طراحی و ارزیابی روش کدبندی ترکیبی برای کانال پوششی زمان‌بندی‌دار در شبکه اینترنت

مهدی دهقانی و محمود صالح اصفهانی

دانشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران، ایران

چکیده

کانال پوششی به معنی مبادلهٔ اطلاعات در پوشش یک کانال آشکار است؛ به‌نحوی‌که اصل وجود ارتباط از دید ناظر مخفی بماند. در کانال‌های پوششی زمان‌بندی‌دار تحت شبکه که از ویژگی‌های زمان‌بندی ارسال بستک‌های شبکه برای مدولاسیون اطلاعات پوششی استفاده می‌شود، طراحی روش کدبندی مناسب اهمیت بالایی دارد. در این پژوهش طراحی روش کدبندی جدید با ترکیب روش‌های «فاصله بین بستک‌ها» و «بازترتیب بستک‌ها» و تأکید بر بهبود ظرفیت و نامحسوسی کانال پوششی ارائه‌شده، ظرفیت کانال به روش کدبندی ترکیبی محاسبه شده و نامحسوسی و استحکام کانال به روش اندازه‌گیری عملی ارزیابی شده‌اند. نتایج پژوهش نشان می‌دهد که مطابق با وضعیت عادی بازترتیب در شبکه، با انتخاب سه تا پنج بستک در جدول کلمه‌کد، ظرفیت از ۱۰٪ تا ۳۰۰٪ می‌تواند افزایش یافته، نامحسوسی تا حد قابل‌قبولی بهبود یافته و استحکام کانال نیز حفظ شده است.

واژگان کلیدی: کانال پوششی، کدبندی، معیار ارزیابی، بازترتیب بستک‌ها، فاصله بین بستک‌ها

۱- مقدّمه

انسان آموخته است که چیزهای با ارزش خود را از دید دیگران پنهان سازد. ابنای بشر در طول تاریخ به ارزشمندی اطلاعات پی‌برده‌اند. انسان از روزگاران قدیم برای پنهان‌سازی اطلاعات و برقراری ارتباط پنهان، راه‌کارهایی را ابداع کرده و مورد استفاده قرار داده است. در این دوران نیز روش‌های پنهان‌سازی اطلاعات متناسب با فناوری اطلاعات و ارتباطات به شکل جدید توسعه یافته است. اطلاعات یا پیام باید در رسانه‌ای به‌عنوان پوشش یا حامل پنهان شود. از سالیان قدیم که هنوز شبکه‌های رایانه‌ای به شکل امروزی گسترش نیافته بودند، اطلاعات در محتوای متن، صوت یا تصویر پنهان می‌شد و آن را پنهان‌نگاری می‌نامیدند. به‌تازگی شبکه نیز به‌عنوان یک رسانه برای پنهان‌سازی اطلاعات مورد استفاده قرارگرفته و نهفته‌سازی اطلاعات در فضاهای خالی یا ویژگی‌های زمان‌بندی پروتکل‌های شبکه نیز به فنون پنهان‌سازی اطلاعات افزوده شده است که به آن «پنهان‌نگاری شبکه‌ای[1]» یا «کانال پوششی شبکه‌ای[2]» گفته می‌شود (زیلینسکا[3]، ۲۰۱۴). کانال پوششی درواقع یک ارتباط پنهان است که در پوشش یک ارتباط آشکار و مجاز برقرار می‌شود و اصل وجود ارتباط و طرفین ارتباط مخفی می‌ماند (آلیس[4]، ۲۰۱۲). کانال پوششی با استفاده از آسیب‌پذیری‌های پروتکل‌های ارتباطی منجر به نشت اطلاعات از یک کاربر با سطح دسترسی بالا به کاربر دیگر با سطح دسترسی پایین می‌شود.

کانال‌های پوششی تحت شبکه به دو دستهٔ انبارشی و زمان‌بندی‌دار تقسیم می‌شوند (زندر[5]، ۲۰۰۷). کانال‌های انبارشی، اطلاعات پوششی را در میدان‌های[6] ذخیره یا میدان‌های استفاده نشده یا در میدان‌هایی که امکان استفاده از آن‌ها بدون تأثیر در عملکرد پروتکل وجود دارد، ذخیره

[1] Network Steganography
[2] Network Covert Channel
[3] Zielinska
[4] Alis
[5] Zander
[6] Field

می‌شوند. فرستنده داده‌های مورد نظر را در این میدان‌ها می‌نویسد و گیرنده آن‌ها را از این میدان‌ها می‌خواند. به‌طور معمول این دسته از کانال‌ها با انجام تنظیمات مناسب روی پروتکل‌های شبکه، حذف می‌شوند و حتی کارایی پروتکل نیز بهبود می‌یابد. کانال‌های پوششی زمان‌بندی‌دار از ویژگی‌های زمان‌بندی بستک‌های شبکه برای مدولاسیون اطلاعات استفاده می‌کنند و داده‌های پوششی را در زمان‌بندی قاب‌ها[1]، بستک‌ها یا پیام‌هایی که به‌طور مستقیم بین فرستنده و گیرنده مبادله می‌شوند، کدبندی می‌نمایند. کانال‌های زمان‌بندی‌دار به‌دلیل عدم دقت زمان‌بندی در فرستنده و گیرنده و لغزش زمانی[2] شبکه، همیشه دارای نوفه هستند. ظرفیت کانال‌های زمان‌بندی‌دار اغلب کمتر از کانال‌های انبارشی است؛ اما درعوض، تشخیص و حذف آنها دشوارتر است. روش‌هایی که برای کدبندی در این دسته کانال‌ها استفاده شده شامل بازترتیب بستک‌ها[3]، فاصله بین بستک‌ها[4]، نرخ بستک[5]، زمان‌بندی توالی پیام[6]، گم‌شدن بستک‌ها[7]، تصادم قاب‌ها است (زندر، ۲۰۱۰). در این مقاله دو روش بازترتیب بستک‌ها و فاصله بین بستک‌ها بهبود داده و ترکیب شده‌اند.

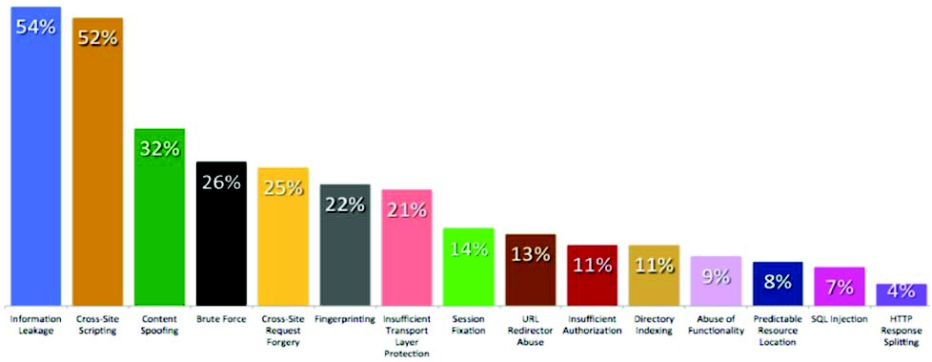
کانال‌های پوششی دارای سه معیار ارزیابی ظرفیت، استحکام و نامحسوسی هستند. ظرفیت کانال به معنای نرخ ارسال اطلاعات پوششی بوده و براساس بیت بر ثانیه یا بیت بر بستک اندازه‌گیری می‌شود. استحکام کانال به معنی میزان سختی حذف کانال پوششی یا محدودکردن ظرفیت آن است و با نرخ خطای بیت[8] اندازه‌گیری می‌شود. نامحسوسی کانال به معنی میزان سختی تشخیص کانال پوششی در مقایسه با ترافیک کانال مجاز است. ظرفیت، نامحسوسی و استحکام، به‌عنوان معیارهای ارزیابی اهداف متضادی هستند. به‌طور معمول بیشینه‌کردن هم‌زمان هر سه معیار غیرممکن است و کاربران باید برای هر وضعیت خاصی، بین این سه معیار تعادل ایجاد کنند. به‌عنوان مثال ارسال داده‌های کمتر، موجب بهبودی نامحسوسی کانال می‌شود و افزایش افزونگی داده‌ها استحکام کانال را بهبود می‌بخشد؛ اما هردوی این‌ها، یعنی ارسال کمتر داده‌ها و افزایش افزونگی داده‌ها، ظرفیت کانال را کاهش می‌دهند. از سوی دیگر، استحکام می‌تواند به‌سادگی با افزایش دامنهٔ سیگنال افزایش داده شود، اما این امر نامحسوسی را کاهش می‌دهد. روش کدبندی در دست‌یابی به مقادیر قابل‌قبول هریک از معیارهای سه‌گانه مذکور اهمیت بالایی دارد. پژوهش‌گران براساس تأکید خود بر هر یک از این معیارها یا برای ایجاد تعادل بین آنها، روش طراحی خاصی برای کدبندی پیشنهاد می‌دهند.

نشت اطلاعات[9] محرمانه یا حساس از طریق کانال‌های پوششی، جزء تهدیدهای مهم امنیتی شناخته می‌شود (دهقانی، ۱۳۹۱). آمارها نشان می‌دهد که نشت اطلاعات در رتبه‌بندی تهدیدها و حملات، در سال‌های متمادی نخستین یا دومین رتبه را به خود اختصاص داده است (حسن‌نیا، ۱۳۹۲). (شکل- ۱) رتبه‌بندی ۱۵ آسیب‌پذیری بالا در سال ۲۰۱۲ را نشان می‌دهد.

کاربرد اصلی کانال پوششی، برقراری ارتباط پنهان است (کاوتور[10]، ۲۰۱۰) و ممکن است توسط افراد خودی یا دوست برای کاربردهای مثبت هم استفاده شود. کاربردهای مثبت کانال پوششی شامل برقراری ارتباط پنهان بین افراد خودی، پنهان‌سازی ارتباطات مدیریت شبکه، مبادله کلید رمزنگاری، تعقیب ترافیک خاص و حفاظت از حقوق معنوی با نشانه‌گذاری[11] است. با توجه به کاربردهای مثبت و منفی کانال‌های پوششی، ابداع روش‌های جدید کانال پوششی و روش‌های تشخیص آنها، همواره موضوع پژوهشی جذابی برای پژوهش‌گران بوده است. مجموعه تحقیقات انجام‌شده در زمینه کانال‌های پوششی؛ بهبود معیارهای ظرفیت، استحکام و نامحسوسی کانال را هدف خود قرار داده‌اند. هرکدام از پژوهش‌های انجام‌شده به‌نحوی تلاش خود را برای نیل به این اهداف معطوف داشته‌اند؛ ولی بهبود این معیارها به‌خصوص افزایش ظرفیت کانال با توجه به کاربردهای ذکرشده برای کانال‌های پوششی، هنوز نتوانسته به حد مطلوب برسد. با توجه به کاربردهای متنوع کانال‌های پوششی و محدودیت‌هایی که از نظر ظرفیت و نامحسوسی در طرح‌های ارائه‌شده قبلی وجود دارد، رفع این محدودیت‌ها و فراهم‌کردن شرایط کاربری بیشتر کانال‌های پوششی همواره یکی از مسائل مهم پژوهش بوده است.

[1] Frame
[2] Jitter
[3] Reordering
[4] Inter-packet gaps
[5] Packet rate
[6] Message sequence timing
[7] Packet loss
[8] BER: Bit Error Rate

[9] Information leakage
[10] Couture
[11] Watermarking



(شکل- ۱): رتبه‌بندی ۱۵ آسیب‌پذیری بالا در سال ۲۰۱۲ (وایت‌هت[1]، ۲۰۱۳)

هدف اصلی این پژوهش ارائه روش کدبندی جدید با بهبود و ترکیب روش‌های بازترتیب بستک‌ها و فاصله بین بستک‌هاست به‌نحوی‌که ظرفیت و نامحسوسی کانال بهبود یابد. در بخش ۲ این مقاله، کارهای مرتبط انجام‌شده در حوزه دو روش طراحی مورد نظر بررسی و مقایسه می‌شوند. در بخش ۳ روش پیشنهادی طراحی کدبندی ترکیبی ارائه‌شده و میزان افزایش ظرفیت حاصل‌شده محاسبه می‌شود و در بخش ۴، ارزیابی عملی نامحسوسی و استحکام کانال ترکیبی ارائه شده و نتایج با کارهای قبلی مقایسه می‌شود. در بخش ۵ نیز جمع‌بندی و نتیجه پژوهش بیان می‌شود.

۲- کارهای مرتبط

در این بخش به‌دلیل این‌که طرح پیشنهادی مبتنی بر ترکیب روش‌های بازترتیب بستک‌ها و فاصله بین بستک‌هاست، کارهای انجام‌شده در این دو حوزه بررسی شده است.

۲-۱- روش بازترتیب بستک‌ها

در این روش ترتیب بستک‌ها مبنای کدبندی داده‌های پوششی قرار می‌گیرد. کندور[2] و همکارانش یک کانال پوششی از طریق بازترتیب بستک‌ها پیاده‌سازی کردند (کندور، ۲۰۰۳). این روش بر این اساس طراحی شده که یک مجموعه n بستکی می‌تواند در !n حالت مرتب شود. بدین ترتیب در چنین کانالی حداکثر تعداد $\log_2 n!$ بیت می‌تواند ارسال شود. در روش‌های بازترتیب بستک‌ها برای هر بستک یک شماره توالی لازم است تا ترتیب اصلی بستک‌ها را بتوان تعیین کرد. از اعداد توالی AH[3] یا ESP[4] یا سایر اعداد توالی مثل عدد توالی TCP می‌توان برای این منظور استفاده کرد. ایشان روشی ساده برای ایجاد کانال پوششی ارائه داده‌اند؛ ولی برای خطای ناشی از بازترتیب ذاتی کانال راه‌کاری ارائه نکرده‌اند.

گالاتنکو[5] و همکارانش یک مجموعه بستک متوالی را براساس نشانی مقصدشان مرتب‌سازی کرده و اطلاعات پوششی را از این طریق ارسال کردند (گالاتنکو، ۲۰۰۵). در این طرح، مجموعه بستک‌های متوالی با نشانی‌های مقصد صعودی به‌منزله «یک» و مجموعه بستک‌های متوالی با نشانی‌های مقصد نزولی به‌منزله «صفر» در نظر گرفته‌شده‌اند. در این طرح، طول مجموعه متوالی بستک‌ها براساس نرخ خطای مطلوب کانال تعیین می‌شود و روش کدبندی یا ارزیابی ظرفیت و نامحسوسی کانال انجام نشده است. *لو*[6] و همکارانش طرحی پیشنهاد کردند که اطلاعات پوششی را در ترتیب N بستک در میان X جریان TCP کدبندی کردند که این امر پهنای باند کانال را افزایش می‌دهد (لو، ۲۰۰۷). در این طرح که Cloak نام‌گذاری شده است، هر پیام پوششی با یک توزیع یکتای N بستک TCP روی X جریان TCP کدبندی می‌شود. کدبند و کدگشا از قبل روی مقادیر N و X توافق می‌کنند. در cloak، کدبند پیام بعدی را فقط بعد از دریافت تأییدیه‌های پیام کنونی می‌فرستد. در طرف دیگر کانال، کدگشا کارش را بعد از جمع‌شدن N بستک رسیده از کدبند شروع می‌کند. در این

[1] WhiteHat
[2] Kundur
[3] IPSec Authentication Header
[4] Encapsulating Security Payloads
[5] Galatenko
[6] Luo

طرح به‌دلیل پیاده‌سازی در سطح لایه TCP، پایداری و استحکام بالایی در مبادله بستک‌ها وجود دارد و مسائلی چون گم‌شدن، بازترتیب و تکرار بستک‌ها در پروتکل TCP حل شده است. بسته به اینکه بستک‌ها یا جریان‌ها از همدیگر قابل تفکیک هستند یا نه راه‌های مختلفی برای کدبندی داده‌های پوششی وجود دارد. اگر جریان‌ها را گلدان و بستک‌ها را توپ در نظر بگیریم، روش کدبندی مذکور مشابه مسئله ترکیب‌شناسی شمارشی گذاشتن N توپ در X گلدان است. لو و همکارانش علاوه‌بر ارزیابی ظرفیت، یک الگوریتم تشخیص را نیز طراحی و آن را ارزیابی کرده‌اند. ایشان به نتایج خوبی دست‌یافته‌اند.

خان[1] و همکارانش (خان، ۲۰۰۹) نیز یک کانال مشابه پیشنهاد داده‌اند. ایشان n اتصال موازی بین فرستنده و گیرنده ایجاد کرده و با ارسال بستک‌ها به روش‌های مختلف، ظرفیت کانال و نامحسوسی آن را افزایش دادند. برای افزایش ظرفیت کانال در یک روش، n اتصال موازی را به‌عنوان n بیت یک کلمه در نظر گرفته و ارسال بستک روی iاُمین اتصال به معنی عدد i تلقی می‌شود و بدین ترتیب ارسال هر بستک حاوی $\log_2(n)$ بیت اطلاعات پوششی خواهد بود. مثلاً اگر n=8 اتصال موازی برقرار شود، ارسال هر بستک حاوی سه بیت اطلاعات خواهد بود. در روش پیشرفته‌تر برای افزایش ظرفیت کانال، n اتصال را مجزا درنظر گرفته و هرکدام را به m اتصال مجازی تقسیم کرده‌اند. خان و همکارانش برای ایجاد اتصالات مجازی از تفاوت طول بستک‌های ارسالی استفاده کرده‌اند. به‌عنوان مثال ارسال بستک‌های با چهار طول متفاوت را به‌منزله اعداد ۰۰، ۰۱، ۱۰ و ۱۱ در نظر گرفته‌اند. بدین ترتیب ظرفیت کانال به $n \times m$ افزایش‌یافته است که n تعداد سوکت‌ها و m تعداد اتصالات مجازی روی هر اتصال است. ایشان ضمن بهبود طرح خود برای افزایش ظرفیت، در جهت بهبود طرح برای فرار از تشخیص قاعده‌مندی نیز تلاش کرده و به نتایج خوبی دست‌یافته‌اند؛ ولی پیاده‌سازی طرح ایشان تاحدودی پیچیده است.

العطائی[2] و همکارانش یک کانال پوششی بر مبنای بازترتیب بستک‌ها توسعه دادند (العطایی، ۲۰۰۹). ایشان روی علل و درصد بروز بازترتیب بستک‌ها در ترافیک شبکه پژوهش کرده و اظهار کردند که بازترتیب بستک‌ها به‌عنوان یک پدیده در شبکه‌های مدرن رایانه‌ای نیز وجود دارد و بهره‌برداری از آن برای ایجاد کانال پوششی، روی کارایی شبکه تأثیر نمی‌گذارد. ایشان هر k بستک را به‌عنوان یک کلمه‌کد[3] یا همان نماد در نظر گرفتند و روی بهترین انتخاب کلمه‌کد (یعنی الگوی جایگشت) برای دستیابی به ظرفیت بالاتر کانال، پایداری و استحکام بیشتر در برابر خطاهای کانال و تقلید ترافیک واقعی و افزایش نامحسوسی کانال پژوهش کردند. آنها برای نیل به این اهداف، دو عامل عمق بازترتیب و حجم بازترتیب را برای محاسبه میزان بازترتیب مناسب بستک‌ها در نظر گرفتند. عمق بازترتیب نشان‌دهنده دورترین بستکی می‌باشد که جابه‌جا شده است یا گستره‌ای که بستک می‌تواند در آن جابه‌جا شود و حجم بازترتیب نشان‌دهنده درصد بستک‌هایی است که نامرتب هستند. ایشان از ترافیک IP برای پیاده‌سازی کانال پوششی پیشنهادی خود استفاده کردند. در (جدول- ۱) کارهای مبتنی بر روش بازترتیب بستک‌ها مقایسه شده است. براساس مطالعات این نگارنده از آخرین پژوهش‌ها می‌توان گفت که در روش‌های بازترتیب بستک فقط لو و خان با استفاده از چند اتصال موازی برای افزایش ظرفیت کانال تلاش کرده‌اند. برای افزایش نامحسوسی کانال نیز، فقط العطائی روشی را برای انتخاب کلمه‌کد و توزیع احتمال آن به‌نحوی‌که از رفتار بازترتیب شبکه منحرف نشود، را پیشنهاد داده است.

۲-۲- روش فاصله بین بستک‌ها

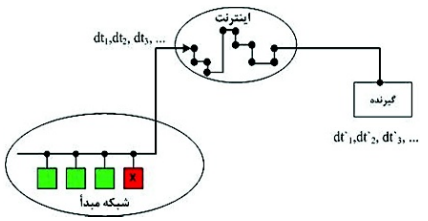
در این روش از فاصلهٔ زمانی بین بستک‌ها در کانال مجاز برای مدولاسیون اطلاعات پوششی استفاده می‌شود (شکل- ۲). *برک*[4] و همکارانش با استفاده از نظریه اطلاعات و در نظر گرفتن وضعیت شبکه و مهارت‌های مهاجم، در مورد تشخیص کانال زمان‌بندی‌دار پوششی مبتنی بر فواصل زمانی بین بستک‌های متوالی تحقیق کردند (برک، ۲۰۰۵). ایشان کانال‌های با مقادیر فاصله دوتایی و چندتایی را مقایسه کردند و با استفاده از الگوریتم آریموتو-بلاهوت[5] سازوکاری ارائه کردند که فرستنده می‌تواند برای یک کانال با مشخصه‌های معلوم و دارای چند نماد، توزیع ورودی بهینه را به دست آورده و بدین ترتیب ظرفیت کانال را بیشینه سازد.

[1] Khan
[2] El-Atawy
[3] CodeWord
[4] Berk
[5] Arimoto-Blahut

آن‌ها با فرض مهارت مهاجم و تلاش او برای بیشینه‌کردن ظرفیت کانال، شباهت این توزیع ورودی بهینه با ترافیک شبکه را مبنای تشخیص وجود کانال پوششی قراردادند. این پژوهش‌گران یک راه بسیار ساده نیز برای تشخیص کانال با استفاده از نمودار ستونی[1] تأخیر بین بستک‌ها پیشنهاد داده‌اند. در این روش اگر تعداد بستک‌ها با مقدار میانگین تأخیر، خیلی کمتر از حداکثر تعداد بستک‌ها با هر تأخیر دیگر باشد، حاکی از وجود کانال پوششی خواهد بود.

(جدول- ۱): مقایسه کارهای مبتنی بر روش بازترتیب بستک‌ها

ویژگی	مرجع	کندور	گلاتنکو	لو	خان	العطائی
پروتکل کانال آشکار	IP Sec	✓				
	TCP		✓	✓	✓	
	IP					✓
نوع کانال پوششی	فعال				✓	
	غیرفعال	✓	✓	✓		✓
تمرکز تحقیق	ظرفیت	✓		✓	✓	
	نامحسوسی				✓	✓
	استحکام		✓			✓
معیار مورد ارزیابی	ظرفیت	✓		✓		✓
	نامحسوسی				✓	
	استحکام		✓			✓
روش ارزیابی	محاسباتی	✓	✓			✓
	اندازه‌گیری عملی			✓	✓	✓
نوع آزمون نامحسوسی	قاعده‌مندی				✓	
	عمق بازترتیب					✓



(شکل- ۲): کانال پوششی زمان‌بندی‌دار مبتنی بر فواصل زمانی بین بستک‌ها (جیانی[2]، ۲۰۰۶)

شاه[3] و همکارانش یک دستگاه سخت‌افزاری ساختند که بین صفحه‌کلید و رایانه قرار می‌گرفت و همه کلیدهای فشرده‌شده حاوی کلمات عبور و دیگر اطلاعات تایپ‌شده را از طریق ترافیک مجاز به خارج شبکه ارسال می‌کرد (شاه، ۲۰۰۶). این طرح که JitterBug نامیده شده، با ایجاد تأخیرهای کوچک در ارسال کد کلیدهای فشرده‌شده، تأخیرهای بین بستک‌های یک نرم‌افزار کاربردی شبکه‌ای را تحت تأثیر قرار می‌دهد. در کاربردهای شبکه‌ای تعاملی همانند SSH، XServer، Telnet،...، فشار هر کلید متناظر با ارسال یک بستک به‌احتمال رمزشده به خارج شبکه است. حال تأخیرهای JitterBug در ارسال کد کلیدهای فشرده، موجب تأخیر در ارسال بستک‌های متناظر به خارج شبکه می‌شود. JitterBug بیت «یک» را با افزودن تأخیر بین بستکی به‌اندازه یک مقدار تصادفی به پیمانه[4] w میلی‌ثانیه ارسال می‌کند و بیت «صفر» را با افزودن تأخیر بین بستکی به‌اندازه یک مقدار تصادفی به پیمانه w/2 میلی‌ثانیه ارسال می‌کند. پنجره زمانی w مبین حداکثر تأخیر است که JitterBug به یک تأخیر بین بستکی می‌افزاید. برای مقادیر کوچک w، توزیع ترافیک JitterBug خیلی شبیه ترافیک مجاز اصلی می‌شود. ایشان برای افزایش نامحسوسی کانال با افزودن مقدار S_i از یک دنباله تصادفی، یک پنجره زمانی چرخان ایجاد کردند.

والز[5] و همکارانش (والز، ۲۰۱۱) یک کانال زمانبندی‌دار پوششی غیرفعال ارائه داده‌اند که برای کدبندی از بخشی از جریان در اختیار گرفته‌شده استفاده می‌کند تا اختلاف‌های قابل‌تشخیص توسط آزمون‌های شکل را هموار سازد. Liquid از ترکیبی از دو دسته تأخیر بین بستکی انتقال[6] و تأخیر بین بستکی شکل‌دهی[7] استفاده می‌کند. تأخیرهای بین بستکی که برای کدبندی پیام پوششی استفاده شده، IPDs انتقال نامیده می‌شوند و تأخیرهای بین بستکی که برای حفظ شکل توزیع استفاده شده، IPDs شکل‌دهی نامیده می‌شوند. Liquid از نیمی از IPDs برای کدبندی پیام‌های پوششی با استفاده از کدبندی Jitterbug استفاده می‌کند و از نیم دیگر IPDs برای افزایش احتمال نمادهایی که در IPDs انتقال در آزمون آنتروپی استفاده نشده است. Liquid آهنگ نمادهای نگاشت‌شده را در طول کدبندی پیام حفظ کرده و تلاش می‌کند تا نمادهای دیگری را که هنوز ایجاد نشده و یا بسیار کم ایجاد شده‌اند، تولید نماید. این کار تضمین می‌کند که احتمال هر نماد در آزمون

[1] Histogram
[2] Giani
[3] Shah
[4] Modulo
[5] Walls
[6] Transmitting IPDs
[7] Shaping IPDs

آنتروپی به‌طور تقریبی یکسان باشد، درنتیجه مقدار آنتروپی افزایش می‌یابد. کانال پوششی Liquid قادر به فرار از هر دو روش تشخیص است؛ ولی در برابر آزمون قاعده‌مندی (آنتروپی شرطی) در حد معمولی است. از سوی دیگر، Liquid تنها قادر به استفاده از پنجاه درصد از ظرفیت کانال است.

جیان‌وچیو[1] و همکارانش یک نوع بهبودیافتهٔ کانال زمان‌بندی‌دار را براساس فاصله بین بستکی توسعه دادند و کارایی آن را ارزیابی کردند (جیان‌وچیو، ۲۰۰۸). این طرح که کانال زمان‌بندی‌دار پوششی مدل‌محور نامیده شده، مدل رفتار ترافیک مجاز را تقلید می‌کند. کانال مدل‌محور یک نمونه از ترافیک مجاز را با چندین مدل شناخته‌شده همانند نمایی[2] ویبول[3]، ... مطابقت داده و مدلی که بهترین تطبیق را دارد، انتخاب می‌کند؛ سپس از تابع توزیع معکوس و تابع توزیع جمعی به‌عنوان توابع کدبندی و کدگشایی برای مدل انتخاب‌شده استفاده می‌کند. ازاین‌رو چون تأخیرهای بین بستکی شبه‌تصادفی براساس مدلی منطبق بر ترافیک مجاز تولید می‌شود، توزیع آنها به ترافیک مجاز بسیار شبیه است. اگر زمان‌های بین بستکی ترافیک عادی، دارای توزیع مستقل و یکسان[4] (iid) باشد، تشخیص این کانال دشوار است؛ ولی *زندر* نشان داده که هیچ ترافیکی زمان‌های بین بستکی دارای توزیع مستقل و یکسان ندارد و بخش بزرگی از ترافیک دارای زمان‌های بین بستکی همبسته[5] است (زندر، ۲۰۱۰). روش جیان‌وچیو خودهمبستگی موجود در فاصله زمانی بین بستک‌ها را خراب می‌کند و موجب سهولت تشخیص کانال می‌شود.

سلکه[6] و همکارانش طرح کدبندی هندسی را برای نهفته‌سازی داده‌های پوششی در زمان‌های بین بستکی پیشنهاد داده و نرخ بیت قابل‌دستیابی و نرخ خطا را براساس آزمایش‌های عملی روی اینترنت ارزیابی کرده‌اند (سلکه، ۲۰۰۹) ایشان نشان دادند که با ترافیک دارای توزیع مستقل و یکسان به‌عنوان پوشش، ایجاد کانال زمان‌بندی‌دار پوششی که به‌طور محاسباتی غیرقابل تشخیص باشد؛ به‌طور نظری امکان‌پذیر است. ایشان به ظرفیت دو تا پنج برابر آخرین پژوهش‌ها دست یافتند و گذشت کمی از ظرفیت، موفق به تقلید حرفه‌ای ترافیک مجاز و دستیابی به نامحسوسی بالا شدند؛ ولی طرح ایشان خودهمبستگی موجود در فاصله بین بستک‌ها را تضعیف می‌کند (زندر، ۲۰۱۰).

زندر و همکارانش با مرور طرح‌های کدبندی جیان‌وچیو و سلکه، مدل بهبودیافته‌ای ارائه دادند که ایراد آن دو طرح را برطرف کرده و خودهمبستگی موجود در فاصله زمانی بین بستک‌ها را حفظ می‌کند (زندر، ۲۰۱۰). ایشان با ارائه دو روش کدبندی کم‌پشت[7] و کدبندی زیرباند[8]، میزان پنهان‌بودن و نامحسوسی کانال را با قربانی‌کردن ظرفیت کانال بهبود دادند.

لی‌یو و همکارانش یک کانال زمان‌بندی‌دار پوششی مطرح کردند که داده‌های پوششی را چنان کدبندی می‌کنند که توزیع زمان‌های بین بستکی خیلی نزدیک به طبیعی تخمین زده شود و روش‌های گسترده‌سازی[9] برای فراهم‌سازی استحکام استفاده شده است (لی‌یو، ۲۰۰۹). تشخیص این کانال با آزمون‌های شکل و قاعده‌مندی دشوار است.

گونگ ژیو لیو[10] و همکارانش یک کانال پوششی مبتنی بر تأخیر بین بستک‌ها پیشنهاد داده‌اند (لیو، ۲۰۱۰). ایشان نمودار ستونی تأخیر بین بستک‌ها را در هر تعداد مشخص بستک محاسبه کرده و کدبندی را به‌نحوی انجام داده‌اند که با ترافیک مجاز تطبیق کند.

احمدزاده در پایان‌نامه دکترای خود، استفاده از رفتار تصادفی پروتکل‌های ارتباطی و محیط‌های شبکه را به‌عنوان منابعی برای ایجاد کانال پوششی رفتاری (زمان‌بندی‌دار) مدنظر قرار داده است (احمدزاده، ۲۰۱۳). ایشان دو طرح برای ایجاد کانال پوششی در شبکه‌های بی‌سیم و شبکه اینترنت ارائه داده که هرکدام به‌طور مجزا از رفتارهای تصادفی ایستگاه‌های کاری شبکه و پروتکل‌های ارتباطی استفاده می‌کند. در شبکه بی‌سیم از رفتار تصادفی زمان‌سنج عقب‌نشینی[11] در پروتکل CSMA/CA استفاده کرده که میزان انتظار هر گره را قبل از تلاش برای دستیابی به کانال تعیین می‌کند. در شبکه اینترنت نیز از روش مدل‌محور برای کدبندی استفاده کرده است.

[1] Gianvecchio
[2] Exponential
[3] Weibull
[4] Independent and identically-distributed
[5] Correlated
[6] Sellke
[7] Sparse
[8] Sub-band
[9] Spreading
[10] Liu
[11] Backoff

(جدول- ۲) کارهای پژوهشی قبلی در حوزهٔ روش فاصله بین بستک‌ها را با همدیگر مقایسه کرده است. در این حوزه، برای افزایش نامحسوسی دو رویکرد اصلی کدبندی مدل‌محور و کم‌پشت ارائه شده است. در کارهای اشاره‌شده در این بخش، هرکدام تنها از یکی از روش‌های بازترتیب بستک‌ها یا فاصله بین بستک‌ها برای ایجاد کانال پوششی استفاده کرده و با تمرکز و پیشرفت نامحسوسی کانال، به‌طور معمول بخشی از ظرفیت را فدا کرده‌اند؛ ولی در این مقاله دو روش بازترتیب بستک‌ها و فاصله بین بستک‌ها ترکیب شده و ضمن حفظ نامحسوسی در حد قابل‌قبول، ظرفیت کانال نیز افزایش یافته است.

۳- طراحی روش کدبندی ترکیبی

در این مقاله با بهره‌گیری از کارهای مرتبط در حوزهٔ طراحی کانال‌های پوششی زمان‌بندی‌دار به روش‌های بازترتیب بستک‌ها و فاصله زمانی بین بستک‌ها و ایده‌گرفتن از روش‌های مدولاسیون مخابرات دیجیتال، تلاش شده ضمن بهبود ظرفیت و نامحسوسی روش‌های موجود، طرحی برای ترکیب این دو روش نیز پیشنهاد شود. در ادامه ابتدا به‌طور تفصیلی هر یک از دو روش بررسی شده و روش ترکیبی در انتها پیشنهاد می‌شود.

۳-۱- روش بازترتیب بستک‌ها

بازترتیب بستک‌ها در ترافیک شبکه عبارت است از اینکه بستک‌ها به ترتیبی غیر از آنچه در مبدأ ارسال شده‌اند، در مقصد دریافت شوند. مطالعات پژوهش‌گران (بنت[1]، ۱۹۹۹) نشان می‌دهد که حدود ۹۰٪ از نشست‌ها[2] درعمل به پدیدهٔ بازترتیب بستک‌ها دچار می‌شوند که باعث ایجاد اشکال و خطا به میزان ۰٫۱٪ تا ۳٪ می‌شود. با این وجود، مطالعات بیشتر که درهمین اواخر صورت گرفته (پیراتلا[3]، ۲۰۰۷) نشان می‌دهد که دلایل وقوع بازترتیب بستک‌ها شامل موارد زیر است:

۱) سامانه‌های تعدیل‌کنندهٔ بار[4]
۲) لایهٔ دو و ارسال مجدد در TCP
۳) مسیرهای ارسال چندگانه در شبکه

تمام این عوامل در شبکه‌های دادهٔ مدرن امروزی همچنان وجود دارند. بنابراین، می‌توان ادعا کرد که این ویژگی گستردگی و فراوانی زیادی دارد و می‌توان به آن به‌عنوان یک رفتار عادی نگاه کرد. مسئله مهمی که برای ایجاد کانال پایدار و دارای ظرفیت مناسب وجود دارد، امکان کاربردی‌کردن بازترتیب بستک است. یکی از مشخصه‌های موردنیاز برای ایجاد کانال‌های پوششی، وجود الگوهای مناسب و مستعد و دارابودن مقدار اندکی نوفه و اختلال ذاتی در کانال برای پنهان‌کردن آن است. بازترتیب بستک‌ها در حد خوبی این ویژگی را دارد (پیراتلا، ۲۰۰۷).

(جدول- ۲): مقایسه پژوهش‌های قبلی در حوزهٔ روش فاصله بین بستک‌ها

ویژگی	مرجع	برک	شاه	جیان‌وچیو	سلکه	لی‌یو	والز	زندر	احمدزاده
پروتکل کانال آشکار	TCP		✓	✓	✓		✓		✓
	UDP	✓				✓		✓	
	IP								✓
نوع کانال پوششی	فعال			✓	✓				✓
	غیرفعال	✓	✓			✓	✓	✓	
تمرکز تحقیق	ظرفیت	✓			✓				
	نامحسوسی	✓		✓	✓	✓	✓	✓	✓
	استحکام					✓			
معیار مورد ارزیابی	ظرفیت			✓	✓			✓	✓
	نامحسوسی	✓	✓	✓		✓	✓	✓	✓
	استحکام		✓	✓	✓	✓		✓	✓
روش ارزیابی	محاسباتی			✓	✓	✓		✓	
	اندازه‌گیری عملی	✓	✓	✓	✓	✓	✓	✓	✓
	شبیه‌سازی								✓
نوع آزمون نامحسوسی	شکل			✓		✓			✓
	قاعده‌مندی		✓	✓		✓			✓
	آنتروپی و آنتروپی شرطی						✓		
	خود-همبستگی							✓	
	الگوریتم آریموتو-بلاهوت	✓							

[1] Bennett
[2] Sessions
[3] Piratla
[4] Load balancers

در پـژوهش‌هـای فـراوان قبلـی در حـوزه بازترتیـب بستک‌هـا، کـارایی بـه‌عنـوان معیـار اصـلی مـورد بررسـی و اندازه‌گیـری قـرار گرفتـه اسـت. در مرجـع (پیـراتلا، ۲۰۰۷) درخصوص معیارهای بازترتیب بررسـی‌هـایی صـورت گرفتـه است. چگالی بازترتیب[1] (RD) و چگالی اشغال بافر بازترتیب[2] (RBD) عمده‌ترین معیـار کـاربردی و مـورد اسـتفاده اسـت. چگالی بازترتیب یـا عمـق بازترتیـب بـه ایـن معناسـت کـه بستک‌های دریافتی چقدر از محل مورد انتظار فاصله دارند یا گستره‌ای که بستک می‌تواند در آن جابـه‌جـا شـود. چگـالی اشغال بافر بازترتیب یا حجم بازترتیب به ایـن معناسـت کـه برای بازترتیب بستک‌ها چه مقـدار بـافر مـورد نیـاز اسـت و نشان‌دهنده درصد بستک‌هایی اسـت کـه نامرتـب شـده‌انـد. براسـاس (پیـراتلا، ۲۰۰۷) چگـالی بازترتیـب یـک معیـار قابل‌قبول برای سنجش میزان بازترتیب بستک‌هـا بـه‌منظـور ایجاد کانال پوششی است.

کدبندی به روش بازترتیب بسـتک‌هـا شـامل چهـار مرحلـه اساسی است:

۱- انتخاب کلمه‌کد

۲- افزایش اسـتحکام کانـال در برابـر خطـا بـا انتخـاب کلمه‌کد مناسب از روش‌های کدبنـدی تشـخیص یـا تصحیح خطا

۳- افزایش نامحسوسی با روش‌های احتمالاتی

۴- افزایش نامحسوسی با تنظیم احتمـالات کلمـه‌کـدها (العطایی، ۲۰۰۹).

در روش بازترتیب بستک‌ها، پارامترهای (جدول- ۳) تعریـف می‌شود.

(جدول- ۳): پارامترهای استفاده‌شده در روابط ریاضی روش بازترتیب بستک‌ها

N	تعداد بستک‌های ارسالی در کانال آشکار در واحد زمان
k	تعداد بستک‌هایی که نمایش‌گر یک کلمه‌کد هستند
N/k	تعداد نمادهای ارسالی در کانال پوششی در واحد زمان
L	مجموعه کلمه‌کدهای معتبر (مجموعه انتخاب‌شده از کل k! جایگشت ممکن برای k بستک)
ℓ	تعداد کلمه‌کدها درمجموعه L به‌عبارت‌دیگر $\ell = \|L\|$
p_L	توزیع احتمال کلمه‌کدها
$H(p_L)$	بیت‌های نمایش داده‌شده توسط هر کلمه‌کد

وقتی ارسال به‌روش بازترتیب k بستک انجام می‌شود، بیشینه k! کلمه‌کد (جایگشت) خواهیم داشـت. هنگـامی‌کـه تمامی k! کلمه‌کد برای کدبندی استفاده شود، به حد بالایی محتوای اطلاعاتی (تعـداد بیـت) کلمـه‌کـد یعنـی $\log_2(k!)$ دست می‌یابیم؛ بنابراین ظرفیت کانال عبارت است از:

$$C = \frac{N}{k} \cdot log_2 k! \quad \text{بیت بر ثانیه} \qquad (۱)$$

این عبارت زمانی صادق است که همه کلمـه‌کـدها بـا توزیع یکنواخت استفاده شوند؛ ولی به‌طور معمـول داده‌هـای واقعی منبـع بـه‌نحـوی اسـت کـه کلمـه‌کـدها دارای توزیـع غیریکنواخت هستند؛ در این صورت میانگین اطلاعات بر هـر کلمه‌کد براساس نظریه شانون به $H(p_L)$ تنـزل مـی‌یابـد. p_L توزیع احتمال L کلمه‌کد است کـه بـرای کدبنـدی انتخـاب شده است و H نیز تابع آنتروپی است. بهتـرین حالـت بـرای کانال پوششی، برقراری شرایط زیر است:

- کاهش اثرات نوفهٔ کانال و بـازترتیبی کـه توسـط خـود شبکه رخ می‌دهد.
- نامحسوسی بالا و عدم گمان هیچ‌کس بـه وجـود کانـال پوششی

اثر نوفه می‌تواند با ساخت کدهای بلـوکی بـزرگ‌تـر و جابه‌جایی عمیق‌تر محـدود شـود؛ در مقابـل، بـرای افـزایش نامحسوسی باید اندازه کد کوتاه‌تر و انتخاب کلمه‌کد مناسـب مد نظر باشد. با اندازهٔ کلمه‌کدهای کوتاه‌تر، طول بازترتیـب و عمق جابه‌جایی کاهش می‌یابد؛ زیرا به‌طور معمول بازترتیـب بلند و طـولانی (بـه‌عنـوان مثـال معکـوس‌شـدن ترتیـب ده بستک) در شبکه‌ها رخ نمی‌دهد. لذا به‌منظور برقراری هر دو شرط بالا، باید انتخاب کلمه‌کد به‌صورت هوشمندانه باشـد و بر اندازه بلوک کد نیز مصالحه شود.

محدودکردن اندازهٔ کلمه‌کد (k) بـه مقـادیر پـایین‌تـر (به‌عنوان مثال کمتر از پنج بستک) برای اغلب مـوارد کـافی اسـت و انتخـاب کلمـه‌کـد و توزیـع احتمـال آن (p_L) بایـد به‌نحوی انجام شـود کـه از رفتـار بازترتیـب طبیعـی شـبکه منحرف نشود.

۳-۲- روش فاصله زمانی بین بستک‌ها

در این روش از فاصلهٔ زمانی بین بسـتک‌هـا در کانـال مجـاز برای مدولاسیون اطلاعات پوششی اسـتفاده مـی‌شـود. یـک طرح کارا که توسط سلکه و همکارانش ارائـه شـده اسـت، L بیت رشته دودویـی را در دنبالـه‌ای از n فاصـله زمـانی بـین بستک به نام‌های $(T_1, T_2 \quad \cdots \quad , T_n)$ کدبندی می‌کنـد و آن

[1] Reorder Density
[2] Reorder Buffer-occupancy Density

را طرح L-بیت به n-بستک می‌نامد (سلکه، ۲۰۰۹). به‌عنوان مثال یک طرح سه‌بیت به دوبستک دارای جدول کلمه‌کد مطابق (جدول- ۴) است.

حال با فرض برابربودن احتمال رخداد هر کلمه‌کد، انتخاب L و n مناسب به‌نحوی‌که ظرفیت کانال حداکثر شود به شرح ادامه انجام شده است. اگر مجموع فاصلهٔ زمانی بین n بستک را t_n در نظر بگیریم به‌نحوی‌که $t_n = \sum_{i=1}^{n} T_i$ باید برای t_n ثابت، طولانی‌ترین رشته‌بیت ممکن را بیابیم. T_i از رابطهٔ (۲) به دست می‌آید:

$$T_i = \Delta + k_i \cdot \delta \qquad (۲)$$

(جدول- ۴): طرح کدبندی ۳-بیت به ۲-بستک

۳-بیت	۲-بستک (میلی‌ثانیه) T_1T_2
000	50 50
001	50 60
010	60 50
011	60 60
100	50 70
101	70 50
110	60 70
111	70 60

در رابطهٔ (۲)، Δ کمینه فاصلهٔ زمانی بین ارسال دو بستک متوالی است به‌نحوی‌که اطلاعات کدبندی زمانی، به‌دلیل تأخیرهای صف مسیریاب‌ها، از بین نرود (یعنی $T_i \geq \Delta$). δ حداقل اختلاف‌زمانی بین دو کلمه‌کد متفاوت است به‌نحوی‌که در اثر لغزش زمانی بین فرستنده و گیرنده، تداخلی بین آنها به وجود نیامده و دو کلمه‌کد در گیرنده قابل تمایز باشند. اگر ε را متغیر تصادفی نشان‌دهندهٔ لغزش زمانی کانال بدانیم، به‌طوری‌که $-\epsilon_{max} < \epsilon < \epsilon_{max}$ نشان داده‌شده که باید $\delta > 4\ \epsilon_{max}$ باشد. k_i نیز عناصر بردار $(k_1, k_2, \cdots, k_n)$ را تشکیل می‌دهند.

اگر رابطهٔ T_i را در رابطهٔ t_n جای‌گذاری نماییم، داریم:

$$t_n = \sum_{i=1}^{n} T_i = \sum_{i=1}^{n} (\Delta + k_i \cdot \delta) = n \cdot \Delta + (\sum_{i=1}^{n} k_i) \cdot \delta \qquad (۳)$$

کمینه‌شدن t_n مستلزم کمینه‌شدن $\sum_{i=1}^{n} k_i$ است. پس مقدار K را در نظر می‌گیریم به‌نحوی‌که:

$$\sum_{i=1}^{n} k_i \leq K \qquad (۴)$$

می‌توان نشان داد که بیشینه تعداد کلمه‌کدهای قابل‌دستیابی در این روش کدبندی برابر است با ترکیب $\binom{n+K}{K}$. بنابراین حداکثر طول رشته‌بیت که می‌تواند در این کدبندی نگاشت شود، برابر است با:

$$L = \left\lfloor log_2 \binom{n+K}{K} \right\rfloor \qquad (۵)$$

نرخ داده R(n, K) در روش کدبندی (n, K) با پارامترهای (Δ, δ) تقریباً برابر است با:

$$R(n,K) = \frac{\text{تعداد بیت‌های کلمه‌کد}}{\text{میانگین زمان } \boldsymbol{\ell}_n \text{ برای همه کلمه‌کدها}} \cong \frac{log_2\binom{n+K}{K}}{n \cdot \Delta + \frac{n}{n+1} K \cdot \delta} \qquad (۶)$$

اگر منحنی نرخ R برای پارامترهای مشخص (Δ, δ) و تعداد بستک n مشخص ترسیم شود، K برای نرخ بیشینه R به دست می‌آید و از K نرخ بیشینه، می‌توان به L تعداد بیت کلمه‌کد رسید. تا اینجا برای بیشینه‌کردن ظرفیت کانال، n و L مناسب محاسبه و انتخاب شدند؛ ولی کانال طراحی‌شده با روش‌های آمارهای مرتبه نخست قابل تشخیص است.

در اینجا سلکه روش خود را با روش مدل‌محور جیان‌وچیو ترکیب کرده (جیان‌وچیو، ۲۰۰۸) و ادعا کرده که یک کانال غیرقابل تمایز از کانال مجاز ایجاد کرده است. ترکیب دو روش بدین‌صورت انجام شده که هر فاصله زمانی T_i با یک عدد تصادفی یکنواخت بین [0, 1] جمع شده و عدد اعشاری r_i تولید می‌شود؛ سپس توسط رابطه $\tau_i = F^{-1}(r_i)$ مقدار τ_i به‌دست‌آمده و در ارسال بستک‌ها به‌عنوان فاصله زمانی بین بستک‌ها استفاده می‌شود. F(x) نیز تابع توزیع تجمعی ترافیک مجاز است که از تطبیق ترافیک مجاز با مدل‌های آماری شناخته‌شده به دست می‌آید. بدین ترتیب چون فاصلهٔ زمانی بین بستک‌ها، به‌صورت شبه‌تصادفی و بر اساس مدلی منطبق بر ترافیک مجاز تولید می‌شود، توزیع آنها به ترافیک مجاز بسیار شبیه می‌شود.

زندر در ادامه کار سلکه، مدل بهبودیافته‌ای را برای حفظ همبستگی فاصلهٔ زمانی بین بستک‌ها ارائه داده است(زندر، ۲۰۱۰). ایشان با ارائهٔ دو روش کدبندی کم‌پشت و کدبندی زیرباند، میزان پنهان‌بودن و نامحسوسی کانال را با قربانی‌کردن ظرفیت کانال بهبود دادند. در روش کدبندی کم‌پشت، به‌جای استفاده از تمام فاصلهٔ زمانی بین بستک‌ها(IPG) برای کدبندی، بخشی از آن (f) را مورد استفاده قرار می‌دهند. اندازهٔ f تعیین‌کنندهٔ توازن بین نامحسوسی و ظرفیت کانال است. در روش کدبندی زیرباند، یک توزیع IPG را که شامل بازه‌ای (بیشینه منهای کمینه) است را به زیرباندهایی به‌اندازهٔ $\boldsymbol{\ell}$ تقسیم کرده و کدبندی روی یکی از زیرباندها انجام می‌دهد. $\boldsymbol{\ell}$ اندازه بخش کم‌ارزش[1] IPGs برحسب میکرو یا میلی‌ثانیه است و انتخاب پارامتر $\boldsymbol{\ell}$ تعیین‌کنندهٔ میزان نامحسوسی و استحکام کانال خواهد بود.

1 Least signifcant part

۳-۳- طرح کدبندی ترکیبی پیشنهادی

در طراحی کانال‌های زمان‌بندی‌دار پوششی، طراح با دو مسئله بیشینه‌کردن ظرفیت کانال و بیشینه‌کردن نامحسوسی مواجه است که این دو مسئله به‌نوعی با هم تعارض داشته و باید بر یک ظرفیت و نامحسوسی متعادل و قابل قبول توافق کرد. در این مقاله روش کدبندی هندسی که برای افزایش ظرفیت کانال توسط سلکه مورد استفاده قرارگرفته است (سلکه، ۲۰۰۹)، مبنا قرار داده شده و علاوه‌بر کدبندی فاصلهٔ زمانی بین بستک‌ها، هم‌زمان از ترتیب بستک‌ها نیز در کدبندی استفاده شده و روش کدبندی ترکیبی ارائه شده است. برای افزایش نامحسوسی کانال نیز با ایده‌گرفتن از روش کم‌پشت زندر تمامی بستک‌ها کدبندی نمی‌شوند (زندر، ۲۰۱۰) و با ایده‌گرفتن از روش مدولاسیون پرش فرکانسی[1] معین می‌شود که در یک قطعه از بستک‌ها، کدام بستک‌ها برای کدبندی استفاده شوند و کدام برای کدبندی استفاده نشوند.

۳-۳-۱-افزایش ظرفیت با ترکیب روش‌های بازترتیب بستک‌ها و فاصلهٔ زمانی بین بستک‌ها

ابتدا با بهره‌گیری از مباحث مطرح‌شده در بخش ۳-۲ این مقاله، طرح کدبندی با استفاده از فاصلهٔ زمانی بین بستک‌ها با L و n مناسب برای بیشینه‌شدن ظرفیت را انتخاب می‌کنیم. به‌عنوان مثال طرح سه‌بیت به دوبستک (جدول-۴) را انتخاب می‌کنیم. حال روی دو بستک انتخاب‌شده در جدول کلمه‌کد، کدبندی بازترتیب بستک‌ها را نیز اِعمال می‌کنیم. وقتی فقط n=2 بستک برای کدبندی داریم، فقط n!=2!=2 ترتیب مختلف برای بستک‌ها داریم؛ پس (جدول-۴) می‌تواند دو بار تکرار شود. یک‌بار برای دو بستک مرتب و بار دیگر نیز برای دو بستک نامرتب. درنتیجه مجموع کلمه‌کدها دو برابر می‌شود و بدین ترتیب می‌توان سه بیت داده را به چهار بیت افزایش داد (جدول-۵). شمارهٔ بالای [] نشان‌دهندهٔ شمارهٔ ترتیب بستک است. این در حالی است که فاصلهٔ زمانی بین بستک‌ها به همان ترتیب قبل برای هر دونیمه جدول کلمه‌کد ثابت است. بنابراین با توجه به ثابت‌ماندن میانگین زمان n بستک (t_n) برای همه کلمه‌کدها، ظرفیت کانال به $4/3$ افزایش می‌یابد. نکته قابل‌توجه دیگر اینکه، اگر به‌صورت کدبندی ساده از رابطهٔ (۲) برای تولید هر شانزده کلمه‌کد استفاده می‌شد، بزرگ‌ترین فاصلهٔ بین بستک‌ها برابر نود میلی‌ثانیه می‌شد. ولی به‌دلیل تکرار دونیمه جدول (۵)، درعمل بزرگ‌ترین فاصله بین بستک‌ها برابر هفتاد میلی‌ثانیه شده است که این امر به نامحسوسی کانال پوششی نیز کمک زیادی می‌نماید.

در حالت کلی، برای n بستک، می‌تواند n! جایگشت وجود داشته باشد. اگر تمامی n! جایگشت بستک‌ها برای کدبندی استفاده شود، به حد بالای $log_2(n!)$ کلمه‌کد دست می‌یابیم؛ ولی چون تعداد کلمه‌کدها باید نمایی از دو باشد به تعداد $b = \lfloor log_2(n!) \rfloor$ بیت محدود می‌شویم. درنتیجه تعداد L بیت داده‌ها به L+b افزایش می‌یابد؛ بنابراین میزان افزایش ظرفیت در روش کدبندی ترکیبی نسبت به روش کدبندی فاصله بین بستک‌ها از رابطهٔ (۷) به‌دست می‌آید.

$$\text{نسبت افزایش ظرفیت روش ترکیبی} = \frac{L+b}{L} \qquad (۷)$$

(جدول- ۵): ترکیب روش‌های بازترتیب بستک‌ها و فاصلهٔ زمانی بین بستک‌ها

۴-بیت	۲-بستک مرتب $T_1^{sn2}\ T_2^{sn1}$	۴-بیت	۲-بستک نامرتب $T_1^{sn1}\ T_2^{sn2}$
0000	$[50]^2\ [50]^1$	1000	$[50]^1\ [50]^2$
0001	$[50]^2\ [60]^1$	1001	$[50]^1\ [60]^2$
0010	$[60]^2\ [50]^1$	1010	$[60]^1\ [50]^2$
0011	$[60]^2\ [60]^1$	1011	$[60]^1\ [60]^2$
0100	$[50]^2\ [70]^1$	1100	$[50]^1\ [70]^2$
0101	$[70]^2\ [50]^1$	1101	$[70]^1\ [50]^2$
0110	$[60]^2\ [70]^1$	1110	$[60]^1\ [70]^2$
0111	$[70]^2\ [60]^1$	1111	$[70]^1\ [60]^2$

در حالت عمومی، ظرفیت این کانال ترکیبی از رابطه (۸) به دست می‌آید:

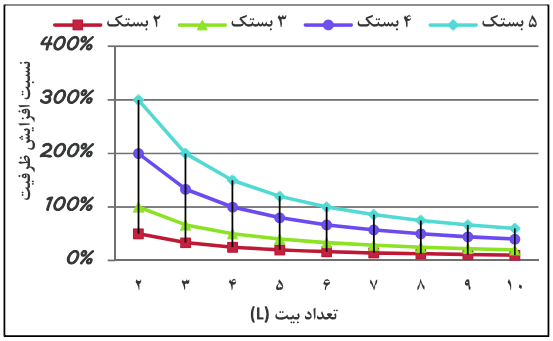
$$R = \frac{\text{تعداد بیت‌های کلمه‌کد}}{\text{میانگین زمان } \boldsymbol{t_n} \text{ برای همه کلمه‌کدها}} = \frac{L+b}{n\cdot\Delta+\frac{n}{n+1}K\cdot\delta} \qquad (۸)$$

(شکل- ۳) نسبت افزایش ظرفیت کانال را در روش ترکیبی نمایش می‌دهد. مشاهده می‌شود که هرچه تعداد بستک‌ها (n) در کدبندی بیشتر باشد، منحنی بالاتر قرار می‌گیرد؛ یعنی ظرفیت افزایش می‌یابد. از سوی دیگر برای تعداد بیت(L) کمتر در کدبندی، نسبت افزایش ظرفیت بیشتر خواهد شد. در شرایط واقعی به‌منظور پیش‌گیری از بازترتیب غیرعادی در ترافیک شبکه، انتخاب اعدادی بین ۳ تا ۵ برای تعداد بستک‌ها در جدول کلمه‌کد، مناسب به نظر می‌رسد و عمق بازترتیب به بیشینه پنج بستک محدود

1 Frequency Hopping Modulation

می‌شود. لذا همان‌طور که در شکل (۳) مشاهده می‌شود، برای تعداد بستک بین سه تا پنج در جدول کدبندی، ظرفیت از ۱۰٪ تا ۳۰۰٪ می‌تواند افزایش یابد.

شکل (۴) مراحل تشکیل جدول کلمه‌کد ترکیبی را که در این بخش تشریح شده است، را به‌صورت نمودار ترتیب اقدامات نشان می‌دهد.



(شکل- ۳): نسبت افزایش ظرفیت در روش ترکیبی در مقایسه با روش فاصلهٔ بین بستک‌ها- رابطهٔ (۷)

۳-۳-۲- افزایش نامحسوسی روش ترکیبی

در این پژوهش برای ارتقای نامحسوسی کانال پوششی، از روش کم‌پشت استفاده می‌شود. بدین معنی که از همه بستک‌های ارسالی برای کدبندی کانال استفاده نمی‌شود، از این‌جهت کدبندی در بین بستک‌های ارسالی، کم‌پشت است. در این پژوهش با ایده‌گرفتن از روش «مدولاسیون پرش فرکانسی» مشخص می‌کنیم که کدام بستک‌ها برای کدبندی انتخاب شوند. اگر مثال سه‌بیت به دو بستک جدول (۴) را در نظر بگیریم، بستک‌ها در قطعه‌های دوتایی کدبندی می‌شوند. در اینجا برای افزایش نامحسوسی، تعداد بستک‌های هر قطعه را به پنج بستک افزایش می‌دهیم که فقط دو بستک از آن کدبندی می‌شوند. برای هر بستک دو حالت کدبندی‌شده (C) و کدبندی نشده (U) در نظر می‌گیریم. پس برای یک قطعه دارای پنج بستک، تعداد 2^5 حالت متفاوت وجود دارد. از بین ۳۲ حالت ممکن، حالاتی که دارای دو بستک کدبندی‌شده (C) هستند را انتخاب می‌کنیم. چون بازترتیب هم روی این کدها اعمال می‌شود، به‌منظور اینکه عمق بازترتیب زیاد نشود، حالاتی را که فاصلهٔ بستک‌های کدبندی‌شده بیش از دو بستک می‌شود، را نیز حذف می‌کنیم (مثل حالت CUUUC). بدین ترتیب جمعاً ۹ حالت متفاوت به‌شرح جدول (۶) به‌دست می‌آید.

به‌منظور این‌که بستک‌های کدبندی‌شده دارای توزیع مستقل و یکسان (iid) باشد، انتخاب هر یک از این ۹ حالت به‌صورت تصادفی با استفاده از یک تابع توزیع یکنواخت با مقدار اولیه[1] مشخص انجام می‌شود. فرستنده و گیرنده باید قبل از برقراری ارتباط روی این مقدار اولیه تابع توزیع یکنواخت توافق نمایند تا امکان یافتن بستک‌های کدبندی‌شده از بین بستک‌های کدبندی نشدهٔ وجود داشته باشد. بدین ترتیب نامحسوسی با ضریب $5/2$ افزایش می‌یابد. از سوی دیگر میانگین زمان ارسال کلمه‌کدها تغییری نمی‌کند و ظرفیت کانال ازنظر تعداد بیت بر ثانیه کاهش نمی‌یابد. این روش را که فاصله بین بستک‌ها (IPG) با ایده گرفتن از مدولاسیون پرش فرکانسی، به‌صورت کم‌پشت کدبندی انجام می‌شود، می‌توان روش کدبندی «پرش کد» نام‌گذاری کرد.

اگر بخواهیم روش پرش کد بالا را روی روش کدبندی ترکیبی ارائه‌شده در بخش ۳-۳-۱ این مقاله اِعمال کنیم، درواقع باید ستون‌های ۲ و ۴ جدول (۵) در قطعه‌های پنج‌تایی، با استفاده از ۹ حالت جدول (۶) کدبندی شوند. چون در جدول (۵) بازترتیب بستک‌ها نیز انجام شده است، می‌توان برای انتخاب هر یک از ۹ حالت جدول (۶)، به‌جای استفاده از تابع توزیع یکنواخت، از روشی که در بخش ۳-۱ این مقاله آورده شده، استفاده کرد. یعنی هر یک از ۹ حالت جدول (۶) به نحوی انتخاب می‌شوند که احتمال رخداد هریک از کلمه‌کدهای جدول (۵) در رفتار نهایی کانال پوششی، از رفتار عادی کانال انحراف قابل‌توجهی پیدا نکند. با توجه به اینکه از نظر نامحسوسی، بهتر است بازترتیب بیشتر در بستک‌های مجاور و نزدیک اتفاق بیفتد، چهار حالت اول جدول (۶) که در آنها بستک‌های مجاور کدبندی می‌شوند را به کلمه‌کدهای ستون ۴، جدول (۵) که در آن‌ها بازترتیب وجود دارد اختصاص می‌دهیم و پنج حالت آخر جدول (۶) را به ستون۲ جدول (۵) که در آنها بازترتیب انجام نمی‌شود، اختصاص می‌دهیم. این روش را «کدبندی پرش کد ترکیبی» نام‌گذاری می‌نماییم. بدین معنی که کد ترکیبی «فاصلهٔ بستک‌ها» و «بازترتیب بستک‌ها» به‌صورت کم‌پشت روی بخشی از بستک‌ها انجام می‌شود و علاوه بر این، مکان کد ترکیبی نیز در هر قطعه از بستک‌ها به‌صورت پرشی تغییر می‌یابد. در پیاده‌سازی طرح پیشنهادی، به این نکته باید توجه شود که اگر کانال به‌صورت غیرفعال

[1] Seed

پیاده‌سازی شود، بستک‌هایی که در قطعهٔ ۵تایی کدبندی نمی‌شوند (U)، همان مشخصات فاصله بستک‌های کانال آشکار را خواهند داشت؛ ولی در پیاده‌سازی کانال فعال، برای تنظیم فاصلهٔ بستک‌هایی که کدبندی نمی‌شوند (U)، باید از یک تابع توزیع متناسب با کانالی که می‌خواهیم تقلید کنیم استفاده نماییم.

(جدول- ۶): کدبندی ۲ بستک از قطعه ۵ بستکی

قطعه ۵ بستکی
CCUUU
UCCUU
UUCCU
UUUCC
CUCUU
UCUCU
UUCUC
CUUCU
UCUUC

(شکل- ۴): مراحل تشکیل جدول کلمه‌کد ترکیبی

در حالت کلی تعداد B بستک برای هر قطعه در نظر می‌گیریم که فقط n بستک از آنها برای کدبندی استفاده می‌شود؛ لذا با استفاده از رابطهٔ (۸) ظرفیت کانال کم‌پشت از رابطهٔ زیر به‌دست می‌آید:

$$R = \frac{L+b}{n\cdot\Delta+\frac{n}{n+1}\cdot K\cdot\delta+(B-n).m} \qquad (۹)$$

که متغیر m میانگین تابع توزیع تصادفی است که برای تولید ترافیک سالم استفاده می‌شود.

۴-ارزیابی عملی کدبندی ترکیبی

در این بخش از مقاله، کدبندی ترکیبی پیشنهادی به‌صورت عملی پیاده‌سازی و ارزیابی می‌شود.

۴-۱- شرایط انجام آزمایش‌ها

برای جمع‌آوری داده‌های کانال پوششی، یک کانال مبتنی بر پروتکل HTTP ایجاد می‌شود تا سامانه‌های امنیتی شبکه در دو طرف کانال به‌راحتی اجازه عبور ترافیک آن را بدهند. این کانال به‌صورت فعال و در لایه سوم شبکه (IP) بین یک رایانه در محل آزمایشگاه شبکه دانشگاه، به‌عنوان فرستنده و یک سرور اجاره‌ای در کشور آلمان به‌عنوان گیرنده، پیاده‌سازی می‌شود. برای پیاده‌سازی کانال پوششی زمان‌بندی‌دار مقادیر T_i مختلف در رابطه (۲) طبق (جدول-۷) تولید شده و برای هر آزمون ۱۲۰۰۰ بستک HTTP به‌عنوان داده‌های کانال پوششی جمع‌آوری شده است.

(جدول- ۷): مقادیر مختلف T_i در آزمون‌ها

شماره آزمون	۱	۲	۳	۴	۵	۶	۷	۸
Δ	۱۰	۲۰	۳۰	۴۰	۱۰	۲۰	۳۰	۴۰
δ	۵	۵	۵	۵	۱۰	۱۰	۱۰	۱۰

۴-۲- ارزیابی نامحسوسی کد ترکیبی

برای ارزیابی میزان نامحسوسی کانال پیشنهادی، براساس مرجع (جیان‌وچیو، ۲۰۱۰) از دو روش آنتروپی و آنتروپی شرطی اصلاح‌شده استفاده شده است. یک فرآیند تصادفی $X = \{X_i\}$ به‌صورت یک دنباله‌ای از متغیرهای تصادفی تعریف می‌شود. آنتروپی یک دنباله از متغیرهای تصادفی به‌صورت رابطهٔ (۱۰) تعریف می‌شود:

$$H(x_1,\dots,x_m) = -\sum_{x_1,\dots,x_m} P(x_1,\dots,x_m)\log P(x_1,\dots,x_m) \qquad (۱۰)$$

که در آن $P(x_1, \dots, x_m)$ احتمال توأم $P(X_1 = x_1, \dots, X_m = x_m)$ است.

نرخ آنتروپی که میانگین آنتروپی به‌ازای متغیرهای تصادفی است، می‌تواند به‌عنوان یک معیار پیچیدگی یا قاعده‌مندی استفاده شود (جیان‌وچیو، ۲۰۱۰). نرخ آنتروپی به‌صورت آنتروپی شرطی دنباله‌ای با طول نامتناهی تعریف می‌شود. یک فرآیند ساده با توزیع مستقل و یکسان (i.i.d) نرخ آنتروپی برابر با آنتروپی مرتبه نخست دارد. یک فرآیند بسیار پیچیده نرخ آنتروپی بالایی دارد، اما کمتر از آنتروپی مرتبه نخست است. یک فرآیند بسیار منظم نرخ آنتروپی پایینی دارد و برای یک فرایند دوره‌ای محض، یعنی یک الگوی تکرارشونده، نرخ آنتروپی صفر است.

نرخ آنتروپی همان آنتروپی شرطی یک دنباله با طول نامتناهی است؛ لذا نمی‌تواند برای نمونه‌های متناهی اندازه‌گیری و بایستی تخمین زده شود. به‌منظور حل مشکل داده‌های متناهی، از آنتروپی شرطی اصلاح‌شده استفاده می‌شود. آنتروپی شرطی اصلاح‌شده به‌صورت رابطه (۱۱) تعریف می‌شود:

$$CCE(x_m|\, x_1, \dots, x_{m-1}) = CE(x_m|\, x_1, \dots, x_{m-1}) + perc(x_m).EN(x_1) \quad (11)$$

که در آن $perc(x_m)$ درصدی از الگوهای یکتا با طول m است و $EN(x_1)$ آنتروپی که m در آن یک است، یعنی تنها آنتروپی مرتبهٔ نخست است.

برای تشخیص وجود کانال پوششی، آزمون‌ها روی نمونه‌های ترافیک پوششی و سالم اجرا می‌شود. از نمرات به‌دست‌آمده آزمون، برای تعیین اینکه آیا یک نمونه، پوششی یا سالم است استفاده می‌کنیم. در ابتدا، نرخ خطای اشتباهی مثبت[1] هدف را با مقدار ۱٪ مقداردهی کرده و برای رسیدن به این نرخ خطای اشتباهی مثبت، نمرات شاخص تعیین می‌شود. نرخ خطای اشتباهی مثبت با توجه به میزان نوفهٔ کانال، می‌تواند تا ۱۰٪ نیز هدف‌گذاری شود. نمرهٔ شاخص نمره‌ای است که تعیین می‌کند آیا یک نمونه پوششی یا سالم است و به‌صورت ۱ امین و ۹۹ امین صدک[2] یعنی کمترین و بیشترین نمرات در آزمون‌های مختلف روی نمونه‌های سالم در مجموعه‌ی آموزشی HTTP به دست می‌آید.

مجموعه داده‌های کانال سالم از ثبت بستک‌های دریافت شده از ارتباط HTTP با اینترنت و گشت‌وگذار کاربران متعدد در سایت‌های مختلف اینترنتی جمع‌آوری شده است. در آزمون‌ها، ما از زیرمجموعه‌های مختلفی از دو دادگان شامل موارد زیر استفاده می‌کنیم:

- مجموعه آموزشیHTTP : ۱۷۶۰۰۰ بستک HTTP
- مجموعه آزمون HTTP (داده‌های کانال مجاز): ۱۷۶۰۰۰ بستک HTTP

میانگین و انحراف معیار نتایج آزمون‌های مختلف تشخیص بر روی ۸۸ نمونه ۲۰۰۰ تایی از تأخیرهای بین بستک ترافیک سالم HTTP در جدول (۸) آمده است که در ادامه از این نتایج برای استخراج نمرات شاخص استفاده می‌شود. نمرات شاخص برای آزمون‌های آنتروپی اصلاح‌شده و آنتروپی شرطی اصلاح‌شده با استفاده از رابطهٔ صدک محاسبه و در جدول (۹) نشان داده‌شده است. هر نمونه با مقدار آنتروپی اصلاح‌شده بیشتر یا مساوی نمره شاخص CEN، به‌عنوان کانال سالم در نظر گرفته خواهد شد. برعکس، نمرات هر نمونه با آنتروپی شرطی اصلاح‌شده کوچک‌تر یا مساوی با نمرات شاخص CCE باشد به‌عنوان کانال سالم در نظر گرفته خواهد شد.

(جدول- ۸): نمرات آزمون بر روی ترافیک سالم HTTP

نوع آزمون	میانگین	انحراف معیار
آنتروپی اصلاح‌شده (CEN)	17.42	1.66
آنتروپی شرطی اصلاح‌شده(CCE)	1.65	0.20

(جدول- ۹): نمرات شاخص آزمون‌های تشخیص سلامت ترافیک HTTP

نوع آزمون	نمرات شاخص	نرخ خطای اشتباهی مثبت
آنتروپی اصلاح‌شده (CEN)	$\geq$ 13.27	1%
	$\geq$ 14.80	10%
آنتروپی شرطی اصلاح‌شده(CCE)	$\leq$ 1.92	1%
	$\leq$ 1.50	10%

نتایج آزمایش‌های انجام‌شده با استفاده از مقادیر T_i (جدول- ۷) در (جدول- ۱۰) آمده است. هر آزمایش روی ۲۰۰۰ بستک نمونه انجام شده است؛ لذا برای هر T_i تعداد

[1] False Positive Error Rate
[2] Percentile

شش مرتبه آزمایش انجام شده و در (جدول- ۱۰) مقادیر میانگین و انحراف معیار این آزمایش‌ها آمده است.

اگر مقادیر نتایج آزمایش آنتروپی بیش از مقدار شاخص باشد، به معنای دارابودن آنتروپی بالا و عدم قاعده‌مندی ترافیک مورد آزمایش و پوششی‌نبودن ترافیک است. اگر مقادیر نتایج آزمایش آنتروپی شرطی اصلاح‌شده کمتر از مقدار شاخص باشد به معنی پوششی‌نبودن ترافیک است.

نتایج آزمون‌های عملی نشان می‌دهد که کانال ترکیبی پیشنهادی، به‌جز برای مقدار $\Delta=10$ نامحسوسی قابل قبولی دارد. این استثنا به‌دلیل انجام آزمایش‌ها در محیط واقعی اینترنت است که فاصله بین فرستنده و گیرنده دارای تعداد گام[1] بالایی است. فاصله زیاد فرستنده و گیرنده سبب می‌شود که کانال به‌طور میانگین دارای مقادیر IPD بزرگ باشد؛ لذا انتخاب مقادیر کوچک برای Δ نامحسوسی کانال را کاهش می‌دهد. این نتایج حتی برای شرایطی که نرخ خطای اشتباهی مثبت، برابر ۱۰٪ در نظر گرفته شود نیز معتبر است.

(جدول- ۱۰): نتایج آزمایش عملی

آزمون آنتروپی شرطی		آزمون آنتروپی		نام آزمون	
$X \leq 1.92$		$X \geq 13.27$		شرط سلامت	
انحراف معیار	میانگین	انحراف معیار	میانگین	Δ	δ
0.018	0.587	0.42	13.83	10	10
0.024	0.593	1.05	15.14	20	10
0.054	0.616	1.56	16.13	30	10
0.032	0.596	1.47	16.02	40	10
0.029	0.573	0.39	13.18	10	5
0.025	0.585	0.64	14.47	20	5
0.035	0.586	0.68	15.03	30	5
0.019	0.589	0.87	15.65	40	5

برای مقایسه نتایج با کارهای پژوهشی پیشین، از نتایج ارزیابی عملی نامحسوسی کانال غیرقابل تشخیص سلکه که توسط بیرامی انجام شده استفاده می‌شود (بیرامی، ۱۳۹۳). (جدول- ۱۱) مقایسه نتایج ارزیابی نامحسوسی کانال ترکیبی با کانال ساده چهار-بیت به دو-بستک و کانال غیرقابل تشخیص سلکه را نشان می‌دهد (سلکه، ۲۰۰۹).

برای کانال چهار-بیت به دو-بستک، در آزمون آنتروپی، نمرات حاصل کمتر از نمرات آستانه و نشان‌دهنده پوششی‌بودن ترافیک است و در آزمون آنتروپی شرطی نیز میانگین نمرات خیلی نزدیک به صفر بوده و قاعده‌مند بودن ترافیک را نشان می‌دهد و بیان‌گر پوششی‌بودن ترافیک است. نتایج آزمون‌های تشخیص بر روی کانال غیرقابل تشخیص سلکه نشان می‌دهد که هیچ‌یک از آزمون‌های تشخیص قادر به شناسایی این کانال نبوده، به‌طوری‌که در آزمون آنتروپی، نتایج به‌دست‌آمده بزرگ‌تر از نمرات آستانه بوده و در آزمون آنتروپی شرطی، نتایج به‌دست‌آمده کوچک‌تر از مقادیر آستانه است که بیان‌گر عدم پوششی‌بودن ترافیک است. بنابراین توزیع این کانال از توزیع ترافیک سالم پیروی کرده و نامحسوسی بالایی دارد. مقایسه نتایج ارزیابی نامحسوسی نشان می‌دهد که کانال ترکیبی از نظر آزمون آنتروپی که یک آزمون شکل محسوب می‌شود، نسبت به کانال غیرقابل تشخیص سلکه شباهت شکلی کمتری به ترافیک سالم دارد. از طرف دیگر با مقایسه نتایج آزمون آنتروپی شرطی، مشاهده می‌شود که کانال ترکیبی نسبت به کانال غیرقابل تشخیص سلکه قاعده‌مندی کمتری داشته و رفتار پوششی بهتری نشان می‌دهد. به‌طورکلی، نتایج مقایسه این دو کانال درواقع مقایسه دو روش مدل-محور و کم‌پشت را نشان می‌دهد.

(جدول- ۱۱): مقایسه نتایج ارزیابی نامحسوسی کانال ترکیبی باکارهای قبلی

آزمون آنتروپی شرطی		آزمون آنتروپی		نام آزمون
$X \leq 1.92$		$X \geq 13.27$		شرط سلامت
انحراف معیار	میانگین	انحراف معیار	میانگین	نوع کانال
0.0076	0.0098	0.285	11.04	کانال ۴-بیت به ۲-بستک
0.008	1.83	0.112	18.94	کانال غیرقابل تشخیص سلکه
0.295	0.591	0.885	14.93	کانال ترکیبی

[1] Hop

۴-۳- ارزیابی استحکام کدبندی ترکیبی

ارزیابی استحکام کانال پوششی در روش کدبندی ترکیبی با به‌دست‌آوردن نرخ خطای بیت انجام می‌شود. نرخ خطای بیت پایین‌تر به‌منزله استحکام بیشتر است. چون هنوز در مرحلهٔ پیاده‌سازی هیچ طرح کدبندی تصحیح خطا یا قاب‌بندی داده‌ها انجام نشده است، برای اندازه‌گیری نرخ خطا باید نرخ خطای خام را به دست آورد. نرخ خطای خام با استفاده از روش «فاصله لون اشتاین[1]» که «فاصله اصلاح[2]» نیز نامیده می‌شود اندازه‌گیری می‌گردد. فاصله اصلاح یک مقیاس برای اندازه‌گیری شباهت دو رشته است و مساوی تعداد درج، حذف و جانشینی مورد نیاز برای تبدیل رشته‌بیت مبدأ (بیت رسیده) به رشته‌بیت هدف (بیت ارسالی) است.

نتایج ارزیابی نرخ خطای روش کدبندی ترکیبی برای مقادیر مختلف Δ و δ در (جدول- ۱۲) نشان داده شده است.

(جدول- ۱۲): نرخ خطای بیت روش کدبندی ترکیبی (درصد)

Δ	δ			
	5	10	15	20
10	12.29	10.43	9.81	8.32
15	7.74	7.14	6.86	6.63
20	7.68	7.37	6.81	6.6
25	6.47	6.74	5.68	6.14
30	6.62	6.27	5.56	5.73
35	5.51	5.45	4.45	4.65
40	5.23	4.73	4.12	3.95
45	5.21	5.08	4.05	3.77
50	4.92	4.12	3.96	2.87
55	4.76	4.76	3.58	3.21

مقایسه نرخ خطای بیت با طرح‌های قبلی به‌سادگی امکان‌پذیر نیست؛ زیرا شرایط آزمایش از نظر محل فرستنده و گیرنده و تعداد گام‌ها و تأخیر زمانی بین آنها باید تاحدودی یکسان باشد تا بتوان نتایج را مقایسه کرد. مقدار قابل قبول نرخ خطای خام نیز به تغییرات عواملی چون سازوکار قاب‌بندی و توانمندی کد تصحیح خطای مورد استفاده و کاربرد بستگی دارد. نتایج ارزیابی نشان می‌دهد که با انتخاب مقادیر مناسب پارامترهای کدبندی، نرخ خطا قابل کنترل است.

[1] Levenshtein distance
[2] Edit distance

۴-۴- ارزیابی هزینه پردازشی کدبندی ترکیبی

مبحث دیگری که در این بخش مطرح است، هزینهٔ پردازشی طرح کدبندی ترکیبی در مقایسه با کیفیت پوشش حاصل از طرح است. در حوزه کانال‌های پوششی به‌دلیل اینکه طرح کدبندی در مقایسه با الگوریتم‌های رمزنگاری هزینه پردازشی بسیار پایینی دارد، در هیچ‌یک از کارهای قبلی، به محاسبه هزینه پردازش پرداخته نشده است. طرح کدبندی ترکیبی نیز از این قاعده مستثنا نیست و هزینهٔ پردازش آن در حد جستجو در یک جدول کلمه‌کد کوچک مشابه (جدول- ۵) و از مرتبه n خواهد بود. n تعداد کلمه‌کد در جدول است.

۵-نتیجه‌گیری

در این مقاله به‌منظور افزایش ظرفیت کانال، روش جدید کدبندی ترکیبی با بهبود و ترکیب روش‌های «بازترتیب بستک‌ها» و «فاصله بین بستک‌ها» ارائه و میزان افزایش ظرفیت کانال محاسبه شد. نتایج ارزیابی محاسباتی در مقایسه با روش کدبندی هندسی ساده، نشان می‌دهد که مطابق با وضعیت عادی بازترتیب در شبکه، با انتخاب سه تا پنج بستک در جدول کلمه‌کد، ظرفیت از ۱۰٪ تا ۳۰۰٪ می‌تواند افزایش یابد.

برای افزایش نامحسوسی نیز از ایدهٔ کلی روش کدبندی کم‌پشت بستک‌ها استفاده شده و برای انتخاب بخشی از بستک‌ها که کدبندی می‌شوند نیز از روش مدولاسیون پرش فرکانسی ایده گرفته شد. در این پژوهش ارزیابی نامحسوسی کانال ترکیبی پیشنهادی به‌صورت عملی انجام شد. نتایج نشان می‌دهد که برای ایجاد کانال زمان‌بندی‌دار پوششی با روش کدبندی «پرش کد ترکیبی»، با توجه به تعداد گام بالا در محیط واقعی اینترنت، با انتخاب مناسب پارامترهای مربوط به کانال (Δ و δ) که حداقل ممکن کوچک‌تر نباشد، می‌توان به نامحسوسی قابل قبولی دست‌یافت. افزایش نامحسوسی با کاهش مختصر ظرفیت کانال در حد قابل قبول محقق شد. مقایسه نتایج ارزیابی نامحسوسی کانال ترکیبی با کارهای قبلی نیز حاکی از رقابت تنگاتنگ آن با نامحسوسی کانال‌های مدل‌محور است.

استحکام کانال با اندازه‌گیری نرخ خطای بیت براساس مقادیر مختلف پارامترهای کدبندی ارزیابی شد.

نتایج نشان می‌دهد که با انتخاب مقادیر مناسب پارامترهای کدبندی، نرخ خطا قابل کنترل است. در ادامهٔ این پژوهش، ترکیب روش کدبندی ترکیبی با روش مدل‌محور برای بیشینه‌کردن نامحسوسی آن، به‌عنوان کارهای بعدی پیشنهاد می‌شود.

۶- مراجع

بیرامی، ب. دهقانی، م. و صالح اصفهانی, م. (۱۳۹۳). تشخیص کانال‌های زمان‌بندی‌دار پوششی به روش‌های آماری. مجله علمی-پژوهشی پدافند الکترونیکی و سایبری ۲(۱). ص ۲۴-۱۳.

حسن‌نیا، م. و دهقانی، م. (۱۳۹۲). بررسی روش‌های نشت اطلاعات و راه‌کارهای جلوگیری از آن. فصلنامه علمی-ترویجی پدافند غیرعامل ۴(۴). ص ۱۲-۱۱.

دهقانی، م. و صالح اصفهانی, م. (۱۳۹۱). کانال‌های پوششی تحت شبکه: یکی از راه‌های اصلی نشت اطلاعات. فصلنامه علمی-ترویجی پدافند غیرعامل ۳(۱). ص ۴۴-۳۷.

Ahmadzadeh, S. A. (2013). Behavioral Mimicry Covert Communication. Electrical and Computer Engineering. Canada, University of Waterloo. PhD Thesis.

Alís, J. B. (2012). Information Leakage and Steganography: Detecting and Blocking Covert Channels. Computer Science Department. Madrid, Carlos III University. PhD Thesis.

Bennett, J. C. R., Partridge, C. and Shectman, N. (1999). Packet reordering is not pathological network behavior. IEEE/ACM Trans.Netw 7(6). pp. 789–798.

Berk, V., Giani, A. and Cybenko, G. (2005). Detection of Covert Channel Encoding in Network Packet Delays. Dartmouth College, Department of Computer Science.

Couture, E. (2010). Covert Channels. The SANS Institute.

El-Atawy, A. and Al-Shaer, E. (2009). Building Covert Channels over the Packet Reordering Phenomenon. Proceedings of 28th Annual IEEE Conference on Computer Communications (INFOCOM).

Galatenko, A., Grusho, A., Kniazev, A. and Timonina, E. (2005). Statistical Covert Channels Through PROXY Server. Proceedings of Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. pp. 424–429.

Giani, A., Berk, V. H. and Cybenko, G. V. (2006). Dat-a Exfiltration and Covert Channels. SPIE Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense.

Gianvecchio, S. and Wang, H. (2010). An Entropy-Based Approach to Detecting Covert Timing Channels.

Gianvecchio, S., Wang, H., Wijesekera, D. and Jajodia, S. (2008). Model-Based Covert Timing Channels: Automated Modeling and Evasion. Proceedings of Recent Advances in Intrusion Detection (RAID) Symposium.

Hasan-Nia, M. H. and Dehghani, M. (2013). Examining the Methods of Information Compromise and its Countermeasures Techniques. Passive Def-ence Quarterly 4(4). pp. 1-12.

Khan, H., Javed, Y., Khayam, S. A. and Mirza, F. (2009). Embedding a Covert Channel in Active Network Connections. Proceedings of IEEE Global Communications Conference (GlobeCom).

Kundur, D. and Ahsan, K. (2003). Practical Internet Steganography: Data Hiding in IP. Proceedings of Texas Workshop on Security of Information Systems.
Liu, G., Zhai, J. and Dai, Y. (2010). Network covert timing channel with distribution matching. Telecommunication Systems Journal.

Liu, Y., Ghosal, D., Armknecht, F., Sadeghi, A.-R., Schulz, S. and Katzenbeisser, S. (2009). Hide and Seek in Time – Robust Covert Timing Channels. Proceedings of 14th European Symposium on Research in Computer Security.

Luo, X., Chan, E. W. W .and Chang, R. K. C. (2007). Cloak: A Ten-fold Way for Reliable Covert Communications (full version). Proceedings of European Symposium on Research in Computer Security (ESORICS).

Piratla, N. M. and Jayasumana, A. P. (2007). Metrics for packet reordering-a comparative analysis. International Journal of Communication Systems 21(1). pp. 99–113.

Piratla, N. M. and Jayasumana, A. P. (2007). Metrics for packet reordering - a comparative analysis. International Journal of Communication Systems 21(1). pp. 99-113.

Sellke, S. H., C.-C.Wang, Bagchi, S. and Shroff, N. B. (2009). Covert TCP/IP Timing Channels: Theory

to Implementation. Proceedings of the 28th Conference on Computer Communications (INFOCOM).

Sellke, S. H., Wang, C.-C., Bagchi, S. and Shroff, N . B. (2009). Covert TCP/IP Timing Channels: Theory to Implementation. Proceedings of The 28th Conference on Computer Communications (INFOCOM).

Shah, G., Molina, A. and Blaze, M. (2006). Keyboards and Covert Channels. Proceedings of USENIX Security Symposium.

Walls, R. J., Kothari, K. and Wright, M. (2011). Liquid: A detection-resistant covert timing channel based on IPD shaping. Elsevier Computer Networks 55. pp. 1217-1228.

WhiteHat (2013). WhiteHat Website Security Statistic Report. Santa Clara, WhiteHat Security Inc.

Zander, S. (2010). Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks. Centre for Advanced Internet Architectures Faculty of Information and Communication Technologies. Melbourne, Swinburne University of Technology. PhD Thesis.

Zander, S., Armitage, G. and Branch, P. (2007). A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials 9(3). pp. 44-57.

Zielinska, E., Mazurczyk, W. and Szczypiorski, K. (2014). Trends in steganography. Communications of the ACM 57(3). pp. 86-95.

مهدی دهقانی دورهٔ کارشناسی خود را در سال ۱۳۶۹ در رشتهٔ مهندسی رایانه (سخت‌افزار) در دانشگاه صنعتی اصفهان و دوره کارشناسی ارشد خود را در سال ۱۳۷۳ در رشتهٔ مهندسی رایانه (معماری) در دانشگاه صنعتی شریف گذرانده و هم‌اکنون فارغ‌التحصیل دوره دکتری در رشته مهندسی رایانه (نرم‌افزار) دانشگاه جامع امام حسین (ع) است. زمینه‌های علمی مورد علاقه وی شبکه‌های رایانه‌ای و امنیت اطلاعات است.

نشانی رایانامهٔ ایشان عبارت است از:

mdehghany@ihu.ac.ir

محمود صالح اصفهانی: استادیار گروه مهندسی رایانه دانشگاه جامع امام حسین علیه السلام کارشناسی ارشد خود را در سال ۱۳۷۲ در دانشگاه ولونگونگ و دکترای خود را در سال ۱۳۷۵ در دانشگاه لاتروب استرالیا در رشته شبکه‌های رایانه‌ای گذرانده است. زمینه‌های تحقیقاتی مورد علاقه ایشان شبکه‌های کامپیوتری و امنیت اطلاعات و ارتباطات است. وی از سال ۱۳۹۲ مشاور امنیت شبکه شرکت ارتباطات سیار نیز می‌باشد.

نشانی رایانامهٔ ایشان عبارت است از:

msaleh@ihu.ac.ir