نشریه علمی پدافند غیرعامل

سال یازدهم، شماره ۱، بهار ۱۳۹۹، (پیاپی ۴۱): صص ۹-۱

علمی- ترویجی

نهان‌نگاری VoIP کاربردها و چالش‌ها

زین‌العابدین نوروزی [۱*]، رستم رستمی [۲]، شهاب امجدیان [۳]

تاریخ دریافت:۱۳۹۷/۱۰/۲۳

تاریخ پذیرش: ۱۳۹۸/۰۵/۱۶

چکیده

نهان‌نگاری روی بستر VoIP یک روش نهان‌نگاری شبکه به‌صورت بی‌درنگ می‌باشد که از پروتکل‌های VoIP به‌عنوان کانال پوششی برای پنهان کردن پیام استفاده می‌کند. در حال حاضر، نهان‌نگاری بی‌درنگ یکی از چالش‌برانگیزترین زمینه‌های تحقیقاتی است. علت این امر ویژگی‌های ذاتی انتقال اطلاعات به‌صورت بی‌درنگ است که منجر به محدود شدن انجام عملیات پیچیده می‌شود. ما در این مقاله ابتدا به معرفی نهان‌نگاری پرداخته، در ادامه مفهوم VoIP را به‌طور مختصر توضیح داده و سپس برخی از کارهای اساسی که در این زمینه انجام‌شده، شرح داده می‌شود. نحوه عملکرد VoIP و مشکلاتی که با آن مواجه هستیم را بیان و چالش‌های موجود در نهان‌نگاری VoIP را مطرح و شرح داده می‌شود. در انتها برخی از روش‌های پرکاربرد نهان‌نگاری VoIP را معرفی نموده و سپس روش‌های مختلف نهان‌نگاری VoIP را با یکدیگر مقایسه نموده و نقاط ضعف و قوت هر یک بیان می‌شود. در بخش پایانی این مقاله به نتایج این تحقیق در خصوص چالش‌ها پرداخته شده است.

کلیدواژه‌ها: نهان‌نگاری، نهان‌نگاری VoIP، کانال پنهان، کانال پوششی

۱- دانشیار دانشگاه جامع امام حسین (ع)، (znorozi@ihu.ac.ir)- نویسنده مسئول

۲- دانشجوی کارشناسی ارشد، دانشگاه امام حسین(ع)

۳- دانشجوی کارشناسی ارشد، دانشگاه امام حسین(ع)

۱. مقدمه

نهان‌نگاری از دو واژه یونانی steganos به‌معنی پوشیده و graphie به‌معنی نوشتن گرفته شده است. نهان‌نگاری هنر پنهان کردن اطلاعات در یک رسانه میزبان مانند صوت، تصویر، ویدئو، متن و غیره است، بدون این‌که تخریب قابل درکی در رسانه‌میزبان پدید آید. امروزه استفاده از روش‌های نهان‌نگاری داده، فصل جدیدی در مخابره امن اطلاعات به‌وجود آورده است. اگرچه نهان‌نگاری هنری قدیمی است، ولی با ظهور داده‌های رقمی، شکلی کاملاً جدید به‌خود گرفته است. برای افزایش امنیت می‌توان ارتباطات خاص را مخفی نمود. یک متن رمز شده به‌طور قطع توجه دیگران را جلب می‌کند، درحالی‌که یک پیام که به‌صورت نامرئی به‌وسیله یک روش نهان‌نگاری در یک شی پنهان‌شده است، توجه دیگران را جلب نخواهد کرد [۱].

VoIP که بانام IP[1] تلفنی نیز از آن یاد می‌شود، امکان استفاده از شبکه برای مکالمات تلفنی را فراهم می‌نماید. در مقابل استفاده از خطوط تلفن سنتی، VoIP از فناوری رقمی استفاده می‌نماید و نیازمند یک اتصال پهن‌باند است. بدین ترتیب به‌جای آن‌که صدا به‌صورت آنالوگ و از طریق ارتباطات مخابراتی انتقال یابد، به‌صورت رقمی و از طریق شبکه IP منتقل می‌شود، از این‌رو، استفاده از VoIP هزینه بسیار کم‌تری نسبت به تماس‌های معمولی خواهد داشت. درواقع با استفاده از فناوری VoIP صدای انسان توسط بسته‌های اطلاعاتی IP و از طریق شبکه ارسال می‌گردد.

ساختار این مقاله در قالب ۵ بخش تدوین گردیده است. در بخش دوم این مقاله، مروری بر کارهایی که در این زمینه انجام‌شده پرداخته می‌شود. در بخش سوم سامانه VoIP را بیان داشته و در بخش چهارم نهان‌نگاری VoIP به‌طور اجمال مورد بررسی قرار خواهد گرفت. در بخش پایانی، جمع‌بندی از مباحث انجام‌شده، ارائه شده است.

۲. مروری بر کارهای انجام‌شده

در سال ۲۰۰۳ یک روش نهان‌نگاری VoIP با استفاده از سیگنال‌های‌صوتی رقمی به‌عنوان یک حامل داده‌پنهان توسط آئوکی پیشنهاد شد. در این مدل از روش LSB[2] برای جایگذاری داده محرمانه در سیگنال صوت رقمی استفاده شد، سپس روش PLC[3] (پنهان‌سازی بسته گم‌شده) که برپایه فشرده‌سازی G.711 بود، ارائه شد. پس از آن، روش PLC بهبود یافت و توسط دیتمن و همکاران، در سال ۲۰۰۵ اولین اجرای نمونه اولیه نهان‌نگاری‌های VoIP ارائه شد که از روش LSB استفاده نموده و توسعه این تحقیق در سال ۲۰۰۶ منتشر شد[۲].

وو و یانگ ثابت کردند، که می‌توان در عمل از یک ارتباطات VoIP معمولی برای اهداف نهان‌نگاری استفاده کرد. آن‌ها طرحی سازگار با LSB برپایه فشرده‌سازی G.711 توصیف کردند که برای برآورد تعداد بیت با کم‌ترین ارزش در هر نمونه صدا به‌کار می‌رود که این بیت‌ها به‌عنوان یک حامل داده‌های پنهان می‌باشند. نتایج نشان داد که این روش بهتر از LSB ساده انجام می‌شود و پهنای باند نهان‌نگاری بالاتر بوده و کیفیت صدا افت کم‌تری را دارد[۳].

تیان و همکاران، یک رویکرد نهان‌نگاری تطبیقی نسبی قابل تنظیم (APMS[4]) ارائه دادند. آن‌ها یک مقیاس اندازه‌گیری (PSV[5]) برای ارزیابی تطبیق نسبی بین پیام‌های آشکار و پنهان معرفی کردند. این روش یک تعادل تطبیقی بین شفافیت نهان‌نگاره و پهنای باند را نشان می‌دهد. علاوه‌بر این، آن‌ها از توالی سه‌جزئی برای از بین بردن وابستگی بین پیام‌های پنهان، فرایند تعبیه تطبیقی و نمونه سیگنالینگ سنکرون رمزگذاری شده، استفاده نمودند [۴].

پروتکل‌های ویژه VoIP اولین بار توسط مازورکزیک و کوتولسکی در سال ۲۰۰۶، به‌عنوان یک حامل برای نهان‌نگاری ارائه شدند. آن‌ها بسته‌های استفاده‌نشده در سرآیند پروتکل‌های RTP را برای نهان‌نگاری اطلاعات محرمانه، پیشنهاد دادند. اطلاعات ضروری در بسته‌های استفاده‌نشده در سرآیند[6] پروتکل‌های RTP، UDP[7]، IP و هم‌چنین در صدای انتقالی، جاسازی‌شده بود [۵]. سپس آن‌ها روی طرح بیش‌تر کارکرده و یک کارکرد RTCP[8] بدون نیاز به استفاده از یک پروتکل جداگانه را ایجاد کردند. درنتیجه، در پهنای باند مورد استفاده توسط اتصال VoIP صرفه‌جویی گردید [۶].

فوفانگ و همکاران بر اساس ویژگی‌های مشخصه کدک، یک روش نهان‌نگاری را با استفاده از موقعیت‌های پالس کدک گفتار G723.1 ارائه داده‌اند [۷].

سابین اشمیت و همکاران به بررسی نحوه ایجاد یک کانال مخفی در مکالمه‌های VoIP پرداختند. همچنین آن‌ها یک روشی را برای جاسازی اطلاعات در بسته‌های سکوت ارائه داده به‌طوری‌که اطلاعات مخفی را در بسته‌های جعلی RTP که در فواصل سکوت تولید می‌شوند، مخفی نمودند [۸].

شروق عبدالرحیم و همکاران یک روش نهان‌نگاری

1- Internet Protocol
2- Least Significant Bit
3- Packet Loss Concealment

4- Adaptive partial-matching steganography
5- Partial Similarity Value
6- Header
7- User Datagram Protocol
8- Real-time Transport Control Protocol

چندلایه‌ای ارائه کردند تا امنیت پیام‌های خاص را با انجام سه مرحله امنیتی پیچیده افزایش دهند. آن‌ها صوت انتخاب‌شده را درون تصویر RGB جاسازی کردند و سپس تصویر را درون یک سیگنال صوتی پنهان کرده و تمامیت داده را با استفاده از پروتکل بی‌درنگ (RTP) انجام دادند. آن‌ها ادعا کردند در الگوریتم پیشنهادی، شنودگران قادر نخواهند بود فرآیند امنیتی چندلایه‌ای آن‌ها را بشکنند. آن‌ها یک روش نهان‌نگاری VoIP را برای مخفی کردن اطلاعات صوتی درون تصویر پیشنهاد دادند [۹].

اصفهانی و همکاران، روشی را برای نهان‌نگاری روی پروتکل VoIP ارائه کردند. آن‌ها با استفاده از روش تسهیم راز آستانه‌ای (k,n) و با اعمال آن به روش نهان‌نگاری LACK[1]، تحمل‌پذیری خطا و قابلیت اطمینان را افزایش دادند. روش پیشنهادی آن‌ها در مقابل حملات نهان‌کاوی بسیار مقاوم است [۱۰].

VoIP که بانام IP تلفنی نیز از آن یاد می‌شود، امکان استفاده از شبکه برای مکالمات تلفنی را فراهم می‌نماید.

۳. نحوه عملکرد و مشکلات VoIP

VoIP که بانام IP تلفنی نیز از آن یاد می‌شود، امکان استفاده از شبکه برای مکالمات تلفنی را فراهم می‌نماید.

۳-۱. نحوه عملکرد VoIP

مراحل انجام این‌کار عبارت است از:

گام اول: سیگنال‌های صوت آنالوگ با استفاده از یک مبدل آنالوگ به رقمی، رقمی می‌شوند. سیگنال‌های صوتی رقمی شده در مقابل نویز ایمن‌تر هستند.

گام دوم: داده‌های رقمی به بسته‌هایی تقسیم‌شده و سازوکارهای پشتیبانی بی‌درنگ و تحویل به‌موقع بسته‌ها باید انجام شود. که این سازوکارها توسط پروتکل‌های سیگنالینگ برای ایجاد لینک‌های ارتباطی بین تلفن‌ها موردنیاز به‌کار گرفته می‌شوند.

گام سوم: بسته‌ها دریافت می‌شوند و داده‌های رقمی بازسازی می‌شوند. داده‌های رقمی ابتدا از حالت فشرده خارج‌شده، سپس توسط یک مبدل رقمی به آنالوگ، به سیگنال صوتی تبدیل می‌شوند [۱۱].

۳-۲. مهم‌ترین مشکلات VoIP

مهم‌ترین مشکلات ناشی از شبکه در ارتباطات تلفنی مبتنی‌بر VoIP عبارت است از:

أ- **تأخیر:** حد فاصل زمانی ارسال تا دریافت بسته‌های صوتی است که در صورت فرا رفتن از یک‌میزان مشخص، امکان تشخیص مکالمات را دشوار می‌کند.

ب- **نوسانات تأخیر:** نوسان در زمان انتقال بسته‌ها، می‌تواند به حذف آن‌ها در سامانه‌های VoIP منجر شود. این عامل مخرب، معمولاً ناشی از بروز پدیده تراکم در داخل شبکه است.

ج- **تخریب بسته‌های صوتی:** خرابی‌ها و خطاهای تجهیزات شبکه می‌تواند به تخریب و حذف بسته‌های صوتی منجر شود. این موضوع در مورد مکالمات تلفنی، به‌معنی از دست رفتن بخشی از مکالمه است.

د- **پیکربندی تجهیزات انتهایی VoIP:** گزینش نادرست نوع کدکننده و سازوکارهای جبران‌سازی بسته‌های تخریب‌شده در شبکه، می‌تواند منجر به کاهش کارایی شود.

ه- **تنظیمات روترها و دیواره آتش:** ترافیک صوتی در صورت تنظیم نبودن یک روتر یا دیواره آتش، در پشت آن به‌دام خواهد افتاد. بنابراین تسهیل عبور این ترافیک از داخل عناصر فوق، الزامی است [۱۱].

۳-۳. برخی از مزایای فناوری VoIP

VoIP فناوری جدیدی است که نسبت به سامانه تلفنی آنالوگ مزایای زیادی دارد. برخی از این مزایا عبارت است از:

- ✓ **کاهش قیمت:** کاهش قیمت به‌واسطه جلوگیری از هزینه‌های دسترسی تلفنی و به اشتراک‌گذاشتن تجهیزات و بهره‌برداری‌هایی که هم برای کاربران صوت و هم برای کاربران داده هزینه‌آور است، انجام می‌شود.
- ✓ **ساده‌سازی:** اجتماع فرم‌های مختلف ارتباطات در یک واسط واحد اجازه استانداردسازی بیش‌تر و کاهش قیمت تجهیزات و سیم‌کشی‌ها در آینده را می‌دهد.
- ✓ **کاربردهای پیشرفته:** توانایی اتحاد صوت و داده در یک شبکه واحد برای اجرای کاربردهای چندرسانه‌ای پیشرفته. یک مثال خوب در این زمینه، ویدئو کنفرانس‌ها هستند.
- ✓ **کارایی پهنای‌باند:** باعث می‌شود که نرخ داده عبوری از خط برای تبادل صوت بالا باشد [۱۲].

محیط‌های VoIP محیط‌های بی‌درنگی هستند که سرعت، در موفقیت آن‌ها عامل مهمی به‌شمار می‌رود، و قابل‌قبول نیست که برای رسیدن به این مهم، از روش‌های زمان‌بری مانند رمزنگاری استفاده گردد. نهان‌نگاری داده علاوه‌بر حفاظت از اطلاعات محرمانه، سرعت انتقال اطلاعات را نیز در سطح مطلوبی نگه می‌دارد.

1- Lost Audio paCKets

نهان‌نگاری شبکه از پروتکل‌های شبکه نظیر IP, RTP, TCP برای نهان‌سازی پیام استفاده می‌کند. در بیش‌تر این پروتکل‌ها بسته‌هایی وجود دارد که با تغییر یا اصلاح آن عملکرد پروتکل تحت تأثیر قرار نمی‌گیرد. برای مثال در شکل (۱) سرآیند یک بسته IP با بسته‌های قابل‌استفاده برای جاسازی پیام نشان داده‌شده است. نواحی تیره در شکل نشان‌دهنده مکان مناسب برای جاسازی می‌باشند [۱۳].

Version	Header Length	Type of Service	Total Length
Time to live		Flags	Fragment Offset
Time to Live		Protocols	Header Checksum
Source Address			
Destination Address			
Options			Padding

شکل (۱): سرآیند یک بسته IP [۱۳]

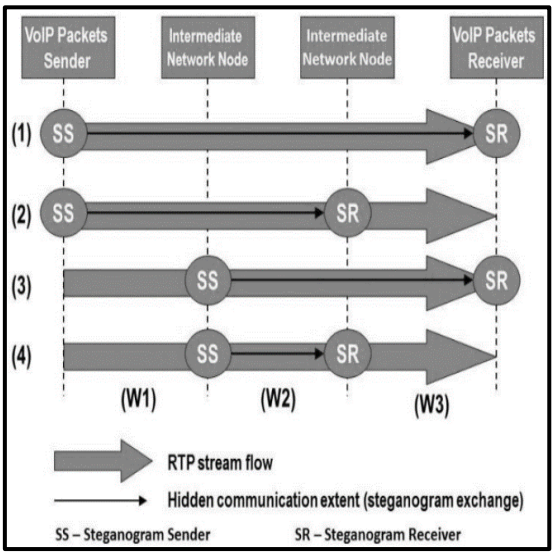
نهان‌نگاری شبکه به‌دلیل استفاده گسترده از سرویس‌های چندرسانه‌ای و شبکه‌های اجتماعی بیش‌تر مورد توجه همگان به‌ویژه نفوذگران، قرار می‌گیرد. زیرا کشف آن دشوار بوده و هیچ ردی از خود برجا نمی‌گذارند. همچنین محدودیت حجم فایل در این روش برطرف شده و می‌تواند به‌صورت قانونی از فایروال‌ها عبور کند. علی‌رغم تمام این مزایا، نهان‌نگاری بی‌درنگ یکی از چالش‌برانگیزترین زمینه‌های تحقیقاتی است. علت این امر ویژگی‌های ذاتی انتقال اطلاعات به‌صورت بی‌درنگ است که منجر به محدود شدن انجام عملیات پیچیده می‌شود [۱۴].

۴. نهان‌نگاری VoIP

نهان‌نگاری VoIP مجموعه‌ای از روش‌های نهان‌نگاری شبکه به‌صورت بی‌درنگ می‌باشد که از پروتکل‌ها و کانال‌های VoIP برای پنهان‌سازی پیام استفاده می‌کند [۱۵]. درنتیجه از قابلیت ردیابی پیام جلوگیری شده و همچنین محدودیت حجم فایل که در روش‌های نهان‌نگاری سنتی وجود داشت، برطرف می‌گردد.

۴-۱. حالت‌های نهان‌نگاری VoIP

برای نهان‌نگاری VoIP، چهار حالت احتمالی در نظر گرفته می‌شود. این حالت‌ها بر مبنای گره‌ای است که الگوریتم‌های نهان‌نگاری در آنجا اجرا می‌شوند. فرستنده و گیرنده پیام محرمانه می‌توانند در گره‌های میانی یا انتهایی باشند. همان‌طور که در شکل (۲) نشان داده‌شده است. حالت اول شایع‌ترین حالت است. فرستنده و گیرنده مکالمه‌های VoIP انجام داده درحالی‌که به‌طور هم‌زمان داده محرمانه مبادله می‌کنند. مسیر مکالمه همان مسیر پنهان است. برای سه حالت بعدی مشخص‌شده (۲ تا ۴) تنها بخشی از طول مسیر VoIP برای ارتباط پنهان مورداستفاده قرار می‌گیرد. به‌عنوان نتیجه، به‌طورکلی فرستنده و گیرنده از اقدامات انجام شده توسط گره‌های میانی برای تبادل داده‌های پنهان بی‌اطلاع هستند. محل احتمالی نگهبان به‌عنوان w3-w1 علامت‌گذاری شده است [۱۳].



شکل (۲): حالتی نهان‌نگاری VoIP [۱۳]

۴-۲. چالش‌های نهان‌نگاری VoIP

نهان‌نگاری شبکه به‌دلیل استفاده گسترده از سرویس‌های چندرسانه‌ای و شبکه‌های اجتماعی بیش‌تر مورد توجه همگان به‌ویژه نفوذگران قرار می‌گیرد، زیرا کشف آن دشوار بوده و هیچ ردی از خود برجای نمی‌گذارد. علی‌رغم تمام این مزایا، نهان‌نگاری بی‌درنگ یکی از چالش برانگیزترین زمینه‌های تحقیقاتی است [۱۶]. علت این امر ویژگی‌های ذاتی انتقال اطلاعات به‌صورت بلادرنگ است که منجر به محدود شدن انجام عملیات پیچیده می‌شود در ادامه این چالش‌ها با جزئیات بیش‌تری بررسی می‌شود.

۴-۲-۱. انتقال غیرقابل اطمینان

در واقع این مسئله یکی از چالش‌های اساسی هنگام استفاده از بسته‌های‌صوتی در پروتکل RTP به‌عنوان رسانه‌پوششی می‌باشد. این پروتکل از UDP به‌عنوان یک پروتکل انتقالی استفاده می‌کند و UDP یک پروتکل غیرقابل اطمینان است. در واقع این پروتکل برای انتقال چندرسانه‌ای، مناسب است. زیرا از دست رفتن چند بسته، صوت یا تصویر را تحت تأثیر قرار نمی‌دهد. یعنی انتقال در چندرسانه‌ای نیاز به‌دقت بالایی ندارد، ولی زمان از اهمیت بالایی برخوردار است (به‌عنوان‌مثال صدا هیچ‌گونه تأخیری را نمی‌پذیرد). به‌همین دلیل این پروتکل بهترین گزینه برای انتقال

چندرسانه‌ای است. در مقابل اگر پروتکلی برای ارسال متن مورد استفاده قرار گیرد، باید اطمینان حاصل شود که تمام بسته‌ها به مقصد می‌رسد. در این انتقال زمان از اهمیت کم‌تری برخوردار است، ولی دریافت تمام بسته‌ها و نظارت بر رعایت ترتیب دریافت بسته‌ها یک ضرورت است. در نتیجه پروتکل UDP انتخاب مناسبی برای انتقال داده‌های متنی نیست.

۴-۲-۲. محدودیت‌های اندازه‌ی رسانه‌ی پوششی

اندازه بسته‌ها در پروتکل RTP بسیار کوچک و مطابق کدک مورد استفاده برای فشرده‌سازی داده است. چنین مسئله‌ای، میزان داده در دسترس برای انتقال و تعداد بیت‌های در دسترس هر بسته، که برای فرستادن پیام محرمانه مورد استفاده قرار می‌گیرد، را محدود می‌کند. یک پیام محرمانه بزرگ برای جاسازی باید در تعداد زیادی بسته پخش شود و در مقصد نیز یک سازوکار سرهم‌کردن پیام لازم است.

۴-۲-۳. تأخیر

پروتکل RTP به‌طور طبیعی مستعد ایجاد تأخیر در بسته‌ها می‌باشد. با نهان‌نگاری VoIP به‌دلیل جاسازی پیام اضافی و بررسی رسانه پوششی انتخابی برای جاسازی، تأخیر بیش‌تری مورد نیاز است. این امر موجب تنزل قابل‌ملاحظه‌ای در کیفیت خدمات می‌شود، که در برخی موارد به‌آسانی توسط کاربر نهایی قابل‌تشخیص است.

۴-۲-۴. داده صوتی فشرده و خام

داده‌های صوتی همواره قبل از ارسال به‌صورت فشرده در می‌آیند. از آنجا که جاسازی پیام به در دسترس بودن بیت‌های اضافی بستگی دارد، انجام عمل جاسازی در داده‌های صوتی خام نتیجه بهتری در پی خواهد داشت. بنابراین همواره توصیه می‌شود که رسانه پوششی را ابتدا از حالت فشرده خارج کرده و سپس داده‌های خام را تغییر داده و دوباره آن را فشرده کنیم. برای فشرده‌سازی داده‌ها دو روش عمده وجود دارد: فشرده‌سازی با اتلاف (مانند کدکSpeex) و بدون اتلاف (مانند G.711). در فشرده‌سازی با اتلاف جامعیت داده حفظ نمی‌شود. فشرده‌سازی یک فایل صوتی با استفاده از این روش، موجب از بین رفتن برخی از اطلاعات به هنگام خروج از حالت فشرده می‌گردد. اگر ما پیام خود را در داده خام جاسازی کرده و سپس آن را به این روش فشرده کنیم، قادر به بازسازی پیام به‌طور کامل نخواهیم بود. در روش فشرده‌سازی بدون اتلاف، جامعیت داده قبل و بعد از فشرده‌سازی حفظ می‌شود. در نتیجه استفاده از این نوع فشرده‌سازی زمانی توصیه می‌شود که ما قصد داریم پیامی را در یک فایل صوتی مخفی کنیم. یک سامانه نهان‌نگاری VoIP باید طوری طراحی شود که عملکرد سامانه و کیفیت خدمات نسبت به زمانی که هیچ پیامی پنهان نشده، تغییر محسوسی نکند [۱۷].

۴-۳. بررسی روش‌های نهان‌نگاری داده در VoIP

روش‌های نهان‌نگاری در VoIP را می‌توان در سه دسته زیر تقسیم‌بندی نمود:

۴-۳-۱. روش‌های نهان‌نگاری که بسته‌ها را تغییر می‌دهند

تغییرات را می‌توان در بسته‌های پروتکل اعمال کرد. پروتکل‌های موجود در VoIP به دو دسته سیگنالینگ و انتقالی تقسیم می‌شوند. بسته‌های اضافی یا اختیاری موجود در این پروتکل‌ها به‌همراه پروتکل‌های شبکه (مانند UDP،TCP/IP) می‌توانند برای نهان‌سازی مورداستفاده قرار گیرند، در این روش سرآیندهای پروتکل شبکه یا بسته‌های ظرفیت بار تغییر می‌یابند. این روش‌ها شامل انواع زیر می‌باشند:

- تغییرات بسته‌های سرآیند در پروتکل‌های IP، UDP، RTP در طول مرحله نشست.
- نهان‌نگاری اطلاعات در بسته‌های صدا با استفاده از الگوریتم نهان‌نگار صوت از جمله DSSS[1]، QIM[2]، LSB [۴].

۴-۳-۲. روش‌های نهان‌نگاری که ارتباطات زمانی بسته‌ها را تغییر می‌دهند

روش‌هایی که ترتیب پیام‌های ارسالی یا دریافتی بسته را تغییر می‌دهند. برنامه‌ریزی مجدد به دو روش صورت می‌گیرد. در روش اول گیرنده را وادار می‌کنیم که بسته‌هایی را نادیده بگیرد (از طریق ایجاد تأخیر به میزان کافی). در روش دوم گیرنده را متقاعد می‌کنیم که تعدادی از بسته‌ها گم شده‌اند (مثلاً بعضی از شماره‌ها را از قلم می‌اندازیم). برنامه‌ریزی مجدد بسته نیازمند هم‌زمانی میان فرستنده و گیرنده است. این امر ظرفیت نهان‌نگاری پایین‌تری نسبت به‌روش‌های تغییر در بسته‌های پروتکل دارد، ولی اجرای آن راحت‌تر است (مانند تغییر دادن ترتیب بسته‌های RTP).

۴-۳-۳. روش‌های نهان‌نگاری ترکیبی VoIP

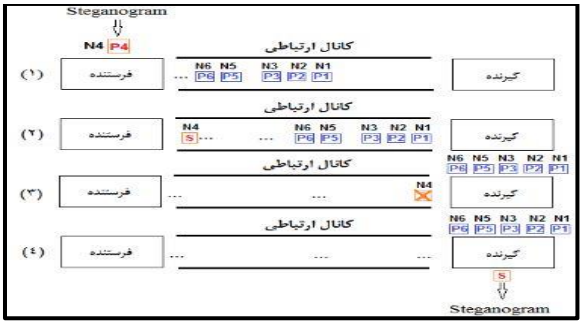
در این دسته هم محتوای بسته‌ها و هم ارتباطات زمانی درون بسته‌ها دچار تغییرات می‌شود. در این زمینه می‌توان به‌روش LACK اشاره کرد[۱۳]. مازورکزیک روش LACK را با استفاده از پروتکل RTP و تأخیر بسته‌ها ارائه داد. روش LACK در دسته نهان‌نگاری ترکیبی قرار می‌گیرد. این روش در ارسال بسته‌ها به‌طور عمدی تأخیر ایجاد کرده تا گیرنده‌ای که فاقد الگوریتم نهان‌نگاری است مجبور به دور انداختن آن‌ها شود. سپس پیام سری را در بسته‌های تأخیری پنهان می‌کند. این روش اساسا

1 - Direct-sequence spread spectrum
2 - Quantization Index Modulation

برای شبکه‌های IP طراحی‌شده است که برخی از بسته‌ها می‌توانند براثر ازدحام و کیفیت پایین شبکه و غیره، مفقود شوند. (البته باید در نظر داشت این روش زمانی کاربردی است که درصد مفقود شدن بسته‌ها در شبکه پایین باشد) برای IP تلفنی می‌توان فرض شود که مفقود شدن بسته‌ها زمانی روی می‌دهد که:

- ✓ بسته به مقصد نرسد.
- ✓ بسته دارای تأخیر بیش‌ازحد باشد، به‌گونه‌ای که در سمت گیرنده بازسازی نشده و به گوش گیرنده نرسد.

بنابراین، برای سرویس VoIP زمانی که بسته‌ای با تأخیر زیاد به مقصد برسد به‌عنوان گمشده تشخیص داده می‌شود و حذف می‌گردد. می‌توان از این ویژگی برای ایجاد روش نهان‌نگاری به‌نام LACK استفاده شود. به‌طور اساسی این روش برای طیف وسیعی از کاربردهای چندرسانه‌ای و بی‌درنگ کاربرد دارد. این روش از این حقیقت استفاده می‌نماید که برای ارتباطات چندرسانه‌ای مانند پروتکل RTP بسته‌هایی که دارای تأخیر بیش‌ازحد می‌باشند در سمت گیرنده به‌عنوان گم‌شده تشخیص داده و بازسازی نمی‌گردند. ایده اصلی روش LACK این‌گونه است که در سمت فرستنده برخی از بسته‌های صدا، انتخاب می‌شوند و با تأخیر به مقصد ارسال می‌گردند. اگر تأخیر برخی از بسته‌های دریافتی در سمت گیرنده بالا باشد، این بسته‌ها توسط گیرنده‌هایی که از پروسه‌ی نهان‌نگاری مطلع نیستند، حذف می‌گردند. درصورتی‌که گیرنده از پروسه نهان‌نگاری مطلع باشد، این بسته‌ها را به‌عنوان داده پنهان تحویل برنامه نهان‌نگاره می‌دهد شکل (۳).



شکل (۳): روش LACK [۱۴]

نهان‌کاوی روش LACK سخت‌تر از روش‌های نهان‌نگاری است که تا اینجا گفته شد. دلیل اصلی آن وجود مقداری گم‌شدگی در پروتکل IP است که نمی‌توان تشخیص داد که آیا این گم‌شدگی به‌صورت عمدی ایجادشده است، یا تحت تأثیر شبکه‌ی ارتباطی می‌باشد. اگر مقدار گم‌شدگی بسته‌ها در سطح معقولی باشد در این صورت تشخیص ارتباط پنهان بسیار مشکل می‌گردد [۱۴].

۴-۴. برخی از روش‌های نهان‌نگاری بر روی پروتکل‌ها

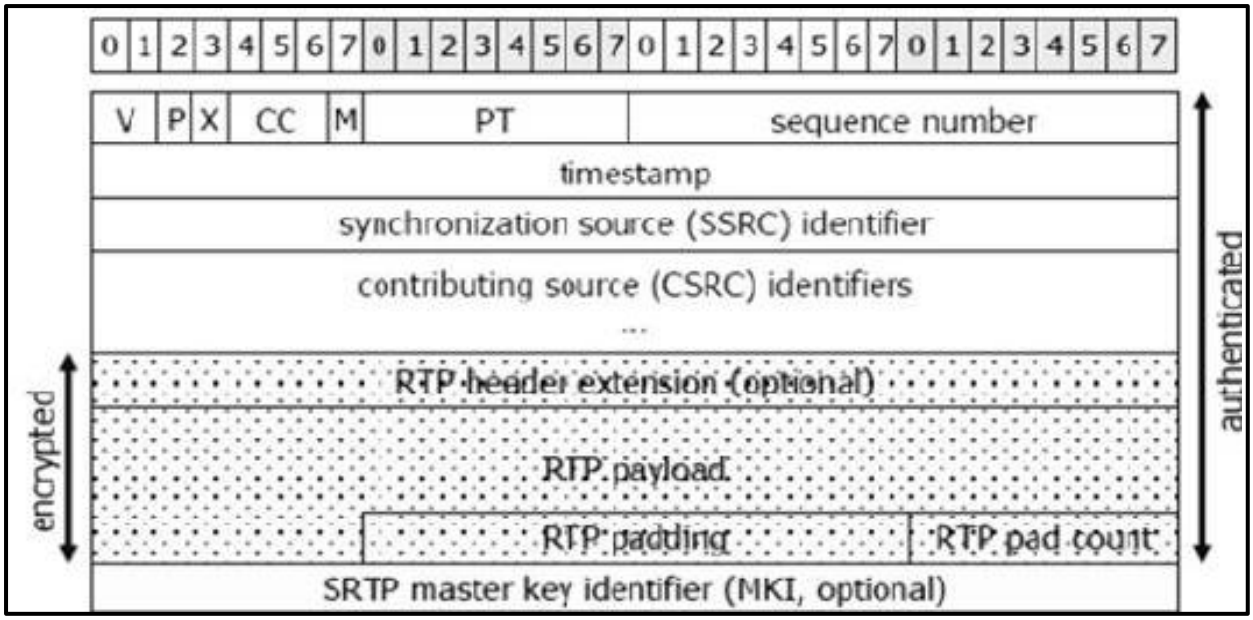
در این بخش به برخی از روش‌های اساسی و پرکاربرد نهان‌نگاری در VoIP پرداخته و آن‌ها را مورد تجزیه و تحلیل قرار داده می‌شود.

۴-۴-۱. نهان‌نگاری پروتکل‌های IP/TCP/UDP

از این حقیقت استفاده می‌کند که فقط تعداد کمی از بسته‌های سرآیند در طول فرآیند ارتباط تغییر می‌کنند. در این پروتکل‌ها بسته‌های استفاده‌نشده و زائد وجود دارد. داده پنهان معمولاً به بسته‌های زائد افزوده‌شده و به مقصد ارسال می‌گردد. در TCP/IP، حتی داده پنهان می‌تواند با داده اصلی تعویض شده و بین طرفین ارتباط به‌صورت امن مبادله گردد. یا در سرآیند IP بسته‌هایی وجود دارد که از آن‌ها می‌توان برای کانال پنهان استفاده کرد. برای مثال در شکل (۱) سرآیند یک بسته IP با بسته‌های قابل‌استفاده برای جاسازی پیام نشان داده‌شده است. نواحی تیره در این شکل نشان‌دهنده مکان مناسب برای جاسازی می‌باشند[۱۸].

۴-۴-۲. نهان‌نگاری بسته‌های استفاده‌نشده RTP

سرآیند پروتکل RTP در شکل (۴) نشان داده‌شده است که شامل بسته‌هایی به‌صورت شماره ترتیب بسته، مهر زمان، ظرفیت بار و سرآیند اضافی می‌باشد. برای ارتباط پنهان در پروتکل RTP می‌توان از بسته‌های زیر استفاده نمود:



شکل(۴): سرآیند پروتکل RTP [۱۹]

الف) بسته لایه‌گذاری: اگر بیت لایه‌گذاری، دارای مقدار یک باشد می‌توان یک یا چند بایت اضافی به انتهای سرآیند بسته اضافه کرد، به‌گونه‌ای که این بایت‌ها جزء قسمت ظرفیت بار محاسبه نشوند. میزان داده‌ای را می‌توان به انتهای سرآیند افزود که در آخرین بایت لایه‌گذاری تعریف گردد.

ب) سرآیند اضافی: زمانی که بیت X دارای مقدار یک باشد، می‌توان از این سازوکار بهره گرفت. این روش شبیه سازوکار لایه‌گذاری می‌باشد و می‌توان از سرآیند اضافی با طول متغیر استفاده نمود.

ج) مقادیر اولیه بسته‌های شماره ترتیب بسته و مهر زمان: چون مقادیر اولیه این بیت‌ها به‌صورت تصادفی انتخاب می‌گردد، اولین بسته RTP دنباله صدا می‌تواند برای ارتباط پنهان مورد استفاده قرار گیرد.

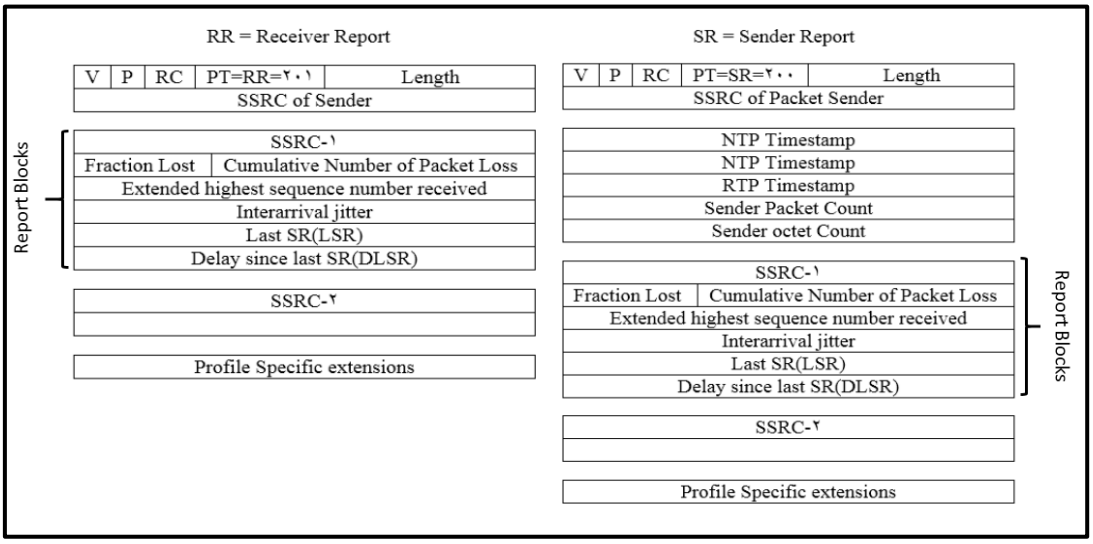
د) کم‌ارزش‌ترین بیت‌های بسته مهر زمان: این بیت‌ها می‌تواند مورد استفاده قرار گیرد. باید تأکید نمود هر چند نهان‌نگاری بر اساس بسته‌های استفاده‌نشده در پروتکل RTP ممکن است توسط ناظر فعال حذف‌شده یا محدود گردد. به حالت طبیعی درآوردن مقادیر بسته‌های سرآیند یا تغییرات کوچک در آن کافی است که پهنای باند پنهان را محدود کند.

۴-۴-۳. نهان‌نگاری بسته‌های استفاده نشده RTCP

بسته RTCP بسته کنترلی است که بین شرکت‌کنندگان در جلسه به‌صورت دوره‌ای در بازه‌ی زمانی خاص مبادله می‌گردد. اساساً دو نوع بسته RTCP وجود دارد: گزارش فرستنده[1] و گزارش گیرنده[2].

مقادیر پارامترهایی که در این گزارش‌ها قرار می‌گیرند، جهت تخمین وضعیت شبکه مورد استفاده قرار می‌گیرند. علاوه براین، تمام پیام‌های RTCP باید در بسته‌های مرکبی که شامل حداقل دو نوع گزارش RTCP منحصربه‌فرد باشند، ارسال گردند. شکل (۵) سرآیند بسته‌های گزارش گیرنده و گزارش فرستنده پروتکل RTCP نمایش داده شده است.

1 - Sender Report
2 - Receiver Report



شکل (۵): گزارش گیرنده و فرستنده RTCP [۱۹]

برای ایجاد کانال پنهان بسته‌های بلوک گزارش که در شکل (۵) نشان داده شده‌اند، مورداستفاده قرار می‌گیرند. با تغییر مقادیر این بسته‌ها می‌توان داده‌های پنهان‌شده را جایگزین نمود. مقدار اطلاعات پنهانی که از این طریق می‌توان به مقصد ارسال نمود، ۱۶۰ بیت می‌باشد. اگر از این نوع روش نهان‌نگاری استفاده گردد، واضح است که مقداری از تأثیرگذاری پروتکل RTCP کاهش می‌یابد. همچنین بسته‌های خالی استفاده‌نشده دیگری در این سرآیند وجود دارند، که می‌توان از آن‌ها به‌روش مشابه استفاده نمود. از معایب این روش می‌توان به پایین بودن حجم داده پنهان ارسالی اشاره نمود. ذکر این نکته مهم می‌باشد که پیام‌های RTCP بر پایه پروتکل IP/UDP می‌باشد، بنابراین، برای یک بسته‌ی RTCP هر دو پروتکل می‌توانند برای انتقال پنهان مورداستفاده قرار گیرند.

برای بهبود ظرفیت انتقال داده پنهان در پروتکل RTCP می‌توان تعداد این بسته‌ها را افزایش داد، به‌جای این‌که هر ۵ ثانیه یک بسته RTCP ارسال گردد (پیش فرضی که در استاندارد لحاظ شده است)، در بازه زمانی کوتاه‌تری این بسته ارسال شود، نهان‌کاوی این روش به‌آسانی نهان‌نگاری بسته‌های سازوکار امنیتی نمی‌باشد. ناظر فعال می‌تواند با حذف‌کردن یا محدود نمودن بسته‌هایی که در ارتباط پنهان مورد استفاده قرار می‌گیرند ارسال داده پنهان را تحت تأثیر قرار دهد. البته با این‌کار محدودیت‌هایی را در تأثیرگذاری پروتکل RTCP ایجاد خواهد نمود [۱۹].

۴-۵. مقایسه روش‌های نهان‌نگاری VoIP

با توجه به گستردگی روش‌ها، انتخاب بهترین روش مبتنی بر انتظاری است که از رسانه انتقال و نحوه ارسال اطلاعات داریم. در پایان برخی از نقاط قوت و ضعف روش‌های نهان‌نگاری داده در VoIPرا بیان می‌داریم [۱۲].

۴-۵-۱. روش‌های نهان‌نگاری که از بسته‌های سرآیند پروتکل‌ها جهت ارسال اطلاعات پنهان استفاده می‌کنند.

- ✓ معمولاً حجم داده بالایی را می‌توانند به‌صورت پنهان منتقل کنند.
- ✓ پیاده‌سازی و تشخیص این روش‌ها آسان است.
- ✓ به‌دلیل اشغال شدن برخی از بسته‌ها به‌وسیله داده پنهان‌شده مقداری از تأثیرگذاری پروتکل کاهش می‌یابد (نقطه ضعف).

۴-۵-۲. روش‌های نهان‌نگاری که محتوای بسته‌ها را تغییر می‌دهند.

- ✓ معمولاً ظرفیت جابجایی داده‌های پنهان‌شده در این روش‌ها نسبت به‌روش‌هایی که بسته‌های سرآیند پروتکل‌ها را تغییر می‌دهند پایین‌تر است.
- ✓ تشخیص و پیاده‌سازی این روش‌ها سخت‌تر می‌باشد.
- ✓ کیفیت صدای ارسالی به‌دلیل تغییر محتوای بسته‌ها پایین می‌آید.

۴-۵-۳. برخی از ویژگی روش‌هایی که وابستگی زمانی بسته‌ها را تغییر می‌دهند، عبارت‌اند از:

- ✓ نیاز به هم‌زمان کردن فرستنده و گیرنده می‌باشد.
- ✓ حجم داده پنهان‌شده آن پایین‌تر است و تشخیص آن نسبت به‌روش‌هایی که بسته‌های خاصی از پروتکل را تغییر می‌دهند سخت‌تر می‌باشد.
- ✓ پیاده‌سازی این روش‌ها آسان می‌باشد.

✓ کیفیت صدا پائین می‌آید (نقطه ضعف) .

۴-۵-۴. برخی از ویژگی‌های روش‌هایی که هم محتوای بسته‌ها و هم وابستگی زمانی بسته‌ها را تغییر می‌دهند عبارت‌اند از:

✓ تشخیص آن‌ها مشکل‌تر است.
✓ قادر به جابجایی حجم بالایی از داده‌ی پنهان‌شده می‌باشند.
✓ محتوای بسته و وابستگی زمانی بسته‌ها را تغییر می‌دهند.
✓ کیفیت خط ارتباطی را پایین می‌آورند (نقطه‌ضعف) [۱۳].

۵. نتیجه‌گیری

در این مقاله مروری بر نحوه عملکرد VoIP نموده و مشکلات ناشی از شبکه در ارتباطات مبتنی‌بر VoIP را بررسی نمودیم. مفهوم نهان‌نگاری VoIP را توضیح دادیم و سناریوهای احتمالی نهان‌نگاری VoIP را مورد بررسی قرار دادیم، سپس چالش‌هایی که در نهان‌نگاری VoIP با آن مواجه هستیم را شرح دادیم.

در ادامه، روش‌های نهان‌نگاری داده بر روی پروتکل VoIP را نام‌برده و برخی از روش‌های مربوط به آن را توضیح دادیم. در انتها این روش‌ها را با یکدیگر مقایسه نمودیم.

۶. مراجع

1. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.
2. N. Aoki, “A packet loss concealment technique for VoIP using steganography,” In Proc. Of International Symposium on Intelligent Signal Processing and Communication System ISPACS 2003, Awaji Island, Japan, pp. 470-473, December 7-10, 2003.
3. Z.Wu and W.Yang , “G. 711-based adaptive speech information hiding approach,” ICIC 2006, LNCS4113, pp. 1139-1144, 2006.
4. H. Tian, H. Jiang, K. Zhou, and D. Feng, “Adaptive partial-matching steganography for voice over IP using triple M sequences,” Computer Communications journal, vol. 34, pp. 2236-2247, 2011.
5. W. Mazurczyk and Z. Kotulski, “New VoIP traffic security scheme with digital watermarking,” In Proc. of25-th International Conference on Computer Safety, Reliability, and Security SafeComp 2006, LectureNotes in Computer Science 4166, pp. 170-181, 2006.
6. W. Mazurczyk and Z. Kotulski, “New security and control protocol for VoIP based on steganography and digital watermarking,” In: Proc 5th Int Conf Computer Science-research and applications (IBIZA2006), Poland, Kazimierz Dolny, 2006.
7. F. Li, B. Li, L. Peng, W. Chen, L. Zheng, and K. Xu, “A Steganographic Method Based on High Bit Rates Speech Codec of G. 723.1,” Springer, pp. 312-322, 2018.
8. S. Schmidt, W. Mazurczyk, R. Kulesza, J. Keller, and L. Caviglione, “Exploiting IP telephony with silence suppression for hidden data transfers,” Computers Security, vol. 79, pp. 17-32, 2018.
9. Sh. AbdelRahim, S. Ghoneimy, and G. Selim, “Adaptive security scheme for real-time VoIP using multi-layer steganography,” Proceedings of the 7th International Conference on Software and Information Engineering, pp. 106-110, 2018.
۱۰. اصفهانی، پ، ذوالفقاری‌نژاد، م، کرمی، پ، ارائه یک روش نهان‌نگاری جدید و قابل اعتماد از طریق VoIP، شانزدهمین کنفرانس مهندسی برق ایران، شهریور ۱۳۹۲.
11. http:// communication.howstuffworks.com/ip-telephony.htm.
12. http://www.voip-iran.com.
13. W.Mazurczyk, “VoIP Steganography and Its Detection – A Survey, ACM Computing Surveys,” accepted for publications, ISSN 0360-0300, 2013.
14. W. Mazurczyk and J.Lubacz, “LACK—a VoIP steganographic method,” Telecommunication Syst: Model Anal Des Manag, vol. 45, no. 2-3, pp. 153-163, 2010.
15. W. Mazurczyk and K. Szczypiorski, “Steganography of VoIP streams,” On the Move to Meaningful Internet Systems: OTM 2008, vol. 5332, pp. 1001-1018, 2008.
16. M. Hamdaqa and L. Tahvildari, “ReLACK: A Reliable VoIP Steganography Approach,” in Fifth Internatinal Conference on Secure Software Integration and Reliability Improvement, pp. 190-197, 2011
17. N. Aoki, “VoIP packet loss concealment based on two-side pitch waveform replication technique using steganography,” IEEE, vol. 100, pp. 52-55, 2004.
18. C. Wang and Q. Wu, “ Information hiding in real-time VoIP streams,” in Proceedings of in Proceedings of Ninth IEEE International Symposium on Multimedia, ser.ISM’ 07. Washington, DC, USA: IEEE Computer Society, pp. 255-262, 2007.
19. Y. Huang, S. Tang, and J. Yuan, “Steganography in inactive frames of VoIP streams encoded by source codec,” IEEE Transactions on information forensics and security, vol. 6, no. 2, pp. 296-306, 2011.

VoIP Steganography, Applications and Challenges

Z. Norouzi*, R. Rostami, S. Amjadian

Abstract

Steganography on the VoIP Platform is a Real-time network Steganography Method, It uses VoIP Protocols as a cover channel to hide messages. At the moment, real-time steganography is one of the challenging research areas. The reason for this is the inherent characteristics of the transfer of information in real time, which limits the complexity of operations. In this paper, we first describe the definition of Steganography and describe the VoIP concept briefly, and then we will describe some of the work done in this field. In continuation, we express the way VoIP works and the problems that we face, and then we consider the concept of VoIP Steganography and describe its challenges. Finally, introduce some of the most widely used methods of VoIP Steganography, and then we compare the different ways of VoIP steganography with each other, and discuss the weaknesses and strengths of each of them. In the final section of this paper, we will give the research results.

Key Words: *Steganography, Network Steganography, VoIP Steganography Methods, Covert Channel, Data Hiding*

* Imam Hossein Comprehensive University (znorozi@ihu.ac.ir)- Writer-in-Charge