نشریه علمی پدافند غیرعامل

سال دهم، شماره ۳، پاییز ۱۳۹۸، (پیاپی ۳۹): صص ۱۰۹-۹۵

مرور و مقایسه روش‌های نهان‌نگاری شبکه بر مبنای طبقه‌بندی‌های مختلف

مینو شعاعی[۱]، وجیهه ثابتی[۲*]

تاریخ دریافت: ۱۳۹۷/۰۶/۲۴

تاریخ پذیرش: ۱۳۹۷/۱۰/۱۵

چکیده

رشد اینترنت و شبکه‌های رایانه‌ای، سبب ساده‌سازی ارسال اطلاعات شده است. این توسعه سبب ایجاد مشکلاتی نیز شده است چون در محیط‌های شبکه‌ای، امکان جاسوسی داده حین ارسال از فرستنده به گیرنده وجود دارد؛ بنابراین، لزوم ایجاد امنیت اطلاعات همواره وجود دارد و در این میان، نهان‌نگاری نقش مهمی را ایفا می‌کند. نهان‌نگاری شبکه یک روش نهان‌نگاری با استفاده از پروتکل‌های شبکه است. روش‌های بسیاری برای نهان‌نگاری شبکه تا به‌حال پیشنهاد شده است که آشنایی با الگوریتم و به‌علاوه مزایا و معایب هرکدام از آن‌ها برای محققان این حوزه جهت ارائه روش نهان‌نگاری جدید و یا جهت پیشنهاد روش نهان‌کاوی جدید ضروری است. در این مقاله تلاش شده است در قالب دو طبقه‌بندی مختلف، ایده‌های گوناگون موجود در روش‌های نهان‌نگاری شبکه تشریح شوند. با توجه به تضاد موجود در سه معیار ارزیابی ظرفیت، عدم تشخیص تمایز و مقاومت، طراحی روشی که در هر سه معیار برتر باشد نقطه ایده‌آل است ولی بسته به اهمیت هر کدام از این معیارها در کاربرد مورد نظر، می‌توان با توجه به مقایسه انجام‌شده در این تحقیق یک یا چند روش برتر را معرفی کرد.

کلیدواژه‌ها: شبکه، کانال نهان، پنهان‌سازی اطلاعات، ارتباطات مخفی، نهان‌کاوی

۱- دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکدهٔ فنی/مهندسی، دانشگاه الزهراء.

۲- استادیار گروه مهندسی کامپیوتر، دانشکدهٔ فنی/مهندسی، دانشگاه الزهراء. (v.sabeti@alzahra.ac.ir) - نویسنده مسئول

۱- مقدمه

بستر اصلی نقل‌وانتقال اطلاعات دیجیتال، شبکه‌های رایانه‌ای و از همه مهم‌تر شبکه جهانی اینترنت است و با اتصال رایانه یا شبکه به اینترنت، این بستر ارتباطی برای میلیون‌ها نفر (که هیچ شناختی از آن‌ها وجود ندارد) در سراسر جهان مهیا می‌شود تا به اطلاعات یکدیگر دسترسی داشته باشند؛ بنابراین در صورت عدم وجود یک سیستم امنیتی برای شبکه و رایانه‌ها، هرلحظه امکان دارد که فایل‌ها و بانک‌های اطلاعاتی شرکت یا سازمان به سرقت رفته یا مخدوش شود. علم پنهان‌سازی اطلاعات یکی از روش‌هایی است که برای برآورده کردن نیاز به امنیت ارتباطات پیشنهاد شده است.

به‌طورکلی موضوعاتی که پنهان‌سازی اطلاعات دربرگیرنده آن‌ها است عبارت‌اند از: ۱- واترمارک: موارد مربوط به حق مالکیت تولیدات نرم‌افزاری و الکترونیکی که جنبه تجاری از این علم هستند. ۲- نهان‌نگاری: استفاده از پنهان‌سازی در ارسال و دریافت پیام به‌صورت غیر محسوس [۱].

نهان‌نگاری[1] یا استگانوگرافی یکی از شاخه‌های علم پنهان‌سازی اطلاعات است. هدف اصلی فرآیند نهان‌نگاری، پنهان کردن اطلاعات سرّی به‌گونه‌ای است که یک ناظر خارجی از وجود ارتباط سرّی آگاه نشود. اگر کسی به‌غیر از فرستنده و گیرنده از این ارتباط سرّی آگاهی پیدا کند، الگوی نهان‌نگاری شکست‌خورده است [۲].

در نهان‌نگاری به‌منظور جلوگیری از دسترسی اشخاص غیرمجاز، علاوه بر پیام مخفی، وجود ارتباط شامل پیام مخفی را نیز پنهان می‌کند که این نکته تفاوت روش‌های نهان‌نگاری و رمزنگاری است [۳]. درواقع برتری نهان‌نگاری در این است که می‌توان پیامی را فرستاد بدون اینکه کسی بفهمد پیامی فرستاده شده است [۴]. سامانه‌های امن‌تر از ترکیبی از این دو روش (نهان‌نگاری و رمزنگاری) استفاده کرده و پیام را قبل از پنهان‌سازی، رمزگذاری می‌کنند. در این صورت اگر اطلاعات پنهان کشف شود، معنای آن امن خواهد ماند [۵].

به‌طورکلی روش‌های نهان‌نگاری از دو فرایند جاسازی و استخراج تشکیل شده‌اند. در فرایند جاسازی، داده با استفاده از یک الگوریتم جاسازی در یک رسانه پوشش یا حامل پنهان می‌شود. در نتیجه این مرحله، رسانه نهان‌نگاری شده تولید می‌شود که باید برای گیرنده مورد نظر ارسال شود. گیرنده با استفاده از الگوریتم استخراج، به داده مخفی دسترسی می‌یابد. برای افزایش امنیت معمولاً از یک کلید جاسازی در این مرحله استفاده می‌شود که گیرنده و فرستنده باید قبل از شروع الگوریتم بر روی آن توافق کنند [۶].

تاکنون الگوریتم‌های گوناگونی برای نهان‌نگاری اطلاعات ارائه شده است. عموماً نهان‌نگاری در دو حوزه مکان و تبدیل انجام می‌شود [۷].

به‌طورکلی در سامانه‌های پنهان‌سازی اطلاعات سه عنصر اصلی ظرفیت، امنیت و مقاومت دخیل هستند. در روش‌های نهان‌نگاری، ظرفیت و امنیت اهمیت اصلی را دارند [۸].

برای انجام فرآیند جاسازی به یک رسانه حامل مناسب نیاز است [۹]. در این خصوص از حامل‌هایی مانند صوت، تصویر، ویدئو و غیره جهت درج اطلاعات استفاده می‌شود. [۷] اما شکل دیگری از حامل‌ها، در شاخه نهان‌نگاری شبکه استفاده می‌شود. واژه «نهان‌نگاری شبکه[2]» اولین بار توسط Szczypiorski ابداع شد [۶]. روش‌های نهان‌نگاری شبکه از ترافیک عمومی شبکه به‌عنوان یک حامل برای داده سرّی استفاده می‌کنند. آن‌ها داده سرّی را در ارتباط عمومی به‌گونه‌ای پنهان می‌کنند که تأثیر آن بر ارسالات عمومی حداقل باشد؛ بنابراین، ارسال نهان به‌گونه‌ای مؤثر پوشانده می‌شود. از ارسال نهان به‌طور رایج به‌عنوان کانال نهان[3] یاد می‌شود [۹].

مفهوم کانال‌های نهان اولین بار توسط لمپسون در سال ۱۹۷۳ معرفی شد [۶]. کانال نهان شبکه یکی از روش‌های بالقوه ارسال سرّی اطلاعات در محیط نظارت است که یک روش ارتباطی پنهان است که امنیت پیام‌های ارسال‌شده از طریق شبکه باز را محافظت می‌کند.

تابه‌حال روش‌های متفاوتی برای نهان‌نگاری در شبکه ارائه‌شده است، به‌علاوه چندین طبقه‌بندی مختلف نیز برای این روش‌ها ارائه شده است. هدف اصلی در این مقاله معرفی و تحلیل بهترین دسته‌بندی‌ها و به‌علاوه معرفی مختصر و مقایسه تعدادی از بهترین روش‌های موجود نهان‌نگاری شبکه است.

در ادامه، در بخش ۲، طبقه‌بندی روش‌های پنهان‌سازی بر اساس چگونگی مخفی‌سازی داده در حامل به‌صورت کامل بررسی می‌شود. در بخش ۳، طبقه‌بندی روش‌های مختلف بر اساس پروتکل‌های لایه‌های OSI ارائه می‌شود. پس از آن، در بخش ۴،

[1] steganography

[2] Network steganography

[3] Covert channel

تعدادی از بهترین‌های نهان‌نگاری شبکه به‌صورت جزئی‌تر بررسی می‌شوند و در بخش ۵، مقایسه کلی روش‌ها، از نظر مزایا و معایب آن‌ها انجام می‌شود. در انتها یک نتیجه‌گیری کلی از مباحث مطرح‌شده، ارائه می‌شود.

۲- طبقه‌بندی روش‌های نهان‌نگاری شبکه بر اساس روش جاسازی داده در حامل

روش‌های پنهان‌سازی بسیاری در چند دهه اخیر ارائه شده است که پوشش تمام آن‌ها در چند صفحه امکان‌پذیر نیست، از طرف دیگر روش‌های پنهان‌سازی مختلف بر اساس یک مفهوم یکسان یا مشابه هستند و بحث در مورد تمام آن‌ها باعث تکرار می‌شود. به همین دلیل، برای اولین بار Wendzel و همکارانش از لغت «الگوهای پنهان‌سازی» برای طبقه‌بندی این روش‌ها استفاده کردند. هر الگوی پنهان‌سازی یک توصیف منحصربه‌فرد و عمومی از یک روش پنهان‌سازی خاص است و ممکن است برای توصیف چندین روش به‌صورت هم‌زمان قابل‌استفاده باشد [۱۰].

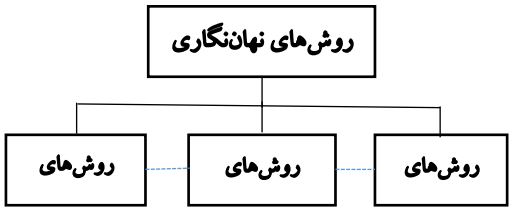
یکی از کامل‌ترین طبقه‌بندی‌های روش‌های نهان‌نگاری شبکه، طبقه‌بندی بر اساس روش جاسازی داده در حامل است که در شکل (۱) نشان داده شده است. در این طبقه‌بندی، روش‌ها به دودسته اصلی «ذخیره» و «زمانی» و یک دسته «ترکیبی» تقسیم می‌شوند که اکثر روش‌های موجود در دسته اول قرار می‌گیرند [۹].

روش‌های ذخیره برای پنهان‌ساختن داده نهان در فیلدهای آغازین یا پایانی پروتکل‌های خاص و یا در فیلدهای محموله خود پیام، تلاش می‌کنند. به‌طورمعمول، ظرفیت بالایی می‌تواند با استفاده از این روش به‌دست آید، اما به‌محض اینکه این کانال‌ها ثبت شوند، یک مدیر شبکه با استفاده از طرح‌های شناسایی بر اساس محتوا به‌سادگی قادر به مکان‌یابی آن‌ها و انتخاب راه‌های مقابله مناسب است.

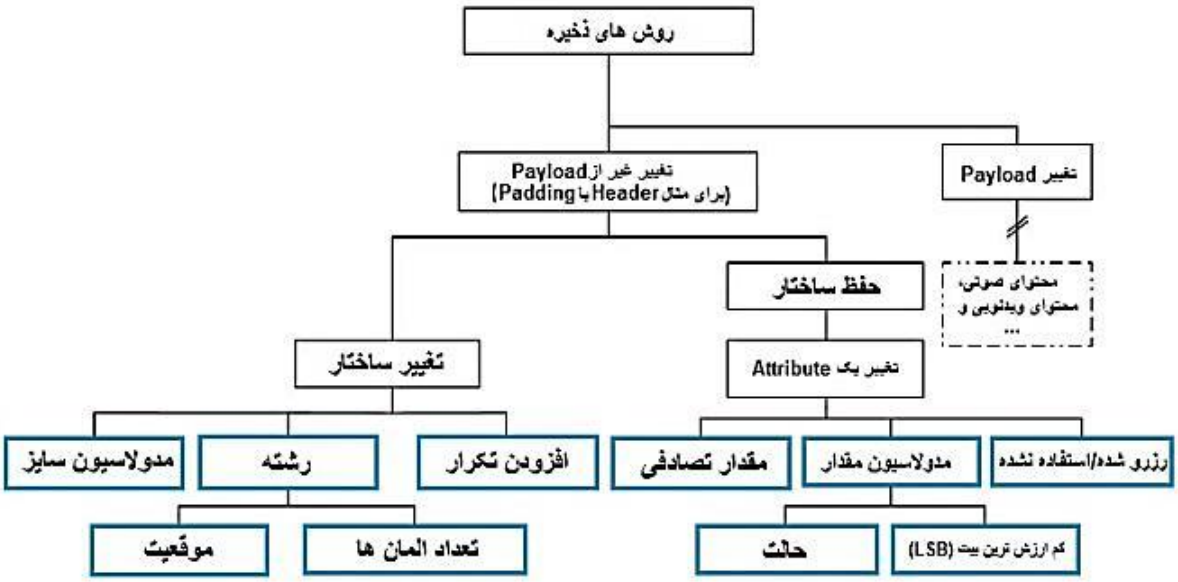
روش‌های زمانی کلاسیک با تغییر سازوکارهای زمانی اطلاعات را پنهان می‌کنند. در یک محیط شبکه‌ای این کار اغلب با تغییر نرخ بسته‌ها یا تغییر تأخیرهای میان بسته‌ای انجام می‌شود. شناسایی کانال‌های زمانی کاری دشوار است به این علت که تنها طرح‌های شناسایی بر اساس ناهنجاری‌ها، کاربردی هستند و این نیز می‌تواند با تقلید مشخصات ترافیک شبکه‌ای قانونی که بر آن نظارت می‌شود، دور زده شود.

عیب عمده کانال‌های زمانی، توان خروجی کم و نیاز مشترک آن‌ها به سنکرون‌سازی زمان به‌صورت مطلق میان فرستنده و گیرنده است که پیاده‌سازی‌های عملی را پیچیده می‌کند. آن‌ها هم‌چنین اغلب در برابر شرایط پویای شبکه مانند تداخل بسته‌ها، گم‌شدن بسته‌ها و نویز، ایمن نیستند [۱۱].

راه‌کارهای ترکیبی روش‌هایی هستند که ویژگی‌های روش‌های ذخیره و زمانی را ترکیب می‌کنند. در ادامه هرکدام از این مفاهیم به‌صورت کامل بررسی می‌شود.



شکل (۱): طبقه‌بندی روش‌های نهان‌نگاری شبکه [۹]



شکل (۲): طبقه‌بندی روش‌های ذخیره [۹]

۲-۱- روش‌های ذخیره

در این گروه، الگوهایی قرار می‌گیرند که پنهان‌سازی را در داده کاربر[1] و یا فیلدهای پروتکل (غیر از داده کاربر) انجام می‌دهند. روش‌های معمول نهان‌نگاری در رسانه‌های دیجیتال مانند تصویر، صوت، متن و ویدئو در دسته روش‌های تغییر داده کاربر قرار می‌گیرد؛ اما دو نوع از الگوهای تغییر غیر از داده کاربر وجود دارد:

- الگوهای تغییردهنده ساختار، ساختار یک واحد داده پروتکل[2] (PDU) را برای مثال با تغییر اندازه آن، تغییر می‌دهند.
- الگوهای حفظ‌کننده ساختار، ساختار PDU داده‌شده را حفظ می‌کنند و انواع مختلفی از فیلدهای سرآیند PDU، برای مثال یک بیت کنار گذاشته شده را تغییر می‌دهند.

هرکدام از این الگوها شامل روش‌های مختلفی می‌شود. در ادامه تمامی الگوها به‌صورت مجزا و با دسته‌بندی داده‌شده در شکل (۲)، بررسی شده و برای هر الگو، روش‌های پنهان‌سازی نمونه توضیح داده می‌شوند. ذکر این نکته ضروری است که برای هر حالت می‌توان روش‌های پنهان‌سازی بیشتری در مقالات مختلف یافت که مجالی برای بیان تمام آن‌ها در اینجا وجود ندارد.

۲-۱-۱- مدولاسیون اندازه PDU: [۹]

روش‌های پنهان‌سازی می‌توانند اطلاعات را با تغییر اندازه یک واحد داده پروتکل و یا از طریق اندازه یک عنصر سرآیند خاص درون یک PDU، ارسال کنند.

۲-۱-۲- مدولاسیون ترتیب در PDU ها: [۹]

الگوی ترتیب شامل تمام روش‌های پنهان‌سازی است که ترتیب عناصر یک PDU را تغییر می‌دهند. چنین رویکردهایی به‌سادگی می‌توانند برای پروتکل‌هایی با ساختار سرآیندی بسیار پویا مثل HTTP طراحی شوند.

دو زیرالگو از الگوی ترتیب موجود است. «الگوی موقعیت» شامل روش‌های پنهان‌سازی است که اطلاعات را تنها با موقعیت یک عنصر PDU خاص درون تعدادی از عناصر PDU دیگر، ارسال می‌کند. زیرالگوی دوم، «تعداد عناصر» است که اطلاعات را توسط تعداد عناصر در یک PDU (خردشده) کدگذاری می‌کند، برای مثال تعداد گزینه‌ها در سرآیند IPV4.

۲-۱-۳- افزودن تکرار به PDU ها: [۹]

«الگوی افزودن تکرار» فضایی را درون یک PDU مورد نظر و یا درون یک عنصر PDU مورد نظر ایجاد می‌کند. برای ایجاد چنین فضایی، بیت‌های تکراری به‌طور مصنوعی به داده ارسال‌شده اضافه می‌شوند و اطلاعات سرّی در این بیت‌های تکراری جاسازی می‌شوند. تعداد زیادی از روش‌های پنهان‌سازی به این الگو تعلق دارند.

۲-۱-۴- مقادیر تصادفی در PDU ها: [۹]

بسیاری از پروتکل‌های شبکه از فیلدهای PDU ای تشکیل‌شده‌اند که حاوی مقادیر (شبه) تصادفی هستند، برای مثال شماره رشته اولیه (ISN) برای اتصالات TCP تازه ایجادشده. این به افراد اجازه جاسازی محتوای نهان رمزشده‌ای را می‌دهد که توزیع مشابهی را نمایش می‌دهد.

۲-۱-۵- مدولاسیون مقدار در PDU ها: [۹]

این الگو شامل روش‌های پنهان‌سازی است که یک مقدار از n مقدار ممکنی که یک عنصر سرآیند می‌تواند شامل شود را انتخاب می‌کنند. برای مثال، یک فیلد دوبیتی ممکن است مجاز به داشتن مقادیر ۰۰، ۰۱ و ۱۱ باشد اما مجاز به داشتن مقدار ۱۰ نباشد و یک روش پنهان‌سازی اطلاعات سرّی را با استفاده از یکی از سه مقدار مجاز ارسال می‌کند. اجازه انتخاب n مقدار می‌تواند به دلایل متفاوتی باشد، مثل تعاریف مشخصات پروتکل یا محیط‌های شبکه‌ای داده‌شده. هم‌چنین می‌توان تصور کرد که یک فیلد ممکن است شامل تمامی مقادیری باشد که می‌تواند توسط تعداد بیت‌هایش نمایش داده شود اما تصادفی نشده و بنابراین، جزئی از الگوی افزایش تکرار نیست. دو زیرالگو از الگوی مدولاسیون مقدار وجود دارد. «الگوی حالت» از روش‌های پنهان‌سازی تشکیل شده است که حالت (بزرگ و یا کوچک بودن حروف) عناصر سرآیند متن خام را تغییر می‌دهند. «الگوی LSB» تنها کم‌ارزش‌ترین بیت (ها) را از فیلد سرآیند تغییر می‌دهد.

۲-۱-۶- بیت‌های کنار گذاشته شده/بلااستفاده در PDU ها: [۹]

آخرین الگوی ذخیره شامل روش‌های پنهان‌سازی است که از فیلدهای کنار گذاشته شده و یا بلااستفاده در PDU ها استفاده می‌کنند. این الگو در تعدادی از روش پنهان‌سازی استفاده شده است [۱۰]. هم‌چنین این الگو می‌تواند به‌عنوان یک الگوی بدیهی در نظر گرفته شود، چون فیلدهای کنار گذاشته شده/بلااستفاده معمولاً توسط پیاده‌سازی‌های پشته‌ای شبکه تفسیر نمی‌شوند.

[1] Payload
[2] Protocol Data Unit (PDU)

اگرچه، تغییرات فیلدهای کنار گذاشته شده و استفاده‌نشده منجر به یک شناسایی ساده و جلوگیری از روش‌های پنهان‌سازی مربوطه می‌شود.

۲-۲- پنهان کردن اطلاعات در زمان‌بندی پیام‌های پروتکل: [۹]

در این بخش، در مورد روش‌هایی که داده پنهان را در زمان‌بندی پیام‌های پروتکل کدگذاری می‌کنند و به‌عنوان کانال‌های نهان زمانی نیز از آن‌ها یاد می‌شود، بحث می‌شود.

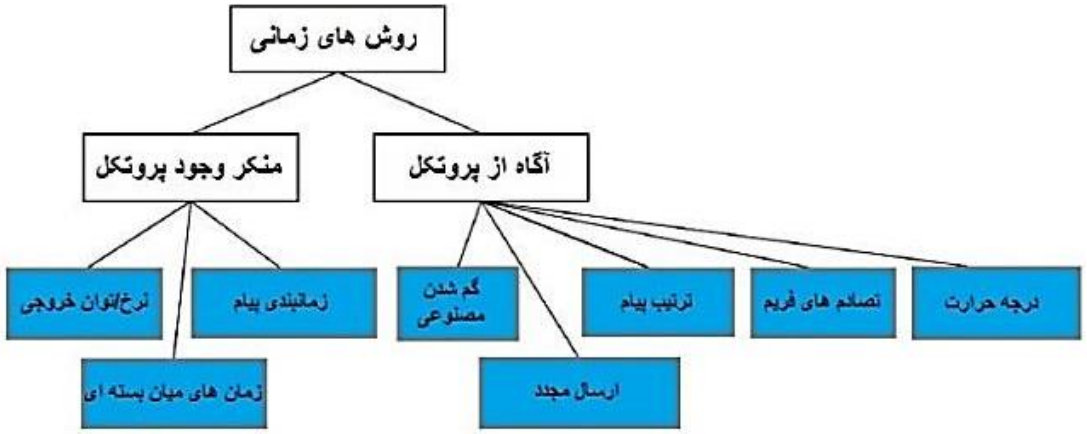
کانال‌های زمانی بر اساس نوع تأثیری که بر جریان ترافیک دیجیتال در شبکه دارند، به‌صورت کانال‌های فعال یا غیرفعال دسته‌بندی می‌شوند. کانال‌های نهان فعال نیاز به تزریق بسته‌ها برای ارسال نهان اطلاعات دارند. درحالی‌که کانال‌های نهان غیرفعال ترافیک بسته‌های موجود را مدوله می‌کنند [۱۱]. پیام‌های پروتکل می‌توانند به هر لایه‌ای از پشته پروتکل تعلق داشته باشند، برای مثال، می‌توانند فریم‌های لایه لینک، بسته‌های لایه شبکه یا پیام‌های پروتکل لایه کاربردی باشند.

کانال‌های زمانی همواره به‌دلیل بی‌دقتی‌های زمانی سمت فرستنده و گیرنده نهان، کانال‌هایی نویزدار هستند. ظرفیت کانال‌های زمانی اغلب کمتر از کانال‌های ذخیره بدون نویز است، اما شناسایی و حذف این کانال‌ها به‌طور بالقوه دشوارتر است.

برخی از کانال‌های زمانی منکر وجود پروتکل هستند، یعنی به ویژگی‌های پروتکل شبکه‌ای حامل بستگی ندارند درحالی‌که سایر کانال‌های زمانی آگاه از پروتکل هستند و به فیلدهای سرآیند خاص و قواعد معنایی پروتکل حامل بستگی دارند. شکل (۳)، انواع مختلفی از روش‌های زمانی را نشان می‌دهد.

۲-۲-۱- نرخ یا توان خروجی ترافیک شبکه: [۹]

اطلاعات نهان می‌تواند به روش منکر وجود پروتکل توسط نرخ‌های متغیر بسته کدگذاری شود که معادل با تغییر توان خروجی ترافیک شبکه است. فرستنده پیام در هر دوره زمانی، نرخ بسته را بین دو (کانال باینری) یا چند نرخ بسته تغییر می‌دهد. گیرنده پیام در هر دوره زمانی نرخ را اندازه‌گیری می‌کند و اطلاعات نهان را دیکد می‌کند. یک کانال باینری می‌تواند یک بیت را به ازای هر دوره زمانی ارسال کند، درحالی‌که یک کانال چند نرخی می‌تواند $\log_2 r$ بیت را به ازای هر دوره زمانی ارسال کند که r تعداد نرخ‌های مجزای بسته یا مقادیر توان خروجی است.



شکل (۳): طبقه‌بندی روش‌های زمانی نهان‌نگاری شبکه [۹]

۲-۲-۲- زمان‌های میان-بسته ای: [۹]

این کانال می‌تواند در لایه IP استفاده شود که در آن اطلاعات نهان در تأخیرهای میان-بسته‌های IP کدگذاری می‌شوند که فواصل میان-بسته‌ای نیز نامیده می‌شود. گیرنده پیام، اطلاعات را از زمان‌های میان ورودی بسته‌ها دیکد می‌کند.

برای افزایش پنهان بودن کانال برای برنامه‌هایی با زمان‌های میان بسته‌ای همبسته، یک روش کدگذاری اطلاعات نهان تنها در کم‌ارزش‌ترین بخش‌های فواصل میان بسته‌ای ترافیک موجود است.

این کار توزیع زمانی میان بسته‌ای و همبستگی ترافیک نرمال را با هزینه نرخ بیتی کاهش‌یافته کانال نهان، تقلید می‌کند.

درحالی‌که کانال‌های زمانی میان-بسته‌ای نیازی به هم‌زمانی دوره‌های زمانی ندارند، هم چنان از نویز ایجادشده به علت بی‌دقتی‌های زمانی در سمت فرستنده و گیرنده پیام و همچنین نویز ایجادشده به علت تأخیرهای بسته‌ای متغیر و گم‌شدن بسته‌ها، رنج می‌برند.

۲-۲-۳- زمان‌بندی ترتیب پیام: [۹]

اگرچه رویکرد کلی به ویژگی‌های پروتکل عمومی وابسته نیست اما پیاده‌سازی‌های واقعی به پیام‌های حقیقی مبادله‌شده پروتکل وابسته هستند.

زمان‌بندی تصدیق‌های پیام (ACKs) نیز می‌تواند برای ساخت کانال‌های نهان دست‌کاری شود. این کار هنگامی‌که یک موجودیت با امنیت پایین قصد ارسال داده را به یک موجودیت با امنیت بالا به‌طور قابل‌اطمینان دارد، تبدیل به یک مسئله مهم می‌شود. ازآنجایی‌که یک ارتباط قابل‌اطمینان موجودیت با امنیت بالا را ملزم به ارسال ACK برای داده دریافت شده می‌کند، زمان‌بندی ACK ها می‌تواند برای ارسال داده نهان مورد دست‌کاری قرار بگیرد.

۲-۲-۴- گم‌شدن مصنوعی پیام / بسته: [۹]

پاک‌شدگی‌های کانال (گم‌شدن پیام یا بسته) که به‌طور عمدی در سمت فرستنده ایجادشده است را می‌توان به‌عنوان کانال نهان استفاده کرد. این یک روش آگاه از پروتکل است چون نیاز به شماره‌های ترتیبی به ازای هر پیام / بسته دارد، بنابراین گیرنده می‌تواند گم‌شدگی را کشف کند. شماره‌های ترتیبی در پروتکل‌های موجود بسیاری وجود دارند. برای مثال، از شماره‌های ترتیبی TCP می‌توان استفاده کرد. اگر فرستنده IP، ID های متوالی ایجاد کند، می‌توان از فیلد ID استفاده کرد. هم‌چنین می‌توان از پروتکل‌های لایه کاربردی در صورت استفاده از شماره‌های ترتیبی استفاده کرد. این پاک‌شدگی‌ها با گم‌شدن مصنوعی پیام‌ها / بسته‌ها در طرف فرستنده ایجاد می‌شود.

کانال‌های گم‌شدن بسته از نویز زمان‌بندی رنج نمی‌برند اما بسته‌های گم‌شده و یا خارج از ترتیب ممکن است نویز ایجاد کنند و ظرفیت کانال را کاهش دهند.

۲-۲-۵- ارسال‌های مجدد مصنوعی: [۹]

یک روش پیشنهادشده، ارسال نهان داده از طریق IEEE 802.11 Wireless LAN ها با تکرار فریم‌هاست. فرستنده نهان فریم‌ها را برای اتصالات انتخاب‌شده به‌منظور بیت «یک» تکرار می‌کند و برای ارسال بیت «صفر» فریم‌ها را برای سایر اتصالات انتخاب‌شده تکرار می‌کند. فرستنده و گیرنده نهان باید از قبل بر ماتریسی که «اتصالات» را تعریف می‌کند (آدرس‌های MAC مبدأ و مقصد) و برای کدگذاری استفاده می‌شود و همچنین بر ماتریس کلیدی که کدگذاری صفر یا یک منطقی را برای هر تکرار مشخص می‌کند، توافق داشته باشند.

اگرچه، راه‌های دیگری نیز برای کدگذاری داده نهان در ارسال مجدد فریم‌ها، بسته‌ها یا پیام‌ها وجود دارد. برای مثال، درخواست‌های DNS انتخاب‌شده می‌توانند یک و یا دو بار برای کدگذاری یک بیت نهان به ازای هر درخواست ارسال شوند.

هم‌چنین کانال‌های نهان ترکیبی نیز وجود دارند که از گم‌شدن بسته‌ها و ارسال مجدد استفاده می‌کنند.

۲-۲-۶- ترتیب دست‌کاری‌شده پیام: [۹]

یک روش پیاده‌سازی این روش، تغییر ترتیب بسته‌های TCP است، چون هر بسته TCP یک شماره ترتیبی دارد. اگرچه، این روش را هم‌چنین می‌توان درصورتی‌که فیلد ID در IP مقادیر منحصربه‌فرد داشته باشد، با بسته‌های IP نیز پیاده‌سازی کرد. هم‌چنین می‌توان آن را با هر پروتکل لایه کاربردی که از شماره‌های ترتیبی استفاده می‌کند نیز پیاده‌سازی کرد. امکان دیگری که وجود دارد تغییر ترتیب بسته‌های IPSec AH و یا IPSec ESP است. کانال‌های تغییر ترتیب - مانند کانال‌های گم‌شدن بسته‌ها - از نویز ایجادشده به علت گم‌شدن یا تغییر ترتیب بسته‌ها/پیام‌ها رنج می‌برند.

۲-۲-۷- تصادم و زمان‌بندی فریم‌ها: [۹]

سازوکاری وجود دارد که اگر فریم‌ها در آن دچار تصادم شوند، یک سیگنال مسدودشدن ایجاد می‌شود و فرستنده‌ها برای یک مدت‌زمان تصادفی خود را کنار می‌کشند. فرستنده نهان به عمد بسته‌های کاربر دیگر را مسدود می‌کند. سپس از یک تأخیر عقب افتادن به اندازه صفر یا حداکثر مقدار استفاده می‌کند؛ بنابراین، همه فریم‌های ارسال‌شده توسط فرستنده نهان بسته‌های کاربر دیگر را هدایت کرده و یا آن‌ها را دچار تأخیر می‌کند که سبب ایجاد یک کانال نهان تصادم یک بیت به ازای فریم می‌شود. گیرنده می‌تواند با شناسایی تصادم و تحلیل ترتیب ورود فریم‌ها بعد از تصادم، اطلاعات را بازیابی کند.

برای بهبود کارایی پروتکل‌های دسترسی به رسانه مشترک، الگوریتم‌های جداسازی برای تقسیم مجموعه‌ای از فرستنده‌های دچار تصادم به زیرمجموعه‌های کوچک‌تر استفاده می‌شوند. سپس، این زیرمجموعه‌ها ارسال مجدد را به ترتیب انجام می‌دهند.

۲-۲-۸- کانال‌های نهان بر اساس درجه حرارت: [۹]

یک روش کدگذاری سیگنال اصلی با تخمین تغییرات در اختلاف ساعت است. این کانال نیاز به یک میزبان میانی دارد که ارسال و دریافت بسته‌ها را برای فرستنده و گیرنده نهان انجام دهد. این کانال از این حقیقت بهره می‌گیرد که دمای CPU به تعداد

پردازش درخواست‌های سرویس در واحد زمان بستگی دارد و انحراف ساعت یک سیستم میزبان نیز به دما وابسته است.

در سمت گیرنده، کانال نیاز به این دارد که میزبان میانی، پروتکلی را با مهرهای زمانی که از آن‌ها انحراف ساعت می‌تواند تخمین زده شود، پشتیبانی کند. گزینه‌های ممکن TCP، پیام‌های ICMP echo، HTTP یا سایر پروتکل‌های لایه کاربردی با مهر زمانی هستند.

فرستنده نهان درخواست‌هایی را به میزبان میانی ارسال می‌کند (بیت «یک») و یا سکوت می‌کند (بیت «صفر») که بنابراین سبب تغییر دما و به‌طور غیرمستقیم تغییر انحراف زمانی در میزبان میانی می‌شود. گیرنده نهان نمونه‌های ساعت را از پاسخ‌های میزبان میانی دریافت می‌کند (برای مثال، مهرهای زمانی HTTP در پاسخ به درخواست GET گیرنده نهان) و از آن‌ها برای تخمین انحراف ساعت در میزبان میانی استفاده می‌کند. با داشتن انحراف ساعت تخمین زده‌شده، گیرنده نهان می‌تواند بیت‌های نهان را استخراج کند.

۲-۳- روش‌های ترکیبی:

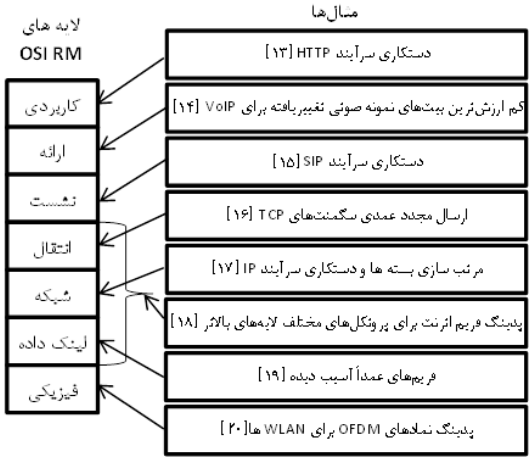
پیچیدگی روش‌های نهان‌نگاری شبکه در طول زمان به‌طور عمده به علت پروتکل‌ها و سرویس‌های شبکه با پیچیدگی زیاد در شبکه‌های ارتباطی، افزایش پیدا کرده است. راه‌حل‌های ترکیبی که روش‌هایی برای تغییر فیلدهای پروتکل و زمان‌بندی پیام‌های پروتکل هستند، تکاملی طبیعی از دو زیرگروه از روش‌های نهان‌نگاری شبکه که قبلاً به آن‌ها اشاره شده، هستند.

به‌طور معمول، یک روش غیرترکیبی نهان‌نگاری شبکه از یک زیر حامل واحد برای اهداف ارتباطی نهان استفاده می‌کند. روش‌های ترکیبی از هر دو روش زمان‌بندی و روش‌های ذخیره استفاده می‌کنند، بنابراین نیاز به دو زیرحامل دارند.

در بخش ۴، دو مثال از نهان‌نگاری شبکه ترکیبی که الگوی اشاره‌شده در بالا را دنبال می‌کنند، ارائه خواهد شد: LACK (نهان‌نگاری صوت ازدست‌رفته) و RSTEG (نهان‌نگاری ارسال مجدد).

۳- طبقه‌بندی روش‌های نهان‌نگاری بر اساس عملکرد پروتکل‌های لایه‌های OSI:

یکی دیگر از دسته‌بندی‌های روش‌های نهان‌نگاری شبکه، بر اساس عملکرد پروتکل‌های مرتبط به لایه‌های OSI RM است که در شکل (۴) نشان داده شده است [۱۲].



شکل (۴): دسته‌بندی روش‌های نهان‌نگاری شبکه بر اساس عملکرد پروتکل‌های مرتبط با لایه‌های OSI RM [۱۲]

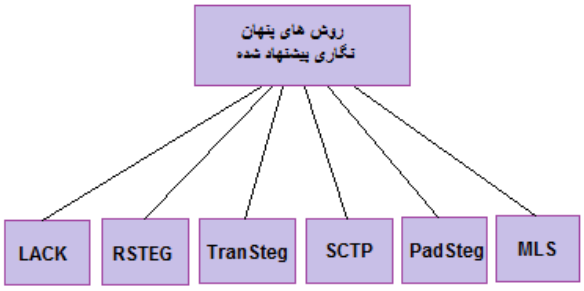
در لایه‌های فیزیکی و لینک داده، روش‌های نهان‌نگاری می‌توانند از ویژگی‌های فیزیکی کانال‌های ارتباطی بهره ببرند یا از نقص‌های آن‌ها استفاده کنند. برای مثال، روش WiPad برای لایه فیزیکی و روش HICCUPS برای لایه لینک داده.

روش‌های نهان‌نگاری شبکه هم‌چنین می‌توانند از تنظیم شکل پیام‌ها به نوع شبکه یا ابزارهای انتقال استفاده کنند. یک روش ارائه‌شده برای لایه شبکه، روش TranSteg برای IP تلفنی است که در بخش ۴ شرح داده خواهد شد. در لایه انتقال، همان‌طور که قبلاً ذکر شد روش RSTEG ارائه شده است. همچنین می‌توان از پروتکل SCTP در این لایه برای ارسال داده نهان استفاده کرد. این روش نیز در بخش ۴ شرح داده خواهد شد. در لایه نشست، استفاده از فیلدهای استفاده‌نشده از پروتکل SIP (پروتکل آغاز نشست) پیشنهاد شده است. در لایه ارائه، روش‌های متعددی پیشنهاد شده است که داده پنهان را در داده کاربر برای مثال با تغییر کم‌ارزش‌ترین بیت‌های سیگنال‌های دیجیتال – نمونه‌های صوت یا پیکسل‌های تصویر- جاسازی می‌کنند. در نهایت برای لایه کاربرد نیز روشی پیشنهاد شده است که داده پنهان را در تگ‌ها و سرآیندهای HTTP درج می‌کند [۱۲]. روش پیشنهادشده دیگر، Google Suggest است که از پروتکل‌های HTTP و TCP برای درج داده نهان استفاده می‌کند [۲۱].

نهان‌نگاری شبکه می‌تواند بیشتر از یک پروتکل استفاده کند، به‌طور خاص پروتکل‌هایی با بیشتر از یک‌لایه OSI RM. اصطلاح «نهان‌نگاری بین پروتکلی» برای این طبقه از روش‌های پیشنهاد شده است. PadSteg از پروتکل‌های ARP، TCP، UDP یا ICMP استفاده می‌کند که به‌عنوان پروتکل‌های حامل شناخته می‌شوند. این روش در بخش ۴ شرح داده خواهد شد.

۴- مرور جزئی تعدادی از روش‌های انتخابی نهان‌نگاری شبکه:

بعد از مرور دو دید مختلف موجود برای طبقه‌بندی روش‌های نهان‌نگاری شبکه در بخش ۲ و ۳، در این بخش، تعدادی از روش‌های نهان‌نگاری شبکه انتخاب شده و به‌صورت جزئی‌تر بررسی خواهند شد. فهرست روش‌های انتخابی در حوزه نهان‌نگاری شبکه در شکل (۵) نشان داده‌شده‌اند.



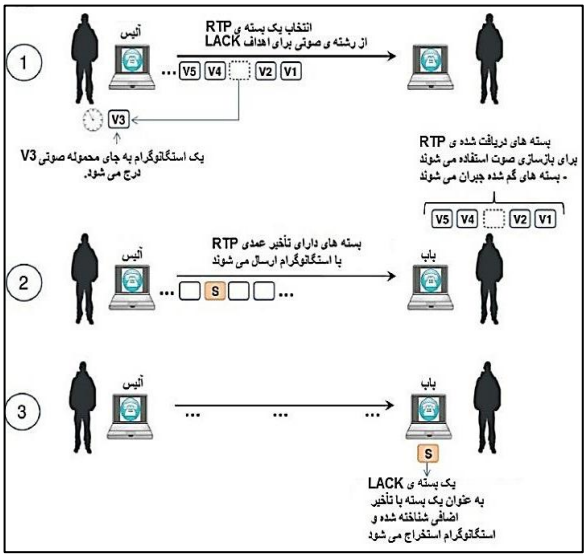
شکل (۵): روش‌های نهان‌نگاری انتخاب‌شده برای مرور جزئی‌تر

۴-۱- نهان‌نگاری بسته‌های صوتی ازدست‌رفته: [۱۹]

روش LACK ابتدا در سال ۲۰۰۸ پیشنهاد شد و سپس مورد مطالعه‌های بیشتری قرار گرفت [۲۵-۲۳]. این روش در حال حاضر به‌عنوان یکی از روش‌های نهان‌نگاری جدید VoIP در نظر گرفته می‌شود.

LACK یک روش نهان‌نگاری IP تلفنی است که بسته‌های RTP را از رشته صوتی و همچنین وابستگی‌های زمانی آن‌ها را تغییر می‌دهد. این روش از این حقیقت سود می‌برد که در پروتکل‌های ارتباطی چندرسانه‌ای معمول مانند RTP، بسته‌هایی با تأخیر اضافی برای بازسازی داده ارسال‌شده در سمت گیرنده استفاده نمی‌شود یعنی این بسته‌ها بلااستفاده در نظر گرفته شده و حذف می‌شوند.

یک مرور جزئی از LACK در شکل (۶) نشان داده‌شده است. در سمت ارسال‌کننده (آلیس)، یک بسته RTP از رشته صوتی انتخاب شده و محموله آن با بیت‌هایی از پیام سرّی جایگزین می‌شود (۱). سپس، بسته صوتی انتخاب‌شده، به‌طور عمدی دچار تأخیر در ارسال می‌شود (۲). هرگاه یک بسته با تأخیر اضافی به یک گیرنده ناآگاه از روند نهان‌نگاری می‌رسد، حذف می‌شود – یعنی به‌گونه‌ای با آن رفتار می‌شود که گویی هیچ‌گاه نرسیده است. اگرچه، اگر گیرنده (باب) از ارتباط نهان آگاه باشد، سپس به‌جای حذف بسته RTP دریافت شده، محموله آن را استخراج می‌کند (۳). محموله بسته‌هایی با تأخیر عمدی تنها حامل استفاده‌شده برای ارسال اطلاعات سرّی به گیرندگان آگاه از این روند است و هیچ بسته اضافی تولید نمی‌شود.



شکل (۶): ایده LACK [۹]

LACK یک رویکرد ترکیبی است چون از دو زیر حامل مختلف و در نتیجه دو روش پنهان‌سازی اطلاعات استفاده می‌کند: زمان‌بندی و ذخیره. روش زمانی برای انتخاب بسته RTP مناسب برای اهداف LACK استفاده می‌شود و روش ذخیره مسئول جاسازی داده سرّی در محموله بسته RTP انتخاب شده است.

کارایی LACK به عوامل زیادی وابسته است که می‌توان آن‌ها را به سه گروه زیر تقسیم کرد [۹]:

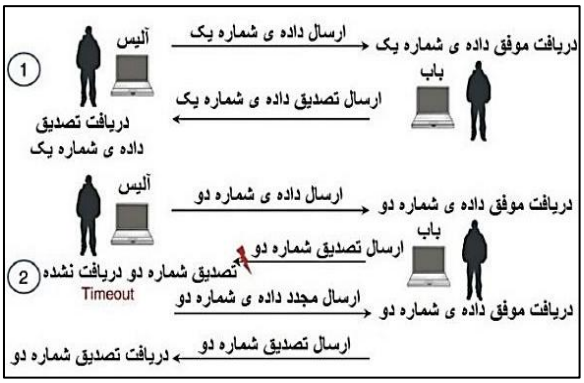
- عوامل مربوط به نقاط پایانی: نوع کدک صوتی استفاده‌شده (به‌طور خاص، مقاومت آن در برابر گم شدن بسته‌ها و کیفیت صوتی پیش‌فرض)، اندازه محموله بسته RTP و اندازه بافر Jitter.
- عوامل مربوط به شبکه: تأخیر بسته، احتمال گم شدن بسته و Jitter.
- عوامل مربوط به LACK: تعداد بسته‌های RTP با تأخیر عمدی، تأخیر بسته‌های LACK و نرخ درج داده نهان (IR) که مرتبط با تعداد بیت‌های داده سرّی حمل شده در واحد زمان است (بیت بر ثانیه).

۴-۲- نهان‌نگاری ارسال مجدد: [۱۶]

RSTEG در سال ۲۰۱۱ پیشنهاد داده شد و پس از آن توسعه داده شد [۲۶]. RSTEG می‌تواند برای تمامی پروتکل‌ها در لایه‌های مختلف OSI که از سازوکار عمومی ارسال مجدد استفاده

می‌کنند، مورداستفاده قرار بگیرد. هم‌چنین می‌تواند به سازوکارهای خاص TCP نیز اعمال شود، مثل FR/R (ارسال مجدد و بهبود سریع) یا SACK (تصدیق انتخابی).

در یک حالت ساده‌شده، یک پروتکل عمومی که از یک سازوکار ارسال مجدد بر اساس Timeout استفاده می‌کند، یک گیرنده را به تصدیق هر بسته دریافت‌شده وادار می‌کند (شکل (۷)، حالت ۱). هنگامی‌که بسته به‌طور موفقیت‌آمیز دریافت نشود، هیچ تصدیقی پس از منقضی شدن Timeout ارسال نمی‌شود و بنابراین بسته دوباره ارسال می‌شود (شکل (۷)، حالت ۲).



شکل (۷): سازوکار عمومی ارسال مجدد بر اساس Timeout [۹]

RSTEG از یک سازوکار ارسال مجدد برای تبادل قابل اطمینان داده سرّی استفاده می‌کند. فرستنده و گیرنده هردو از روند نهان‌نگاری آگاه هستند. در بعضی نقاط طی یک اتصال پس از دریافت موفق یک بسته، گیرنده به‌طور عمد یک پیام تصدیق را صادر نمی‌کند. در یک وضعیت نرمال، یک فرستنده هنگامی‌که فریم، زمانی که در آن یک تصدیق بسته باید دریافت شود منقضی می‌شود، مجبور به ارسال مجدد یک بسته گمشده است. در مفاد RSTEG، یک فرستنده به‌جای ارسال مجدد همان بسته، محموله اصلی را با داده سرّی عوض می‌کند. هنگامی‌که بسته مجدداً ارسال‌شده به گیرنده می‌رسد، او می‌تواند اطلاعات پنهان را استخراج کند (شکل (۸)، حالت ۳).

شکل (۸): مفهوم نهان‌نگاری ارسال مجدد [۹]

فرستنده و گیرنده داده پنهان ممکن است هردو با هم فرستنده و گیرنده ارتباط عمومی نباشند؛ در بعضی سناریوها، هردو ممکن است در محل گره‌های میانی شبکه واقع شده باشند. در این حالت، کشف ارتباط پنهان دشوارتر است چون موقعیت عمومی گره استفاده‌شده برای نهان‌کاوی نزدیک به فرستنده و گیرنده ارسال عمومی است.

مشابه LACK، RSTEG یک رویکرد ترکیبی است چون از یک روش زمانی برای نشان دادن بسته‌ای که باید مجدداً ارسال شود و از یک روش ذخیره برای جاسازی داده سرّی استفاده می‌کند؛ بنابراین، از دو زیرحامل استفاده شده است: یک زیرحامل سازوکار ارسال مجدد و دیگری محموله بسته انتخابی است.

کارایی RSTEG بستگی به عوامل متعددی دارد، مانند جزئیات روند ارتباطی (به‌طور خاص، اندازه محموله بسته، نرخی که با آن سگمنت‌ها تولید می‌شوند و ...).

ارسال‌های مجدد عمدی ایجادشده توسط RSTEG به‌منظور جلوگیری از شناسایی باید در یک سطح منطقی نگه‌داشته شوند. برای دست‌یابی به این هدف، تعیین تعداد میانگین ارسال‌های مجدد طبیعی در ترافیک اینترنت بر اساس TCP ضروری است.

۴-۳- روش TranSteg: [۲۷]

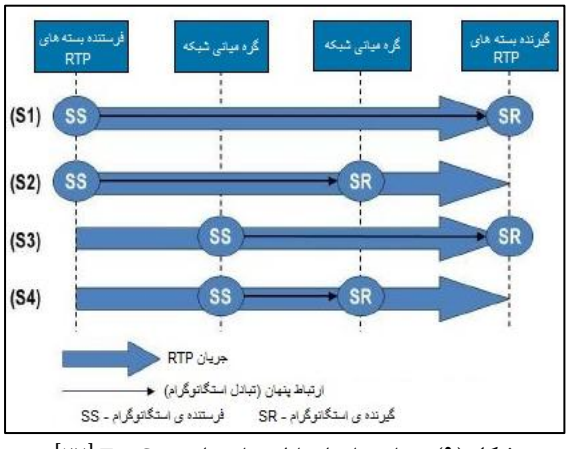
روش TranSteg توسعه‌ای از گروه روش‌های نهان‌نگاری برای VoIP است. در مقایسه با راه‌کارهای موجود، مزایای اصلی آن پهنای باند نهان‌نگاری بالا، هزینه نهان‌نگاری کم (یعنی کاهش اندکی از کیفیت صوتی) و شناسایی دشوار آن است. اگرچه مورد آخر به سناریوی ارتباط پنهان استفاده‌شده وابسته است. کارایی TransSteg به‌طور عمده بر مشخصات زوج کدک وابسته است: یکی که برای کدگذاری گفتگوی کاربر استفاده‌شده (کدک عمومی)، دیگری کدک استفاده‌شده برای تبدیل کد است (کدک نهان).

ذکر این نکته مهم است که بر اساس سناریوی ارتباط پنهان، TransSteg ممکن است بر انتخاب این کدک تأثیرگذار و یا بی‌تأثیر باشد. فرض این است که همواره یافتن یک کدک نهان به ازای هر کدک عمومی ممکن است. اگرچه، باید ذکر شود که برای کدک‌هایی با نرخ بیتی بسیار پایین، پهنای باند نهان‌نگاری باید محدود شود. در شرایط ایده‌آل کدک نهان باید کیفیت صوتی کاربر را (ایجادشده به علت عملیات تبدیل کد و تأخیرهای ایجادشده) در مقایسه با کیفیت کدک عمومی به‌طور قابل ملاحظه‌ای کاهش ندهد و کوچک‌ترین اندازه محموله صوتی قابل

دست‌یابی را ایجاد کند درحالی‌که بیشترین فضای خالی را در یک بسته RTP برای حمل استگانوگرام ایجاد می‌کند.

TranSteg می‌تواند در چهار سناریوی ارتباط پنهان نمایش داده‌شده در شکل (۹) مورد استفاده قرار بگیرد. اولین سناریو (S1 در شکل (۹)) رایج‌ترین و معمولاً مطلوب‌ترین سناریو است: فرستنده و گیرنده یک مکالمه VoIP را هدایت می‌کنند، درحالی‌که به‌طور هم‌زمان استگانوگرام‌ها را مبادله می‌کنند. مسیر مکالمه مشابه مسیر داده پنهان است. در سه سناریوی بعدی (S2-S4 در شکل (۹))، تنها بخشی از مسیر VoIP برای ارتباط پنهان مورد استفاده قرار می‌گیرد. به‌عنوان نتیجه‌ای از اقدامات انجام‌شده توسط گره‌های میانی، فرستنده و/یا گیرنده در اصل از تبادل داده نهان‌نگاری آگاه نیستند. کاربرد TranSteg در اتصالات IP تلفنی شانس محافظت از مکالمات کاربر را در کنار ارسال استگانوگرام‌ها ایجاد می‌کند. این قضیه به‌خصوص برای سناریوهای S2-S4 اهمیت دارد.

در سناریوهای اشاره‌شده، فرض بر این است که شناسایی بالقوه (پنهان‌شکنی) که معمولاً توسط یک نگهبان رخ می‌دهد، به علت مسائل حریم خصوصی مربوط به این قضیه قادر به حسابرسی گفتگوی حمل‌شده در بسته‌های RTP نخواهد بود؛ بنابراین، وجود یک استگانوگرام داخل محموله یک بسته RTP می‌تواند کشف‌نشده باقی بماند.



شکل (۹): سناریوهای ارتباط پنهان برای TranSteg [۲۷]

۴-۴- نهان‌نگاری با استفاده از پروتکل SCTP: [۲۸]

۴-۴-۱- نمای کلی پروتکل SCTP:

SCTP ، به‌منظور انتقال سیگنالینگ تلفنی روی شبکه‌های بر اساس IP مورداستفاده قرار می‌گیرد، مانند TCP انتقال داده را به‌صورت رشته‌ای و قابل‌اطمینان با کنترل ازدحام ممکن می‌کند و محدودیت‌های TCP را که در بسیاری از برنامه‌های کاربردی دشوار هستند را حذف می‌کند. هم‌چنین SCTP تحویل «ترتیب ورود» را نیز ممکن می‌سازد که به این معنی است که داده به‌محض دریافت به لایه بالاتر انتقال داده می‌شود. ارسال بدون ترتیب می‌تواند بر اساس نیاز برنامه‌های کاربردی برای تمامی پیام‌ها و یا بخشی از آن‌ها تنظیم شود. در SCTP، داده به‌صورت پیام‌های مجزای انتقال داده‌شده توسط لایه بالاتر ارسال می‌شود. این ویژگی توسعه برنامه‌های کاربردی بر اساس SCTP را نسبت به برنامه‌های بر اساس TCP ساده‌تر می‌کند.

هر اتصال SCTP، می‌تواند از یک یا تعداد بیشتری جریان استفاده کند که این جریان‌ها کانال‌های منطقی یک جهته‌ای میان نقاط پایانی SCTP هستند. تحویل «ترتیب ارسال» و یا «ترتیب ورود» داده میان هر جریان به‌طور جداگانه انجام می‌شود نه به‌صورت سراسری. اگر یکی از جریان‌ها مسدود شود، بر سایر جریان‌ها تأثیر نخواهد داشت. هم‌چنین از چند خانگی (Multi-homing) نیز پشتیبانی می‌شود.

۴-۴-۲- روش‌های نهان‌نگاری خاص SCTP:

روش‌های نهان‌نگاری خاص SCTP می‌توانند به سه گروه تقسیم شوند:

۱. روش‌هایی که محتوای بسته‌های SCTP را تغییر می‌دهند:

هر بسته SCTP شامل قطعات داده و کنترل است و هر قطعه می‌تواند شامل پارامترهای متغیری باشد. ۱۳ روش جدید نهان‌نگاری که محتوای بسته‌های SCTP را در قطعات و پارامترهای زیر تغییر می‌دهند، پیشنهاد شده است.

- قطعات INIT و INIT ACK: استفاده‌شده طی فعال‌سازی اتحاد SCTP (روش‌های I1، I2).
- قطعات DATA که شامل داده کاربر هستند (روش‌های D1، D2).
- قطعات SACK: استفاده‌شده برای تصدیق قطعات داده دریافتی (روش‌های S1 و S2).
- قطعات AUTH: استفاده‌شده برای احراز هویت قطعات (روش A1).
- قطعات PAD: استفاده‌شده برای بسته‌های pad (روش P1).
- پارامترهای متغیر: استفاده‌شده در قطعات خاص (روش VP1-5).

۲. روش‌هایی که چگونگی تبادل بسته‌های SCTP را تغییر می‌دهند:

- **چند خانگی:** SCTP اجازه چند خانگی را می‌دهد یعنی قابلیت اینکه میزبان از طریق بیشتر از یکی از آدرس‌های IP در شبکه قابل‌رؤیت باشد، برای مثال، اگر میزبان مجهز به تعدادی NIC (کارت‌های واسط شبکه) باشد. چند خانگی در SCTP برای ارسال داده با قابلیت اطمینان بیشتر استفاده می‌شود.
- **چند جریانی:** در SCTP، چند جریانی (برای تحویل با ترتیب) با استفاده از دو شناساگر به‌دست می‌آید: شناساگر جریان (SI)، برای علامت‌گذاری منحصربه‌فرد جریان و شماره ترتیبی جریان (SSN) برای اطمینان از ترتیب صحیح بسته‌ها در سمت گیرنده. باوجود این دو شناساگر، هر قطعه DATA هم‌چنین شامل شماره ترتیبی ارسال (TSN) است که به‌طور مستقل به هر قطعه تخصیص داده شده است.

۳. روش‌هایی که محتوای SCTP و چگونگی تبادل آن‌ها را تغییر می‌دهند (روش‌های ترکیبی):

برای SCTP، توسعه جزئی قابلیت اطمینان پیشنهاد داده شده است. این روش اجازه عدم ارسال مجدد داده مشخصی را برخلاف اینکه به‌طور موفق دریافت نشده است را می‌دهد. این کار از طریق قطعه FORWARD TSN (FT) امکان‌پذیر است که در آن TSN تصدیق جدید درج می‌شود. پس از دریافت چنین پیامی، سمت گیرنده با قطعات گمشده با TSN های مساوی یا کمتر به‌گونه‌ای رفتار می‌کند که گویی به‌درستی تحویل داده شده‌اند. این کارایی ممکن است برای اهداف نهان‌نگاری اتخاذ شود. ایده این روش مشابه LACK است.

۴-۵- روش PadSteg: [۱۸، ۲۹]

ابهامات موجود در استانداردسازی سبب ایجاد تفاوت‌هایی در پیاده‌سازی پدینگ در فریم‌های اترنت می‌شود. بعضی از سامانه‌ها عملیات پیاده‌سازی‌شده پدینگ را در سخت‌افزار کارت شبکه دارند (که پدینگ خودکار نامیده می‌شود)، سایر سامانه‌ها آن را در درایورهای نرم‌افزاری دستگاه و یا حتی در یک پشته لایه دوم جداگانه دارند.

به علت ناسازگاری محتوای پدینگ فریم‌های کوتاه اترنت (بیت‌های آن باید مقدار صفر داشته باشد اما در بسیاری از حالات این‌گونه نیست)، امکان پنهان‌سازی اطلاعات ایجاد می‌شود که از آن به‌عنوان آسیب‌پذیری EtherLeak یاد می‌شود. این قضیه دلیل این است که چرا استفاده از بیت‌های پدینگ به‌عنوان یک حامل استگانوگرام ممکن است [۱۸].

پدینگ می‌تواند در هر لایه از OSI RM یافت شود، اما معمولاً تنها از آن برای ارتباطات نهان در لایه لینک داده، شبکه و انتقال استفاده می‌شود. PadSteg ارتباط سرّی را در یک گروه پنهان در یک محیط LAN فعال می‌کند. در چنین گروهی، هر میزبانی که قصد تبادل استگانوگرام‌ها را دارد باید قادر به مکان‌یابی و شناسایی سایر میزبان‌های پنهان باشد. برای ایجاد چنین کارایی، سازوکارهای خاصی باید مشخص شوند. پروتکل ARP در کنار پدینگ فریم نامناسب اترنت برای محلی‌سازی و شناسایی اعضاء یک گروه پنهان استفاده می‌شود.ARP، آدرس لایه دوم (لینک داده) را برای یک آدرس لایه سوم (لایه شبکه) داده‌شده برمی‌گرداند. این کارایی با دو پیام درخواست و پاسخ به‌دست می‌آید. برای تبادل استگانوگرام‌ها، پدینگ فریم نامناسب اترنت در فریم‌هایی استفاده می‌شود که در لایه‌های بالاتر از پروتکل TCP استفاده می‌کنند. PadSteg از پروتکل‌های ARP و TCP برای کنترل گروه‌های پنهان و تبادل استگانوگرام‌ها استفاده می‌کند. عملیات PadSteg می‌تواند به دو فاز تقسیم شود:

- فاز اول: انتشار گره‌های پنهان
- فاز دوم: تبادل پنهان داده

فاز اول: این فاز بر اساس تبادل پیام‌های درخواست ARP با پدینگ نامناسب فریم اترنت است. گره پنهانی که قصد معرفی خودش به سایرین را در گروه دارد، یک پیام درخواست ARP را پخش می‌کند و رشته انتشار[1] را در بیت‌های پدینگ درج می‌کند که شامل یک عدد تصادفی غیر صفر و هش محاسبه‌شده بر اساس این عدد تصادفی و آدرس MAC مبدأ است.

تمامی گره‌های پنهان ملزم به تحلیل پدینگ تمامی درخواست‌های ARP دریافت‌شده هستند. اگر یک درخواست ARP با پدینگی که تماماً صفر نباشد دریافت شود، با استخراج عدد تصادفی تحلیل‌شده و هش مربوطه محاسبه می‌شود. اگر هش‌های دریافت‌شده و محاسبه‌شده مساوی باشند، به این معنی است که یک گره پنهان جدید برای تبادل نهان‌نگاری موجود است. هر گره پنهان یک لیست از گره‌هایی که اطلاع‌رسانی‌ها را از آن‌ها دریافت کرده، ذخیره می‌کند. هم‌چنین هر گره در دوره‌های زمانی مشخص درخواست‌های ARP را برای اطلاع سایرین از وجود خودش، مجدداً ارسال کند.

[1] advertising sequence

اتخاذ پیام‌های ARP برای شناسایی گره‌های پنهان جدید دو مزیت دارد:

- پیام‌های پخش‌شده توسط تمامی میزبان‌ها در LAN دریافت خواهد شد.
- ترافیک ARP درمجموع ۰٫۱٪ کل ترافیک است بنابراین این گزینه از دیدگاه کارایی نیز سودمند است. هر گره پنهان تنها نیاز به تحلیل درخواست‌های ARP دارد نه تمامی ترافیک.

فاز دوم: پس از شناسایی یک گره جدید، سایر گره‌های پنهان پدینگ فریم اترنت را در هر سگمنت TCP ارسال‌شده از آن آدرس MAC تحلیل می‌کنند. پدینگ سگمنت‌های TCP دریافت شده شامل بیت‌های استگانوگرام است.

ارسال دوطرفه به این صورت است که دو گره پنهان یک اتصال TCP عمومی را برای مثلاً ارسال یک فایل ایجاد می‌کنند. در طی یک اتصال، سگمنت‌های TCP ACK با پدینگ نامناسب فریم اترنت ارسال می‌شوند. سگمنت‌های TCP دریافت‌شده برای بررسی وجود پدینگ نامناسب اترنت تحلیل می‌شوند و داده سرّی استخراج می‌شود. برای یک ناظر سوم چنین ارتباطی مشابه یک ارسال داده عادی به نظر می‌رسد [۲۹].

۴-۶- نهان‌نگاری چند سطحی (MLS) :[۳۰]

نهان‌نگاری چند سطحی مفهومی جدید از پنهان‌سازی اطلاعات در شبکه‌های ارتباطی است که از ویژگی‌های یک روش نهان‌نگاری موجود (روش لایه بالاتر) برای ساخت یک روش جدید (روش لایه پایین‌تر) استفاده می‌کند. در نهان‌نگاری تک‌روشی شبکه، ترافیک ارتباطی آشکار به‌عنوان حاملی برای داده سرّی مورداستفاده قرار می‌گیرد.

MLS بر اساس حداقل دو روش نهان‌نگاری است. ابتدا، روش لایه بالاتر از ترافیک عمومی به‌عنوان حامل داده سرّی استفاده می‌کند. سپس، روش لایه پایین‌تر از طرز کار لایه بالاتر به‌عنوان حامل استفاده می‌کند. حامل‌های غیرمستقیم برای روش‌های لایه پایین‌تر همچنان بسته‌های ترافیک عمومی هستند، اما حامل مستقیم روش دیگری (سطح بالاتر) است.

در یک سناریوی عمومی‌تر، MLS ممکن است بر اساس بیشتر از دو روش نهان‌نگاری باشد؛ بنابراین، ممکن است در بیشتر از دو سطح ایجاد شود. در هر سطح ممکن است از بیشتر از یک روش نهان‌نگاری استفاده شود؛ اگرچه، این کار کیفیت حامل را به‌سرعت کاهش می‌دهد و بنابراین، سبب ساده‌سازی شناسایی می‌شود.

۴-۶-۱- ویژگی‌های MLS:

MLS در حالت کلی دو ویژگی مهم دارد. اولین ویژگی این است که پهنای باند روش سطح پایین‌تر کسری از پهنای باند روش سطح بالاتر است. این مشابه رابطه میان پهنای باند ارتباط آشکار و پهنای باند نهان‌نگاری سطح بالاتر است. هرقدر تکرار و پیچیدگی در ارتباط آشکار بیشتر باشد، داده پنهان بیشتری می‌تواند درج‌شده و به‌طور نهان مبادله شود.

دومین ویژگی این است که شناسایی روش سطح پایین‌تر دشوارتر از شناسایی روش سطح بالاتر است. این واقعیت از این حقیقت نتیجه شده است که کارکرد روش سطح پایین‌تر به‌طور کامل وابسته به روش سطح بالاتر است؛ بنابراین، فرد نفوذگر به‌منظور جستجوی روش سطح پایین‌تر، ابتدا باید روش سطح بالاتر را شناسایی کند. علاوه بر این، قابلیت کشف نشدن MLS بسته به انتخاب روش‌های سطح بالاتر و پایین‌تر، ممکن است مشابه، بیشتر یا کمتر از حالتی باشد که تنها از روش سطح بالاتر استفاده شود.

۴-۶-۲- کاربردهای MLS:

MLS می‌تواند برای رسیدن به اهداف بسیاری مورداستفاده قرار گیرد و همه این‌ها بستگی به چگونگی استفاده از آن دارد. مزایای MLS برای تبادل داده پنهان در جدول (۱) خلاصه‌شده است.

۵- مقایسه کلی روش‌های نهان‌نگاری:

اگرچه واضح‌ترین هدف نهان‌نگاری، پنهان‌سازی داده است، پارامترهای مرتبط دیگری نیز برای قضاوت در مورد قدرت نهان‌نگاری یک روش مورد استفاده قرار می‌گیرند. هر روش نهان‌نگاری مجموعه‌ای از ویژگی‌ها و اهداف دارد و می‌توان روش‌ها را به‌طورکلی از نظر مزایا و معایب مقایسه کرد.

هر روش نهان‌نگاری شبکه‌ای مجموعه ویژگی‌های زیر را دارد [۳۱]:

- پهنای باند نهان‌نگاری: اصطلاح «پهنای باند نهان‌نگاری» اشاره به حجم داده پنهانی دارد که می‌تواند در واحد زمان هنگام استفاده از یک روش خاص، ارسال شود.
- عدم تشخیص تمایز: این ویژگی به‌عنوان عدم توانایی در کشف یک استگانوگرام درون یک حامل خاص تعریف

می‌شود. رایج‌ترین روش کشف یک استگانوگرام، تحلیل ویژگی‌های آماری داده ضبط‌شده و مقایسه آن‌ها با مقادیر رایج برای آن حامل است.

- مقاومت (Robustness): این ویژگی به‌عنوان حجمی از تغییرات تعریف می‌شود که یک استگانوگرام می‌تواند بدون تخریب داده سرّی آن را تحمل کند. یک روش نهان‌نگاری خوب باید در کنار داشتن مقاومت و دشواری شناسایی، بیشترین پهنای باند ممکن را ارائه کند.

علاوه بر این، محاسبه هزینه نهان‌نگاری نیز سودمند است. در جدول (۲)، روش‌های نهان‌نگاری به‌طورکلی از نظر مزایا و معایب و در جدول (۳)، از نظر معیارهای ارزیابی ظرفیت، عدم تشخیص تمایز و مقاومت با یکدیگر مقایسه شده‌اند.

جدول (۱): مزایا و کاربردهای ممکن MLS [۳۰]

کاربرد توصیف‌شده MLS	مزیت MLS
استفاده از دو یا تعداد بیشتری روش نهان‌نگاری پهنای باند کلی به‌دست‌آمده برای داده کاربر را در مقایسه با یک روش نهان‌نگاری افزایش می‌دهد.	پهنای باند نهان‌نگاری افزایش‌یافته برای داده کاربر
یک روش سطح بالاتر کنترل‌شده با اطلاعات حمل‌شده توسط روش سطح پایین‌تر	قابلیت کشف‌نشدن افزایش‌یافته
روش سطح پایین‌تر حمل‌کننده اطلاعات برای تأیید جامعیت استگانوگرام	قابلیت اطمینان ارسال استگانوگرام
۱. کلید رمزنگاری حمل شده توسط روش سطح پایین‌تر و استگانوگرام روش سطح بالاتر رمزشده ۲. بخش‌هایی از استگانوگرام با استفاده از روش سطح بالاتر ارسال‌شده و سایر بخش‌ها با استفاده از روش سطح پایین‌تر ارسال‌شده است ۳. استگانوگرام تنها توسط روش سطح پایین‌تر حمل شده؛ استگانوگرام سطح بالاتر تنها برای پوشاندن است	استخراج و تحلیل دشوارتر استگانوگرام
در سناریوی بهترین حالت، به روش‌های سطح بالاتر و پایین‌تر استفاده‌شده بستگی دارد اما می‌تواند مشابه استفاده روش سطح بالاتر به‌تنهایی باشد	هزینه بدون تغییر نهان‌نگاری

جدول (۲): مقایسه روش‌های نهان‌نگاری از نظر مزایا و معایب [۲]

روش	مزایا	معایب
تغییر PDU/PCI	• پهنای باند نهان‌نگاری بالا • پیاده‌سازی آسان • عدم نیاز به هم‌زمان‌سازی فرستنده-گیرنده	• از دست رفتن بالقوه بعضی از کارکردهای پروتکل • شناسایی آسان
تغییر PDU/SDU	• شناسایی دشوارتر نسبت به روش PDU/PCI • عدم نیاز به هم‌زمان‌سازی • پهنای باند بالا • شناسایی دشوار	• پهنای باند کمتر نسبت به روش PDU/PCI • پیاده‌سازی دشوارتر نسبت به روش PDU/PCI • احتمال از دست رفتن داده کاربر
تغییر ترکیبی/PDU	• پهنای باند بالا • شناسایی دشوار • عدم نیاز به هم‌زمان‌سازی	• پیاده‌سازی دشوارتر نسبت به روش‌های PDU/PCI و PDU/SDU • احتمال افزایش نرخ خطای ارسال
تغییر روابط زمانی میان PDU ها	• پیاده‌سازی آسان • شناسایی دشوار	• پهنای باند بسیار کم • نیاز به هم‌زمان‌سازی فرستنده-گیرنده • تأخیرهای ارسال افزایش‌یافته
ترکیبی	• پهنای باند بالا • شناسایی دشوار • عدم نیاز به هم‌زمان‌سازی • پیاده‌سازی آسان	• احتمال از دست رفتن داده کاربر

جدول (۳): مقایسه روش‌های نهان‌نگاری ازنظر معیارهای ارزیابی

روش	ظرفیت	عدم تشخیص تمایز	مقاومت
تغییر PDU/PCI	بالا	پایین	بالا
تغییر PDU/SDU	بالا	بالا	پایین
تغییر ترکیبی/PDU	بالا	بالا	پایین
تغییر روابط زمانی میان PDU ها	پایین	بالا	بالا
ترکیبی	بالا	بالا	پایین

۶- نتیجه‌گیری

در این مقاله ابتدا خلاصه‌ای از مفهوم نهان‌نگاری شبکه ارائه‌شده است و سپس طبقه‌بندی روش‌های گوناگون در این حوزه با دو دید مختلف بررسی شد. در دید اول روش‌های نهان‌سازی اطلاعات به سه دسته تغییر فیلدهای پروتکل، زمان‌بندی پیام‌های پروتکل یا ترکیب آن‌ها تقسیم شدند و دید دوم طبقه‌بندی را بر اساس عملکرد پروتکل لایه‌های OSI RM انجام داد. سپس در مورد روش‌های پیشنهادشده برای هر روش بحث شد و درنهایت مقایسه کلی روش‌ها ازنظر مزایا و معایب و مقایسه آن‌ها از نظر معیارهای ارزیابی ظرفیت، عدم تشخیص تمایز و مقاومت ارائه شد. با توجه به عدم انجام تحقیقات جامع و خوب برای شناسایی مناسب‌ترین روش‌ها بر اساس پارامترهای مختلف، این موضوع برای تحقیقات آتی مناسب است.

۷- منابع

1. H. Sajedi and Sh. R. Yaghoubi, "Review on Steganographic Methods in Texts," 2018. (In Persian)
2. A. Stančić, I. Grgurevic, and V. Vyroubal, "Usage of the Steganography within Highway Information and Communication Network," 4th International Virtual Research Conference In Technical Disciplines (RCITD 2016), Slovakia, 2016.
3. J. Zhai, M. Wang, G. Liu, and Y. Dai, "SkyLen: a Skype-Based Length Covert Channel," Journal of Information Hiding and Multimedia Signal Processing, vol. 6, no. 3, May 2015.
4. B. G. Banik and S. K. Bandyopadhyay, "Review on Steganography in Digital Media," International Journal of Science and Research (IJSR), vol. 4, pp. 1-10, 2015.
5. M. M. Pontón Loaiza, "Steganography using RTP Packets," University of Abertay Dundee, Dundee, September 2014.
6. A. P. Dhamade and K. J. Panchal, "Packet Data Based Network Steganography," International Journal of Advance Engineering and Research Development, vol. 2, no. 5, pp. 1520-1526, May 2015.
7. A. NoorAzar, Z. Norouzi, and M. Mir, "Representing an Enhanced Method based on Image Steganography based on Linear Codes Features," Journal of Electronic and Cyber Defence, vol. 5, no. 4, pp. 43-53, 2018. (In Persian)
8. V. Sabeti, Sh, Samavi, and M. R. Ahmadzadeh, "Steganalysis of the Steganographic Method based on Pixels Value Differencing in Random Intervals using Neural Networks," 14th National Conference of Computer Society of Iran, March 2009. (In Persian)
9. W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, and K. Szczypiorski, "Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures," IEEE Press Series on Information & Communication Networks Security, 2016.
10. S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-Based Survey and Categorization of Network Covert Channel Techniques," ACM Computing Surveys (CSUR), vol. 47, no. 3, pp. 50-77, 2015.
11. J. P. Black, "Techniques of Network Steganography and Covert Channels", Sciences, 2013.
12. J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and Overview of Network Steganography," IEEE Communications Magazine, vol. 52, no. 5, pp. 225-229, 2014.
13. M. Van Horenbeeck, "Deception on the Network: Thinking Differently About Covert Channels," Proc. 7th Australian Info, Warfare and Security Conf., 2006.
14. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," IBM. System Journal, vol. 35, no. 3, pp. 313–336, 1996.
15. W. Mazurczyk and K. Szczypiorski, "Covert Channels in SIP for VoIP signaling," Proc. of 4th International Conference on Global E-security, United Kingdom, pp. 65-72, June 2008.
16. W. Mazurczyk, M. Smolarczyk, and K. Szczypiorski. "Retransmission steganography and its detection," Soft Computing, vol. 15, no. 3, pp. 505-515, 2011.
17. D. Kundur and K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Wksp. Security of Information Systems, 2003.
18. B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "PadSteg: Introducing Inter-Protocol Steganography," Telecommunication Systems, vol. 52, no. 2, pp. 1101-1111, 2013.
19. K. Szczypiorski, "Steganography in TCP/IP Networks," State of the Art and a Proposal of a New System – HICCUPS, Institute of Telecommunications' seminar, Warsaw University of Technology, Poland, November 2003.
20. K. Szczypiorski and W. Mazurczyk, "Steganography in IEEE 802.11 OFDM Symbols," International Journal of Security and Communication Networks, vol. 3, no. 2, pp. 118-129, 2011.

21. P. Bialczak, W. Mazurczyk, and K. Szczypiorski, “Sending Hidden Data via Google Suggest,” 2011.

22. W. Mazurczyk and K. Szczypiorski, “Steganography of VoIP streams”, OTM Confederated International Conferences, On the Move to Meaningful Internet Systems, pp. 1001-1018. Springer, Berlin, 2008.

23. W. Mazurczyk and J. Lubacz, “LACK: a VoIP steganographic method,” Telecommunication Systems: Modelling, Analysis, Design and Management, vol. 45, no. 2, pp. 153-163, 2010.

24. W. Mazurczyk, J. Lubacz, and K. Szczypiorski. “On steganography in lost audio packets,” International Journal of Security and Communication Networks, vol. 7, no. 12, pp. 2602-2615, 2014.

25. W. Mazurczyk, “Lost audio packets steganography: a first practical evaluation,” International Journal of Security and Communication Networks, vol. 5, no. 12, pp. 1394-1403, 2012.

26. W. Mazurczyk, M. Smolarczyk, and K. Szczypiorski. “On information hiding in retransmissions,” Telecommunication Systems, vol. 52, no. 2, pp. 1113-1121, 2013.

27. W. Mazurczyk, P. Szaga, and K. Szczypiorski, “Using Transcoding for Hidden Communication in IP Telephony,” Multimedia Tools and Applications, vol. 70, no. 3, pp. 2139-2165, 2014.

28. W. Fraczek, W. Mazurczyk, and K. Szczypiorski, “Stream Control Transmission Steganography,” arXiv preprint arXiv: 1006.0247, 2010.

29. B. Jankowski, W. Mazurczyk, and K. Szczypiorski, “Information Hiding Using Improper Frame Padding,” Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International. IEEE, 2010.

30. W. Fraczek, W. Mazurczyk, and K. Szczypiorski, “Multi-Level Steganography: Improving Hidden Communication in Networks,” Journal of Universal Computer Science (J. UCS), Journal of Universal Computer Science (J. UCS), vol. 18, no. 14, pp. 1967-1986, 2012.

31. S. Ghanbari, N. Ghanbari, M. Keshtgari, and H. N. Karizi, “Steganalyisis in Images using Co-occurrence Matrix and Neural Networks,” Iranian Journal of Electrical and Computer Engineering, vol. 9, no. 3, 2012. (In Persian)

Review and Comparison of Network Steganography Methods Based On Different Classifications

M. Shoaei, V. Sabeti*

Abstract

The growth of Internet and computer networks has led to the ease of information transfer. This development has also caused some problems due to the fact that in network environments, data may be snooped while transferring from the sender to the receiver. So, it is always necessary to provide information security and in order to achieve this goal, steganography plays an important role. Network steganography is a method that uses network protocols. Many techniques for network steganography have been suggested up to this time so that familiarity with different algorithms, as well as recognizing the advantages and disadvantages of each of them, are required for researchers in this field who wish to introduce a new approach to steganography or to propose a new method of steganalysis. In this paper, it has been attempted to describe the various ideas behind network steganography methods in terms of two different classifications, and the result of the research have been presented. Although it would be ideal to devise a method which satisfies the three steganography evaluation criteria: capacity, undetectability and robustness simultaneously, but bearing in mind the conflict between them, a method can be proposed for each application which excels in the criterion that is most relevant in that application.

Key Words: *Vulnerability, Infrastructure, Passive Defense, West Azerbaijan province*

* Alzahra University (v.sabeti@alzahra.ac.ir) - Writer-in-Charge