# نشت اطلاعات از طریق کانال مخفی زمانی مبتنی بر پروتکل دی.ان.اس.

سینا سهیلی[۱]، حمیدرضا حمیدی[۱]

[۱] گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بین المللی امام خمینی(ره)، قزوین، ایران
sinasoheili79@gmail.com,hamidreza.hamidi@eng.ikiu.ac.ir

**چکیده**

یک کانال مخفی یا کانال پوششی (Covert Channel) یک کانال ارتباطی پنهان است که برای مبادله و یا نشت اطلاعات از یک شبکه استفاده می‌شود که منبع آن هرگز برای این هدف ایجاد نشده است. هدف از ایجاد کانال مخفی خارج‌کردن اطلاعات حساس سازمان‌ها است که با دورزدن اقدامات امنیتی سازمان‌ها مثل دیواره‌های آتش و سامانه‌های تشخیص نفوذ (ای. دی. اس.) همراه است. یکی از انواع کانال‌های مخفی، کانال مخفی زمانی است که از یک طرح زمانی دسترسی به منابع مشترک (مانند زمان ارسال بین بسته‌های شبکه) برای ارسال اطلاعات استفاده می‌کند. پیاده‌سازی کانال مخفی روی پروتکل‌های مختلف شبکه امکان‌پذیر است. یکی از پروتکل‌های پرکاربرد در بستر اینترنت پروتکل دی.ان.اس. است. پروتکل دی.ان.اس. به علت کوچکی و استفاده زیاد، کمتر موردتوجه دیواره‌های آتش و مدیران سیستم قرار می‌گیرد به همین دلیل این پروتکل یکی از پروتکل‌های محبوب و مناسب برای ایجاد کانال مخفی است. در این پژوهش، عوامل مؤثر در عملکرد کانال مخفی زمانی مبتنی بر پروتکل دی.ان.اس و شیوه‌های شناسایی و مقابله با آن‌ها نیز مورد ارزیابی قرار گرفته است.

**کلمات کلیدی:** امنیت سایبری، کانال مخفی زمانی، پروتکل دی.ان.اس، امنیت شبکه.

## ۱ مقدمه

امروزه جرایم رایانه‌ای یکی از مهمترین تهدیدها برای کسب و کارها محسوب می‌شوند که گاها عواقب سنگین و غیرقابل جبرانی را برای شرکت‌ها، افراد و یا دولت‌ها به همراه دارد [۱]. یکی از مهمترین دغدغه‌های کاربران سامانه‌ها آن است که خدمات[۱] فقط به اطلاعاتی[۲] که مجوز دسترسی مربوط به آن را دارند دسترسی داشته باشند و نتوانند اطلاعاتی که مجوز لازم برای دسترسی به آن را ندارند بخوانند و یا آن‌ها را تغییر دهند. از این رو یکی از مهمترین نگرانی‌های طراحان سامانه‌های امنیتی، حفاظت از اطلاعات در مقابل دسترسی غیر مجاز است که راه حل‌های شناخته شده‌ای برای حل این مشکل وجود دارد [۲].

[1] Service
[2] Data

نشت اطلاعات یکی از اتفاقات در جرایم رایانه‌ای است که با هدف دزدیدن و خارج کردن اطلاعات حساس مورد استفاده قرار می‌گیرد. یکی از مهمترین روش‌های نشت اطلاعات کانال مخفی[۳] است که مقابله با آن بسیار چالش‌برانگیز است [۱]. یک کانال مخفی یا کانال پوششی یک کانال ارتباطی پنهان است که برای مبادله و یا نشت اطلاعات از یک شبکه استفاده می‌شود که منبع آن هرگز برای این هدف ایجاد نشده است. هدف از ایجاد کانال مخفی خارج کردن اطلاعات حساس سازمان‌ها است که با دور زدن اقدامات امنیتی سازمان‌ها مثل دیواره‌های آتش[۴] و سامانه‌های تشخیص نفوذ (ای.دی.اس.[۵]) همراه است [۱]. پروتکل‌های مختلف در سطح اینترنت وجود دارند که مهاجمان با سوءاستفاده از آسیب پذیری آنها و همچنین بکار بردن بدافزارها حملات هدفمندی را اجرا می‌کنند که باعث نشت و یا از دست دادن اطلاعات می‌شود [۳]. با گذشت زمان کانال‌های مخفی رایج تر، پیچیده تر و تشخیص آنها سخت تر شده است [۴].

## ۱.۱ کانال مخفی

تعاریف متفاوتی برای کانال مخفی بیان شده است که شالوده آن‌ها بدین صورت است: به یک ارتباط پنهان جهت انتقال پیام‌های پنهان خلاف قوانین یک سامانه، کانال پنهان گفته می‌شود. کانال پنهان می‌تواند در مسیر افشای اطلاعات حساس کاربران مانند رمز عبور به کار گرفته شود. همچنین این اطلاعات می‌تواند موجب کنترل از راه دور خودرو یا قلب مصنوعی شده و جان افراد را به خطر اندازد [۵].

به صورت کلی دو نوع کانال مخفی وجود دارد [۴]: کانال مخفی با حافظه[۶] که در آن یک فرآیند به شکل مستقیم یا غیر مستقیم داده‌ای را در محل مشخصی می‌نویسد و فرآیند دیگر به شکل مستقیم یا غیر مستقیم از آن محل مشخص داده را می‌خواند. کانال مخفی زمانی[۷] که از یک طرح زمانی دسترسی به منابع مشترک (مانند زمان ارسال بین بسته‌های شبکه) برای ارسال اطلاعات استفاده می‌کند.

کانال‌های مخفی هم برای اهداف مثبت و هم برای اهداف مخرب استفاده می‌شوند [۴]، [۶]. به عنوان مثال برای اهداف مخرب می‌توان افشای اطلاعات حساس درون یک سازمان و یا ارسال مخفیانه دستورات برای شبکه ربات‌ها[۸] را نام برد و از اهداف مثبت برای ایجاد کانال مخفی می‌توان به برقراری ارتباط مخفیانه بین خدمت‌های امنیتی و یا نظامی اشاره کرد [۴].

## ۲.۱ کانال مخفی پروتکل دی.ان.اس.

از پروتکل‌های مختلفی برای ایجاد کانال مخفی می‌توان استفاده کرد [۴]، [۶]. پروتکل دی.ان.اس.[۹] (سامانه نام دامنه) یکی از پرکاربردترین پروتکل‌های شبکه محسوب می‌شود که به ندرت توسط دیواره‌های آتش مسدود

[3] Covert Channel
[4] Firewall
[5] Intrusion Detection System (IDS)
[6] Storage Covert Channel
[7] Timing Covert Channel
[8] Botnet
[9] Domain Name System (DNS)

می‌شود به همین دلیل برای ایجاد کانال مخفی مناسب است [۴] [۷]. دی.ان.اس. یک سامانه غیر متمرکز، توزیع شده[۱۰] و سلسله مراتبی است که در سطح وب خدمت می‌دهد که در آن گروهی از خدمت دهنده‌ها مسئول دامنه‌های مشخصی هستند که در سراسر جهان پراکنده شده‌اند. سامانه نامِ دامنه برای تبدیل یک آدرس دامنه به یک آدرس آی.پی.[۱۱] استفاده می‌شود که باعث می‌شود به جای استفاده از آدرس عددی مربوط به خدمت‌دهنده‌ها به راحتی نامِ دامنه را در حافظه خود نگه‌داریم و بتوانیم به ارائه کننده‌ی خدمت دسترسی پیدا کنیم [۶]، [۸].

سامانه نامِ دامنه یا همان دی.ان.اس. یکی از مهمترین خدمت دهنده‌های شبکه است چرا که خدمات مهمی همچون وب[۱۲]، پروتکل انتقال فایل یا اف.تی.پی.[۱۳]، پست الکترونیکی یا ایمیل و غیره که نیاز به دسترسی به خدمت دهنده راه دور دارند از پروتکل اینترنت یا آی.پی. استفاده می‌کنند [۸]. از آنجا که پروتکل دی.ان.اس. معمولا توسط دیواره‌های آتش بررسی نمی‌شود، به یکی از محبوب‌ترین پروتکل‌ها برای رفتارهای مخرب توسط نفوذگران انتخاب شده است. همچنین ابزارهای امنیتی امکاناتی برای تشخیص و محدود سازی کانال‌های مخفی دارند اما این ابزارها معمولا پروتکل دی.ان.اس. را در نظر نمی‌گیرند و همین عوامل باعث شده است که این پروتکل یکی از پراستفاده‌ترین پروتکل‌ها برای ایجاد کانال مخفی باشد [۷]. در کانال‌های مخفی مبتنی بر پروتکل دی.ان.اس. نفوذ کنندگان اطلاعات را در بسته‌های[۱۴] پروتکل دی.ان.اس. کپسوله[۱۵] می‌کنند و به این روش آنها را جابه‌جا می‌کنند [۶].

## ۲ روش‌های شناسایی و مقابله

در پژوهشی با عنوان «رویکرد مستقل از پروتکل در کانال مخفی شبکه» پژوهشگر سعی در بررسی پروتکل‌های مختلف شبکه در سه لایه‌ی شبکه[۱۶]، لایه انتقال[۱۷] و لایه کاربرد[۱۸] کرده است و روش‌های مختلف یادگیری ماشین را روی لایه‌های مختلف شبکه بررسی می‌کند تا بتواند روش یادگیری ماشین مناسب برای کشف کانال مخفی را پیدا کند [۴]. مجموعه داده استفاده شده در این پژوهش ترکیبی از بسته‌های سالم و بسته‌های حاوی کانال مخفی در شبکه بوده است. همانطور که گفته شد بررسی کانال مخفی در سه لایه شبکه، انتقال و کاربرد انجام شده است. در لایه‌ی شبکه از پروتکل آی.پی. نسخه چهار، در لایه انتقال از پروتکل تی.سی.پی.[۱۹] و در لایه کاربرد از دی.ان.اس. استفاده شده است. قبل از آنکه از داده برای استخراج ویژگی‌ها استفاده کنیم نیاز به یک مرحله پیش‌پردازش داریم که پژوهشگر برای این کار یک موتور طراحی کرده است که ورودی

[10] Distributed
[11] IP Address
[12] Web
[13] File Transfer Protocol (FTP)
[14] Packet
[15] Encapsulate
[16] Network layer
[17] Transport layer
[18] Application layer
[19] Transmission Control Protocol (TCP)

آن مجموعه‌ای از بسته‌های شبکه است و خروجی آن یک مجموعه داده با قالب عمومی است. بعد از گذار از مرحله پیش‌پردازش، مرحله استخراج ویژگی [۲۰] را باید انجام دهیم. در این مرحله ویژگی‌هایی که استخراج می‌شوند بر اساس نوع پروتکل مشخص می‌شود. برای استخراج ویژگی از بسته‌ها از ضریب همبستگی [۲۱] و دامنه اطلاعاتی [۲۲] استفاده شده است. در طراحی مدل یادگیری از مدل‌های با نظارت [۲۳] استفاده شده است. از جمله این مدل‌ها رگرسیون لجستیک [۲۴]، اس.وی.ام. [۲۵]، درخت تصمیم [۲۶] و کی.ان.ان. [۲۷] بوده است. همچنین در مدل اس.وی.ام. از دو نوع کرنل خطی [۲۸] و گاوسی [۲۹] استفاده شده است. پیاده‌سازی کانال مخفی در لایه‌ها و پروتکل‌های مختلف به شکل‌های متفاوتی انجام شده است. به عنوان مثال در لایه شبکه کانال مخفی در سرآیند [۳۰] بسته‌ها قرار داشته است به این شکل که هر کاراکتر در ۱۶ بیت غیر استفاده در قسمت مشخصات آی.پی. قرار گرفته است و در لایه انتقال کانال مخفی تی.سی.پی. در قسمت شماره بسته در دنباله تی.سی.پی. پیاده سازی شده است. در تمام لایه‌ها نتایج مدل لاجستیک رگرسیون به عنوان معیاری برای مقایسه با دیگر لایه‌ها در نظر گرفته شده است. با توجه به نتایج حاصل از این پژوهش درمی‌یابیم که مدل اس.وی.ام با کرنل گاوسی در لایه‌های شبکه و انتقال به خوبی توانسته است کانال مخفی را کشف کند این در حالی است که در لایه کاربرد درخت تصمیم عملکرد بهتری را از خود نشان داده است.

در پژوهشی دیگر پژوهشگر تلاش کرده است تا با استفاده از مدل ال.اس.تی.ام. [۳۱] کانال‌های مخفی در پروتکل دی.ان.اس. را شناسایی کند [۶]. فرآیند پردازش و شناخت کانال‌های مخفی در پژوهش شامل سه مرحله است که در مرحله اول یک پیش‌پردازش روی بسته‌های دی.ان.اس. انجام می‌شود. مرحله پیش‌پردازش شامل چهار زیر مرحله به شرح زیر می‌باشد:

۱. جدا کردن زیر دامنه از دامنه سطح بالا
۲. تبدیل تمام کارکترهای بزرگ به کوچک در دامنه
۳. حذف جداکننده‌ی نقطه از داخل آدرس‌ها
۴. یکپارچه‌سازی [۳۲] طول رشته‌های دامنه

[20] Feature extract
[21] Correlation coefficient
[22] Domain knowledge
[23] Supervised classification machine learning model
[24] Logistic regression
[25] Support Vector Machine (SVM)
[26] Decision Tree (DT)
[27] KNN: K-nearest neighbors
[28] Linear kernel
[29] Gaussian kernel
[30] Header
[31] LSTM: Long-Short Term Memory
[32] Unify

در مرحله بعد خروجی این مرحله که مجموعه‌ای از رشته‌ها است به یک مدل ال.اس.تی.ام. داده می‌شود. از آنجایی که طول دامنه‌ها کوتاه است پس مدل ال.اس.تی.ام. فقط شامل یک لایه پنهان[۳۳] است. در مرحله سوم که مرحله آخر است یک فیلتر گروهی روی بسته‌ها اعمال می‌شود. اساس کار این فیلتر مبتنی بر لیست سفید[۳۴] است که بر اساس دانش موجود ایجاد شده است. داده ورودی در مرحله سوم در واقع خروجی مدل ال.اس.تی.ام. است. خروجی مدل ال.اس.تی.ام. در واقع ترافیکی از شبکه است که به عنوان ترافیک با کانال مخفی شناسایی شده است. هدف از فیلتر اعمال شده در مرحله سوم این است که ارتباطاتی که به اشتباه به عنوان کانال مخفی شناسایی شده اند اصلاح شوند. این فیلتر دقت نتیجه خروجی را افزایش می‌دهد. برای اعمال فیلتر گروهی ابتدا ترافیک شبکه بر اساس روز گروه‌بندی می‌شود یعنی ترافیک مربوط به هر روز در یک گروه قرار می‌گیرد. بعد از گروه بندی ترافیک چهار مرحله زیر روی گروه‌ها اعمال می‌شود:

۱. در هر گروه دامنه‌هایی که درخواست تکراری برای آنها ارسال شده اند حذف می‌شوند.

۲. گروه‌هایی که تعداد نمونه‌های آنها کم است حذف می‌شوند.

۳. گروه‌هایی که در آن دامنه‌ها توسط چند آی.پی. پرس و جو شده اند حذف می‌شوند.

۴. ترافیک گروه‌ها بر اساس لیست سفید فیلتر می‌شود.

نتایج حاصل از این پژوهش روی مجموعه داده مختلف نشان می‌دهد که مدل ال.اس.تی.ام. نسبت به مدل سی.ان.ان. در معیارهای دقت و صحت عملکرد بهتری از خود نشان داده است.

در یک پژوهش دیگر پژوهشگر یک کانال مخفی را شبیه سازی می‌کند تا کارایی و امکان پیاده سازی کانال مخفی رو پروتکل دی.ان.اس. را نشان دهد. نتایج این پژوهش نشان می‌دهد که یک کانال مخفی مبتنی بر پروتکل دی.ان.اس. می‌تواند با تاخیر ۱۵۰ میلی ثانیه و سرعت ۱۱۰ کیلومتر بر ثانیه داده جابه‌جا کند [۹]. این کانال مخفی بر روی شبکه دانشگاه ولونگنگ[۳۵] پیاده‌سازی شده است. دیواره آتش شبکه این دانشگاه اجازه دسترسی مستقیم سامانه‌های داخل شبکه به اینترنت را نمی‌دهد با این حال بسته‌های دی.ان.اس. را ارزیابی نکرده و به راحتی عبور می‌دهد. کانال مخفی این پژوهش به دو روش مختلف پیاده سازی شده است. در روش اول که همان تونل دی.ان.اس. است ترافیک شبکه از طریق یک دی.ان.اس. محلی مسیریابی می‌شود و در روش دوم مشتری به شکل مستقیم به سرور تونل متصل شده است. برای آزمایش این کانال مخفی در محیط واقعی از دو سیستم مجزا که یکی در شبکه دانشگاه بوده است و نقش مشتری را داشته و دیگری در اینترنت بوده است و نقش خدمت دهنده را داشته است استفاده شده است.

نتایج این آزمایش نشان می‌دهند که کانال مخفی مبتنی بر دی.ان.اس. علاوه بر آنکه قابل پیاده سازی است و امکان عبور از دیواره آتش را دارد عملکرد خوبی نیز در انتقال داده داشته است. اما سربار ناشی از این ارتباط قابل توجه است تا جایی که در بعضی مواقع این سربار تا ۲۰۰۰ درصد نیز رسیده است.

[33] Hidden layer
[34] Whitelist filtering method
[35] Wollongong

در پژوهشی دیگر پژوهشگر کانال مخفی زمانی مبتنی بر پروتکل انتقال اَبَرمتن را مورد ارزیابی قرار می‌دهد و همچنین روش تشخیص مبتنی بر آنتروپی اطلاعات را طراحی و پیاده سازی می‌کند. پژوهشگر کانال مخفی را یک ارتباط خلاف سیاست‌های امنیتی سامانه تعریف می‌کند که در آن مهاجم می‌تواند به راحتی تنها با یک مجوز دسترسی عمومی باعث نشت اطلاعات از سامانه قربانی شود [۵]. کانال‌های مخفی زمانی برخلاف کانال‌های مخفی ذخیره سازی، حافظه ندارند و کمتر باعث جلب توجه می‌شوند. ماهیت کاربردی پروتکل انتقال اَبَرمتن به نفوذگر این امکان را می‌دهد که کانال مخفی زمانی را در سطوح مختلف و با مشخصه‌های مختلف ایجاد کرد. آزمایش‌های این پژوهش توسط یک گیرنده و فرستنده در بستر یک شبکه عمومی فعال انجام شده است. گیرنده روی یک ماشین مجازی خارج از شبکه محلی و در محیط اینترنت قرار دارد و فرستنده هم روی یک رایانه در شبکه داخلی قرار دارد. عمل پنهان سازی بر اساس تاخیر بین پیام‌ها و بر روی پروتکل ابر متن ایجاد شده است. ارزیابی نتایج این پژوهش بر اساس سه پارامتر می‌باشد:

۱. آستانه: حد تشخیص کانال توسط تحلیلگر را مشخص می‌کند که مقدار ثابت ۱/۷۲ برای آن در نظر گرفته شده است. میزان آستانه آنتروپی برای تشخیص همواره ثابت نیست چرا که مهاجم می‌تواند با شگردهایی مانند تغییر سطح کانال و یا ایجاد نویز روی کانال مقدار آنتروپی را تغییر دهد تا از تشخیص در امان بماند.

۲. بیشینه کانال: گیرنده بعد از دریافت پیام و رمزگشایی آن حد آنتروپی پیام‌های داخل کانال را محاسبه می‌کند.

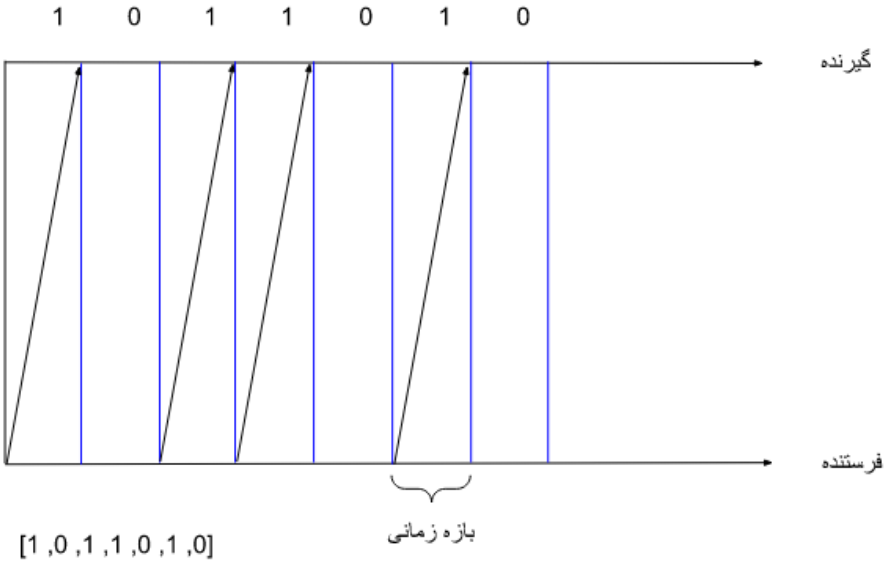
۳. کمینه نویز: پیام‌های موجود در ترافیک عمومی شبکه که داخل کانال پنهان نیستند نویز محسوب می‌شوند.

تحلیلگر زمانی می‌تواند به درستی کانال پنهان را تشخیص دهد که میزان آستانه از بیشینه کانال بیشتر باشد و از کمینه نویز کمتر باشد. کانال پنهان زمانی در دو سطح صفحه و تابع ایجاد شده است و تحلیلگر در سه سطح درگاه، صفحه و تابع قرار می‌گیرد. کانال و تحلیلگر نسبت به هم در سه سطح مختلف می‌توانند قرار بگیرند:

۱. زمانی که کانال و تحلیلگر هم سطح باشند شرایط تشخیص برای تحلیلگر به خوبی مهیا می‌شود در نتیجه کانال مخفی به راحتی قابل تشخیص است.

۲. اگر کانال در سطح پایین‌تری نسبت به تحلیلگر قرار بگیرد در این حالت تحلیلگر علاوه بر پیام‌های کانال پنهان پیام‌های دیگر نیز دریافت می‌کند و در شرایطی که تعداد پیام‌ها افزایش میابد تحلیلگر در تشخیص دچار مشکل می‌شود.

۳. اگر تحلیلگر در سطح پایین‌تری نسبت به کانال قرار بگیرد 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.




شکل ۱: نمونه‌ای از نحوه عملکرد یک کانال مخفی زمانی مبتنی بر الگوی زمانی.

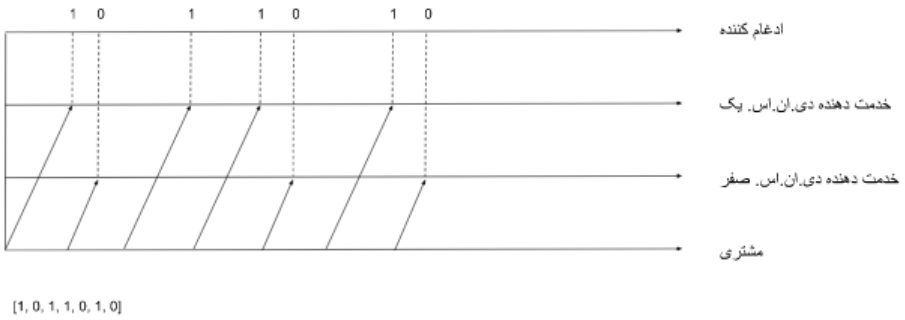
نتایج این پژوهش نشان می‌دهد که تحلیلگر باید در تمام سطوح مختلف ترافیک را بررسی کند. همچنین مشخص می‌شود که با ایجاد نویز روی کانال پنهان ظرفیت کانال کاسته می‌شود اما همین نویز باعث می‌شود که آنتروپی افزایش یابد و تشخیص سخت‌تر شود.

## ۳ نحوه طراحی کانال مخفی زمانی

در یک دسته بندی ساده به شکل خاص می‌توانیم پیاده سازی کانال‌های مخفی زمانی را به دو گروه، کانال مخفی زمانی مبتنی بر الگوی زمانی تبادل بسته‌ها و کانال مخفی زمانی مبتنی بر ترتیب بسته‌ها تقسیم بندی کرد [۱۰]. در کانال مخفی زمانی مبتنی بر الگوی زمانی، یک الگوی زمانی بین فرستنده و گیرنده ایجاد می‌شود که فرستنده بر اساس این الگو داده را منتقل می‌کند و گیرنده نیز از طریق همین الگو می‌تواند داده را دریافت کند [۵]. در شکل ۱ می‌توانید نمونه‌ای از نحوه عملکرد این کانال را مشاهده کنید.

همانطور که در شکل ۱ مشاهده می‌کنید یک بازه زمانی که به عنوان مثال اندازه آن یک ثانیه است الگوی زمانی را تشکیل می‌دهد. طبق این الگوی زمانی، اگر در بازه زمانی تعیین شده بسته‌ای جا به جا شود به معنای بیت یک و اگر بسته‌ای جا به جا نشود مقدار بیت صفر در نظر گرفته می‌شود.

در روش کانال مخفی زمانی مبتنی بر ترتیب بسته‌ها، دیگر الگوی زمانی بین فرستنده و گیرنده وجود ندارد. در روش پیشنهادی این پژوهش به جای استفاده از یک گیرنده از چند گیرنده استفاده می‌کنیم و بر اساس یک قرارداد که از قبل بین فرستنده و گیرنده‌ها تنظیم شده است اقدام به انتقال داده می‌کنیم. بر اساس این قرارداد و با توجه به تعداد گیرنده‌ها به هر گیرنده یک کد اختصاص داده می‌شود و این کد

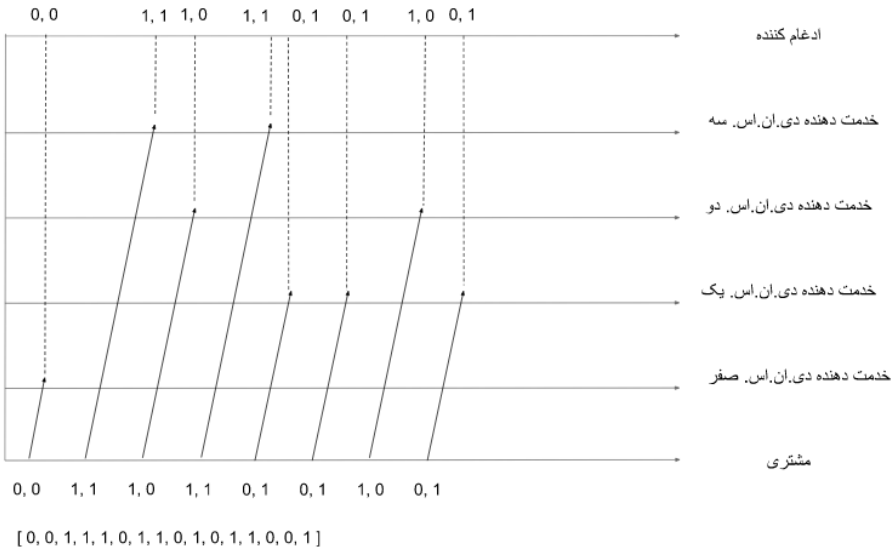



شکل ۲: مثال از نحوه عملکرد کانال مخفی زمانی مبتنی بر ترتیب بسته‌ها

نماینده‌ی داده‌ای است که قرار است منتقل شود. به عنوان مثال اگر دو گیرنده داشته باشیم و به یکی کد صفر و به دیگری کد یک اختصاص داده شود هر درخواستی که به گیرنده با کد صفر برسد معادل با مقدار صفر و هر درخواست که به گیرنده با کد یک برسد برابر با مقدار یک است. در این روش ترتیب داده بر اساس زمان رسیدن بسته‌ها به خدمت‌دهنده‌ی دی.ان.اس. تعیین می‌شود. به عبارت دیگر بعد از آنکه فرآیند انتقال داده تکمیل شد تمامی داده بر اساس زمان رسیدن بسته‌ها به خدمت‌دهنده‌های دی.ان.اس. مرتب می‌شوند و پس از این مرتب سازی، داده‌ای که از سمت فرستنده به گیرنده ارسال شده بود بازیابی می‌شود. شکل ۲ نمونه از نحوه‌ی عملکرد این نوع از کانال را نشان می‌دهد.

برای درک بهتر از نحوه‌ی عملکرد این نوع از کانال مخفی فرض کنید که قصد داریم داده‌ای را از سمت مشتری با استفاده از کانال مخفی زمانی مبتنی بر ترتیب جابه‌جا کنیم. در این مثال ما از چهار خدمت‌دهنده دی.ان.اس. به عنوان چهار گیرنده استفاده می‌کنید. خدمت‌دهنده‌ها به ترتیب با کدهای صفر تا سه مشخص می‌شوند. میدانیم که برای ایجاد کدهایی از شماره صفر تا شماره سه تنها به دو بیت داده در مبنای دو نیاز داریم پس هر درخواست که از سمت مشتری به سمت یکی از این گیرنده‌ها فرستاده می‌شود شامل دو بیت داده خواهد بود. در سمت گیرنده علاوه بر خدمت‌دهنده‌های دی.ان.اس. که دریافت کننده داده از سمت مشتری هستند نیاز به یک خدمت ادغام کننده نیز داریم . همانطور که از نام این خدمت‌دهنده مشخص است وظیفه آن تجمیع و ادغام کردن تمام بسته‌هایی است که به خدمت‌دهنده‌های دی.ان.اس. می‌رسد. در شکل ۳ می‌توانید طرحی از نحوه‌ی عملکرد این کانال را مشاهده کنید.

همان‌طور که مشاهده می‌کنید مشتری قصد دارد یک آرایه شامل اعداد صفر و یک را منتقل کند و از آنجایی که هر درخواست در این کانال به شکل خاص شامل دو بیت است پس مشتری داده را با اندازه‌های دو بیتی جدا می‌کند. سپس با توجه به مقداری که در این دو بیت داده قرار دارد (که می‌تواند مقداری بین صفر تا سه باشد) خدمت‌دهنده مقصد را مشخص کرده و به ترتیب داده را ارسال می‌کند. توجه شود که در بسته‌هایی که از سمت مشتری به گیرنده ارسال می‌شود هیچ داده‌ای قرار ندارد.

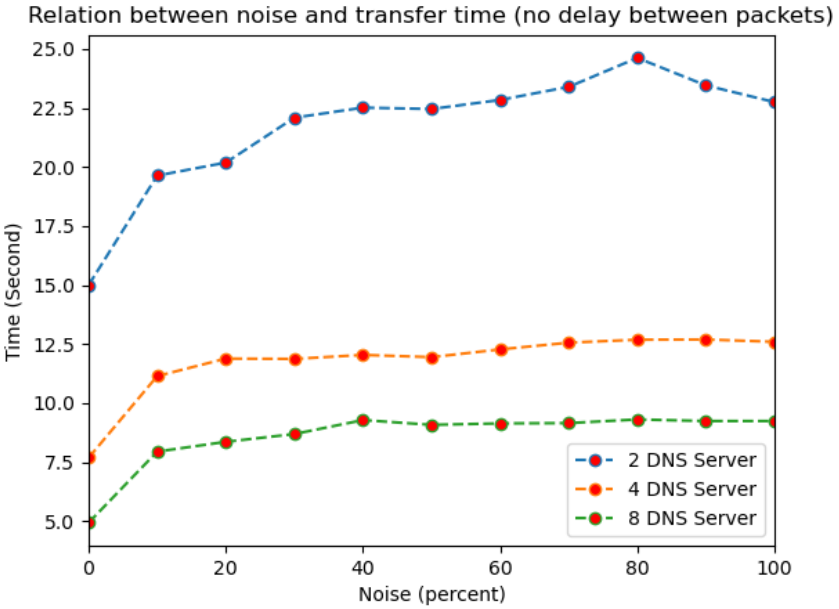



شکل ۳: نحوه‌ی انتقال داده در کانال مخفی زمانی مبتنی بر ترتیب

## ۴ ارزیابی عملی

نویز ناخواسته‌ای که برای آزمایش‌های خود در نظر گرفتیم یک نویز زمانی است که باعث می‌شود با اعمال تاخیر در ارسال بسته‌ها، بسته‌ها خارج از ترتیب عادی خود به مقصد برسند. بدیهی است که با افزایش نویز انتظار داشته باشیم زمان انتقال ما افزایش یابد چرا که با افزایش نویز تعداد بسته‌های بیشتری تحت تاثیر نویز قرار می‌گیرند و از آنجایی که نوع نویز ما زمانی است پس در زمان انتقال تاثیر مستقیم دارند.

نکته‌ای که از شکل ۴ می‌توان دریافت آن است که با افزایش تعداد خدمت‌دهنده‌های دی.ان.اس. زمان انتقال ما کاهش یافته است. به عبارت دیگر افزایش تعداد خدمت‌دهنده‌های دی.ان.اس. به معنای افزایش تعداد بیت منتقل شده در هر درخواست است و چون تعداد بیت بیشتری در هر درخواست ارسال می‌شود در نتیجه به درخواست‌های کمتری برای انتقال داده نیاز داریم و تعداد درخواست کمتر به معنای زمان کمتر برای انتقال است. در شکل ۴ مشاهده می‌کنیم که افزایش نویز باعث افزایش زمان انتقال شده است اما به همان نسبت که نویز را افزایش داده‌ایم زمان انتقال افزایش نیافته است. دلیل این مسئله آن است که ارسال درخواست‌ها به شکل همروند و چندنخی اتفاق می‌افتد و در نتیجه همپوشانی زمانی بین بسته‌ها وجود دارد به همین دلیل است که با افزایش نویز، زمان انتقال به همان نسبت افزایش پیدا نکرده است در حالی که اگر نحوه‌ی انتقال به شکل سریالی بود به همان نسبت که نویز افزایش می‌یافت زمان انتقال نیز افزایش می‌یافت.




شکل ۴: تأثیر نویز بر زمان انتقال برای ۲، ۴ و ۸ خدمت‌دهنده‌ی دی.ان.اس.

## ۵ جمع‌بندی

در این پژوهش سعی کردیم یک روش جدید برای ساخت کانال مخفی ایجاد کنیم. پروتکل دی.ان.اس. به دلیل کوچک بودن و همچنین استفاده مکرر از آن در ارتباطات اینترنتی کمتر مورد توجه دیواره‌های آتش و مدیران شبکه می‌باشد به همین دلیل این پروتکل را برای ساخت کانال مخفی انتخاب کردیم.

در ابتدا پژوهش‌های انجام شده با موضوع ایجاد و یا کشف کانال مخفی بر اساس پروتکل دی.ان.اس. را بررسی کردیم و با انواع روش‌های ساخت و کشف کانال مخفی در این پروتکل آشنا شدیم. با این بررسی متوجه شدیم که کانال‌های مخفی ایجاد شده مبتنی بر پروتکل دی.ان.اس. همگی از نوع کانال مخفی باحافظه هستند به همین دلیل سعی کردیم کانال مخفی مبتنی بر پروتکل دی.ان.اس. ایجاد کنیم که به روش دیگری عمل کند.

کانال مخفی که در این پژوهش ایجاد کردیم یک کانال مخفی مبتنی بر ترتیب است که عملکرد آن بر اساس پروتکل دی.ان.اس. است. در این کانال مخفی به جای آنکه داده‌ای را در قسمتی از بسته‌های دی.ان.اس. ذخیره کند و یا از الگوی زمانی برای انتقال داده استفاده کند از ترتیب رسیدن بسته‌ها به خدمت دهنده‌های دی.ان.اس. استفاده شد. در این روش با توجه به تعداد خدمت‌دهنده‌های دی.ان.اس. به هر خدمت‌دهنده‌ی دی.ان.اس. یک کد اختصاص داده می‌شود. مشتری با توجه به داده‌ای که قصد جابه‌جایی آن را دارد و با توجه به کدهای اختصاص داده شده به خدمت‌دهنده‌های دی.ان.اس. درخواست خود را به خدمت‌دهنده دی.ان.اس. مناسب ارسال می‌کند. خدمت دهنده‌ی دی.ان.اس. زمان دریافت

بسته را ذخیره کرده و سپس یک درخواست مبتنی بر پروتکل اچ.تی.تی.پی. که شامل زمان ثبت شده و کد خدمت‌دهنده‌ی دی.ان.اس. است را برای یک خدمت‌دهنده‌ی اچ.تی.تی.پی. که وظیفه‌ی دریافت و تجمیع داده‌ی منتقل شده را دارد ارسال می‌کند. ادغام کننده بعد از دریافت همه‌ی بسته‌های ارسال شده از سمت خدمت‌دهنده‌های دی.ان.اس. بر اساس زمان بسته‌ها را مرتب می‌کند و در پایان از در کنار هم قرار دادن کدهای خدمت‌دهنده‌های دی.ان.اس. داده‌ی منتقل شده شکل می‌گیرد.

## مراجع

[1] S. Saeli, F. Bisio and L. Pierangelo, “DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach”, 2020.

[2] B. W. Lampson, “A Note on the Confinement Problem”, Association for Computing Machinery, 1973.

[3] N. Ishikura and D. Kondo, “DNS Tunneling Detection by Cache-Property-Aware Features”, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, 2021.

[4] M. A. Ayub, S. Smith and A. Siraj, “A Protocol Independent Approach in Network Covert Channel Detection”, International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2019.

[5] M. Naseralfoghara and H. Hamidi, “Web Covert Timing Channels Detection based on Entropy”, International Conference on Web Research, 2019.

[6] S. Chen, B. Lang, H. Liu, D. Li and C. Gao, “DNS Covert Channel Detection Method Using the LSTM Model”, Elsevier Ltd, 2020.

[7] P. Yang, X. Wan, G. Shi, H. Qu, J. Li and L. Yang, “Identification of DNS Covert Channel Based on Stacking Model”, International Journal of Computer and Communication Engineering, 2020.

[8] A. Karasaridis, K. Meier-Hellstern and D. Hoeflin, “Detection of DNS Anomalies using Flow Data Analysis”, IEEE, 2016.

[9] T. v. Leijenhorst, K.-W. Chin and D. Lowe, “On the viability and performance of DNS tunneling”, International Conference on Information Technology and Applications, 2008.

[10] S. Chen, B. Lang, H. Liu, D. Li and C. Gao, “DNS Covert Channel Detection Method Using the LSTM Model”, Elsevier Ltd, 2020.

[11] H. Hovhannisyan, K. Lu and J. Wang, “A Novel High-speed IP-Timing Covert Channel: Design and Evaluation”, 2015.