نشریه علمی "پدافند الکترونیکی و سایبری"
سال هشتم، شماره ۳، پاییز ۱۳۹۹، ص ۲۳-۱۳

علمی- پژوهشی

تشخیص کانال پنهان زمانی در وب بر پایه آنتروپی

مهرداد ناصرالفقرا[۱]، حمیدرضا حمیدی[۲*]

۱- کارشناسی ارشد، ۲- استادیار دانشگاه بین المللی امام خمینی(ره)، قزوین

(دریافت: ۹۸/۰۲/۱۶، پذیرش: ۹۸/۱۱/۱۲)

چکیده

همگام با استقبال عمومی از وب، تحلیل ضعف‌ها و آسیب‌پذیری‌های آن در جهت یافتن حملات امنیتی از اهمیت بالایی برخوردار شده است. در صورت ایجاد ارتباط خلاف سیاست‌های امنیتی سامانه، کانال پنهان ایجاد شده است. مهاجم می‌تواند به راحتی تنها با یک مجوز دسترسی عمومی باعث نشت اطلاعات از سامانه قربانی شود. کانال‌های پنهان زمانی بر خلاف کانال‌های پنهان ذخیره‌سازی حافظه ندارند و کمتر باعث جلب توجه می‌شوند. روش‌های مختلفی برای شناسایی آن‌ها بیان شده است که عموماً از شکل ترافیک و قاعده‌مندی کانال سود می‌جویند. ماهیت کاربردی پروتکل انتقال ابرمتن امکان ایجاد کانال پنهان زمانی مبتنی بر مشخصه‌های مختلف این پروتکل (یا سطوح مختلف) را می‌دهد که در پژوهش‌های گذشته مورد توجه قرار نگرفته است. در این مقاله، روش تشخیص مبتنی بر آنتروپی اطلاعات طراحی و پیاده‌سازی شد. مهاجم می‌تواند با شگردهایی مانند تغییر سطح کانال و یا ایجاد نویز روی کانال در صدد تعدیل مقدار آنتروپی کانال باشد تا از تشخیص تحلیلگر در امان بماند. در نتیجه میزان آستانه آنتروپی برای تشخیص همواره ثابت نیست. با مقایسه آنتروپی حاصل از سطوح مختلف کانال و تحلیلگر به این نتیجه رسیده شد که تحلیلگر باید در تمام سطوح ممکن ترافیک را بررسی کند. همچنین نشان داده شد که با ایجاد نویز روی کانال پنهان از ظرفیت آن کاسته ولی با بالا رفتن آنتروپی، تشخیص آن سخت‌تر می‌شود.

کلیدواژه‌ها: امنیت اطلاعات، کانال پنهان، کانال زمانی، وب، آنتروپی

۱- مقدمه

تعاریف متفاوتی برای کانال پنهان[1] بیان شده است که شالوده آن‌ها بدین صورت است: به یک ارتباط پنهان جهت انتقال پیام‌های پنهان خلاف قوانین سامانه، کانال پنهان گفته می‌شود [۹-۱]. کانال پنهان می‌تواند در مسیر افشای اطلاعات حساس کاربران مانند رمز عبور به‌کار گرفته شود [۱۰]. همچنین این اطلاعات می‌تواند موجب کنترل از راه دور خودرو [۱] یا قلب مصنوعی [۲] شده و جان افراد را به خطر اندازد.

کانال‌های پنهان به گونه‌های مختلفی دسته‌بندی شده‌اند که در جدول (۱) مشاهده می‌شود. معیارهای مختلف دسته‌بندی از اجزای کانال پنهان شامل ارتباط پنهان، پیام تبادل شده و نقض امنیت مشتق شده‌اند.

کانال پنهان را می‌توان به کانال پنهان زمانی و کانال پنهان ذخیره‌سازی دسته‌بندی نمود. در کانال پنهان زمانی، مشابه شکل (۱)، اطلاعات با استفاده از منابع زمانی مشترک تبادل می‌شوند [۱۱].

جدول (۱): انواع کانال‌های پنهان.

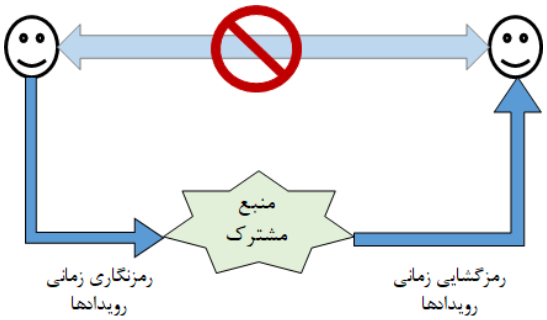
مرجع	معیار	دسته‌بندی
[۳ و ۴]	رسانه ارتباطی	زمانی، ذخیره‌سازی، ترکیبی
[۳ و ۵]	روش ارتباط	دو طرفه، یک طرفه، ساده
[۵]	نویز ارتباط	با نویز، بدون نویز
[۵]	پنهان بودن ارتباط	قابل تشخیص، غیر قابل تشخیص، غیر قابل تشخیص امن
[۶]	بستر ایجاد ارتباط	شبکه‌ای، سامانه عامل، سخت‌افزار
[۵]	مانیتور مرجع	مبتنی بر میزبان، مبتنی بر شبکه، فیزیکی- منزوی
[۷]	محتویات پیام	مبتنی بر مقدار، مبتنی بر تغییر
[۵ و ۸]	پوشش پیام	بدون پوشش پنهان، با پوشش پنهان
[۹]	نقش کانال	فعال، غیر فعال
[۳ و ۵]	نقش فرستنده	اشتراکی، دخالتی
[۵]	اصلاحات مانیتور مرجع	مهاجم، نیمه مهاجم، غیر مهاجم

بر خلاف نوع ذخیره‌سازی کانال پنهان زمانی فاقد حافظه است. در نتیجه در صورت عدم دریافت پیام در زمان مناسب،

* رایانامه نویسنده مسئول: hamidreza.hamidi@eng.ikiu.ac.ir

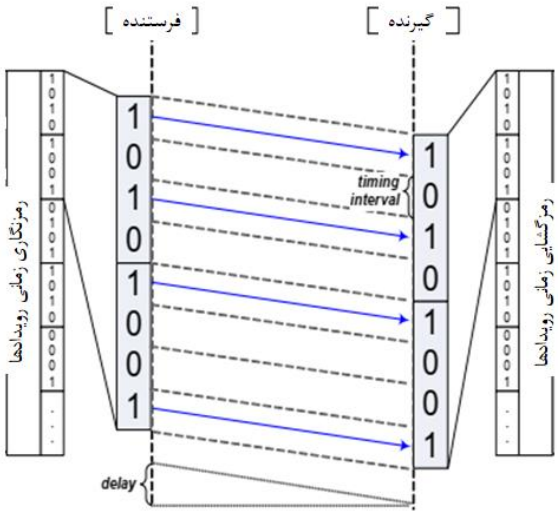
[1] Covert Channel

اطلاعات غیر قابل بازگشت است [۷]. برای نمونه در بستر وب با مشخص کردن یک بازه زمانی و نظارت بر ارسال یا عدم ارسال درخواست در زمان مذکور، مشابه شکل (۲)، می‌توان یک کانال پنهان زمانی ایجاد کرد [۱۱]. به دلیل دسترسی عمومی به وب و نبودن حساسیت زیاد این بستر دارای ظرفیت بالایی برای این‌گونه حملات است.



شکل (۱): نحوه ساخت کانال پنهان زمانی.

پروتکل انتقال ابرمتن[1] بنیاد ارتباط اطلاعات در وب است. این پروتکل به صورت «درخواست کننده – پاسخ دهنده» است. در حالت عادی فقط پاسخ درخواست برای کاربر اهمیت دارد. در حالی که کانال‌های پنهان زمانی در بستر وب می‌توانند از ترتیب پیام‌ها [۱۲و ۱۳]، سرآیند پیام‌ها [۱۴] و یا تأخیر بین پیام‌ها [۱۵] و یا برای ارسال اطلاعات استفاده کنند. پارامترهایی که کاربر عادی نیاز به توجه به آن‌ها ندارد.



شکل (۲): نحوه کار رمز زمانی رویدادها [۱۱].

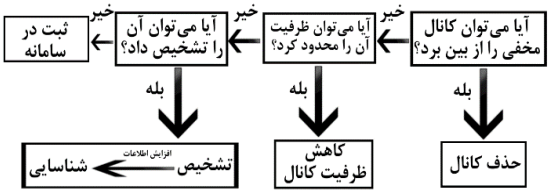
در بخش بعدی روش‌های مقابله با کانال پنهان زمانی بحث می‌شود. پس از بررسی پژوهش‌های مرتبط، رویکرد پیشنهادی این مقاله شرح داده و نتایج ارزیابی می‌شوند.

[1] Hyper Text Transport Protocol (HTTP)

۲- مقابله با کانال پنهان زمانی

تشخیص کانال پنهان نیاز به بار محاسباتی سنگین دارد و معمولاً بعد از شروع به فعالیت کانال قابل انجام است. اما از آنجا که کانال پنهان بر اساس دسترسی به منبع مشترک ایجاد می‌شود، شاید با محدودسازی دسترسی به منابع قابل حذف باشد. بنابراین اولین تلاش در جهت مقابله با کانال پنهان زمانی، حذف آن است. از آنجا که عموماً کانال از ترافیک مجاز استفاده می‌کند حذف آن ممکن است منجر به از کار افتادن سامانه‌های درگیر شود که مطلوب نیست. تلاش بعدی برای کاهش ظرفیت کانال است. این کار نیز می‌تواند باعث پایین آمدن کارایی سامانه‌ها شود.

قدم بعدی تشخیص و شناسایی کانال پنهان است. از آنجا که تشخیص کانال می‌تواند روی کارایی سامانه‌های درگیر تأثیرگذار نباشد، بنابراین از اهمیت خاصی برخوردار است. در صورت عدم تشخیص هشدار لازم در جایی ثبت می‌شود تا کاربران از احتمال خطر اطلاع یابند [۱۰]. روال مقابله را می‌توان به‌صورت شکل (۳) بیان کرد.



شکل (۳): گام‌های مقابله با کانال پنهان.

آزمایش‌های تشخیص کانال پنهان زمانی به دو بخش کلی تقسیم می‌شوند، آزمایش‌های شکلی و آزمایش‌های قاعده‌مندی. شکل ترافیک توسط احتمالات مرتبه اول مانند میانه و توزیع، توصیف می‌شود در حالی که قواعد کانال توسط احتمالات مرتبه دوم و یا بالاتر نظیر همبستگی بین اطلاعات توصیف می‌شود [۱۲].

تشخیص تغییرات در شکل ترافیک با آزمون آماری ممکن است. این آزمون‌ها به بررسی تغییرات در توزیع آماری می‌پردازند. یکی از این آزمون‌ها کلموگرف □ اسمیرنف[2] نام دارد که با مقایسه دو توزیع آماری، حداکثر فاصله بین آن‌ها را اندازه‌گیری می‌کند [۱۳].

آزمون قاعده‌مندی[3] بر اساس واریانس تأخیرهای بین پیام‌ها عمل می‌کند. این روش مبتنی بر این واقعیت است که در ترافیک سالم، واریانس تأخیرها در طول زمان تغییر می‌کند در حالی که در یک کانال پنهان زمانی این مقدار تقریباً ثابت باقی می‌ماند

[2] Kolmogorov – Smirnov
[3] Regularity

[۱۱]. در روش دیگر فرض بر آن است که تأخیرهای بین پیام‌ها تقریباً منطبق به یک توزیع نرمال است. بنابراین اگر یک هیستوگرام از تأخیرهای بین پیام‌ها ایجاد شود، انتظار می‌رود مقادیر وسط هیستوگرام بیشترین فراوانی را داشته باشند. وجود یک توزیع دووجهی یا چندوجهی، بیانگر وجود کانال پنهان زمانی خواهد بود [۱۴].

در پژوهش دیگری، از آزمون تراکم پذیری یا فشردگی استفاده شده است [۱۵]. بر اساس این معیار، ابتدا تأخیرهای شبکه جمع‌آوری می‌شود. سپس این اعداد به ترتیب از بالا به پایین مرتب می‌شوند و اختلاف نسبی بین تأخیرها محاسبه می‌شود. در آخر درصد اعدادی که از یک مقدار ثابت کمتر هستند به‌عنوان معیار آزمایش استفاده شده و با ترافیک معمولی مقایسه می‌شود. این روش برای کانال‌های پنهان بدون نویز به خوبی کار می‌کند. با افزایش نویز در کانال پنهان دقت این روش کمتر می‌شود [۱۵].

روش دیگر تشخیص بر اساس میزان آنتروپی کانال است. در این روش بی‌نظمی ترافیک مجاز و کانال مشکوک با هم مقایسه می‌شوند. محاسبه آنتروپی بر اساس توزیع نمونه‌های تأخیر بین پیام‌ها انجام می‌شود. هر گونه انحراف از این توزیع آموزشی باعث افت آنتروپی شده و می‌تواند نشانگر افشای اطلاعات توسط کانالی غیرمجاز باشد [۱۲].

از ویژگی‌های کانال پنهان زمانی می‌توان به استحکام، ظرفیت و نامحسوسی آن اشاره کرد [۱۶]. استحکام کانال نشان دهنده بیشینه نویز قابل تحمل روی کانال است در حالی که قابلیت رمزگشایی پیام‌ها توسط گیرنده حفظ شود. ظرفیت کانال میزان اطلاعات مفید قابل انتقال توسط کانال در واحد زمان است. و نامحسوسی عبارت از احتمال تشخیص کانال توسط ناظران بیرونی است. کارهای انجام شده روی کانال‌های پنهان زمانی که از تأخیر بین پیام‌ها استفاده می‌کنند بسیار است. عموماً برای ایجاد کانال یک یا چند خصیصه کانال برای طراح اهمیت ویژه دارد و در اولویت است. برخی به دنبال ساخت کانال پنهانی هستند که فقط مستحکم باشد. برخی نیز تنها به دنبال ظرفیت بالا هستند که البته خود این ویژگی به تنهایی تضمینی برای بالا ماندن ظرفیت ندارد چون در صورت تشخیص کانال پنهان و مقابله با آن، ظرفیت آن نیز ممکن است محدود شود. عموماً ظرفیت بالا کانال باعث جلب توجه شده و با قابلیت نامحسوسی در تضاد است. بین این دو ویژگی باید تعادل برقرار باشد.

۳- پژوهش‌های مرتبط

بررسی پژوهش‌های انجام شده در حوزه کانال‌های پنهان زمانی مبتنی بر تبادل پیام نشان دهنده این است که بهبود کدام ویژگی (استحکام، ظرفیت و نامحسوسی) برای محققان مهم بوده است، جدول (۲).

پژوهشی برای ایجاد کانال پنهان زمانی اینگونه عمل کرده است که ابتدا فرستنده و گیرنده روی یک مجموعه بازه زمانی توافق می‌کنند. هر بازه زمانی نشان دهنده یک عدد است که بستگی به نحوه تبدیل پیام دارد. برای مثال اگر پیام ورودی به باینری تبدیل و سپس فرستاده شود، دو عدد برای بازه‌های زمانی ارسال یک بیت توافق می‌شود. سپس با توجه به این اعداد، فرستنده پیام را ارسال می‌کند. در انتها برای سخت‌تر شدن تشخیص به کانال نویز اضافه شده است [۱۱].

در پژوهشی دیگر، ابتدا ترافیک معمولی آنالیز و بررسی شده است. سپس با استفاده از توزیع‌های آماری معروف نزدیک‌ترین توزیع به این ترافیک انتخاب می‌شود. در مرحله بعد پیام ورودی به نمادهایی تبدیل می‌شود. هر نماد به یک عدد تصادفی نگاشت شده و سپس با آن مجموعه اعداد تصادفی یک توزیع آماری درست می‌شود. با استفاده از این توزیع آماری ترافیک جدیدی ایجاد می‌شود که حامل پیام پنهان است. گیرنده باید جدول نگاشت توافق شده را داشته باشد. هدف از این کار نزدیک شدن ترافیک پنهان به ترافیک معمولی و در امان ماندن از تشخیص کانال بوده است [۱۷].

هنگامی که بین فرستنده و گیرنده یک مسیریاب و یا عامل شبکه‌ای دیگری قرار بگیرد، دیگر تأخیر پیام‌ها مطابق میل فرستنده نخواهد بود و بر اساس نظریه صف انجام می‌شود. فرآیند مارکوف یک مدل ریاضی برای زمان‌بندی بین کارها در نظریه صف است. یکی از تأثیرات این موضوع کاهش ظرفیت کانال زمانی است. در پژوهشی سعی شده است تا با استفاده از فرمول‌های ریاضی و توزیع‌های آماری ظرفیت کانال زمانی در این شرایط را بالا ببرند [۱۸ و ۱۹].

کارهایی سعی بر مستحکم‌تر کردن کانال و پنهان ماندن در برابر سامانه‌های تشخیص کرده‌اند. معمولاً هنگام ارسال پیام توسط فرستنده، کدهایی برای تصحیح خطا به پیام اصلی اضافه می‌شود [۲۰، ۲۱ و ۲۲]. در این پژوهش‌ها به جای اضافه کردن کد تصحیح خطا و بازیابی پیام اصلی، خود پیام را گسترش داده‌اند. به‌طوری که برای خطاهای کم و قابل قبول، پیام اصلی قابل مشاهده توسط گیرنده می‌باشد. برای بهبود قابلیت عدم تشخیص نیز از توزیع‌های آماری استفاده شده است. نزدیک‌ترین توزیع به ترافیک معمولی انتخاب و پیام پنهان روی آن توزیع ارسال می‌شود.

در کانال‌های پنهان زمانی با کاهش رشته باینری می‌توان ظرفیت کانال پنهان را افزایش داد. پژوهشی با تبدیل پیام ورودی

به کد هافمن توانسته است درصد بالایی ظرفیت کانال پنهان را افزایش دهد [۲۸ و ۲۹].

استفاده از توزیع آماری ترافیک معمولی در ترافیک پنهان که به کانال پنهان مبتنی بر مدل نیز شناخته می‌شود، در بعضی کارها دیده می‌شود [۳۰]. در این تحقیق پیام پنهان به یک عدد نگاشت شده است. در ادامه تأخیرهای دیگری به آن اضافه می‌شود تا توزیع مورد نظر ایجاد شود. در تنظیم کردن بیت‌های پیام پنهان به تأخیر، از یک الگوریتم بازگشتی استفاده می‌شود که باعث وابستگی تأخیرهای پیام پنهان به یکدیگر می‌شود. بنابراین گیرنده نیاز دارد یک الگوریتم چرخشی را اجرا کند. این کار باعث استحکام کانال پنهان زمانی نیز می‌شود.

شاید استفاده از توزیع آماری خیلی مناسب نباشد. زیرا ترافیک معمولی در حالت عادی دارای هیچ توزیع خاصی نیست و تصادفی است. نزدیک کردن ویژگی‌های آماری توزیع ترافیک پنهان به ترافیک معمولی ایده خوبی است که آن را انجام داده‌اند [۳۱]. در این پژوهش هر دو معیار شکل و قاعده‌مندی ترافیک معمولی تقلید شده است که این کانال پنهان زمانی را از تشخیص انواع سامانه‌های امنیتی مصون می‌دارد.

پژوهش‌های حوزه کانال پنهان زمانی را در جدول (۲) جمع‌بندی شده است. روش پیاده‌سازی کانال پنهان زمانی مورد نظر در این پژوهش‌ها مبتنی بر تأخیر زمانی بین پیام‌ها است. کارهای زیادی در جهت مصون ماندن از تشخیص انجام شده است. مشخصه‌های متعدد پروتکل ابرمتن به سازندگان کانال پنهان امکان می‌دهد تا به‌صورت ثابت یا متغیر کانال را روی هر یک از این مشخصه‌ها (سطوح) ایجاد کنند. در هیچ یک از پژوهش‌های مرتبط تأثیر ایجاد کانال پنهان زمانی در سطوح مختلف وب بر تشخیص کانال سنجیده نشده است. به همین دلیل در این پژوهش تلاش شده تا این عامل‌هایی که در تشخیص کانال پنهان زمانی در وب مؤثر هستند، مورد ارزیابی قرار گیرند.

۴- تشخیص مبتنی بر آنتروپی ترافیک وب

محیط مورد پژوهش به‌صورت شبکه‌ای فرض شده که تعدادی فرستنده و گیرنده و یک تحلیلگر ترافیک در آن حضور دارند. تبادل پیام بر اساس پروتکل انتقال ابرمتن است و پنهان‌سازی بر پایه تأخیر بین پیام‌ها انجام می‌شود. شکل (۴) اجزای یک نمونه درخواست این پروتکل را نمایش می‌دهد. یک فرستنده باید درخواست را با توجه به مکان گیرنده (آدرس آی.پی. و پورت[1]) ارسال کند. گیرنده می‌تواند روی آدرس‌های مختلف آی.پی. و یا روی پورت‌های مختلف منتظر دریافت پیام باشد. متن پیام حاوی آدرس صفحه (منبع) درخواستی، عنوان تابع مورد نظر و همچنین پارامترهای تابع درخواستی است. بنابراین محتوی پیام پنهان می‌تواند بر اساس ترتیب سطوح (مشخصه‌های)، از بالا به پایین، به شرح زیر ایجاد گردد:

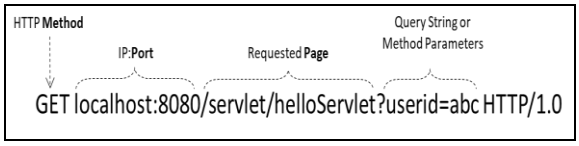
۱. آدرس آی.پی. و شماره پورت؛
۲. آدرس صفحه درخواستی؛
۳. عنوان تابع درخواستی؛
۴. عنوان و مقدار پارامترهای تابع درخواستی.

جدول (۲): پژوهش‌های مرتبط با کانال‌های پنهان زمانی.

مرجع	ایده اصلی	پارامتر هدف
[۱۳]	اضافه کردن نویز به کانال	تشخیص
[۱۷ و ۳۵]	مدل‌سازی توزیع آماری تأخیرها	تشخیص
[۱۸ و ۱۹]	خنثی کردن تأثیر تأخیر صف با استفاده از فرمول‌های ریاضی	استحکام
[۲۰]	مبهم سازی کد برنامه گیرنده	تشخیص
[۲۱ و ۲۲]	توسعه‌ی طول پیام	استحکام
	استفاده از شبیه‌ترین توزیع معروف به ترافیک اصلی	تشخیص
[۲۳]	متعادل سازی پارامترها بر اساس توزیع مارکوف	تشخیص
[۲۴ و ۲۵]	شبیه ساختن توزیع کانال به توزیع ترافیک اصلی	تشخیص
[۲۶]	کدگذاری ترافیک شبکه	تشخیص
[۲۷]	تطابق شکل ترافیک در طول زمان	تشخیص
[۲۸]	استفاده از کد هافمن	ظرفیت
[۲۹]	استفاده از کد فونتین	استحکام
[۳۰]	مدل‌سازی توزیع آماری بر اساس ترافیک معمولی	تشخیص
[۳۰]	استفاده از الگوریتم بازگشتی جهت وابسته کردن اعداد دنباله تأخیرها	استحکام
[۳۱]	نزدیک کردن ویژگی‌های آماری توزیع ترافیک معمولی به توزیع ترافیک پنهان	تشخیص
[۳۲]	استفاده از لایه فیزیکی شبکه	ظرفیت، استحکام، تشخیص

[1] IP Address and Port Number.

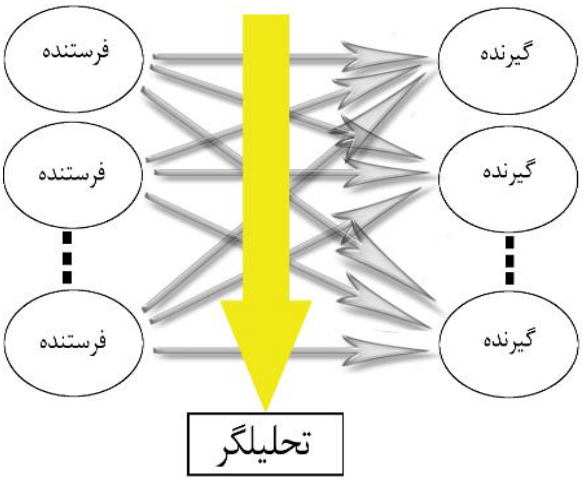
برای ایجاد کانال پنهان، یک فرستنده باید درخواست‌های پروتکل انتقال ابرمتن را با توجه به مکان گیرنده (آدرس آی.پی. و پورت)، محتوی پیام پنهان، زمان تأخیر برای بیت صفر، زمان تأخیر برای بیت یک، مشابه شکل (۲)، و سطح ایجاد کانال پنهان ارسال نماید.



شکل (۴): اجزای یک درخواست پروتکل انتقال ابرمتن.

فرض بر این است گیرنده کانال پنهان نیز از جزئیات کانال خبر دارد. گیرنده با جمع‌آوری پیام‌های دریافتی مبتنی بر پروتکل انتقال ابرمتن و بر اساس تأخیر بین آن‌ها می‌تواند پیام پنهان را بازیابی کند. از آنجا که ترافیک در وضعیت عمومی قرار دارد، بنابراین بسیاری از پیام‌های بی‌ارتباط با کانال پنهان نیز ارسال می‌شود که آن‌ها نویز نامیده شده است.

تحلیلگر پیشنهادی این پژوهش به‌صورت هم‌زمان با فرستنده‌ها و گیرنده‌ها، ترافیک وب را ارزیابی می‌کند. شکل (۵) مؤلفه‌های محیط شبیه‌سازی را نشان می‌دهد.



شکل (۵): مؤلفه‌های محیط آزمایشی.

روش پیشنهادی این مقاله استفاده از آنتروپی ترافیک تبادل پیام‌ها است. در نظریه اطلاعات[1] برای اندازه‌گیری میزان تصادفی بودن داده از معیار آنتروپی استفاده می‌شود. فرض کنید x یک متغیر تصادفی باشد که می‌تواند مقادیر الفبای مجموعه S را بپذیرد. توزیع احتمالی آن برابر است با [۳۳]:

$$P_X(x) = \Pr\{X = x\}(x \in S)$$

بنابراین آنتروپی متغیر تصادفی گسسته x وقتی I تابع میزان اطلاعات رویداد و b مقدار آنتروپی در واحد اطلاعات باشد، به صورت زیر تعریف می‌شود [۳۳]:

$$\mathrm{H}(X) = \sum_{i=1}^{n} \mathrm{P}(x_i)\,\mathrm{I}(x_i) = -\sum_{i=1}^{n} \mathrm{P}(x_i)\log_b \mathrm{P}(x_i).$$

برای مثال فرض کنید در یک کانال ارتباطی می‌خواهید یک رشته دودویی را ارسال کنید. فرض کنید رشته حاوی ۲۵٪ رقم *"1"* و ۷۵٪ رقم *"0"* باشد و واحد اطلاعات یک بیت است بنابراین $b=2$. در این صورت:

$$\mathrm{H}(X) = -\left(\frac{1}{4}\log_2(\frac{1}{4}) + \frac{3}{4}\log_2(\frac{3}{4})\right) \approx 0.81$$

با این تعریف می‌توان آنتروپی هر مجموعه‌ای از داده را به‌دست آورد. هر چه داده منظم‌تر باشند، مقدار آنتروپی آن پایین‌تر و هر چه بی‌نظم‌تر و تصادفی‌تر باشند، آنتروپی بالاتر است. بالاترین مقدار آنتروپی زمانی اتفاق می‌افتد که تمام احتمالات با یکدیگر برابر باشند (داده دارای بیشینه تصادف باشد).

تحلیلگر پیشنهادی این پژوهش با محاسبه آنتروپی پیام‌های بین هر دو زوج مجزا (فرستنده - گیرنده) میزان تصادفی بودن آن‌ها را بررسی می‌کند.

در این پژوهش، کانال پنهان تنها از دو نماد (صفر و یک) برای ارسال اطلاعات استفاده می‌کند. بنابراین آنتروپی کانال برای رشته باینری ۱ است. اگر نماد دیگری (خواسته یا ناخواسته) به دو نماد اصلی اضافه شود، بی‌نظمی در وقوع دو نماد اصلی بیشتر شده و لذا آنتروپی افزایش می‌یابد. اگر احتمال خطا (مثلاً ناشی از تأخیرهای ناخواسته) را P_e درنظر بگیرید، آنگاه آنتروپی کانال به میزان زیر افزایش می‌یابد [۳۳]:

$$\mathrm{H_e} = -\left(\mathrm{P_e}\log_2(\tfrac{1}{Pe}) + (1-\mathrm{P_e})\log_2(\tfrac{1}{1-Pe})\right)$$

تحلیلگر مبتنی بر آنتروپی لازم دارد تا یک حد «آستانه» مجاز آنتروپی در نظر بگیرد و سپس بر اساس آن کانال پنهان زمانی را تشخیص دهد. هر گاه رفتاری به نسبت منظم که آنتروپی آن کمتر از حد «آستانه» باشد را بیابد، آن را کانال پنهان اعلام می‌کند. در این پژوهش حداکثر ۲۰ درصد خطا درنظر گرفته شده است (P_e =۰/۲)، بنابراین «آستانه» تشخیص کانال پنهان برابر ۱/۷۲۱ خواهد بود.

[1] Information Theory

۵- ارزیابی نتایج عملی

آزمایش‌های متعددی برای ارزیابی تأثیر پارامترهای متفاوت در تشخیص کانال پنهان زمانی انجام گرفت. ایجاد کانال پنهان توسط یک فرستنده و یک گیرنده مشخص در بستر یک شبکه عمومی فعال[۱] انجام شده است. گیرنده بر روی یک ماشین مجازی خارج از شبکه محلی (اینترنت) و فرستنده بر روی یک رایانه در شبکه محلی مستقر شده است. پیام‌ها در سطح وب (پروتکل انتقال ابرمتن) رد و بدل شده‌اند و عمل پنهان‌سازی بر اساس تأخیر بین پیام‌ها انجام شده است. بنابراین ثبت ویژگی زمانی پیام‌ها در سمت گیرنده و تحلیلگر ضروری است. پیام‌های شبکه بر روی مسیریاب میانی شبکه محلی (جهت استفاده تحلیلگر) ثبت شده[۲] است. ابتدا اطمینان حاصل شد که گیرنده توانسته است به درستی پیام را دریافت کند، سپس تحلیلگر را برای تشخیص کانال فعال شد.

در کلیه آزمایش‌های انجام شده در این پژوهش، فرستنده پیام‌هایی با طول ۲۰۰ نماد ارسال کرده است. تبادل پیام‌ها در شبکه با ترافیک واقعی بوده است و لذا نویز (خطای ناخواسته) ناشی از ترافیک واقعی شبکه حضور دارد. گیرنده از نحوه پنهان‌سازی آگاه بوده و پیام‌ها را رمزگشایی نموده است. ارزیابی‌های انجام شده بر پایه سه پارامتر زیر تحلیل شده است:

- «آستانه»: حد تشخیص کانال توسط تحلیلگر که با فرض ۲۰ درصد خطا، مقدار ثابت ۱/۷۲۱ است.
- «بیشینه کانال»: گیرنده بعد از رمزگشایی صحیح از پیام‌ها، حد آنتروپی پیام‌های داخل کانال را محاسبه کرده است. با توجه به حضور نویز، این آنتروپی قطعا از آنتروپی ایده‌آل (مقدار ۱) بیشتر است.
- «کمینه نویز»: پیام‌های موجود در ترافیک عمومی شبکه که داخل کانال پنهان نیستند، نویز محسوب شده و آنتروپی آن‌ها محاسبه شد. در آزمایش‌ها فقط نویز ترافیک معمولی شبکه وجود داشته است. اگر فرستنده جهت افزایش نامحسوسی کانال نیز نویز ساختگی ایجاد کند، قطعا آنتروپی بیشتر از این مقدار می‌شود.

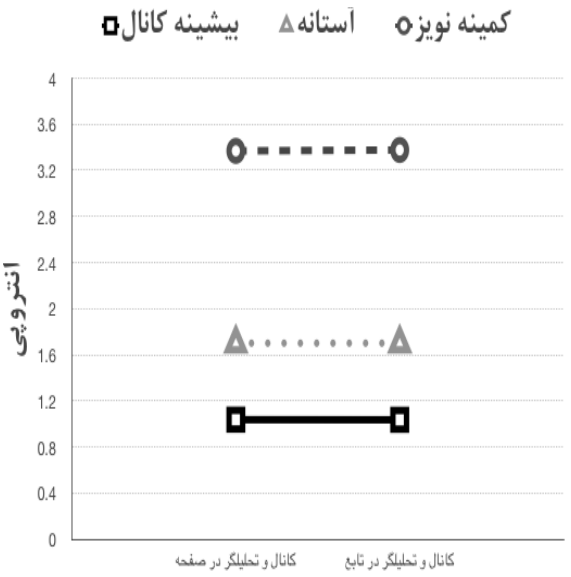
در صورتی که «آستانه» بیشتر از «بیشینه کانال» و کمتر از «کمینه نویز» شود، آنگاه تحلیلگر می‌تواند کانال پنهان را به درستی تشخیص دهد. در غیر این صورت، یا کانال را تشخیص نمی‌دهد (منفی کاذب[۳]) و یا به اشتباه نویز را به‌عنوان کانال در نظر می‌گیرد (مثبت کاذب[۴]).

کانال پنهان زمانی در دو سطح (صفحه و تابع) ایجاد شد و تحلیلگر نیز در سه سطح (پورت، صفحه و تابع) ارزیابی آنتروپی را انجام داد. در ادامه به ارزیابی نتایج آزمایش‌ها بسته به اینکه سطح نمونه‌برداری تحلیلگر نسبت به کانال پنهان چگونه بوده است، پرداخته می‌شود.

۵-۱- کانال و تحلیلگر هم‌سطح

زمانی که کانال پنهان در سطح صفحه ایجاد شده باشد، اگر تحلیلگر نیز در سطح صفحه باشد آنگاه کانال و تحلیلگر هم سطح هستند. برای کانال در سطح تابع نیز تحلیلگر هم‌سطح، در سطح تابع قرار می‌گیرد.

همان‌طور که در شکل (۶) مشاهده می‌شود، در حالت هم‌سطح، تحلیلگر توانسته است با توجه به میزان «آستانه»، کانال پنهان را به خوبی تشخیص دهد («آستانه» بیشتر از «بیشینه کانال» و کمتر از «کمینه نویز» است).



شکل (۶): کانال و تحلیلگر هم‌سطح.

۵-۲- کانال در سطح پایین‌تر

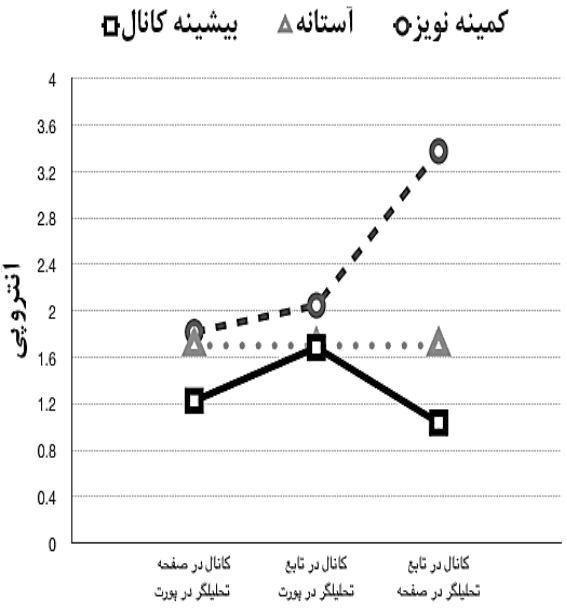
کانال در دو سطح صفحه و تابع ایجاد شده بنابراین فقط سه حالت وجود دارد که کانال در سطح پایین‌تری از تحلیلگر قرار دارد: کانال در صفحه و تحلیلگر در پورت، کانال در تابع و تحلیلگر در صفحه یا پورت. هنگامی که تحلیلگر بالاتر از کانال قرار می‌گیرد، می‌تواند کانال پنهان را مشاهده کند. اما به جز پیام‌های کانال پنهان، پیام‌های دیگری نیز می‌توانند در حیطه

[۱] شبکه عمومی دانشگاه بین‌المللی امام خمینی(ره)
[2] Tcpdump Packet Analyzer.
[3] True Negative
[4] False Positive

دید تحلیلگر قرار بگیرند. برای مثال زمانی که تحلیلگر روی پورت قرار دارد و کانال پنهان روی صفحه ایجاد شده است، علاوه بر درخواست‌های آن صفحه خاص، بقیه درخواست‌های دیگر صفحات آن آدرس را نیز برداشت می‌کند. به همین علت در صورت وجود درخواست‌های زیاد به سایر صفحات، تحلیلگر دچار اشتباه می‌شود.

مطابق شکل (۷)، در این آزمایش نیز کانال‌های پنهان، توسط تحلیلگر در هر سه بخش به درستی تشخیص داده شدند. اما اتفاق جالب، تشخیص کانال‌های پنهان دیگری توسط تحلیلگر از پورت‌های استفاده نشده در آزمایش بود. تشخیص این موارد باعث شد تا مقادیر «کمینه نویز» و «بیشینه کانال» گزارش شده توسط تحلیلگر کمی غیر قابل انتظار باشد. در خوشبینانه‌ترین حالت کانال‌ها و نویزهای اضافی تشخیص داده شده فرآیندهای سامانه‌ای مثل تلاش برای اتصال به سرور مجازی، به‌روزرسانی مطالب وبسایت و یا هر فرآیند سامانه‌ای دیگری که در پس‌زمینه انجام می‌شود، هستند.

اما در بدبینانه‌ترین حالت، سامانه مورد حمله کانال پنهان قرار گرفته است. با توجه به گزارش تأخیرها توسط تحلیلگر، مقادیر تأخیرهای کانال‌ها و نویزهای غیر قابل انتظار در بازه صفر تا یک ثانیه بودند. به دلیل فرض اولیه در مورد استحکام کانال پنهان، تحلیلگر تأخیرها را در مقیاس ثانیه محاسبه می‌کند. نتیجه این که فرآیندهای پس زمینه باعث عوض شدن نمودار شدند.

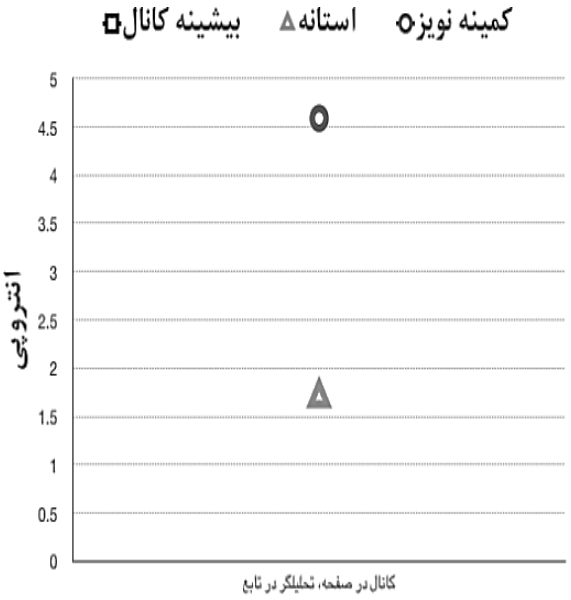


شکل (۷): کانال در سطح پایین‌تر از تحلیلگر.

۵-۳- تحلیلگر در سطح پایین‌تر

با توجه به سطوح کانال و تحلیلگر، تنها هنگامی که کانال در سطح صفحه و تحلیلگر در سطح تابع باشند، تحلیلگر در سطح پایین‌تر از کانال است.

مطابق شکل (۸)، در این حالت «بیشینه کانال» از «کمینه نویز» بیشتر می‌شود و هر دو فاصله قابل توجهی از حد «آستانه» تشخیص آنتروپی دارند. بنابراین کانال پنهان تشخیص داده نمی‌شود. علت آن به طراحی کانال پنهان برمی‌گردد. هنگامی که درخواست‌ها به یک صفحه ارسال می‌شوند، توابع سرآیند پروتکل ابرمتن به صورت نامنظم دیده می‌شوند. بنابراین تحلیلگر یک دنباله تصادفی را می‌بیند که آنتروپی آن از میزان آستانه بالاتر است.



شکل (۸): تحلیلگر در سطح پایین‌تر؛ بیشینه کانال بسیار بالاتر از کمینه نویز بوده است.

۵-۴- تأثیر ظرفیت در نامحسوسی کانال

هر چند هدف این پژوهش ایجاد کانال پنهان زمانی با احتمال کم در تشخیص (نامحسوسی بالا) نبوده است، اما تلاش شده تأثیر سطح قرارگیری تحلیلگر نسبت به کانال را در تشخیص سنجیده شود.

در یک آزمایش رفتار آنتروپی کانال پنهان را با افزایش نویز به کانال (خطای عمدی) و در نتیجه کاهش ظرفیت آن سنجیده شد. در این آزمایش فرستنده، گیرنده و تحلیلگر بر روی یک رایانه قرار گرفته بودند تا ترافیک عمومی شبکه (نویز ناخواسته) حضور نداشته باشد. با افزایش نویز به کانال پنهان طول

دنباله‌های آن افزایش پیدا می‌کند. بنابراین میزان آنتروپی نیز افزایش پیدا می‌کند. برای حذف وابستگی آنتروپی به طول دنباله از آنتروپی نسبی استفاده می‌شود [۳۳]:

$$H(X) = -\sum \frac{PX(x)\log PX(x)}{\log(|S|)}$$

ظرفیت کانال هنگامی که هیچ نویز (خطای خواسته یا ناخواسته) وجود ندارد، برابر ۱ است. با افزایش نویز، ظرفیت مفید کانال به‌صورت زیر کاهش می‌یابد [۳۳]:

$$C = 1 - (P_e \log_2 (\frac{1}{Pe}) + (1 - P_e) \log_2 (\frac{1}{1-Pe}))$$

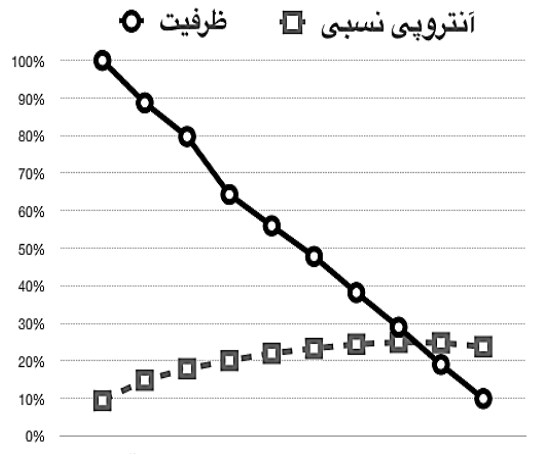
اگر مقدار نویز به ۵۰ درصد ($P_e = 0.5$) برسد، ظرفیت کانال صفر می‌شود. یعنی گیرنده توان تشخیص پیام پنهانی را ندارد. اما اگر مقدار نویز از ۲۰ درصد فراتر برود، با توجه به اینکه «کمینه» آنتروپی نویز از مقدار فرضی این پژوهش به‌عنوان «آستانه» تشخیص کانال (۱/۷۲۱) کمتر می‌شود، در نتیجه تحلیلگر قابلیت تشخیص را از دست می‌دهد.

همان‌گونه که در شکل (۹) نشان داده شده است، با افزایش عمدی نویز به کانال، میزان آنتروپی کانال و نامحسوسی آن افزایش می‌یابد؛ ولی از سوی دیگر ظرفیت کانال نیز کاهش می‌یابد. با افزایش نویز به حدی که منجر به کاهش ظرفیت بیشتر از ۲۰ درصد شود، سطح آنتروپی نیز از حد «آستانه» (که ۲۰ درصد فرض شده) عبور می‌کند و بعد از آن تحلیلگر قابلیت تشخیص ندارد و نامحسوسی کانال حفظ می‌شود.

۵-۵- تأثیر سطح تحلیلگر در نامحسوسی کانال

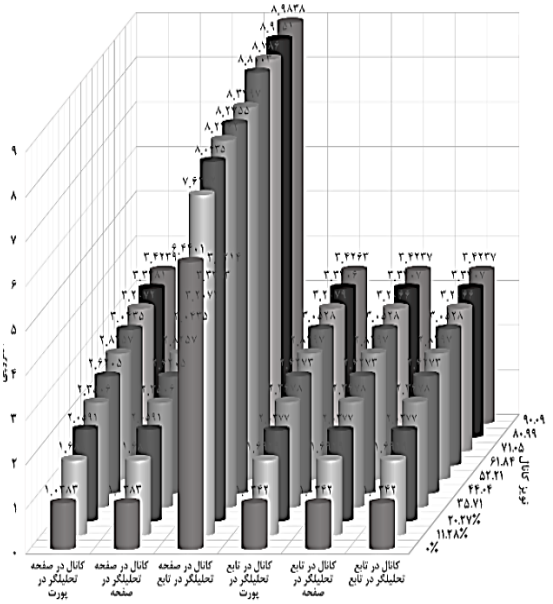
تأثیر میزان نویز عمدی روی تشخیص کانال پنهان در تمامی حالات ممکنِ قرارگیری نسبی کانال پنهان زمانی و تحلیلگر در یک آزمایش دیگر سنجیده شده است.

با توجه به شکل (۱۰)، اضافه کردن ۲۰ درصد نویز کافی است تا کانال پنهان بتواند از تشخیص تحلیلگر هم‌سطح با میزان آستانه ۱/۷ در امان ماند و نامحسوس شود. با افزایش میزان «آستانه»، کانال‌های بیشتری اعم از پنهان یا معمولی در رصد تحلیلگر قرار می‌گیرند که پوشش آن را افزایش می‌دهد اما احتمال تشخیص خطای "مثبت کاذب" بیشتر می‌شود. با کاهش میزان «آستانه» پوشش تحلیلگر کاهش پیدا می‌کند اما احتمال تشخیص خطای "منفی کاذب" بیشتر می‌شود.



شکل (۹): با کاهش ظرفیت کانال به صورت خطی، آنتروپی نسبی به صورت لگاریتمی افزایش می‌یابد.

هنگامی که تحلیلگر هم‌سطح کانال قرار ندارد نیز تفاوتی در استحکام کانال در شکل (۱۰) مشاهده می‌شود. وقتی تحلیلگر در سطح بالاتری از کانال قرار دارد، امکان تشخیص کانال بهتر از زمانی است که تحلیلگر پایین‌تر از کانال است. از آنجا که در یک شبکه عمومی انتظار می‌رود بیشتر پیام‌ها دارای درخواست‌های عمومی (در سطح بالاتر) باشند بنابراین نرخ پیام‌ها در سطوح بالاتر بسیار بیشتر از نرخ پیام‌ها در سطوح پایین‌تر است. بنابراین اگر تحلیلگر در سطوح پایین‌تر از کانال قرار بگیرد، آنتروپی بیشتری را مشاهده می‌کند و در نتیجه نامحسوسی کانال بیشتر است.



شکل (۱۰): بسته به اختلاف سطح کانال و تحلیلگر، میزان نامحسوسی کانال متفاوت است.

۶- نتیجه‌گیری

روشی که در این پژوهش برای تشخیص کانال پنهان زمانی استفاده شد مبتنی بر آنتروپی است. این ایده قبلاً هم در دیگر پژوهش ها استفاده شده است اما در این پژوهش حساسیت پارامترهای مختلف مؤثر در تشخیص بیان شد و مورد آزمایش قرار گرفت. سطح قرارگیری تحلیلگر نسبت به کانال پنهان و همچنین تأثیر افزایش نویز عمدی (یا کاهش ظرفیت کانال) بر نامحسوسی کانال در آزمایش‌ها به نمایش در آمده است.

با توجه به آزمایش‌های انجام شده معیار جدیدی به نام سطح قرارگیری کانال پنهان و تحلیلگر بررسی شد. قرارگیری مناسب تحلیلگر برای تشخیص کانال پنهان مهم است. زیرا در سطوح بالاتر به دلیل وجود درخواست‌های بیشتر از درخواست‌های کانال پنهان، دنباله تأخیرها دارای خطا خواهد بود و در سطوح پایین‌تر، تحلیلگر دچار اشتباه می‌شود. همچنین میزان آستانه آنتروپی برای تمیز دادن کانال‌های مجاز و غیر مجاز دارای اهمیت است. مقدار این آستانه می‌تواند در فاز یادگیری محاسبه شود.

کانال پنهان ایجاد شده جزو ساده‌ترین کانال‌های پنهان است. با پیچیده‌تر کردن ابعاد مختلف آن می‌توان تشخیص آن را سخت‌تر کرد. برای مثال کانال پنهان زمانی می‌تواند حاوی ۴ نماد معتبر باشد که در هر نماد یک جفت بیت "۰۰, ۰۱, ۱۰, ۱۱" را ارسال کند. همچنین برای تبدیل پیام پنهان می‌توان به جای کد اسکی از کدهای پیچیده‌تر مثل کد هافمن استفاده کرد تا به صفر و یک‌های کمتر و در نتیجه زمان کمتری برای ارسال نیاز باشد. در این صورت ظرفیت کانال بالا می‌رود. در آزمایش‌های انجام شده، تنها خود پیام پنهان ارسال می‌شد. در موارد پیشرفته‌تر می‌توان از کدهای تشخیص خطا و یا حتی تصحیح خطا نیز استفاده نمود. گیرنده باید از شیوه ارسال پیام فرستنده آگاه باشد تا بتواند پیام پنهان را به درستی بازیابی کند.

در این پژوهش، مشخصات اصلی کانال (آی.پی.، پورت، صفحه و تابع) در تمام طول عمر کانال ثابت بودند. برای مثال فرستنده همواره از آی.پی. و پورت خاصی برای ارسال درخواست‌های پروتکل انتقال ابرمتن استفاده کرده است. برای سخت‌تر کردن تشخیص توسط تحلیلگر، فرستنده می‌تواند مقدار آی.پی. و یا پورت و یا هر دو را در طول ارسال پیام در بازه مشخصی تغییر دهد. گیرنده باید از این تغییرات با خبر باشد. همچنین گیرنده می‌تواند ثابت نباشد، در واقع پروسه‌ای که به‌عنوان گیرنده در نظر گرفته می‌شود باید چند آی.پی. یا چند صفحه یا چند تابع خاص یا ترکیبی از این حالات را که از قبل با فرستنده توافق شده است، مشاهده کند تا بتواند تأخیرها را به درستی تشخیص دهد. همچنین پروتکل ارسال درخواست نیز می‌تواند الزاما پروتکل انتقال ابرمتن نباشد. برای مثال می‌توان از پروتکل انتقال فایل[1] استفاده نمود.

۷- مراجع

[1] F. Sommer, D. Jürgen, and K. Reiner, "Survey and Classification of Automotive Security Attacks," Information 10.4, 148, 2019. https://doi.org/10.3390/info10040148

[2] F. Mikhail, A. Flor, D. Steinmetzer, S. Paul Gardner, and M. Hollick, "Survey and Systematization of Secure Device Pairing," Communications Surveys & Tutorials IEEE, vol. 20, no. 1, pp. 517-550, 2018. https://doi.org/10.1109/COMST.2017.2748278

[3] US Department of Defense, "Trusted Computer System Evaluation Criteria," ISBN 978-0-333-53947-7, Palgrave Macmillan, London, 1985. https://doi.org/10.1007/978-1-349-12020-8_1

[4] V. D. Gligor, "A Guide to Understanding Covert Channel Analysis of Trusted Systems," National Computer Security Center (U.S.) Meade, Maryland, NCSC-TG-030. 1994.

[5] B. Carrara and C. Adams, "A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels," In Proc. of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 115-126, 2016. https://doi.org/10.1145/2909827.2930800

[6] H. Okhravi, S. Bak, and S. T. King, "Design, Implementation and Evaluation of Covert Channel Attacks," in Technologies for Homeland Security (HST), 2010 IEEE Int. Conf. on, pp. 481-487, 2010. https://doi.org/10.1109/THS.2010.5654967

[7] Z. Wang and R. B. Lee, "New Constructive Approach to Covert Channel Modeling and Channel Capacity Estimation," In Int. Conf. on Information Security, pp. 498--505, 2005. https://doi.org/10.1007/11556992_37

[8] ChangXiang Shen, HuangGuo Zhang, DengGuo Feng, ZhenFu Cao and JiWu Huang, "Survey of Information Security," Science in China Series F: Information Sciences 50.3, 273-298, 2007. https://doi.org/10.1007/s11432-007-0037-2

[9] XIAOSONG ZHANG, YU-AN TAN, CHEN LIANG, YUANZHANG LI, AND JIN LI, "A Covert Channel Over Volte via Adjusting Silence Periods," IEEE Access 6, 9292-9302, 2018. https://doi.org/10.1109/ACCESS.2018.2802783

[1] FTP: File Transfer Protocol

[10] Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, Krzysztof Szczypiorski, "Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures," John Wiley & Sons, 2016. https://doi.org/10.1002/9781119081715, PMid:27000183

[11] S. Cabuk, C. E. Brodley, and C. Shields, "IP Covert Timing Channels: Design and Detection," In Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 178--187, 2004. https://doi.org/10.1145/1030083.1030108

[12] S. Yao, W. Yang, and H. Liusheng, "Concealed in Web Surfing: Behavior-based Covert Channels in HTTP," J. of Network and Computer Applications 101, 83-95, 2018. https://doi.org/10.1016/j.jnca.2017.10.019

[13] Ang Chen, W Brad Moore, Hanjun Xiao, Andreas Haeberlen, Linhthi Phan, Micah Sherr and Wenchao Zhou, "Detecting Covert Timing Channels with Time-Deterministic Replay," 11th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 14), 2014.

[14] V. Berk, A. Giani, G. Cybenko, and N. Hanover, "Detection of Covert Channel Encoding in Network Packet Delays," Rapport technique TR536, de lUniversité de Dartmouth, pp. 19, 2005.

[15] S. Cabuk, C. E. Brodley, and C. Shields, "IP Covert Channel Detection," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 4, pp. 22, 2009. https://doi.org/10.1145/1513601.1513604

[16] E. Brown, B. Yuan, D. Johnson, and P. Lutz, "Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks," in Int. Conf. on Cyber Warfare and Security, pp. 56, 2010.

[17] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based Covert Timing Channels: Automated Modeling and Evasion," In Int. Workshop on Recent Advances in Intrusion Detection, pp. 211-230, 2008. https://doi.org/10.1007/978-3-540-87403-4_12

[18] T. P. Coleman and N. Kiyavash, "Sparse Graph Codes and Practical Decoding Algorithms for Communicating over Packet Timings in Networks," In Information Sciences and Systems, CISS 2008. 42nd Annual Conf. on, pp. 447-452, 2008. https://doi.org/10.1109/CISS.2008.4558568

[19] T. P. Coleman and N. Kiyavash, "Practical Codes for Queueing Channels: An Algebraic, State-Space, Message-Passing Approach," In Information Theory Workshop, ITW'08. IEEE, pp. 318-322, 2008. https://doi.org/10.1109/ITW.2008.4578677

[20] R. M. Stillman, "Detecting IP Covert Timing Channels by Correlating Packet Timing with Memory Content," In Southeastcon, IEEE, pp. 204-209, 2008. https://doi.org/10.1109/SECON.2008.4494286

[21] Y. Liu, D. Ghosal, and F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzenbeisser, "Hide and Seek in time---Robust Covert Timing Channels," In European Symposium on Research in Computer Security, pp. 120-135, 2009. https://doi.org/10.1007/978-3-642-04444-1_8

[22] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzenbeisser, "Robust and Undetectable Steganographic Timing Channels for Iid Traffic," In Int. Workshop on Information Hiding, pp. 193-207, 2010. https://doi.org/10.1007/978-3-642-16435-4_15

[23] N. Kiyavash and T. Coleman, "Covert Timing Channels Codes for Communication Over Interactive Traffic," In Acoustics, Speech and Signal processing, ICASSP 2009. IEEE Int. Conf. on, pp. 1485-1488. 2009. https://doi.org/10.1109/ICASSP.2009.4959876

[24] G. Liu, J. Zhai, Y. Dai, and Z. Wang, "Covert Timing Channel with Distribution Matching," In Multimedia Information Networking and Security, MINES'09. Int. Conf. on, vol. 1, pp. 565-568, 2009. https://doi.org/10.1109/MINES.2009.28, PMCid:PMC2683182

[25] G. Liu, J. Zhai, and Y. Dai, "Network Covert Timing Channel with Distribution Matching," Telecommunication Systems, vol. 49, no. 2, pp. 199-205, 2012. https://doi.org/10.1007/s11235-010-9368-1

[26] S. Zander, G. Armitage, and P. Branch, "Stealthier Inter-Packet Timing Covert Channels," Networking, pp. 458-470, 2011. https://doi.org/10.1007/978-3-642-20757-0_36

[27] R. J. Walls, K. Kothari, and M. Wright, "Liquid: A Detection-Resistant Covert Timing Channel Based on IPD Shaping," Computer Networks, vol. 55, no. 6, pp. 1217-1228, 2011. https://doi.org/10.1016/j.comnet.2010.11.007

[28] Jianhua Liu, Wei Yang, Liusheng Huang and Wuji Chen, "A Detection-Resistant Covert Timing Channel Based on Geometric Huffman Coding," Int. Conf. on Wireless Algorithms, Systems, and Applications. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-94268-1_26

[29] R. Archibald and D. Ghosal, "A Covert Timing Channel Based on Fountain Codes," In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th Int. Conf. on, pp. 970--977, 2012. https://doi.org/10.1109/TrustCom.2012.21

[30] Tae-Seok Ahn, Ji-Won Jung, Ha-Hyun Sung, Dong-Won Lee, and Tae-Doo Park, "Turbo Equalization for Covert Communication in Underwater Channel," Eighth Int. Conf. on Ubiquitous and Future Networks (ICUFN). IEEE, 2016. https://doi.org/10.1109/ICUFN.2016.7537071

[31] Jing Wang, Le Guan, Limin Liu, and Daren Zha, "Implementing a Covert Timing Channel Based on Mimic Function," Int. Conf.on Information Security Practice and Experience. Springer, Cham, 2014. https://doi.org/10.1007/978-3-319-06320-1_19

[32] K. S. Lee, H. Wang, and H. Weatherspoon, "{PHY} Covert Channels: Can You See the Idles?," In 11th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 14), pp. 173-185, 2014.

[33] T. S. Han and K. Kobayashi, "Mathematics of Information and Coding," American Mathematical Society, 2007. https://doi.org/10.1090/mmono/203, PMid:17014848

[34] M. Saadati, M. Dehghani, and M. Saleh Esfahani, "Simulation and Evaluation of Jitter and Packet Loss Noises Influence on Covert Timing Channel Performance," J. of Electronic & Cyber Defence, vol. 2, no. 3, pp. 35-49, 2014. (In Persian)

[35] B. Beyrami, M. Dehghani, and M. Saleh Esfahani, "Covert Timing Channel Detection Based on Statistical Methods," J. of Electronic & Cyber Defence, vol. 2, no. 5, pp. 13-24, 2014. (In Persian).

Journal of Electronical & Cyber Defence
Vol. 8, No. 3, 2020, Serial No. 31

Web Covert Timing Channel Detection based on Entropy

M. Naserolfoghara, H. R. Hamidi*

*Computer Engineering Department, Imam Khomeini International University

(Received: 06/05/2019, Accepted: 01/02/2020)

ABSTRACT

Regarding the general acceptance of the web, analyzing its weaknesses and vulnerabilities in order to find and face security attacks has become more urgent. In case there is a communication contrary to the system security policies, a covert channel has been created. The attacker can easily disclose information from the victim's system with just one public access permission. Covert timing channels, unlike covert storage channels, do not have memory storage and draw less attention. Different methods have been proposed for their identification, which generally benefit from the shape of traffic and the channel's regularity. The applicative nature of HTTP protocol allows the creation of a covert timing channel based on different features (or different levels) of this protocol, which has not been addressed in previous researches. In this article, the entropy-based detection method was designed and implemented. The attacker can adjust the amount of channel entropy by controlling measures such as changing the channel's level or creating noise on the channel to hide from the analyst's detection. As a result, the entropy threshold is not always constant for detection. By comparing the entropy from different levels of the channel and the analyst, we concluded that the analyst must investigate the traffic at all possible levels. We also illustrated that by making noise on the covert channel, although its capacity would decrease, but as the entropy has increased, the attacker would have more difficulty in its detection.

Keywords: Information Security, Convert Channel, Timing Channel, WEB, Entropy

*Corresponding Author Email: hamidreza.hamidi@eng.ikiu.ac.ir