فصلنامه علمی-ترویجی پدافند غیرعامل
سال ششم، شماره ۲، تابستان ۱۳۹۴، (پیاپی ۲۲): صص ۳۶-۲۷

مروری بر روش‌های ردیابی نفوذ در شبکه گمنامی با استفاده از نشان‌گذاری جریان شبکه

احمد احمدی[۱]، مهدی دهقانی[۲]، محمود صالح اصفهانی [۳]

تاریخ دریافت: ۹۳/۰۱/۲۰
تاریخ پذیرش: ۹۳/۰۹/۱۲

چکیده

با گسترش اینترنت، ناامنی و جرائم آن رو به افزایش است. از طرفی توانمندی ردیابی نفوذ، نقش بازدارنده‌ای در ناامنی دارد و می‌توان آن را به‌عنوان یکی از راه‌کارهای پدافند غیرعامل در نظر گرفت. یکی از روش‌های ردیابی نفوذ، روش نشان‌گذاری ترافیک شبکه می‌باشد. در این روش با تغییر در الگوی جریان شبکه، ترافیک جریان خاص نشان‌گذاری می‌شود و در مرزهای خروجی شبکه آن جریان قابل‌ردیابی می‌باشد. روش‌های متعددی برای نشان‌گذاری ارائه شده است که بر روی زمان‌بندی ترافیک شبکه اعمال می‌شوند. در این تحقیق تمامی روش‌های مختلف موجود پس از بررسی، به دسته‌های مبتنی بر فاصله بین بسته‌ها و مبتنی بر پنجره زمانی دسته‌بندی می‌گردند و روش‌ها با معیارهای خاص مانند قابلیت اجرا در شبکه گمنامی، باهم مقایسه می‌شوند و در نهایت به‌صورت تحلیلی نشان خواهیم داد که روش‌های ترکیبی و روش‌های طیف گسترده دارای استحکام و کارایی بالاتری نسبت به دیگر روش‌ها می‌باشند.

کلیدواژه‌ها: ردیابی نفوذ، نشان‌گذاری، جریان شبکه.

۱- کارشناسی ارشد مهندسی نرم‌افزار، دانشگاه جامع امام حسین(ع) ahmadi.ihu@chmail.ir- نویسنده مسئول
۲- مربی گروه کامپیوتر، دانشگاه جامع امام حسین(ع)
۳- استادیار گروه کامپیوتر، دانشگاه جامع امام حسین(ع)

۱- مقدمه

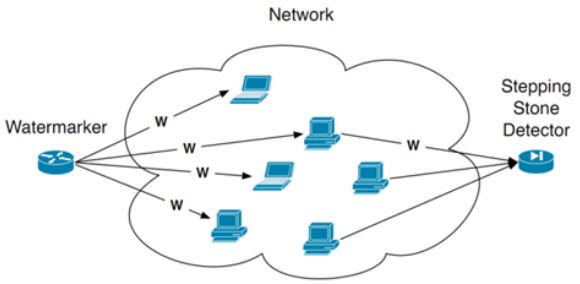
نشان‌گذاری[1]، کاربردهای مختلفی در علوم کامپیوتر دارد و در تحقیقات از آن با عنوان نشان‌گذاری دیجیتال نیز یاد شده است. از نشان‌گذاری برای مشخص کردن حق کپی محصولات چند رسانه‌ای مانند صوت، عکس و ویدیو استفاده می‌شود. اما در دهه اخیر از نشان‌گذاری برای نشانه‌دار کردن جریان شبکه به‌عنوان تحلیل ترافیک شبکه جهت شناسایی بهتر و کاراتر جریان‌ها، در مقایسه با تحلیل ترافیک غیرفعال و منفعل استفاده شده است و علاقمندی به نشان‌گذاری جهت کمک به تحلیل ترافیک رشد فزاینده ای پیدا کرده‌است. همچنین نشان‌گذاری جریان شبکه برای ردیابی نفوذ و حمله، پیشنهاد شده است. طرح‌های نشان‌گذاری مختلفی طراحی شده‌اند که اساساً از ایده‌های نشان‌گذاری چندرسانه‌ای اقتباس شده‌اند و به‌کارگیری آن ایده‌ها در محتوای جریان شبکه می‌باشد ولی به‌طورکلی می‌توان تغییر در الگوی محتوای جریان شبکه را نشان‌گذاری ترافیک شبکه نامید [۱]، مانند ایجاد تغییر در زمانبندی بسته‌ها که باعث نشان‌گذاری در ترافیک شبکه می‌شود. نشان‌گذاری‌ها یک روش مستقل از محتوا را برای برچسب زدن به ترافیک ارائه می‌دهند که جریان‌های همبسته بعد از گذشت از شبکه‌های مختلف قابل بازشناسی می‌باشند [۱].

به‌طورکلی کاربردهای نشان‌گذاری شامل ردیابی مبدأ نفوذ، کشف گمنامی ایجادشده در شبکه‌های گمنامی و شناسایی شبکه بات می‌باشد. مهاجمین شبکه معمولاً کوشش می‌کنند که مکان واقعی خودشان را با استفاده از بازتاب ترافیک[2] خود از طریق تعدادی میزبان آلوده[3]، پنهان کنند و بدین صورت ردپا یا هویت خود را پنهان می‌کنند. نشان‌گذاری ترافیک شبکه می‌تواند در شناسایی ترافیک‌های بازتاب شده استفاده شود. همان‌طور که در شکل ۱ آمده است، اگر جریان شبکه در نشان‌گذاری‌کننده نشان‌گذاری شود، درصورت عبور ترافیک نشان‌شده از شناسایی‌کننده موجود در شبکه، آن جریان نشان‌شده، قابل تشخیص می‌باشد [۲].

تا به حال دسته‌بندی برای روش‌های نشان‌گذاری بیان نشده است. این دسته‌بندی در شناخت روش‌ها و کارایی آن ها کمک می‌کند و می‌تواند ضعف‌ها و قوت‌های روش‌های مختلف را برآورد و احصا کند. در این مقاله به دسته‌بندی این روش‌ها و مقایسه معیارهای کارایی آن‌ها پرداخته می‌شود.

در ساختار این مقاله ابتدا فعالیت‌های مرتبط در بخش ۲ مرور

1– Watermarking
2– relaying
3– Zombi



شکل ۱-ردیابی با استفاده از نشان‌گذاری[۲].

می‌شود سپس در بخش ۳ مفاهیم نشان‌گذاری بررسی می‌شود و در ادامه به بررسی روش‌های نشان‌گذاری در بخش ۴ خواهیم پرداخت و در بخش ۵ با شناخت از روش‌ها، یک دسته بندی جدید ازروش‌های نشان‌گذاری ارائه می‌شود و در بخش ۶ مقایسه‌ی کلی از دسته‌های روش‌های متفاوت عنوان می‌گردد. در انتها نیز نتایج مقایسه‌ها، در بخش ۷ بیان می‌شود.

۲- پیشینه تحقیق

روش‌های مختلفی برای نشان‌گذاری ترافیک شبکه ابداع شده است که به‌طور کلی این روش‌ها، از روش‌های نشان‌گذاری دیجیتال الهام گرفته شده‌اند که در بعضی از موارد با ترکیب دو یا چند روش، شیوه‌ی جدیدی ارائه شده‌است. البته در بعضی از موارد با افزودن الگوریتم یا رمزنگاری خاص، روش‌های قبلی اصلاح و بهینه‌شده و در برابر بعضی از حملات به نشان‌گذاری، مقاوم شده‌اند.

یکی از اولین روش‌ها، روش ونگ و همکارانش می‌باشد، آن ها نشان‌گذاری مبتنی بر IPD[4] را معرفی می‌کنند که قبل از ارسال نیازمند آن است که بین نشان‌گذاری‌کننده و شناسایی کننده هماهنگی مستحکمی انجام شود [۳]. در مقاله دیگر ونگ و همکارانش در [۴]، طرحی با نام ICBW[5] را ارائه کرده‌اند. این طرح مبتنی بر تقسیم‌بندی جریان در فاصله‌های با طول مساوی می‌باشد. پیپون و همکارانش طرحی با نام IBW[6] را ارائه کرده‌اند [۵]. در این طرح نشان‌گذاری‌کننده و شناسایی‌کننده بر روی پارامترهای محرمانه توافق می‌کنند. این طرح در برابر بسته‌سازی مجدد[7] استحکام دارد.

البته این روش دارای نرخ‌های بسیار پایین در خطای مثبت کاذب و خطای منفی کاذب می‌باشد ولی در برابر حملات چند

4– Inter Packet Delay
5– Interval Centroid Based Watermarking
6– Interval Based Watermark
7– Repacketzation

جریانی مقاومت ندارد [۶]. ژنگ و همکارانش تلاش کرده‌اند که طرح IBW را در برابر حملات چند جریانی بهینه کنند [۷].

هومن صدر و همکارانش در [۸] روشی ارائه می‌دهند که روش ICBW را در برابر حملات چند جریانی مقاوم می‌کند و نام روش جدید را MAR-ICBW قرار می‌دهد. ونگ و همکارنش در تحقیقی دیگر [۹] روش جدیدی را با استفاده از روش ICBW و ترکیب آن با تکنیک کدگذاری طیف گسترده، ارائه می‌دهند که نام آن را با توجه به شیوه استفاده شده در آن DICBW قرار می‌دهند که کارایی و محرمانگی بالاتری نسبت به ICBW دارد و قادر به ردیابی جریان‌های چند گانه می‌باشد.

یو و همکارانش در [۱۰]، طرح DSSS را ارائه می‌کنند، این روش یک نشان‌گذاری دودویی می‌باشد که در جریان تعبیه‌شده و نامحسوس است ولی در برابر حملات چند جریانی آسیب‌پذیر است. با توجه به این‌که روش DSSS برای ردیابی جریان‌ها نیاز به نرخ ثابتی دارد، لو ژنگ و همکارانش روشی را برای بهبود این محدودیت ارائه می‌دهند [۱۱]. لیو و همکارانش در [۱۲]، روش ترکیبی جدیدی را با استفاده از روش‌های طیف گسترده و ICBW با نام ICBSSW ارائه کرده‌اند. هومن صدر و همکارانش در [۱۳]، روش رنگین‌کمان را ارائه می‌دهند که مبتنی بر بسته می‌باشد، این طرح به علت استفاده از یک سیستم هماهنگ‌کننده که توسط نشان‌گذار و شناسایی‌کننده قابل‌دسترس است، این روش اولین روش نشان‌گذاری جریان به‌صورت غیرکور است. آن‌ها در [۱۴] برای بالا بردن کارایی شناسایی در روش رنگین‌کمان از الگوریتم رمز تجمع تکراری استفاده و روش C-RAINBOW را ایجاد می‌کنند.

لیانگچن ژنگ و همکارانش روشی با نام MMAR-SSW را ارائه می‌کنند که در برابر حملات MSAC و MFA مقاوم می‌باشد. این روش دارای محرمانگی بیشتری است [۱۵]. هوآنگ و همکارانش در [۱۶] روشی را برای بهبود DSSS ارائه می‌دهند. در این روش با طولانی‌ترکردن شبه نویز در روش سابق، نامحسوسی نشان‌گذاری را افزایش می‌دهند.

هومن‌صدر و همکارانش در [۲] با ارائه طرح جدید SWIRL اولین رویکرد عملی را برای تحلیل ترافیک مقیاس بزرگ آماده کرده‌اند. همچنین در انتهای رساله دکترای هومن صدر، یک چارچوب تشخیص با نام BotMosaic، برای شناسایی و ردیابی شبکه بات با استفاده از نشان‌گذاری ارائه شده است [۱۷]، هدف اصلی این طرح شناسایی ماشین‌های آلوده در داخل یک شبکه کوچک می‌باشد. یک شبکه بات دارای یکسری ماشین‌های آلوده و یک نفوذگر به‌عنوان هدایت‌کننده بات‌ها می‌باشد. که با استفاده از BotMosaic می‌توان موجودیت‌های شبکه بات را ردیابی کرد.

۳- مفاهیم نشان‌گذاری

در این بخش مختصری در مورد مفاهیم پایه‌ی روش‌های فعال ردیابی نفوذ یا همان روش‌های نشان‌گذاری تعاریفی مطرح می‌شود.

۳-۱- تحلیل ترافیک و نشان‌گذاری

نشان‌گذاری به معنی نشان‌گذاشتن یا نقش بر آب زنی می‌باشد. اگر یک چوبی را در دست خود بگیرید و بر روی آب نقشی حک کنید، بعد از مدتی محو می‌شود. ولی این نوشته وجود داشته است. نشان‌گذاری علائمی هستند که در زمینه کاغذها، تمبرها یا اسکناس‌ها قرار داده می‌شوند و در حالت عادی قابل‌مشاهده نیست.

روش‌های تحلیل ترافیک شبکه را می‌توان به چهار نوع مختلف تقسیم‌بندی کرد که انواع آن‌ها را می‌توان در یکی از دسته های فعال مبتنی بر میزبان، غیرفعال مبتنی بر شبکه، غیرفعال مبتنی بر میزبان و فعال مبتنی بر شبکه تقسیم‌بندی کرد [۱۸]. جدول یک

جدول ۱- دسته‌بندی روش‌های تحلیل ترافیک و مصادیق آن‌ها [۱۸].

	Passive	Active
Host-based	DIDS, CIS	Caller ID
Network-based	Thumb printing	IDIP
	Timing-Based	CITRA
	Deviation-Based	SWT
	Online Sketching	RAINBOW
		SWIRL

روش‌های تحلیل ترافیک را به‌همراه مصادیق عنوان می‌کند.

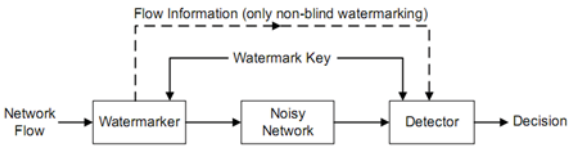
نشان‌گذاری ترافیک شبکه از نوع روش تحلیلی فعال مبتنی بر شبکه می‌باشد. نشان‌گذاری به‌طور قابل توجهی محاسبات و هزینه‌های ارتباطی تحلیل ترافیک را کاهش می‌دهد. همچنین می‌توان شناسایی دقیقی را با کمترین خطای مثبت اشتباهی انجام داد. در روش‌های قدیمی، با استفاده از الگوهای اصلی جریان ترافیک شبکه مانند زمان‌بندی، اندازه و تعداد بسته‌ها، پیوندهای جریان ورودی با جریان خروجی مقایسه شده است [۴].

تحلیل ترافیک می‌تواند برای شناسایی اینکه چه کسی با چه

کسی در یک شبکه عمومی ارتباط دارد، به‌کار گرفته شود. در تحلیل ترافیک غیرفعال با بررسی جریان‌های مختلف، جریان‌های مرتبط استخراج می‌شود، با تحلیل ترافیک غیرفعال اگر یک تحلیل‌کننده n جریان ورودی و m جریان خروجی را مشاهده کند. تحلیل ترافیک غیرفعال به تحلیل مرتبه O(n) ارتباط بین نفوذگرها و تحلیل O(nm) محاسبه نیازمند خواهد بود. برای مثال یک تحلیل‌کننده مجبور است مشخصات تمام n جریان را به دیگران ارسال کند و سپس جریان خروجی باید با هر جریان ورودی مقایسه شود. یکی از روش‌های فعال در پایین آوردن سربار محاسبات، استفاده از نشان‌گذاری جریان ترافیک شبکه است. در این روش بعد از برقراری اشتراک کلید محرمانه بین دو تحلیل‌کننده، نیازی به هیچ ارتباطی نیست و هزینه محاسبات آن O(n) و O(m) به‌ترتیب در نشان‌گذاری‌کننده و شناسایی‌کننده می‌شود [۱۹]. از کاربردهای مثبت کانال پوششی نشان‌گذاری ارتباطات خاص است [۲۰]، نشان‌گذاری در حقیقت نوعی کانال زمانبندی‌دار پوششی می‌باشد که در سطح دیگر تنها برای نشان گذاشتن ترافیک استفاده می‌شود با این تفاوت که در نشان گذاری معیار ظرفیت به‌هیچ وجه اهمیت ندارد ولی در کانال پوششی معیار ظرفیت از اهمیت بالایی برخوردار است. شیوه‌های هردو شبیه به هم هستند ولی در کانال پوششی شناسایی‌کننده از پیغام موجود در کانال اطلاعی ندارد و باید آن را در یک جریان خاص کشف کند. درصورتی که شناسایی‌کننده در نشان‌گذاری از پیغام کاملا مطلع است و در تلاش است پیغام را در جریان‌های متفاوت کشف کند.

نشان‌گذاری‌کننده جریان ورودی مورد نظر را نشان‌گذاری می‌کند و شناسایی‌کننده هر جریان خروجی را برای یافتن نشان شده‌های موجود کنترل می‌کند. در تحلیل ترافیک‌های با حجم بالا به صورت منفعل نسبت به تحلیل‌های فعال کمبود عدم مقیاس‌پذیری مشاهده می‌شود. که استفاده از روش‌های نشان‌گذاری جریان شبکه راه حل مناسبی برای حل این مشکل است. شکل ۲ مدل عمومی نشان‌گذاری جریان شبکه را نمایش می‌دهد. یک جریان شبکه‌ای که از نشان‌گذاری‌کننده عبور می‌کند، به‌وسیله تغییر دادن اطلاعات زمان‌بندی بسته‌ها نشان‌گذاری می‌شود. برای مثال با به‌کار بردن تأخیر مشخصی بر روی بسته‌ها نشان‌گذاری انجام می‌شود.

جریان از امتداد یک کانال نویزدار عبور می‌کند که ممکن است شامل شبکه‌های مختلف و سیستم‌های گمنامی باشد. این کانال



شکل ۲- مدل عمومی نشان‌گذاری[۲].

تأخیرهای اضافی را نشان می‌دهد و ممکن است باعث از بین رفتن، جابجایی و تکثیر بسته‌ها گردد. بعد از گذشت از کانال، جریان به شناسایی‌کننده نشان‌گذاری می‌رسد. که جریان را برای یافتن الگوی نشان‌گذاری شده مندرج در آن تفتیش می‌کند که الگوی کد گذاری باید مبتنی بر کلید محرمانه نشان‌گذاری باشد. که بین نشان‌گذاری‌کننده و شناسایی‌کننده اشتراک گذاشته شده است [۲].

۳-۲- حملات نشان‌گذاری

قبل از حمله به نشان‌گذاری لازم است ابتدا وجود نشان‌گذاری در جریان شبکه تشخیص داده شود. جهت تشخیص نشان گذاری می‌توان از روش‌های آماری تشخیص کانال‌های زمانبندی دار پوششی استفاده کرد [۲۱]. زمانی که نفوذگری بتواند پس از تشخیص، چندین جریان نشان‌گذاری‌شده را مشاهده کند، درصورت ضعف روش نشان‌گذاری می‌تواند آن را از بین ببرد. ممکن است، نفوذگر عمداً مشخصات ترافیک را تغییر دهد، تا از نشان گذاری انجام‌شده جلوگیری کند و با این اقدام، نفوذگر به نوعی در برابر ردیابی انجام‌شده در برابر حمله‌اش که در واقع یک ضدحمله از طرف قربانی است، می‌تواند واکنش ضد، ضدحمله انجام دهد. سرانجام جریان تغییریافته به نقطه شناسایی می‌رسد که با تغییرات حاصل‌شده در جریان، شناسایی‌کننده قادر به تشخیص جریان نشان‌دار نخواهد بود. به‌طورکلی چهار حمله به روش‌های مختلف نشان‌گذاری تا به حال مطرح شده است. این حملات شامل PNR [۲۲]، MFA [۶]، MSAC [۱۵] و BACKLIT [۲۳] می‌باشد. در بخش ۵ یکی از معیارهای که در مورد طرح‌ها و روش‌ها بررسی خواهد شد، معیار مقاومت در برابر حملات است.

۳-۳- شبکه گمنامی

شبکه گمنامی، شبکه‌ای است از تونل‌های مجازی که به افراد و گروه‌ها اجازه می‌دهد تا امنیت و حفاظت از حریم خصوصی خود را در اینترنت تقویت کنند. این شبکه با پنهان کردن هویت و مبدأ افراد سعی در پنهان کردن حریم افراد دارد. در سیستم گمنامی، تعدادی جریان‌های ورودی به تعدادی جریان‌های خروجی نگاشت

1– Drake and Little, 1983; Westine and Friesenhahn, 1983; Henrych, 1979; Drake et al, 1989;
2- Drake and Little (1983)
3- Little- Drake

می‌شوند که جریان ورودی به‌صورت رمزشده به سرورهای میانی شبکه متصل و هر کدام از این اتصالات نیز رمز شده می‌باشند، به‌طوری‌که رابطه بین آن‌ها مانند یک جعبه سیاه پنهان می‌باشد، البته با استفاده از نشان‌گذاری ترافیک شبکه گمنامی می‌توان مبدأ اصلی نفوذ را کشف کرد. یکی از انواع شبکه‌های گمنامی مسیریاب‌های پیازی شکل است. هدف از مسیریابی پیازی شکل، حفاظت در مقابل تحلیل ترافیک و حفاظت از افشای محتوای پیام ارسالی است. انواع شبکه‌های مختلف از جمله TOR, I2P, FreeNet از مسیریابی پیازی شکل استفاده می‌کنند که TOR برجسته‌ترین آن‌هاست [۲۴]. لذا در این مقاله یکی از ارزیابی‌ها از روش های نشان‌گذاری، سابقه کار در محیط TOR فرض می‌شود. در شبکه TOR، در راه رسیدن پیام از فرستنده به گیرنده پیام‌ها به‌طور مداوم و تکراری در نودهای شبکه که به آن‌ها مسیریاب پیازی شکل می‌گویند، رمزنگاری و رمزگشایی می‌شوند. امکان این وجود ندارد که کسی با این رمزنگاری و رمزگشایی قادر به شناسایی مبدأ، مقصد و محتوای پیام باشد. محتوای پیام تنها در مقصد بعد از طی مسیر شبکه، قابل آشکار شدن است. فرستنده به‌طور تصادفی تعدادی از مسیریاب‌ها را برای ساختن مسیری تا مقصد انتخاب می‌کند. سپس فرستنده محتوای پیام و دستورالعمل را برای مسیریاب بعدی، توسط رمزنگاری کلیدهای عمومی، به‌صورت رمز شده در می‌آورد و به همین شکل ادامه می‌یابد.

۴- بررسی روش‌های نشان‌گذاری

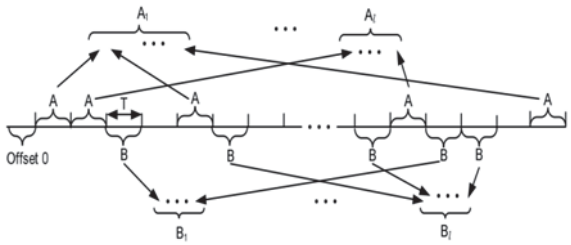
نشان‌گذاری دیجیتال و به‌خصوص نشان‌گذاری چندرسانه ای، موضوعاتی نسبتاً جا افتاده هستند. در اصل بسیاری از طرح های نشان‌گذاری جریان، الهام گرفته از نشان‌گذاری در عرصه چند رسانه‌ای هستند. چند نمونه از این موارد عبارتند از: طرح ونگ و همکارانش نمونه‌ی بارزی است از نشان‌گذاری QIM، که نوعی روش نشان‌گذاری چند رسانه‌ی است. طرح IBW که توسط پیون و همکارانش ارائه شده است [۵]، مبتنی بر نشان گذاری وصله‌ای مربوط به بندر و همکارانش است. طرح یو و همکارانش،که DSSS نام دارد، بر نشان‌گذاری طیف گسترده استوار است.

در ادامه طرح‌های نشان‌گذاری را از لحاظ کاربرد و شیوه‌های اجرا بررسی می‌کنیم تا بتوان آن‌ها را دسته‌بندی کنیم. طرح IPD که طرحی ساده است به‌دلیل عدم مقاومت در برابر تلفات بسته، جابجایی و لغزش زمانی شبکه، استحکام پایینی نسبت به طرح‌های دیگر دارد. این نشان‌گذاری همچنین مستعد شناسایی توسط روش‌های تشخیص نشان‌گذاری می‌باشد که خود باعث از بین رفتن نشان‌گذاری است. طرح ICBW که مبتنی بر تقسیم‌بندی جریان در فاصله‌های با طول مساوی می‌باشد، جهت استفاده در شبکه‌های گمنامی ارائه شده است.

دو پارامتر o که offset اولین فاصله و T که طول هر فاصله می‌باشد در این طرح تعریف شده است و طول فاصله با استفاده از اعداد تصادفی تولیدشده از یک مقدار شروع‌کننده یکسان S، به‌طور تصادفی به دو زیرمجموعه A وB تقسیم می‌شود که هر مجموعه A و B به طور تصادفی به l زیرمجموعه تقسیم می‌شود که هر کدام دارای فاصله r می‌باشد. شکل۳ نحوه تقسیم بندی را نمایش می‌دهد.

بنابراین یک نشان‌گذاری با طول l می‌تواند در جریان جاسازی شود. برای نشان‌گذاری بیت صفر، تمام زیرمجموعه‌های A را بدون تأخیر، ارسال می‌کند و تمام زیرمجموعه‌های B را با تأخیر ارسال می‌کند، که شکل ۴ نشان‌گذاری بیت صفر را نمایش می‌دهد.

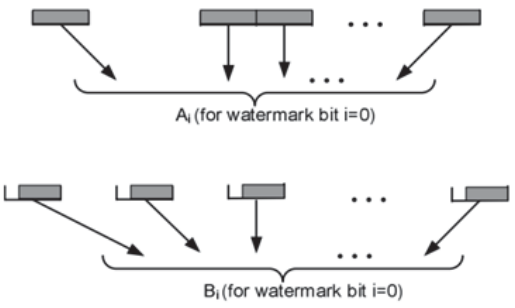
برای نشان‌گذاری بیت یک، تمام زیرمجموعه‌های B را بدون تأخیر و تمام زیرمجموعه‌های A را با تأخیر ارسال می‌کند. در طرح IBW زمان‌های ورود بسته‌ها بر اساس یک مجموعه از فاصله های زمانی از قبل انتخاب‌شده دست‌کاری می‌شود. درج نشان‌گذاری با



شکل ۳- تقسیم‌بندی فاصله T به‌صورت تصادفی در روش ICBW [۴]

استفاده از تغییرات نرخ و آهنگ ترافیک در فاصله‌های متوالی حاصل می‌شود.

این تغییر به دو صورت قابل انجام است: در یک فاصله Ii ممکن است با تأخیر ایجادشده، تمام بسته‌ها از فاصله Ii تا فاصله Ii+۱ پاک شده باشد یا ممکن است با تأخیر تمام بسته‌ها از فاصله Ii-۱

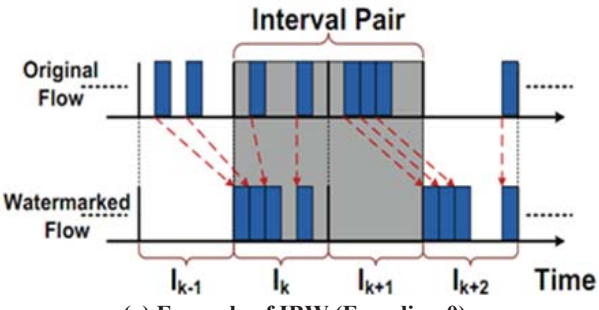


شکل ۴- نشان‌گذاری بیت صفر در فاصله T در روش ICBW [۴]

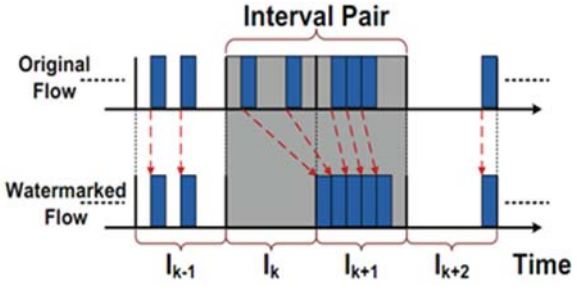
تا فاصله Ii بارگذاری شده باشد. در فاصله زمانی بارگذاری‌شده، تعداد بسته‌های مورد انتظار دو برابر می‌شود و در فاصله زمانی پاک شدن، بسته‌ای دریافت نمی‌شود. در ارسال بیت صفر در مکان i بسته‌های فاصله زمانی Ii پاک شده است و بسته‌های Ii+۱ بارگذاری شده است. در ارسال یک در فاصله زمانی بسته‌های موجود در Ii بارگذاری و در Ii+۱ پاک شده است. این طرح در ابتدا از استحکام مناسبی برخوردار بوده است ولی با ارائه حملات چند جریانی استحکامی در برابر این حمله نداشته و نامحسوسی خود را از دست داده است. شکل ۵ نحوه نشان گذاری IBW را نمایش می‌دهد.

طرح DSSS یک نشان‌گذاری دو دویی می‌باشد که با رویکرد ردیابی در شبکه‌های گمنامی ارائه شده است. در این روش هر بیت با طول n نشان‌گذاری دودویی در فاصله‌ای با طول Ts تعبیه شده است. از این رو تمام نشان‌گذاری در یک فاصله به طول nTs مندرج شده است. برای درج نشان‌گذاری بیت۱، نرخ بسته‌های در فاصله معین‌شده با طول Ts مطابق کد نویز ساختگی دستکاری و تغییر می‌شوند. این کد یک علامت سریع و متنوعی می‌باشد که بین +۱ و -۱ عوض می‌شود. شکل ۶ ساختار نشان‌گذاری DSSS را نمایش می‌دهد.

البته به‌علت عدم نامحسوسی این روش دو طرح دیگر برای بهبود آن ارائه شده است. از طرفی به‌دلیل این‌که جریانی که در DSSS باید نشان‌گذاری شود، باید نرخ ترافیک ثابتی داشته باشد،

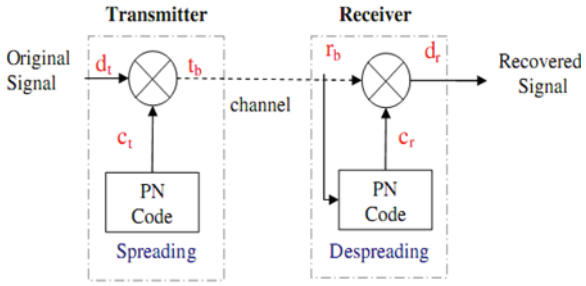


(a) Example of IBW (Encoding 0).



(b) Example of IBW (Encoding 1).

شکل ۵- نشان‌گذاری به روش IBW [۵]



شکل ۶- ساختار نشان‌گذاری DSSS [۱۰]

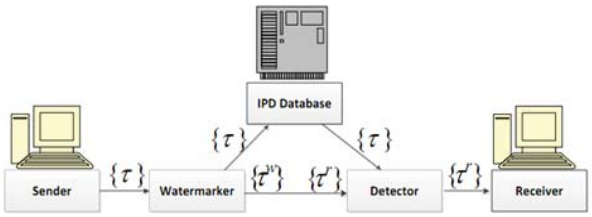
که این محدودیت، طرح را در اجرا دچار مشکل خواهد کرد. برای همین در [۱۱] به‌جای استفاده از نرخ ترافیک از تحمیل خصوصیات آماری مربوط به زمان رسیدن بسته‌ها در جریان استفاده می‌شود البته نتایج DSSS بهینه‌شده، کارایی بیشتر آن را نمایش می‌دهد.

طرح MAR-ICBW در حقیقت بهینه کننده طرح ICBW جهت مقاومت در برابر حملات MFA می‌باشد. آسیب‌پذیری که در طرح‌های مبتنی بر فاصله مانند ICBW وجود دارد، آن است که در این روش‌ها نشان‌گذاری که در جریان درج می‌شود در مکان‌های ثابتی درج می‌گردد، بنابراین یک نفوذگر می‌تواند چندین جریان نشان‌گذاری شده را باهم بررسی کند و در این‌صورت نشان‌گذاری قابل مشاهده می‌باشد. راه‌کاری که برای حل این آسیب‌پذیری در طرح MAR-ICBW آمده است، آن است که برای درج نشان‌گذاری از مکان‌های متفاوت استفاده شود و برای این امر استفاده از مقادیر اولیه تولید عدد تصادفی متفاوت برای هر جریان پیشنهاد شده است [۸]. روش MMAR-SSW بهبوددهنده و مقاوم کننده روش طیف گسترده در برابر حملات MFA و MSAC می‌باشد. این روش با استفاده از چندین کد شبه نویز مستقل، برای انتقال بیت‌های متفاوت سعی در غلبه بر حملات نشان‌گذاری دارد. روش MAR-IBW آسیب‌پذیری روش IBW را در برابر حملات چند جریانی بهینه و ایمن می‌کند. در این روش علاوه بر اشتراک پارامترهای نشان‌گذاری بین نشان‌گذاری و شناسایی‌کننده، یک لیست از اعداد را برای تولید اعداد تصادفی اشتراک‌گذاری می‌کنند. از این اعداد برای تولید تصادفی فاصله استفاده می‌شود، تا جریان‌های مختلف باهم متفاوت باشند [۷].

روش رنگین‌کمان روشی مبتنی بر فاصله بین بسته می‌باشد، این طرح به‌علت استفاده از یک سیستم هماهنگ‌کننده که توسط نشان‌گذاری و شناسایی‌کننده قابل‌دسترس است، اولین روش نشان‌گذاری جریان به‌صورت غیر کور می‌باشد. که در برابر تلفات بسته و گم شدگی و جابه‌جایی آن مقاوم است. ولی در سناریوهای

بزرگ مقیاس‌پذیر نیست. با استفاده از ذخیره زمان‌بندی جریان ورودی و مقایسه آن با زمان‌بندی جریان خروجی، این روش یک طرح غیر کور می‌باشد که شکل ۷ غیر کور بودن آن را نمایش می‌دهد.

این طرح در ابتدا از استحکام مناسبی برخوردار بود. ولی با ارائه ابزار BACKLIT توسط لیو و همکارانش در برابر حملات و شناسایی آن مقاومتی نداشته و در نتیجه نامحسوسی خود را از



شکل ۷- ساختار روش رنگین‌کمان [۱۳]

دست داد [۲۳].

در طرح C-RAINBOW که برای بالا بردن کارایی شناسایی در رنگین‌کمان، از کدهای تجمع تکراری استفاده شده است. این کدها دارای پیچیدگی پایین و کارایی بالا در تصحیح خطا می‌باشند. این کد به این‌صورت کار می‌کند که یک قطعه اطلاعاتی به اندازه n_A به تعداد q مرتبه تکرار می‌شود و سپس با استفاده از تابع جای‌گشتی به اندازه $q \times n_A$ کد می‌شود و توسط یک انباشت‌گر با نرخ یک رمز می‌شود [۱۴].

در کل طرح C-RAINBOW شبیه به رنگین‌کمان است با این تفاوت که اختلافاتی در شیوه شناسایی در شناسایی‌کننده برای بالابردن کیفیت شناسایی ایجاد شده است.

طرح SWIRL در برابر آشفتگی و اختلال شبکه مقاوم است. این روش، از نوع نشان‌گذاری کور می‌باشد، که باعث کاهش سربار ارتباطات و سربار محاسبات در مقایسه با تحلیل ترافیک غیرفعال یا طرح‌های نشان‌گذاری غیر کور می‌شود. در این روش، الگوی نشان‌گذاری مبتنی بر مشخصات جریان نشان‌دار شده، انتخاب‌شده است. در نتیجه هر جریان نشان‌دار با یک الگوی متفاوت نشان‌دار می‌شود.

نشان‌گذاری SWIRL تأخیرهای کوچک را در جریان شبکه معرفی می‌کند. SWIRL در برابر بسته‌های از بین رفته و بی‌ثباتی شبکه ناشی از لغزش زمانی مقاوم می‌باشد. این روش تأخیرهای کوچکی را مطرح می‌کند. که هم برای کاربران عادی و هم برای حمله‌کننده غیرقابل رویت می‌باشد [۲].

تاکنون دو مورد طرح ترکیبی برای نشان‌گذاری در ترافیک شبکه عنوان شده است. یکی از آن‌ها طرح ترکیبی ICBSSW است که از ترکیب دو روش ICBW و روش طیف گسترده استفاده می‌کند. این روش یک شیوه مناسب برای چندین جریان شبکه به‌صورت موازی بدون پیش‌فرض و محدودیت محسوب می‌شود و با استفاده از کدهای شبه نویز به‌صورت تصادفی، می‌تواند حملات MFA و MSAC را خنثی کند [۱۲].

طرح ترکیبی دیگر طرح DICBW می‌باشد، این طرح نیز شبیه به طرح ICBW است با این تفاوت که در گرفتن فاصله نشان‌گذاری به جای گرفتن یک فاصله، دو فاصله هم‌زمان می‌گیرد و تمام اعمال و پارامترهای که در ICBW انجام می‌شود، در این روش جدید برای هر دو فاصله استفاده می‌شود [۹]. در این روش نیز یک حالت ترکیبی با استفاده از طیف گسترده توصیه می‌شود. که باعث بالا رفتن کارایی روش ترکیبی می‌گردد.

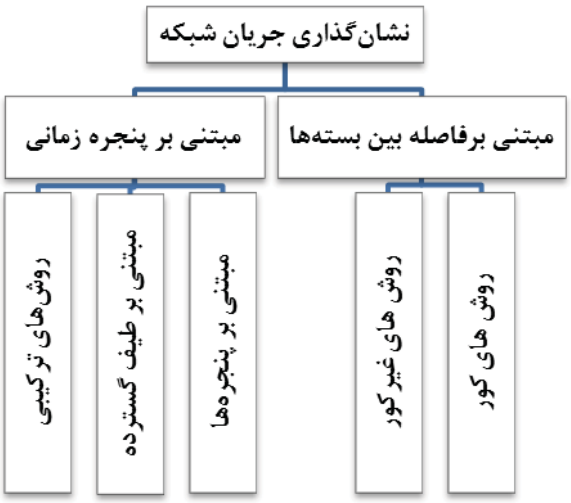
۵- دسته‌بندی روش‌های نشان‌گذاری

روش‌های مختلفی برای نشان‌گذاری ترافیک شبکه ابداع شده است. همان‌طور که در بخش قبل اشاره شد، معمولاً این روش‌ها از روش‌های نشان‌گذاری دیجیتال الهام گرفته شده‌اند. این روش‌ها در بعضی از موارد با ترکیب دو یا چند روش، به‌صورت یک روش ترکیبی ارائه شده است. در بعضی از موارد با افزودن الگوریتم خاص به روش‌های قبلی، آن را اصلاح و بهینه کرده‌اند و در برابر بعضی از حملات، آن‌ها را مقاوم کرده‌اند.

دسته‌بندی‌های متفاوتی از دیدگاه‌های مختلف برای طرح‌های نشان‌گذاری مطرح شده است، از منظر قابل‌تشخیص بودن جریان نشان‌گذاری‌شده در فاصله بین شناسایی‌کننده و نشان‌گذاری‌کننده می‌توان طرح‌های نشان‌گذاری را به دو دسته محسوس و نامحسوس تقسیم نمود، از منظر هماهنگی بین شناسایی‌کننده و نشان‌گذاری‌کننده این روش‌ها را می‌توان به دو دسته کور و غیر کور تقسیم‌بندی کرد. با مطالعه و بررسی تمامی روش‌های نشان‌گذاری ترافیک شبکه، تقسیم‌بندی جامعی از روش‌های نشان‌گذاری در شکل ۸ ارائه شده است [۲۵].

این روش‌ها را می‌توان به دو قسمت مبتنی بر فاصله بین بسته‌ها و پنجره زمانی تقسیم کرد. در روش‌های مبتنی بر فاصله بین بسته‌ها [۳, ۱۳, ۱۴] منحصراً بر روی تأخیرهای بین بسته ها عمل می‌کند. این روش‌ها در برابر تلفات بسته‌ها، جابجایی و جا اندازی مقاوم نیستند. ولی در روش‌های مبتنی بر پنجره زمانی [۲, ۴, ۵, ۸-۱۲, ۱۵, ۱۶] یک عمل را در یک فاصله زمانی کامل

انجام می‌دهد. که این نوع نشان‌گذاری‌ها مستعد حمله چند جریانی



شکل ۸- دسته‌بندی روش‌های نشان‌گذاری [۲۵].

می‌باشند که البته در بعضی از آن‌ها، با اعمال تغییراتی در برابر حملات مقاوم می‌شوند. در روش‌های مبتنی بر فاصله بین بسته‌ها سه روش تا کنون ارائه شده است که این بخش را می‌توان در دو قسمت کور و غیرکور تقسیم‌بندی کرد.

روش‌های مبتنی بر پنجره زمانی تنوع بیشتری را به خود اختصاص داده‌اند، به‌طوری که می‌توان آن را به سه قسمت مختلف مبتنی بر پنجره‌ها، مبتنی بر طیف گسترده و روش‌های ترکیبی دسته‌بندی کرد.

در جدول ۲ هر کدام از روش‌ها بر اساس معیارهای خاص، ارزیابی و بررسی‌شده‌اند. بعضی از این معیارها، همان معیارهای کارایی روش‌های نشان‌گذاری در ترافیک شبکه می‌باشد. اساس یک روش نشان‌گذاری توانمندی در نامحسوسی در بین مسیر و استحکام در برابر نویز و لغزش زمانی شبکه می‌باشد. از طرفی یکی از خطراتی که نشان‌گذاری را تهدید می‌کند، حملات به نشان‌گذاری است، لذا در این جدول استحکام روش‌ها را در برابر حملات موجود بررسی شده‌اند. توانمندی اجرا در مقیاس‌های واقعی نیز یکی دیگر از معیارهای بررسی روش‌ها می‌باشد. یک روش نشان‌گذاری علاوه بر این‌که ترافیک حجم بالا را پشتیبانی می‌کند باید بتواند چندین جریان را ردیابی کند. از طرفی به‌علت این‌که یکی از کاربردهای اساسی نشان‌گذاری ردیابی ترافیک‌های گمنامی است، معیار آخر برای مقایسه را سابقه اجرای روش در ردیابی در یکی از شبکه‌های گمنامی قرار داده‌ایم. تمامی روش‌ها بر اساس پنج معیار در جدول۲ بررسی شده‌اند.

جدول ۱- دسته‌بندی روش‌های تحلیل ترافیک و مصادیق آن‌ها [۱۸].

روش‌ها				معیارها	مقیاس پذیری	شبکه گمنامی (anonymous)	ارزیابی شده در TOR	نامحسوسی	استحکام در برابر جیتر و...	استحکام در برابر حملات: MSAC	استحکام در برابر حملات: BACKLIT	استحکام در برابر PNR	استحکام MFA
روش های مبتنی بر فاصله بین بسته ها	روش های کور	IPD			[2]	✓	✓	[2]	[2]		✓	[22]	[2]
	روش های غیر کور	RAINBOW			[2]	✓	✓	[13]	[13]		[23]		[2]
		C-RAINBOW			✓	✓	✓	[14]	[14]	✓	✓	✓	[2]
روش های مبتنی بر پنجره زمانی	مبتنی بر پنجره ها	IBW			[2]	✓	[25]	[2]	[5]		[23]	✓	[2]
		ICBW			[2]	[4]	✓	[2]	[4]		[23]	✓	[2]
		MAR-ICBW			[2]	✓	✓	✓	[8]	✓	✓	✓	[8]
		MAR-IBW			[2]	✓	✓	✓	[7]	✓	✓	✓	[7]
		SWRL			[2]	✓	✓	[17]	[17]	✓	[23]	✓	[17]
	مبتنی بر طیف گسترده	DSSS			[2]	✓	[10]	[2]	[10]			✓	[15]
		Improved DSSS			✓	✓	✓	✓	[11]			✓	✓
		SSW			[15]	✓	✓	[15]	[15]	[15]	✓	✓	[15]
		MMAR			✓	✓	✓	✓	[16]	[16]	✓	✓	✓
		long PN DSSS			✓	✓	✓	✓	[16]	[16]	✓	✓	✓
	روش های ترکیبی	DICBW			[9]	✓	✓	✓	[9]		✓	✓	✓
		ICBSSW			[12]	✓	✓	[12]	[12]	[12]	✓	✓	✓

۶- تحلیل و مقایسه روش‌ها

در نگاه اول به جدول۲ می‌توان تنوع و گستردگی روش‌های مبتنی بر پنجره زمانی نسبت روش‌های مبتنی بر فاصله بین بسته‌ها را ملاحظه کرد و این به‌لحاظ کارایی بالای روش‌های مبتنی بر پنجره زمانی می‌باشد. در حالت کلی، استحکام در برابر حمله MFA در تمامی روش‌های مبتنی بر فاصله بین بسته‌ها مناسب است. ولی این حمله استحکام طرح‌های اولیه روش‌های مبتنی بر پنجره زمانی [۴، ۵، ۱۰] را از بین برده‌است. البته بعضی از روش‌ها

که بهبود روش‌های قبلی است، خود را در برابر این حمله مقاوم کرده‌اند. در برابر حمله BACKLIT ، حتی طرح‌های آخری مانند SWIRL و رنگین‌کمان نیز از خود مقاومت نشان نمی‌دهد. ولی در حالت کلی روش‌های مبتنی بر پنجره زمانی نسبت به روش‌های مبتنی بر فاصله بین بسته‌ها از خود مقاومت بیشتری در برابر حملات دارند.

معیار استحکام در برابر تغییرات شبکه و نویز و معیار نامحسوسی هر کدام به خودی خود لازمه‌ی نشان‌گذاری می‌باشند. لذا تقریباً در تمامی روش‌های مطرح‌شده بجز روش اولیه‌ی IPD استحکام در برابر نویز وجود دارد. در مورد معیار نامحسوسی نیز در ابتدای ارائه روش‌ها نامحسوسی وجود داشته است ولی با ارائه حملات مختلف، نامحسوسی بعضی از روش‌ها از بین رفته است. لذا در حالت کلی می‌توان گفت که تمامی روش‌ها بجز روش های اولیه دارای نامحسوسی می‌باشند.

با توجه به بررسی ردیابی نفوذ در شبکه گمنامی، در معیار سابقه ارزیابی در شبکه گمنامی تنها چهار مورد از روش‌ها در این شبکه ارزیابی شده‌اند. ولی در شبکه گمنامی TOR تنها روش DSSS و IBW ارزیابی شده است و در شبکه گمنامی anonymouse.com روش‌های ICBW و Long PN DSSS ارزیابی شده‌اند. ولی به‌علت رمزنگاری‌ها و بسته‌سازی‌های مجدد موجود در شبکه‌های گمنامی، روش‌های مبتنی بر فاصله بین بسته‌ها توانمندی کمتری در ردیابی نفوذ نسبت به روش‌های مبتنی بر پنجره زمانی دارند.

در مورد معیار مقیاس‌پذیری تنها روش‌های غیر کور مبتنی بر فاصله بین بسته‌ها، توانمندی انجام آن را ندارند و این هم به‌علت آن است که همگام‌سازی تعداد زیادی جریان را در محیط واقعی، بین نشان‌گذاری‌کننده و شناسایی‌کننده نیاز به زیرساخت‌های مختلف و زیادی دارد. که عملاً انجام ناپذیر است. ولی در حالت کلی می‌توان عنوان کرد که روش‌های ترکیبی و روش‌های طیف گسترده دارای استحکام و کارایی بالاتری نسبت به دیگر روش‌ها دارند.

همچنین می‌توان نتیجه گرفت که بیشتر روش های اخیر، روش‌های طیف گسترده و ترکیبی هستند، که این دلیلی دیگر بر کارایی آن‌ها محسوب می‌گردد و از طرفی روش کور مبتنی بر فاصله بین بسته‌ها ناکارآمدترین روش نشان‌گذاری محسوب می‌گردد.

۷- نتیجه‌گیری

روی‌کرد فعلی برای طراحی نشان‌گذاری‌های جریان شبکه دچار چندین معضل است. یکی از این معضلات این است که این طرح‌ها الهام گرفته از نشان‌گذاری‌های دیجیتال هستند و لذا با توجه به این تشابه توجه کمتری به این مشکلات طراحی نشان‌گذاری در سطح کلان معطوف می‌شود. برای مثال در نشان‌گذاری دیجیتال، مشخصه‌های آماری چندرسانه‌ای مربوطه از جمله موضوعات مهمی است که همیشه مد نظر قرار می‌گیرد، اما در تحقیقات مربوط به نشان‌گذاری شبکه، اثرات ناشی از مشخصه‌های ترافیک شبکه بر نشان‌گذاری به‌خوبی مورد توجه قرار نمی‌گیرد. تراکم حجم ترافیک، درج نامحسوسی نشان‌گذاری را در ترافیک شبکه مشکل می‌سازد.

نتایجی که در بررسی تحلیلی روش‌ها به‌دست آمد این بود که روش‌های مبتنی بر پنجره زمانی نسبت به روش‌های مبتنی بر فاصله بین بسته‌ها از خود مقاومت بیشتری در برابر حملات دارند و و تمامی روش‌ها بجز روش‌های نسل اول دارای نامحسوسی می‌باشند. همچنین می‌توان نتیجه گرفت که روش‌ها مبتنی بر فاصله بین بسته‌ها توانمندی کمتری در ردیابی نفوذ نسبت به روش‌های مبتنی بر پنجره زمانی دارند. و درنهایت می‌توان عنوان کرد که روش‌های ترکیبی و روش‌های طیف گسترده دارای استحکام و کارایی بالاتری نسبت به دیگر روش‌ها می‌باشند.

۸- مراجع

1. A. Houmansadr, T. Coleman, N. Kiyavash, and N. Borisov, "On the channel capacity of network flow watermarking," Poster at CCS, November **(2009)**.
2. A. Houmansadr and N. Borisov, "SWIRL: A Scalable Watermark to Detect Correlated Network Flows," in Network and Distributed System Security Symposium, Internet Society, Feb **(2011)**.
3. X. Wang and D. S. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by anipulation of interpacket delays," in ACM Conference on Computer and Communications Security, New York, NY, USA, pp. 20-29, **(2003)**.
4. X. Wang S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems," IEEE Symposiumon Security and Privacy, pp. 116–130, (2007).
5. Y. J. Pyun, Y. H. Park, X. Wangy, D. S. Reeves, and P. Ning, "Tracing Traffic through Intermediate Hosts that Repacketize Flows," IEEE Conference on Computer Communications (IN-FOCOM), pp. 634–642, May **(2007)**.

6. N. Kiyavash, A. Houmansadr, and N. Borisov, "Multi-flow attacks against network flow watermarks analysis and countermeasures," arXiv preprint arXiv:1203.1390, **(2012)**.

7. L. Zhang, Z. Wang, J. Xu, and Q. Wang, "Multi-flow Attack Resistant Interval-Based Watermarks for Tracing Multiple Network Flows," in Computing and Intelligent Systems, ed: Springer, pp. 166-173, **(2011)** .

8. A. Houmansadr, N. Kiyavash, and N. Borisov, "Multi-flow attack resistant watermarks for network flows," in IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1497 -1500, **(2009).**

9. X. Wang, J. Luo, and M. Yang, "A Double Interval Centroid-Based Watermark for Network Flow Traceback," in 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD'2010), Shanghai, China, pp. 146–151, April **(2010).**

10. W. Yu, F. Xinwen, S. Graham, D. Xuan, and W. Zhao, "DSSS-Based Flow Marking Technique for Invisible Traceback," presented at the EEE Security and Privacy Symposium (S&P), **(2007)**.

11. L. Zhang, J. Luo, and M. Yang, "An Improved DSSS-Based Flow Marking Technique for Anonymous Communication Traceback," in Multidisciplinary Autonomous Networks and Systems (MANS 09), Brisbane, Australia, pp. 563 - 567 , May **(2009).**

12. J. Luo, X. Wang, and Y. Ming, "An interval centroid based spread spectrum watermarking scheme for multi-flow traceback," Journal of Network and Computer Applications, Elsevier, **(2011)**.

13. A. Houmansadr, N. Kiyavash, and N. Borisov, "RAINBOW A Robust And Invisible Non-Blind Watermark for Network flow," in Network and Distributed System Security Symposium, Feb **(2009)**.

14. A. Houmansadr and N. Borisov, "Towards Improving Network Flow Watermarks using the Repeat-accumulate Codes," in 36th International Conference on Acoustics, Speech and Signal Processing, **(2011)**.

15. L. Zhang, Z. Wang, Q. Wang, and F. Miao, "MSAC and Multi-flow Attacks Resistant Spread Spectrum Watermarks for network flows," in Information and Financial Engineering (ICIFE), 2010 2nd IEEE International Conference on, pp. 438-441, **(2010).**

16. J. Huang, X. Pan, X. Fu, and J. Wang, "Long PN Code Based DSSS Watermarking," presented at the Annual IEEE International Conference on Computer Communications (INFOCOM), **(2011)**.

17. A. Houmansadr, "Design Analysis And implementation of effective network flow watermarking schemes," Doctor of Philosophy Thesis, in Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, University of Illinois, Urbana-Champaign, **(2012)**.

18. J. Gilbert,"Scalable Wavelet-Based Active Network Stepping Stone Detection," Master of Science Air Force Institute of Technology, AIR University, Wright-Patterson Air Force Base, Ohio, **(2012).**

19. N. Kiyavash, A. Houmansadr, and N. Borisov, "Multi-flow attacks against network flow watermarking schemes," in USENIX Security Symposium, Berkeley, CA, USA:USENIX Association, **(2008)**.

20. M. Dehghani and M. S. Esfahani, "Network Covert Channels: An Information Leakage Flow," Passive Defence Quarterly, vol. 9, **(2012)**, (in Persian).

21. B. Birami, M. Dehghani and M. S. Esfehani, "Detect Covert Timing Channel with Statistic Method," Electronic and Cyber Defence Quarterly, vol. 5, pp. 13-24, spring **(2014)**, (in Persian).

22. P. Peng, P. Ning, and D. S. Reeves, "On the secrecy of timing-based active watermarking traceback techniques," in IEEE Symposiumon Security and Privacy, Washington, DC, USA, pp. 334-339, (**2006).**

23. X. Luo, P. Zhouz, J. Zhangx, R. Perdisciy, W. Leex, and R. K. C. Changz, "Exposing Invisible Timing-based Traffc Watermarks with BACKLIT," in 27th Annual Computer Security Applications Conference, ACSAC '11, Orlando, FL,USA, Dec. **(2011)**.

24. J. G. Thanh Truong, "Is TOR the last hope for Crypto-Anarchism?," Uppsala University, **(2009)**.

25. A. Ahmadi, "Intruder Tracing in Anonymous Networks Using the Network Flow Watermarking," M. S. Thesis, I.T.C. Department, Imam Hussin Comprehensive University, Tehran, **(2014),** (in Persian).

Survey of intruder tracing methods in anonymous networks using the network flow watermarking

A. Ahmadi[1]
M. Dehghani[2]
M. Saleh Esfehani[3]

Abstract

With the development of Internet, the insecurity and crime is increasing. Furthermore, the ability of intruder tracing, is deterrence to insecurity and it can solution for passive defense. One of the methods of intruder tracing is network flow watermark. In this technique, the pattern of network flow is changed, to watermark the special flow of traffic and we can be tracing it in the output boundaries of the network. Several methods have been proposed to watermarking the network flow on the timing of their actions. In this study, after investigating all the different methods, these classified into two categories, interval between the packages and based on the time window and compare their methods with specific criteria. Finally, we show that the combination methods and Spread Spectrum methods strength and performance is higher than other methods.

Key Words: *Intruder Tracing, Watermark, Flow Network*

1- M.Sc. in computer Engineering,of Imam Hussein Comprehensive University (ahmadi.ihu@chmail.ir) - Writer-in-Charge
2- Instructor of Computer department Imam Hussein Comprehensive University
3- Assistant Professor and Academic Member of Computer department Imam Hussein Comprehensive University