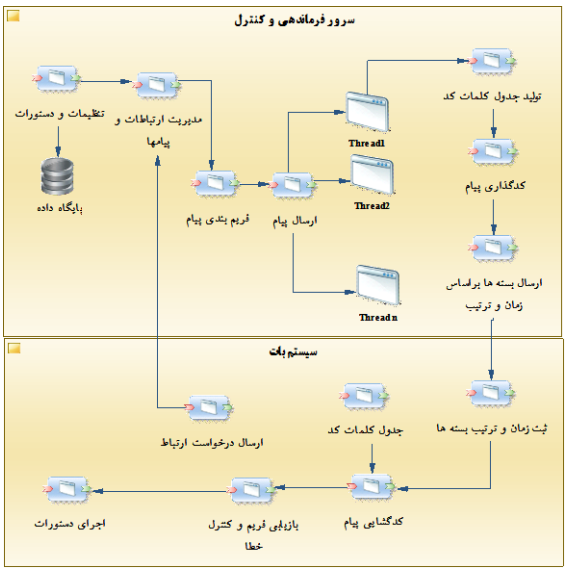


شکل (۶). روال مدیریت وضعیت‌ها و ارتباطات در برنامه فرماندهی و کنترل



شکل (۷). فرآیندهای عملیاتی زیرمجموعه در هر لایه

براساس فرآیندها، ساختار برنامه‌ها شامل مؤلفه‌ها و ارتباطات بین آنها تعریف می‌شود. هر یک از مؤلفه‌ها متناظر با یک یا چند فرآیند اصلی یا فرعی می‌باشد و بسته به میزان پیچیدگی، توابع و پیمانه[1]های مجزایی را در بر دارد. شکل (۸) ساختار برنامه‌ها را نشان می‌دهد.



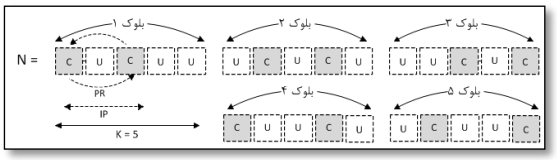
شکل (۸). مدل ساختار سازمانی فرماندهی و کنترل و بات

در بخش ارسال پیام از تکنیک چندنخی[2] استفاده شده است، یعنی برای ارتباط با هر سیستم ابتدا یک نخ تولید و سپس جدول کلمات کد براساس پارامترهای تنظیم شده برای سیستم مورد نظر ایجاد و سپس پیام ارسال می‌شود.

۴-۳- چارچوب پیاده‌سازی پروتکل ارتباطی

چارچوب پیاده‌سازی پروتکل پیشنهادی شامل مشخصات شبکه فرماندهی و کنترل و تنظیمات کانال پوششی زمانبندی‌دار می‌باشد و شامل موارد زیر است:

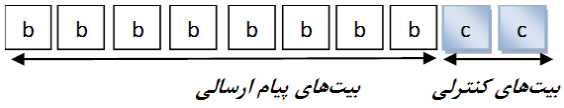
- **جدول کلمات کد:** قالب کدگذاری کانال به صورت مستقیم بر کارآیی و معیارهای ارزیابی کانال تأثیرگذار است و شامل پارامترهای طول بلاک، طول رشته بیت و تعداد فواصل زمانی در جدول کلمات کد می‌باشد. این پارامترها بر روی ظرفیت، استحکام و نامحسوسی کانال ارتباطی، پیچیدگی و حجم حافظه مصرفی تأثیرگذارند. سلکه در طرح خود، مناسب‌ترین حالت در ابعاد جدول کلمات کد را ۴ بیت به ۲ بسته عنوان می‌کند [۲۷]. در این حالت هم نرخ انتقال کانال و هم پیچیدگی جدول کلمات کد در وضعیت بهینه‌ای قرار می‌گیرند. آقای دهقانی نیز در طرح کانال ترکیبی از همین ابعاد در جدول کلمات کد استفاده کرده است [۲۸]. این ابعاد در شکل (۹) نشان داده شده است.



شکل (۹). شیوه کدگذاری ترکیبی با استفاده از بلاک‌های ۵ بسته‌ای [۸]

دو پارمتر مهم دیگر، اندازه بلاک و تعداد بسته‌های بازترتیبی در هر بلاک می‌باشد. عامل مهم در انتخاب این پارامترها این است که افزایش حجم بازترتیب بسته‌ها باعث کشف کانال نگردد. در طرح ترکیبی به دلیل استفاده از قالب ۴ بیت به ۲ بسته باید تعداد بسته‌های بازترتیبی را نیز ۲ بسته در نظر گرفت. آتاوی نیز بلاک‌هایی با طول ۵ بسته و همچنین بازترتیبی ۲ تا ۳ بسته در هر بلاک را مناسب‌ترین حالت عنوان کرده است [۲۵]. در طراح حاضر این ابعاد توسط مدیر بات قابل تغییر است که باعث تغییر رفتار کانال و ارتقاء نامحسوسی آن خواهد شد.

- **اندازه قالب:** اندازه هر قالب تأثیر مستقیمی بر روی کارآیی مکانیزم کشف خطا و همچنین ایجاد افزونگی بر روی حجم بیت‌های ارسالی دارد. هر چه طول قالب کوتاهتر باشد دقت کشف خطا بیشتر خواهد بود در عوض افزونگی بیتی بیشتر می‌شود. در مقابل اگر طول قالب افزایش یابد، افزونگی کاهش می‌یابد ولی دقت کشف خطا نیز کاهش یافته و یا احتمال بروز خطای منفی کاذب[3] بیشتر می‌شود. در طرح مورد نظر با توجه به این که کوچکترین واحد داده‌ای ۴ بیت می‌باشد، حداقل باید فریمی با طول دو واحد، یعنی ۸ بیت در نظر بگیریم. ترکیب قالب در شکل (۱۰) نشان داده شده است.



شکل (۱۱). ساختار هر قالب در کانال

- **نوع کانال:** در این طرح از کانال نوع فعال استفاده می‌شود، زیرا در صورت غیرفعال بودن، مشخص نیست شرایط ترافیکی در شبکه با شرایط لازم جهت ایجاد کانال در مواقع تبادل دستورات مناسب باشد یا خیر؟ همچنین به منظور اطلاع از دریافت صحیح دستورات و جمع‌آوری اطلاعات از سامانه‌ها باید کانال ارتباطی در شبکه به صورت دو طرفه طراحی و پیاده‌سازی گردد.

1 -Module
2 -Multi Threading
3 -False Negative

- **بستر ترافیکی:** در این طرح می‌توان از پروتکل‌ها و پورت‌های مختلف در لایه شبکه (TCP و UDP) و لایه کاربرد (HTTP) استفاده کرد. تنوع پورت‌ها باعث تغییر رفتار شبکه و نامحسوسی بیشتر آن خواهد شد. با توجه به ویژگی‌ها و عدم حساسیت نسبی سامانه‌های امنیتی از پروتکل HTTP و مدل رفتار ترافیکی آن یعنی ویبول استفاده می‌شود.

۵- ارزیابی شبکه فرماندهی و کنترل مبتنی بر کانال پوششی زمانبندی‌دار

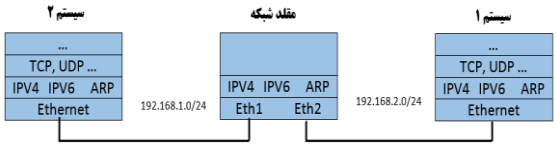
با توجه به تطبیق معیارهای ارزیابی دو حوزه، معیارهای ظرفیت، استحکام و نامحسوسی کانال زمانبندی‌دار پوششی که نشان‌دهنده میزان تأمین معیارهای متناظر در حوزه شبکه بات می‌باشد، مورد ارزیابی قرار می‌گیرند و به دلیل پیاده‌سازی نمونه واقعی، ارزیابی طرح نیز به صورت واقعی انجام می‌شود. همچنین به علت ارث‌بری مشخصات دو روش فاصله زمانی و بازترتیبی از کانال ترکیبی به عنوان شاخص ارزیابی استفاده می‌شود.

برای سنجش استحکام، میزان رخداد خطا در کانال مدنظر قرار دارد، یعنی نرخ وقوع خطای بیتی در کانال[1]. اما با توجه به اینکه اولویت مهم در پایداری شبکه بات، ارسال بدون خطا و حفظ صحت و درستی پیام است، این معیار برای سنجش پایداری شبکه مناسب نیست. به عبارتی دیگر واحد سنجش پایداری، میزان انتقال صحیح دستورات می‌باشد. به همین دلیل برای ارزیابی استحکام رویه‌ای مجزا در نظر گرفته شده است، به این صورت که یک پیام با طول و به تعداد دفعات مشخص، از سمت سرور به سیستم بات ارسال می‌گردد. استحکام کانال درصد دفعاتی است که این پیام به درستی در سمت گیرنده دریافت می گردد، یعنی نرخ خطای دستور[2]. برای سنجش نامحسوسی کانال نیز از روش‌های آماری استفاده می‌شود که به دو دسته آزمون های شکل و قاعده‌مندی تقسیم می‌شوند. در این آزمایش برای سنجش شکل از آزمون آنتروپی و برای سنجش قاعده‌مندی از آزمون آنتروپی شرطی استفاده می‌شود.

۵-۱- محیط آزمایش

سامانه‌های بات دارای ویژگی‌ها و شرایط ترافیکی متفاوتی هستند. همچنین انواع خطاهای ممکن در شبکه اعم از لغزش زمانی، حذف و بازترتیبی بسته‌ها بر روی ترافیک ارتباطی وجود دارد. چارچوب آزمایشی باید دارای حداکثر تطبیق با شرایط ممکن برای سامانه‌های عضو شبکه باشد. بر این اساس رویکرد اصلی در ارزیابی، پیاده‌سازی شرایط محیطی متناسب با محیط واقعی با استفاده از ابزارهای مقلد[3] شبکه است. این ابزارها شرایط آزمایش را در یک محیط ترکیبی و کنترل شده و منطبق با محیط واقعی فراهم می‌کنند [۳۵-۳۴]. و هر یک دارای قابلیت‌ها و امکانات متفاوتی هستند.

با توجه به تنظیمات مورد نیاز در ایجاد شرایط آزمایش از ابزار نت‌ام[4] استفاده می‌شود. دلیل اصلی استفاده از این ابزار، قابلیت‌های برتر و وجود پارامترهایی برای تنظیم خطاهای حذف، بازترتیبی و لغزش زمانی در شبکه می‌باشد که جزء نیازمندی‌های اصلی در ارزیابی می‌باشد. بستر آزمایشی نت‌ام براساس شکل (۱۱) می‌باشد.



شکل (۱۱). ساختار آزمایشی با استفاده از ابزار نت‌ام [۳۶].

۵-۲- وضعیت‌های آزمایشی

شرایط مختلف ترافیکی و نرخ وقوع انواع خطاها در شبکه مورد بررسی قرار گرفت و برای تنظیم و تطبیق هر چه بیشتر محیط آزمایش با این شرایط، چهار وضعیت مجزا با دسته‌بندی و مشخصات جدول (۱) در نظر گرفته شده است که با تنظیم پارامترهای نت‌ام ایجاد می‌شوند.

جدول (۱). وضعیت‌های ترافیکی محیط آزمایش

وضعیت	تأخیر (ms)	لغزش زمانی (ms)	حذف بسته (٪)	بازترتیب بسته (٪)
وضعیت اول	۳۰	۳	۰/۰۰۱	۰/۰۱
وضعیت دوم	۸۰	۶	۰/۱	۱
وضعیت سوم	۱۳۰	۱۰	۰/۵	۲
وضعیت چهارم	۲۰۰	۱۵	۱	۳

پس از راه‌اندازی هر وضعیت، روال انجام آزمایش به این صورت است که با تنظیم پارامترهای Δ و δ، برای ۱۰۰ بار متوالی یک پیام با طول ۱۰ کاراکتر تصادفی تولید و بر روی کانال ارسال می‌شود و مقادیر معیارها محاسبه و ثبت می‌شود. در صورتی که

1 -Bit Error Rate (BER)
2 -Command Error Rate (CER)
3- Emulator
4 -Netem

ارتباط بر روی کانال به حالت پایدار و حداقل خطا رسیده و ثابت بماند، مقادیر ثبت شده به‌عنوان مقادیر نهایی در وضعیت مورد نظر در نظر گرفته می‌شوند و در غیر این صورت پارامترهای کانال افزایش یافته و این فرآیند تا رسیدن کانال به حالت پایدار ادامه می‌یابد.

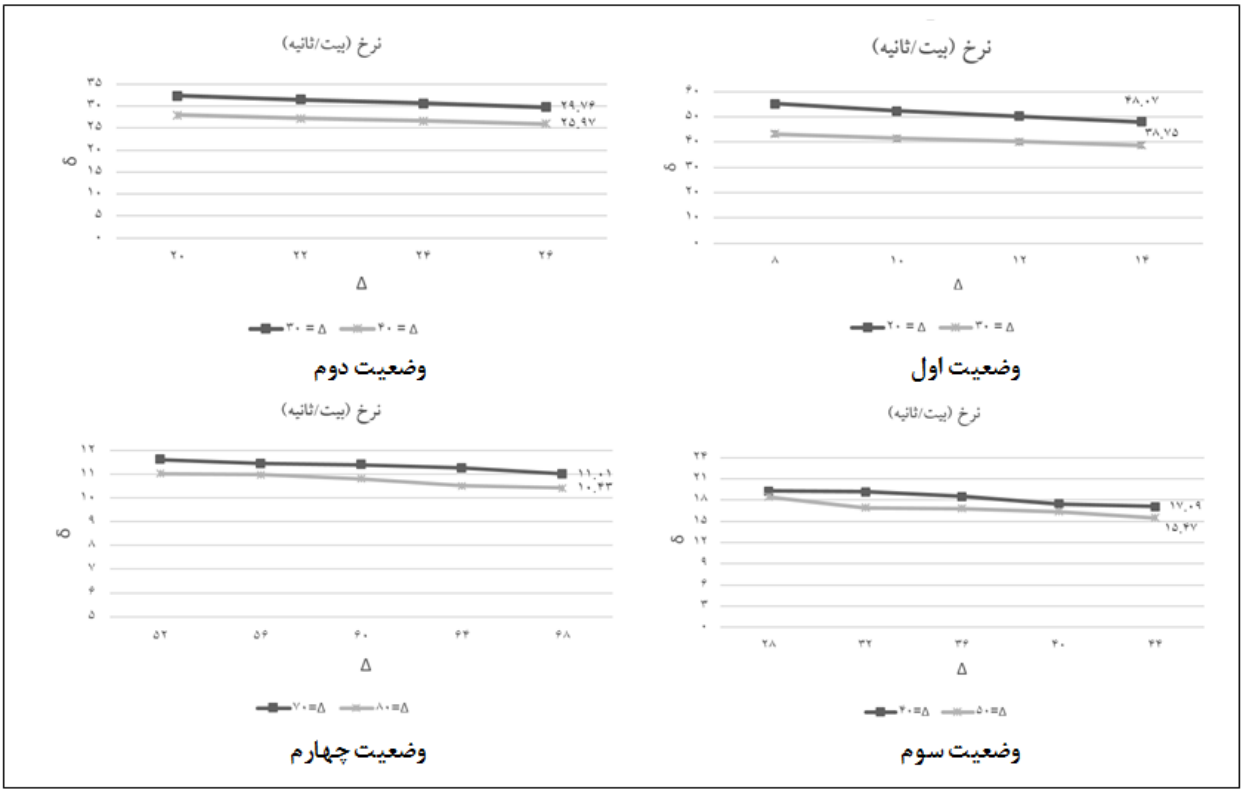
۵-۳- آزمایش ۱: ارزیابی ظرفیت کانال ارتباطی

بررسی مقدار و تغییرات ظرفیت کانال در شبکه با مقدار Δ =۲۰ و با تغییر مقادیر پارامتر δ در وضعیت اول شروع شد. آزمایش برای چهار وضعیت با افزایش مقادیر این پارامترها ادامه یافته و ظرفیت کانال محاسبه شد. در شکل (۱۲) نمودار تغییرات ظرفیت کانال در دو حالت نهایی و پایدار کانال و در چهار وضعیت نشان داده شده است.

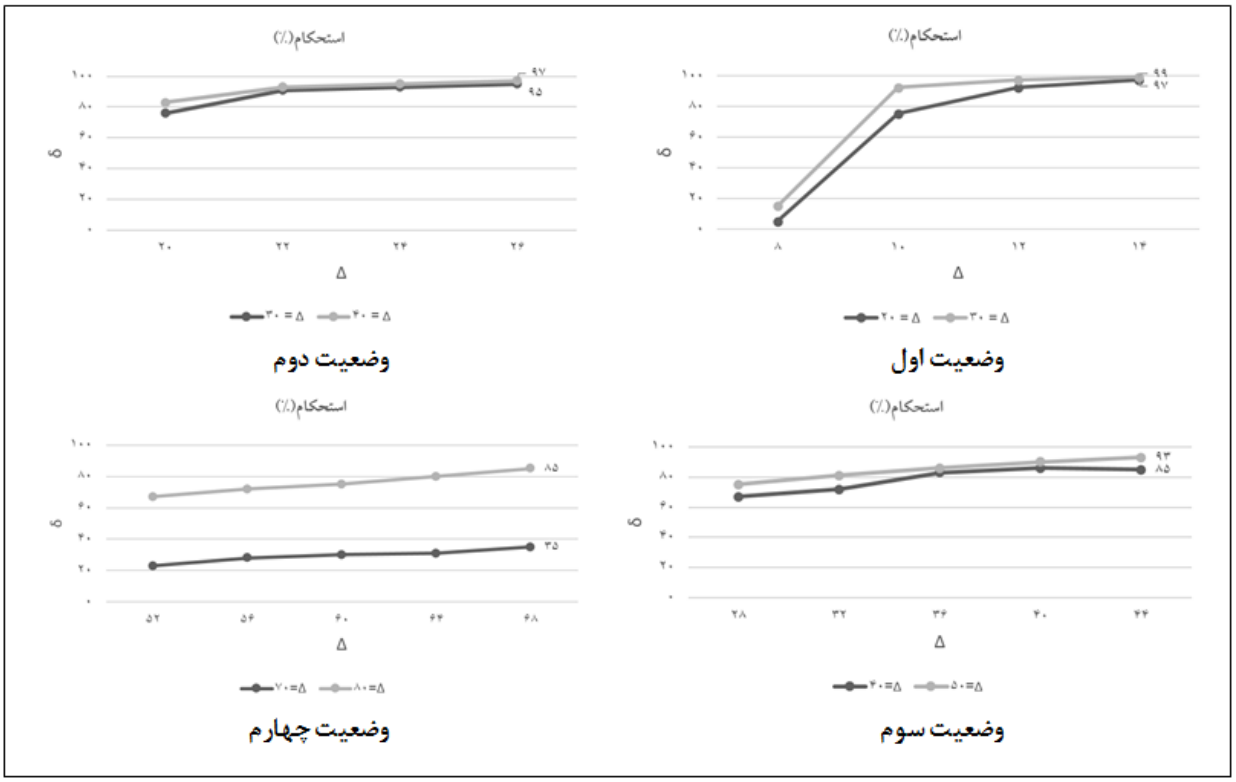
در هر وضعیت با افزایش پارامترهای کانال یعنی افزایش میانگین زمانی برای انتقال پیام، نرخ کانال طبق انتظار کاهش یافته است. با تغییر وضعیت و افزایش نرخ وقوع خطاها، برای ارتقاء و حفظ پایداری کانال باید مقادیر پارامترهای کانال و فواصل زمانی بسته‌ها افزایش یابد که موجب کاهش نرخ کانال شده است. با توجه نتایج در چهار وضعیت، ظرفیت کانال در بهترین شرایط ترافیکی، حداکثر ۳۸/۷۵ بیت بر ثانیه و در بدترین شرایط، حداکثر ۱۰/۴۳ بیت بر ثانیه به دست آمده است.

۵-۴- آزمایش ۲: ارزیابی استحکام کانال ارتباطی

براساس چارچوب تشریح شده برای ارزیابی استحکام معیار نرخ خطای انتقال دستور یا CER در هر وضعیت اندازه‌گیری می‌شود و در هر بار انجام آزمایش طبق روال، تعداد پیام‌هایی که همراه با خطا می‌باشند، محاسبه می‌شود. استحکام کانال درصد مواقعی است که انتقال پیام با خطایی مواجه نباشد. بررسی استحکام کانال در شبکه با مقدار Δ =۲۰ در وضعیت اول شروع شد و برای چهار وضعیت با تغییر مقادیر پارامترهای Δ و δ تا رسیدن کانال به حالت پایدار ادامه و استحکام کانال محاسبه شد. در شکل (۱۳) نمودار تغییرات استحکام در چهار وضعیت نشان داده شده است.



شکل (۱۲). نمودار تغییرات ظرفیت در چهار وضعیت در شبکه فرماندهی و کنترل



شکل (۱۳). نمودار تغییرات استحکام در چهار وضعیت در شبکه فرماندهی و کنترل

با توجه به نتایج آزمون ۲ در وضعیت‌های مختلف، همگام با تغییر شرایط ترافیکی و افزایش نرخ وقوع خطاها در شبکه، استحکام کانال کاهش یافته است. میزان استحکام و پایداری کانال در بهترین وضعیت حداکثر ۹۹٪ و در بدترین شرایط ترافیکی، حداکثر ۸۵٪ محاسبه شده است. البته دستیابی به این میزان استحکام باید با توجه تأثیر متقابل بر روی معیارهای دیگر صورت گیرد. به طور مثال در وضعیت چهارم به دلیل نرخ خطای بالا برای افزایش میزان استحکام، باید مقادیر Δ و δ در کانال افزایش یافته تا جایی که میانگین زمانی برای انتقال ۴ بیت داده در بهترین شرایط به ۱۴۸ میلی ثانیه خواهد رسید. این مقادیر باعث کاهش شدید ظرفیت و همچنین افزایش احتمال کشف کانال خواهد شد.

۵-۵- آزمایش ۳: ارزیابی نامحسوسی کانال ارتباطی

برای ارزیابی نامحسوسی کانال، باید آزمون‌های آنتروپی و آنتروپی شرطی بر روی داده‌های ثبت شده از کانال، اعمال گردند. در هر وضعیت نمرات آستانه و میانگین آنها برای ترافیک سالم و ترافیک کانال به صورت مجزا محاسبه می‌شوند و برای مشخص شدن نامحسوسی کانال براساس هر آزمون، میانگین نمرات در هر وضعیت با هم مقایسه می‌شوند. برای این کار باید نرخ مثبت اشتباهی[1] در هر وضعیت نیز مشخص شود. در نظر گرفتن این نرخ، دقت نتیجه ارزیابی و مقایسه نمرات آزمون را افزایش می‌دهد. براساس شرایط وقوع خطا در هر وضعیت این نرخ به صورت تقریبی در نظر گرفته شده است.

۵-۵-۱- آزمون آنتروپی شرطی

روال مورد نظر برای جمع‌آوری داده و محاسبات نمرات آستانه در ترافیک سالم و کانال ارتباطی انجام و طبق جدول (۲) جمع‌بندی شده است. این نمونه‌ها برای ۱۰۰۰۰۰ فاصله زمانی بر روی پروتکل HTTP جمع‌آوری و محاسبه شده است. در آزمون آنتروپی شرطی، ملاک نامحسوسی کمتر بودن نمره آستانه نمونه داده مورد آزمایش از نمره آستانه در نمونه داده سالم است. با توجه به نتایج به دست آمده در نمودار شکل (۱۴) مشخص است که در هر چهار وضعیت این شرط برقرار است. بنابراین کانال پوششی زمانبندی‌دار ترکیبی براساس آزمون آنتروپی شرطی در تمامی شرایط ترافیکی در شبکه C&C نامحسوس است.

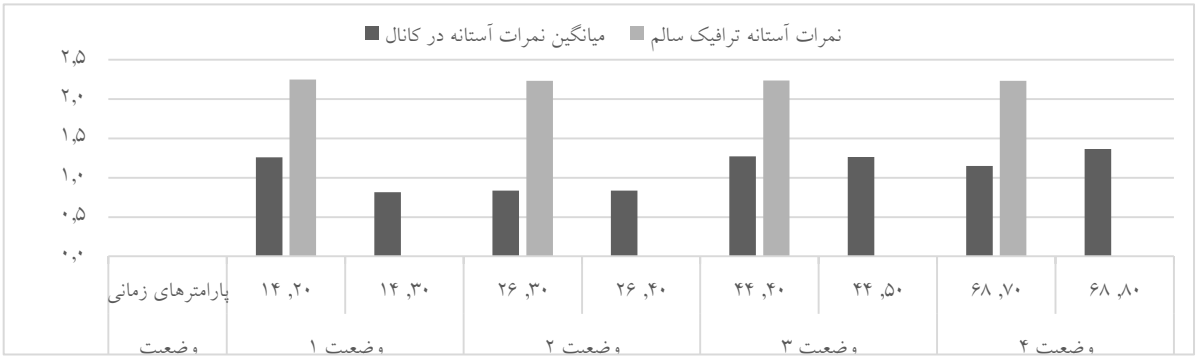
۵-۵-۲- آزمون آنتروپی

در این آزمون نیز نمرات آستانه در نمونه داده‌های سالم و کانال محاسبه شد و طبق جدول (۳) جمع‌بندی شد. این نمونه‌ها نیز برای ۱۰۰۰۰۰ فاصله زمانی بر روی پروتکل HTTP جمع‌آوری و محاسبه شده است.

1- False Positive

جدول (۲). نمرات آستانه در آزمون آنتروپی شرطی

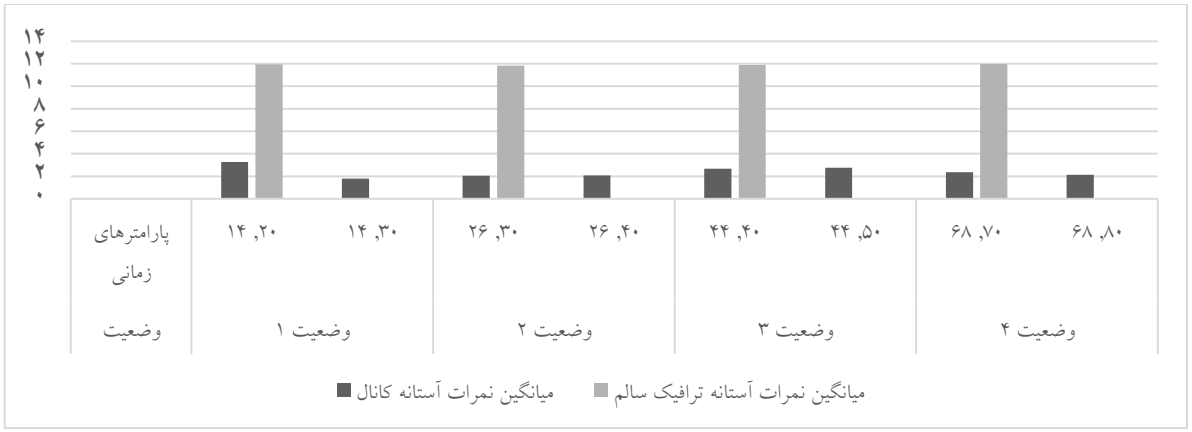
ترافیک سالم					ترافیک کانال پوششی ارتباطی		
وضعیت	میانگین	انحراف معیار	شرط نمرات آستانه	نرخ مثبت کاذب	Δ و δ	میانگین	انحراف معیار
وضعیت ۱	۲/۲۱۶۳۸۵۷	۰/۰۱۳۸۷۳۷۵۷	CCE <= ۲/۲۴۷۲۵	٪۲	۱۴ ,۲۰	۱/۲۶۰۷۲۵۸۳۳	۰/۵۱۱۳۸۲۹۲
					۱۴ ,۳۰	۰/۸۱۵۷۳۹	۰/۱۷۲۵۴۴۴۴
وضعیت ۲	۲/۲۱۴۷۴۱۳	۰/۰۱۳۱۵۷۸۰۷	CCE <= ۲/۲۳۲۸۱۷	٪۴	۲۶ ,۳۰	۰/۸۳۷۰۴۹	۰/۲۶۱۳۶۴۰۲
					۲۶ ,۴۰	۰/۸۳۶۲۸۲۵	۰/۲۶۳۷۸۹۶۹
وضعیت ۳	۲/۲۱۵۳۶۳۷۶	۰/۰۱۳۶۲۹۳۳۶	CCE <= ۲/۲۳۵۹۳۸	٪۶	۴۴ ,۴۰	۱/۲۷۲۴۱۲۸۳۳	۰/۰۱۶۶۷۷۱۳
					۴۴ ,۵۰	۱/۲۶۴۹۰۰۶۶۷	۰/۰۱۰۷۰۹۷۴
وضعیت ۴	۲/۲۱۶۵۱۹	۰/۰۱۳۴۸۱۴۷۲	CCE <= ۲/۲۳۱۸۰۴	٪۱۰	۶۸ ,۷۰	۱/۱۴۹۶۱۳۱۶۷	۰/۳۰۲۸۷۷۰۹
					۶۸ ,۸۰	۱/۳۶۴۵۰۷۸۳۳	۰/۱۹۲۵۰۶۹۶



شکل (۱۴). مقایسه نمرات آستانه کانال در وضعیت‌های مختلف در آزمون آنتروپی شرطی

جدول (۳). نمرات آستانه در آزمون آنتروپی

ترافیک سالم					ترافیک کانال پوششی ارتباطی		
وضعیت	میانگین	انحراف معیار	نمرات آستانه	نرخ مثبت کاذب	Δ و δ	میانگین	انحراف معیار
وضعیت ۱	۱۲/۰۹۵۹۹۳۰۸	۰/۰۹۷۰۷۵۰۱۳	CEN >= ۱۱/۹۲۹۴۵۹	٪۲	۱۴ ,۲۰	۳/۲۵۸۳۱۸۵	۰/۰۳۷۸۲۰۹۴
					۱۴ ,۳۰	۱/۷۹۲۴۷۱۳۳۳	۰/۵۰۹۴۹۰۸۶۷
وضعیت ۲	۱۲/۰۶۲۹۰۲۷۲	۰/۱۱۷۱۵۰۲۹۶	CEN >= ۱۱/۸۴۳۰۳۲	٪۴	۲۶ ,۳۰	۲/۰۵۷۶۱۴۱۶۷	۰/۰۰۴۵۷۳۴۶۳
					۲۶ ,۴۰	۲/۰۶۹۵۴۳۸۳۳	۰/۵۰۹۴۹۰۸۶۷
وضعیت ۳	۱۲/۰۸۰۰۹۵۸۸	۰/۱۰۹۸۵۵۹۸۷	CEN >= ۱۱/۸۹۱۰۰۶	٪۶	۴۴ ,۴۰	۲/۶۷۱۱۰۹	۰/۰۰۸۹۸۶۸۰۲
					۴۴ ,۵۰	۲/۷۵۵۷۳۳۵	۰/۰۲۲۷۷۲۶۸
وضعیت ۴	۱۲/۱۰۷۱۳۹۱۲	۰/۱۱۱۷۹۳۳۳۹	CEN >= ۱۱/۹۶۳۹۸۹	٪۱۰	۶۸ ,۷۰	۲/۳۶۱۵۸۸۳۳۳	۰/۳۵۵۶۹۷۱۶۱
					۶۸ ,۸۰	۲/۱۳۴۵۰۲۸۳۳	۰/۰۱۵۶۱۹۵۱۶



شکل (۱۵). مقایسه نمرات آستانه کانال در وضعیت‌های مختلف در آزمون آنتروپی

براساس آزمون آنتروپی، ملاک نامحسوسی بیشتر بودن نمرات آستانه در کانال از نمرات آستانه در نمونه داده سالم است. با توجه به نتایج به دست آمده و مقایسه این نتایج در هر وضعیت براساس نمودار شکل (۱۵)، مشخص است که شرط نامحسوسی در هیچ یک از وضعیت‌ها برقرار نیست. بنابراین کانال مورد نظر براساس آزمون آنتروپی دارای نامحسوسی مناسب نیست.

۶- نتیجه‌گیری

نیاز به زیرساخت ارتباطی همراه با محرمانگی و قابلیت گریز از کشف، موجب شد تا ایده توسعه کاربرد کانال پوششی زمانبندی‌دار در ساختار شبکه بات و استفاده از قابلیت‌های نامحسوسی، استحکام و ظرفیت مناسب این نوع کانال در تأمین و ارتقاء معیارهای ارزیابی در شبکه بات شکل گیرد. بر این اساس، طرح زیرساخت ارتباطی شبکه فرماندهی و کنترل بات مبتنی بر کانال پوششی زمانبندی‌دار به عنوان یک پروتکل ارتباطی پوششی مدنظر قرار گرفت. با توجه به نیازمندی‌های اصلی و ویژگی‌های این کانال‌ها، طراحی این پروتکل براساس معماری لایه‌ای و ساختاری پیمانه‌ای ارائه شد.

پروتکل پیشنهادی مستقل از الگو و محتوای بسته‌ها بوده و روش‌ها و ابزارهای مبتنی بر تحلیل محتوایی بر روی این روش، از کارایی لازم برخوردار نیستند. همچنین پارامتری بودن تنظیمات کانال و انتخاب دلخواه روش ارسال، باعث تنوع الگوی رفتاری و ترافیکی در پروتکل ارتباطی شده و از طرفی استفاده از ویژگی‌ها و الگوی ترافیک شبکه میزبان در تنظیم پارامترهای کانال، باعث عدم کارایی نسبی در کشف و تشخیص جریان‌های کانال از جریان‌های موجود در شبکه مجاز می‌شود و ارتقاء ویژگی‌های امنیتی را به دنبال دارد.

علاوه بر این، جهت جلوگیری از وقوع خطاهای مختلف و ارتقاء قابلیت اطمینان در پروتکل پیشنهادی، سازوکارهای کشف و کنترل خطا در دو لایه اول و دوم پیش‌بینی شده است. ساختار پروتکل نیز به صورت پیمانه‌ای طراحی شده است و تنظیم ویژگی های کانال به صورت پارامتری می‌باشد و با توجه به شرایط ترافیک شبکه میزبان، قابل تغییر است. بنابراین طرح مورد نظر از قابلیت انعطاف‌پذیری مناسبی برخوردار است. عدم ارسال محتوای پیام در شبکه و کدگذاری آن بر روی بسته‌ها نیز باعث می‌شود که حتی در صورت کشف کانال، محرمانگی پیام حفظ شود.

با توجه به تنوع ویژگی‌های ارتباطی در شبکه بات از ابزار مقلد شبکه برای ایجاد محیط آزمایشی واقعی استفاده شد و معیارهای استحکام، ظرفیت و نامحسوسی کانال ترکیبی مورد استفاده در پروتکل پیشنهادی مورد ارزیابی قرار گرفته‌اند. بررسی ظرفیت کانال در وضعیت‌های مختلف ترافیکی نشان می‌دهد که حتی با وجود بیشترین نویز، کانال ارتباطی دارای نرخ انتقال ۱۱،۰۱ بیت بر ثانیه بوده و حداقل حجم تبادل داده در شبکه فرماندهی و کنترل را تأمین می‌کند. در خصوص استحکام کانال، ارزیابی میزان انتقال صحیح پیام در سطح شبکه به عنوان معیار اصلی مدنظر قرار گرفت و در شرایط ترافیکی با کمترین نویز ۹۹ درصد پیام‌ها به صورت کامل و درست مبادله می‌شوند و در وضعیت وجود بیشترین نویز و با وجود کاهش ظرفیت و نامحسوسی کانال، کماکان استحکام کانال در سطح مناسبی قرار دارد، بنابراین قابلیت اطمینان کانال در بدترین شرایط ترافیکی در سطح مناسبی قرار دارد. ارزیابی نامحسوسی کانال براساس آزمون آنتروپی شرطی نیز نشان از نامحسوس بودن شبکه در شرایط مختلف ترافیکی دارد.

براساس نتایج حاصل از انجام تحقیق، کانال پوششی زمانبندی‌دار دارای قابلیت‌های مناسب ارتباطی بوده و حتی در بدترین شرایط ترافیکی، قابلیت تأمین زیرساخت ارتباطی با حداقل نرخ تبادل و استحکام مناسب را دارد و دارای محرمانگی قابل قبول براساس روش‌های آماری مرتبه دوم است. بنابراین با استفاده از این نوع کانال و پیش‌بینی یک چارچوب مناسب، می‌توان پروتکل ارتباطی پوششی همراه با ارتقاء معیارهای ارزیابی کمی و کیفی برای شبکه فرماندهی و کنترل طراحی و به‌کارگیری نمود.

۷- مراجع

[1] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, "A Survey of Botnet Technology and Defenses," Ann Arbor, Michigan, 2009.

[2] Y. Ho Shin and E. Gyu Im, "A Survey of Botnet : Consequences, Defenses and Challenges," pp. 133-791, 2009.

[3] P. Vaclav, "Information hiding and covert channel," prague, 2001.

[4] Z. Wang and R. B. Lee, "New Constructive Approach to Covert Channel Modeling and Channel Capacity Estimation," Springer, pp. 498-505, 2005.

[5] M. Smeets and M. Koot, "Covert Channels," RP1, Amsterdam, 2006.

[6] S. Zander, "Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks," Swinburne University, Melbourne, 2010.

[7] D. Anthony, D. Johnson, P. Lutz, and B. Yuan, "A Behavior Based Covert Channel within Anti-Virus Updates," Rochester, 2012.

[8] M. Saadati, "Simulation and Analysis of IPD-Reo Covert Timing Channels in Computer Networks," Thesis, IHU, Tehran, 2014.

[9] W. C. Henry, "covert channels within IRC," 2011.

[10] F. Brezo, J. Gaviria de la Puerta, I. Santos, D. Barroso, and P. G. Bringas, "C&C Techniques in Botnet Development," Springer, vol. 189, no. 2194-5357, pp. 97-108, 2013.

[11] M. Casenove and A. Miraglia, "Botnet over Tor: The Illusion of Hiding," in 6th International Conference on Cyber Conflict, 2014.

[12] D. Monica and C. Ribeiro, "Leveraging Honest Users: Stealth Command-and-Control of Botnets," INESC-ID/IST, 2011.

[13] A. Nappa, A. Fattori, M. Balduzzi, M. Dell'Amico, and L. Cavallaro, "Take a Deep Breath: a Stealthy, Resilient and Cost-Effective Botnet Using Skype," Springer, vol. 6201, no. 0302-9743, pp. 81-100, 2010.

[14] M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S. Yamaguchi, "A proposal of metrics for botnet detection based on its cooperative behavior," Takayama, 2005.

[15] H. Rouhani zeidanloo and A. Bt Abdul Manaf, "Botnet Detection by Monitoring Similar Communication Patterns," IJCSIS, vol. 7, no. 1947-5500, pp. 36-46, 2010.

[16] R. Kannan and A. V. Ramani, "Flow Based Analysis to Identify Bonet Infected Systems," JATIT, vol. 67, no. 1817-3195, pp. 290-296, 2014.

[17] L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, and C. Kruegel, "Disclosure: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis," in 28th annual computer security application conference, New York, USA, 2012.

[18] G. GU, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustring Analysis of Network Traffic for Protocol and Structure Independent Botnet DDetection," In 17 USENIX Security Symosium, Berkeley, 2008.

[19] A. Berger and M. Hefeeda, "Exploiting SIP for Botnet Communication," ftw, 2009.

[20] B. Francois, "BYOB: Build Your Own Botnet," SANS, 2011.

[21] F. Conzetti, "A Historical evaluation of C&C complexity," B. Thomas Golisano College, 2012.

[22] E. Stinson and J. C. Mitchell, "Towards Systematic Evaluation of the Evadability of Bot/Botnet Detection Methods," 2008.

[23] K. Mahathi, "Botnets: Overview and Case Study," Department of Mathematics and Computer Information Science, 2008.

[24] M. Dehghani and M. Saleh Esfahani, "Network Covert Channels: An Information Leakage Flow," Passive Defence Quarterly, 2012.

[25] A. El-Atawy and E. Al-Shaer, "Building Covert Channels over the Packet Reordering Phenomenon," In 28th Annual IEEE Conference on Computer Communications (INFOCOM), Chicago, USA, 2009.

[26] A. P. Jayasumana and A. A. Bare Nischal and M. Piratla, "Reorder density (rd): A formal, comprehensive metric for packet reordering," NETWORKING, 2005.

[27] H. Sellke, C. Chun Wang, and S. Bagchi, "TCP/IP Timing Channels: Theory to Implementation," in 28th Conference on Computer, West Lafayette, 2009.

[28] M. dehghani, M. saleh esfahani, "compound covert timing channel design and analysis with petrinet," Advanced Defence Science and Technology, vol. 2, no. 5, pp. 157-169, 2014.

[29] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: Automated modeling and evasion," in RAID 08: Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection, Springer-Verlag, Berlin, Heidelberg, 2008.

[30] X. Zi, L. Yao, L. Pan, and J. Li, "Implementing a passive network covert timing channel," Elsevier, no. 10.1016, pp. 686-696, Dec. 2009.

[31] H.Sellke, "Analytical charaterization of internet security attacks, thesis of phd," Purdue University, West Lafayette, Indiana, 2010.

[32] S. Zander and G. Armitage, "CCHEF – Covert Channels Evaluation Framework Design and Implementation," Melbourne, Australia, 2008.

[33] G. Liu, J. Zhai and Y. Dai, "Network covert timing channel with distribution matching," Springer, no. DOI 10.1007/s11235-010-9368-1, pp. 199–205, 1 August 2010.

[34] L. Nussbaum and O. Richard, "A Comparative Study of Network Link Emulators," LIG, 2006.

[35] S. Hemminger, "Network Emulation with NetEm," Open Source Development Lab, April 2005.

[36] H. P. Pfeifer, "Network Emulation," Protocol Labs, 2011.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 4, 2017, Serial No. 16

Botnet C&C Network based on Covert Timing channel

H. Gorzin, M. Dehghany*, M. Saleh Esfahani

*Imam Hossein University

(Received: 19/10/2015 , Accepted: 03/05/2016)

ABSTRACT

Privacy and avoiding being detected by security systems are both two important features of Botnet whose communication structure affects them directly. In this paper, covert communication protocol based on covert timing channel is presented for Botnet and the capabilities of these types of channels are used for enhancing the features. The proposed Protocol is designed with layered and modular structure which is scalable and flexible. In this project, in addition to developing the usage of these channels in Botnet, the interaction of evaluation criteria in two areas is investigated in a real condition. According to the various traffic Circumstances of systems involved in botnet, the Emulator Tool is used for implementing a test Environment in real Circumstances and channel evaluation criteria including capacity, robustness and stealthy are evaluated. The results show that in the best traffic condition, the average time is equival to 48.07 bits per second with robustness factor of 99% and in the worst traffic condition with different types of errors, the capacity is equival to 11.01 per second with robustness of 85% in proposed Protocol. Conditional Entropy method also shows stealthy of communication in the protocol. The results show the appropriate capability of covert timing channel to supply communication infrastructure in botnet.

Keywords: Botnet, Covert Timing Channel, Botnet Command and Control Network, Network Emulator

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