هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

دانشگاه صنعتی خواجه نصیرالدین طوسی

بهبود حمله‌ی افشای آماری در پروتکل‌های گمنامی

نوید امام‌دوست، محمدصادق دوستی، رسول جلیلی

مرکز امنیت شبکه شریف، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف

{emamdoost@ce., dousti@ce., jalili@}sharif.edu

چکیده

تاکنون حملات مختلفی به پروتکل‌های گمنامی مطرح شده است. غالب این حملات با بهره‌گیری از یک ضعف در طراحی و یا پیاده‌سازیِ پروتکل، سعی در کاهش میزان گمنامی دارند. با معرفی حمله‌ی افشا و همچنین گونه‌ی آماری آن، مشخص شد که یک مهاجم بدون توجه به مکانیزم داخلی پروتکل گمنامی و فقط از طریق مشاهده قادر است از میزان گمنامی فراهم شده بکاهد. گلوگاه این حملات، تعداد مشاهدات مورد نیاز برای رسیدن به نتیجه‌ی مناسب است. در مقاله‌ی حاضر از یک سو فرضیات حمله‌ی افشای آماری را واقعی‌تر می‌کنیم، و از سوی دیگر با بکارگیری دانش پس‌زمینه‌ای درباره‌ی الگوی رفتار کاربران، تعداد مشاهدات مورد نیاز برای رسیدن به نتیجه‌ی مناسب را کاهش می‌دهیم.

واژه‌های کلیدی

حریم خصوصی، گمنامی، تحلیل ترافیک، حمله‌ی افشای آماری.

۱- مقدمه

گسترش شبکه‌های ارتباطی در دهه‌های اخیر توانسته است پاسخگوی بسیاری از نیازهای ارتباطی کاربران باشد. اما این تحولات نتایج ناخوشایندی را نیز در پی داشته‌اند، که از مهمترین آنها نقض حریم خصوصی[1] افراد است. امروزه زیرساخت‌های ارتباطی که کاربران را با جهان بیرون مرتبط می‌سازد به راحتی می‌تواند اطلاعاتی درباره‌ی الگو، محتوا، و همچنین مبدأ و مقصد ارتباطی آنها را در اختیار دیگران قرار دهد. اگرچه استفاده از رمزنگاری می‌تواند محتوای ارتباطات را از دسترس دیگران مخفی نگه دارد، اما هنوز اطلاعات مفیدی از مبدأ، مقصد، و الگوی ارتباطات قابل کشف است، و چه بسا به کمک این اطلاعات بتوان محتوای پیام‌ها را نیز حدس زد.

رمزنگاری به تنهایی قادر به حفظ حریم خصوصی نیست [3]. امروزه گمنامی[2] به عنوان مهمترین راهکار حفظ حریم خصوصی کاربردهای بسیاری پیدا کرده‌است. از مرور وب و ارسال نامه الکترونیکی گمنام گرفته تا کاربردهایی نظیر رای‌گیری الکترونیکی، ابراز عقیده و نظایر آن، همگی جزو کاربردهای گمنامی به شمار می‌آید.

سرویس‌های در بستر شبکه‌های ارتباطی، پروتکل‌های گمنامی متعددی با ویژگی‌های متفاوت و برای کاربردهای مختلف ارائه شده‌اند. همان گونه که طراحی و معرفی پروتکل‌های مناسب بحثی مهم است، تحلیل آسیب‌پذیری و حمله به این پروتکل‌ها نیز از اهمیت ویژه‌ای برخوردار است. چرا که اگر از نقاط ضعف و قوت یک سیستم آگاهی داشته باشیم، در نحوه و موارد بکارگیری آن نیز موفق‌تر عمل خواهیم کرد.

تاکنون حملات بسیاری به پروتکل‌های گمنامی وارد شده است. غالب این حملات با بهره‌گیری از یک ضعف در مکانیزمِ طراحی و یا پیاده‌سازی پروتکل‌ها، سعی در از بین بردن گمنامی کاربران دارند. در عین حال روش‌هایی نیز برای مقابله با این حملات ارائه شده که با صرف هزینه‌هایی (عموماً از کارایی)، در جهت فراهم کردن گمنامی مناسبی برای کاربران برآمده‌اند.

[1] Privacy

[2] Anonymity

در چند سال اخیر گونه‌ای از حملات مطرح شده است که مستقل از مکانیزم درونی پروتکل گمنامی، و تنها با مشاهده‌ی پیام‌های وارد شده به و خارج شده از سیستم ارتباطی گمنام، قادر به تقلیل میزان گمنامی کاربران هستند. حمله‌ی افشا[1] [7] را می‌توان نخستین حمله از این گونه دانست. با ارائه‌ی چنین حملاتی مشخص شد که یک پروتکل گمنامی هر قدر هم که دقیق و درست طراحی و پیاده‌سازی شده باشد، در مقابل مهاجمی که در طول زمان فقط به مشاهده‌ی رفتار سیستم می‌پردازد، آسیب‌پذیر است. مهاجم از طریق این حمله می‌تواند اطلاعات مفیدی برای یافتن ارتباط کاربران سیستم با یکدیگر به دست‌آورد.

تاکنون هیچ راه‌حل موثری برای دفاع در برابر چنین حملاتی معرفی نشده است. تنها مشکل این حملات این است که برای رسیدن به جواب قطعی نیازمند تعداد زیادی مشاهده هستند. از همین رو گونه‌های تقریبی و احتمالی این حملات معرفی شده‌اند که سعی دارند با مشاهدات کمتری بتوانند کاربران را با دقت مناسبی به هم مربوط کنند.

ساختار ادامه‌ی مقاله به ترتیب زیر خواهد بود. در بخش ۲ تعاریف و مفاهیم اولیه‌ی گمنامی را می‌آوریم. در بخش ۳ به مرور کارهای صورت گرفته در زمینه‌ی پروتکل‌های گمنامی و حملات می‌پردازیم. نوآوری مقاله و شبیه‌سازی در بخش‌های ۴ و ۵ آورده شده است، و در نهایت در بخش ۶ به نتیجه‌گیری می‌پردازیم.

۲- مفاهیم اولیه

یک تعریف کامل و فراگیر برای مفهوم گمنامی در [8] ارائه شده است: "گمنامیِ یک موجودیت، به معنای شناخته‌نشدنش در میان مجموعه‌ای از موجودیت‌ها است." به چنین مجموعه‌ای «مجموعه گمنامی» گفته می‌شود. بنابراین مفاهیمی مانند گمنامی فرستنده، گمنامی گیرنده، و ربط‌ناپذیری[2] در بستر شبکه‌های ارتباطی به صورت زیر قابل بیان است:

گمنامی فرستنده: فرستنده‌ی واقعی یک پیام، در میان مجموعه‌ای از فرستندگان بالقوه قابل تشخیص نباشد.

گمنامی گیرنده: گیرنده‌ی واقعی یک پیام، در میان مجموعه‌ای از گیرندگان بالقوه قابل تشخیص نباشد.

ربط‌ناپذیری: ناظر در مربوط کردن دو شیء خاص به یکدیگر ناتوان باشد.

برای روشن شدن موضوع می‌توان سناریویی را در نظر گرفت که مجموعه‌ای از کاربران پیام‌هایی را از طریق سیستم گمنامی به کاربر A ارسال می‌کنند. اگر کاربر A نتواند تشخیص دهد هر پیام از کدام یک از اعضای مجموعه برایش ارسال شده، در این حالت گمنامی فرستنده فراهم است. این سناریو از دید یک ناظر خارجی نیز قابل بیان است؛ بدین شکل که ناظر نتواند تشخیص دهد هر پیام توسط کدام یک از اعضای مجموعه ارسال شده است. طبیعی است که چنین مجموعه‌ای، مجموعه گمنامی فرستندگان نامیده شود.

از طرف دیگر می‌توان سناریویی را در نظر گرفت که کاربر A پیام‌هایی را از طریق سیستم گمنامی ارسال کند. اگر گیرندگان هر پیام قابل تشخیص نباشد، گمنامی گیرنده فراهم است. مجموعه تمام گره‌هایی را که به صورت بالقوه می‌توانند گیرنده‌ی پیام باشند؛ مجموعه گمنامی گیرندگان می‌نامند.

برای توضیح ربط‌ناپذیری می‌توان گفت که ناظر امکان مشاهده تبادل پیام بین برخی از کاربران را داشته باشد ولی نتواند تعیین کند کدام دو کاربر با هم تبادل پیام داشته‌اند؛ و یا ناظر ارسال دو پیام را مشاهده کند، اما نتواند تعیین کند که این دو پیام توسط یک کاربر خاص ارسال و یا دریافت شده است.

هدف از حمله به یک سیستم گمنامی، شناسایی گیرنده یا فرستنده‌ی یک پیام و یا مرتبط کردن دو کاربر به یک دیگر است. یک مهاجم می‌تواند خصوصیاتی مانند داخلی/خارجی، سراسری/محلی و فعال/منفعل داشته‌باشد، که در ادامه این خصوصیات را تعریف می‌کنیم [9].

خارجی و یا داخلی: یک مهاجم می‌تواند فقط خطوط ارتباطی را مشاهده کند (خارجی)، و یا اینکه کنترل گره‌هایی را نیز در اختیار داشته‌باشد (داخلی).

فعال و یا منفعل: یک مهاجمِ فعال می‌تواند به دلخواه خود پیام‌ها و محاسبات را دستکاری کند؛ درحالی که مهاجم منفعل فقط قادر به گوش‌دادن است.

محلی یا سراسری: یک مهاجم سراسری به تمام منابع ارتباطی دسترسی دارد. در حالیکه یک مهاجم محلی، تنها به بخشی از منابع سیستم ارتباطی دسترسی دارد.

ایستا و یا تطبیقی: یک مهاجم ایستا، منابعی را که در کنترل خود در می‌آورد، قبل از آغاز پروتکل انتخاب می‌کند. با شروع اجرای پروتکل او دیگر قادر به در اختیار گرفتن منابع جدید نیست. از سوی دیگر مهاجم تطبیقی در حین اجرای پروتکل قادر به تغییر منابع خود منطبق با شرایط و نیازهای خود است. مثلاً می‌تواند مسیر یک پیام را دنبال کند.

[1] Disclosure Attack

[2] Unlinkability

طبیعی است که یک مهاجم بتواند تمام این خصوصیات را یک-جا داشته‌باشد.

۳-کارهای مرتبط

نخستین تلاش به منظور ارائه سیستم ارتباطی گمنام توسط *چام* [1] با معرفی مفهوم میکس[1] صورت گرفت. امروزه نیز پرکاربردترین گونه‌ی پروتکل‌های گمنامی بر پایه‌ی میکس‌نِت[2] هستند. به طور کلی میکس پردازه‌ای است که چندین پیام ورودی را به صورت رمز شده دریافت کرده و پس از تغییر الگوی بیتی و برهم زدن ترتیب پیام‌ها، آنها را به سمت مقصدشان ارسال می‌کند.

پس از آن پروتکل‌های دیگری مانند مسیریابی پیازی[3] [10]، دی‌سی‌نِت[4] [2]، کراودز[5] [11] و غیره ارائه شد که هر کدام مشخصات و کاربردهای خاص خود را دارند. در [6] به تفصیل به مرور پروتکل‌های گمنامیِ ارائه شده و مشخصات آنها پرداخته شده است.

در ادامه معروف‌ترین حملات به سیستم‌های گمنامیِ مبتنی بر میکس را بررسی کرده و در هر مورد قدرتی که یک مهاجم باید داشته‌باشد تا بتواند آن حمله را اجرا کند، بیان می‌کنیم.

۳-۱- حملات زمان‌بندی

سیستم‌های گمنامی مانند مسیریابی پیازی که برای کاربردهای وب و نظایر آن طراحی شده‌اند، هیچگونه تاخیری بر روی پیام‌های عبوری اعمال نمی‌کنند. بنابراین یک مهاجم منفعل سراسری که می‌تواند ورود و خروج بسته‌ها را از سیستم گمنامی مشاهده کند، با تقریب خوبی می‌تواند ورودی‌ها و خروجی‌ها را براساس الگوی زمانی بین بسته‌ها به هم مرتبط کند. در مورد میزان کارایی حملات زمانبندی[6] مطالعات بسیاری صورت گرفته است [13]. معمولاً روش‌هایی که برای کاهش تاثیر حملات زمانبندی بکارمی‌رود، اثر منفی بر روی کارایی خواهد داشت. به عنوان نمونه یک روش پیشنهادی این است که از پیام‌های ساختگی[7] در کنار پیام‌های واقعی استفاده شود و در طول مسیر بر اساس یک تابع احتمالی، پیام‌های ساختگی به تدریج دور ریخته شوند. چنین راه‌حل‌هایی برای مهاجم منفعل مفید است. در حالیکه یک مهاجم فعال می‌تواند به میل خود تاخیرهایی در ورود پیام-ها اعمال کرده و تاثیر را در خروجی مشاهده کند.

۳-۲- حملات برچسب‌گذاری

در حملات برچسب‌گذاری[8] یک مهاجمِ فعال، قبل از ورود پیام-ها به سیستم گمنامی یک برچسب بر روی آن گذاشته و در خروجی به دنبال مشاهده‌ی برچسب می‌گردد [6]. بنابراین چنین حمله‌ای بر پروتکل‌هایی که بر پیام‌های ورودی تاخیر اعمال می‌کنند نیز موثر است. نخستین بار این حمله بر طراحی اولیه‌ی میکس وارد شد. در این طراحی از رمزنگاری RSA استفاده می‌شد که به مهاجم اجازه می‌داد با دستکاری در یک ورودی رمز شده، خروجی متناظر را شناسایی کند. به منظور اصلاح این نقص روش‌های رمزگذاری ترکیبی پیشنهاد شد. بدین ترتیب که از RSA برای رمزکردن یک کلید مشترک استفاده شود و کلید مشترک برای رمزگذاری بقیه‌ی پیام بکار رود.

۳-۳- حملات سیلابی

سیستم‌های مبتنی بر میکس که از پردازش دسته‌ای استفاده می‌کنند، نسبت به حمله‌ای با عنوان حمله‌ی سیلابی[9] و یا حمله‌ی (n-1) آسیب‌پذیر هستند [12]. یک مهاجم فعال می‌تواند با انتخاب یک پیام مشخص مانند M، به عنوان قربانی، مانع از ورود آن به میکس شود. مهاجم سپس با ارسال پیام‌های ساختگی باعث می‌شود میکس تمام پیام‌های خود را به بیرون ارسال کند. اگر اندازه‌ی دسته در میکس برابر با n باشد، مهاجم پیام M را به همراه n-1 پیام ساختگی، به میکسِ خالی وارد می‌کند. مهاجم با مشاهده‌ی خروجی میکس می‌تواند مقصد پیام M را کشف کند؛ زیرا تمام n-1 پیام دیگر متعلق به خودش بوده و مقصد آنها را از قبل می‌دانست. به منظور کشف و مقابله با این حمله، دنزیس و دیگران در [4] روشی ارائه دادند که در آن هر میکس به صورت دوره‌ای پیام‌هایی را در شبکه تزریق می‌کند که گیرنده این پیام‌ها، خودِ میکس است. به چنین پیامی در اصطلاح «پیام قرمز» گفته می‌شود. از آنجا که در حمله‌ی (n-1)، مهاجم پیامِ قربانی را با پیام‌های ساختگیِ خودش همراه می‌کند، اگر میکس نتواند پیام‌های قرمزش را ببیند، مشکوک به وقوع حمله می‌شود. در این صورت میکس به همراه پیام‌های خروجی‌اش یک سری پیام ساختگی هم از خود خارج می‌کند تا پیامِ قربانی در میان این پیام‌های ساختگی مخفی شود.

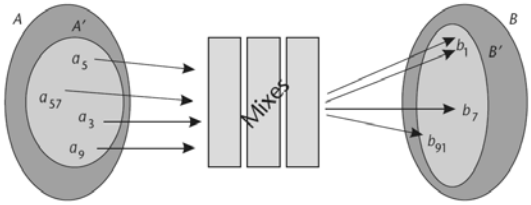
[1] Mix
[2] MixNet
[3] Onion Routing
[4] DC Net
[5] Crowds
[6] Timing Attacks
[7] Dummy
[8] Tagging Attacks
[9] Flooding Attacks

۳-۴- حمله‌ی افشا

در تمام حملات معرفی شده قبلی در این مقاله، مهاجم سعی در سوءاستفاده از یک ضعف در طراحی یا پیاده‌سازی سیستم گمنامی داشت. اما دسته‌ای از حملات معرفی شده‌اند که بدون توجه به مکانیزم درونیِ سیستم گمنامی سعی در کاهش درجه‌ی گمنامی دارند. در این دسته از حملات که به حملات اشتراک‌گیری[1] معروف‌اند، مهاجم تنها با انجام مشاهده از رفتار سیستم در ارتباطات طولانی مدت، قادر خواهد بود کاربران مختلف را به یکدیگر مربوط سازد. بنابراین شرط اساسی برای موفقیت چنین حملاتی، این است که مهاجم بتواند دوره‌های زیادی از اجرای پروتکل را زیر نظر بگیرد.

کِزدُگان و همکارانش در [7] حمله‌ای را ارائه کردند که در یک سیستم گمنامیِ مبتنی بر میکس سعی در یافتن همه‌ی مخاطبان یک کاربر خاص دارد. مدل سیستمی که مورد استفاده قرار می‌گیرد در شکل۱ آمده است. در این حمله مهاجم فرض می‌کند که پیاده‌سازی سیستم گمنامی ضعفی ندارد. مهاجم توجهی به مکانیزم درونی سیستم گمنامی نداشته و فقط به ورود و خروج پیام‌ها توجه می‌کند. در هر ارتباط گمنام، زیر مجموعه‌ی از مجموعه‌ی تمام فرستندگان به زیر مجموعه‌ی از مجموعه‌ی تمام گیرندگان پیام ارسال می‌کنند.

در حمله‌ی افشا هدف شناسایی تمام مخاطبان یک کاربر خاص به نام A است. فرض می‌شود که A با m نفر از طریق سیستم گمنامی در تماس است؛ مهاجم با دانستن مقدار m سعی در شناسایی این مخاطبان دارد. در هر دور b پیام به سیستم گمنامی وارد می‌شود (اندازه‌ی دسته). A در هر دور از پروتکل که شرکت می‌کند، یک نفر را از میان m مخاطب خود به عنوان گیرنده در آن دور انتخاب می‌کند؛ و b-1 فرستنده‌ی دیگر هر یک، مخاطبان خود را به صورت یکنواخت از کل کاربران سیستم انتخاب می‌کنند. مهاجم پس از این با انجام یک محاسبه‌ی ان-پی-سخت سعی در یافتن m مجموعه‌ی دو به دو مجزا از مجموعه‌ی گیرندگان دارد. هر یک از این مجموعه‌ها لزوماً شامل یک مخاطب از A هستند. در ادامه، مهاجم با اشتراک گرفتن از این مجموعه‌ها و مشاهدات بعدی قادر خواهد بود مخاطبان A را شناسایی کند.



شکل۱- مدل سیستم گمنامی در حمله‌ی افشا [7]

دنزیس گونه‌ی آماری این حمله موسوم به *حمله‌ی افشای آماری*[2] را معرفی کرد [5]. در این حمله نیازی به حل یک مسئله‌ی ان-پی-سخت نبوده و مهاجم با انجام مشاهدات می‌تواند به صورت احتمالی مخاطبان A را شناسایی کند. هرچه تعداد مشاهدات بیشتر باشد، نتیجه‌ی حمله دقیق‌تر خواهد بود. بدلیل اینکه در ادامه قصد بهبود حمله‌ی افشای آماری را داریم، این حمله را با جزئیات کامل بیان می‌کنیم.

فرض کنید N تعداد کل کاربران سیستم گمنامی باشد، و در هر دور b نفر به صورت گمنام پیام ارسال کنند (اندازه‌ی مجموعه‌ی گمنامی فرستندگان). همچنین فرض کنید A مخاطب خود را مستقل از دیگر کاربران سیستم و با احتمال یکسان از بین m نفر انتخاب می‌کند، و دیگر کاربرانی که در آن دور پیام ارسال می‌کنند مخاطب خود را با احتمال یکسان از میان کل کاربران سیستم انتخاب می‌کنند.

توزیع احتمالی بکار رفته توسط A برای انتخاب مخاطبانش را با بردار $\vec{v}$ نمایش می‌دهیم؛ $\vec{v}$ برداری است با N مولفه که تنها m مولفه از آن مقداری برابر با $1/m$ داشته و بقیه‌ی مولفه‌ها برابر با صفر هستند. توزیع بکار رفته توسط دیگر کاربران سیستم برای انتخاب مخاطب توسط بردار $\vec{u}$ نمایش داده می‌شود که برداری است با N مولفه و هر مولفه مقدار $1/N$ دارد. در واقع در هر یک از این بردارها مولفه‌ی iام بیانگر احتمال انتخاب شدن کاربر iام به عنوان مخاطب است.

مهاجم از مشاهده‌ی هر دور اجرای پروتکل، یک بردار $\vec{o}$ می‌سازد که دارای N مولفه است؛ هر مولفه از این بردار مقدار $1/b$ به خود می‌گیرد اگر کاربر متناظر با آن، در مجموعه‌ی گیرندگان باشد. در غیر اینصورت آن مولفه از بردار $\vec{o}$ مقدار صفر به خود می‌گیرد. در واقع هر مولفه از این بردار بیانگر این احتمال است که کاربر متناظرش مخاطب A در آن دور باشد.

براساس قانون اعداد بزرگ[3]، وقتی‌که تعداد مشاهدات به اندازه‌ی کافی زیاد شد، رابطه‌ی زیر برقرار خواهد بود:

$$\overline{O} = \frac{1}{t}\sum_{i=1}^{t}\vec{o_i} = \frac{\vec{v}+(b-1)\vec{u}}{b} \qquad (۱)$$

[1] Intersection Attacks

[2] Statistical Disclosure Attack

[3] Law of Large Numbers

بنابراین به کمک دانش حاصل از مشاهدات و دانستن b (تعداد پیام‌های ارسالی در هر دور) و بردار $\vec{u}$ (مدل ارسال دیگر کاربران) می‌توان بردار $\vec{v}$ را محاسبه کرد:

$$\vec{v} = \frac{b}{t}\sum_{i=1}^{t}\vec{o_i} - (b-1)\vec{u} \qquad (۲)$$

در [5] نویسنده توانسته است حداقل تعداد مشاهدات مورد نیاز را برای رسیدن به حد مشخصی از اطمینان بدست آورد.

۴- بهبود حمله‌ی افشای آماری

همانطور که در بخش ۳-۱-۴ اشاره شد، حمله‌ی افشای آماری تنها به دورهایی که A در آن شرکت کرده، توجه دارد. همچنین در این حمله فرض بر این است که A مخاطبان خود را با احتمال مساوی از یک مجموعه‌ی m عنصری انتخاب می‌کند؛ ولی بقیه کاربران سیستمِ گمنامی مخاطبان خود را با احتمال مساوی از کل مجموعه‌ی کاربران انتخاب می‌کنند. این در حالیست که هر کاربر مجموعه‌ی مخاطبان خاص خود را دارد و علاوه بر این، الزامی به هم احتمال بودن مخاطبان برای یک کاربر خاص وجود ندارد.

برای بهبود حمله‌ی افشای آماری فرض می‌کنیم که هر کاربر بردار ارسال خاص خود را دارد. همچنین فرض می‌کنیم که مخاطبان یک کاربر الزاماً با هم هم‌احتمال نیستند. بقیه‌ی فرض‌های مسئله همانند حمله‌ی افشای آماری است؛ یعنی تعداد کاربران سیستم برابر با N بوده و برای ساده‌سازی کاربران سیستم از 1 تا N شماره‌گذاری شده‌اند. در هر دور b کاربر از طریق سیستم گمنامی پیام ارسال می‌کنند و هر کاربر حداکثر یک پیام در هر دور ارسال می‌کند. هر کاربر مخاطبان خود را از مجموعه مخاطبانش و مستقل از دیگر کاربران، انتخاب می‌کنند. هدف شناسایی مخاطبان A است. همانند قبل کافیست که مهاجم قادر به مشاهده‌ی پیام‌های وارد شده و خارج شده از سیستم گمنامی باشد.

جنبه‌ی دیگری از نوآوری این مقاله در بکارگیری دانش پس زمینه‌ای برای کاستن میزان گمنامی کاربران است. این دانش پس زمینه‌ای می‌تواند در مورد الگوی رفتاری و یا سلیقه‌ی کاربران باشد. اگر این فرض را بپذیریم که دو کاربر با سلایق مشترک با احتمال بیشتری به تبادل پیام با یکدیگر می‌پردازند، آنگاه می‌توان از این دانش پس زمینه‌ای برای تقویت حمله به گمنامی استفاده کرد. در ادامه هر یک از این ایده‌ها را با جزئیات بیشتر بیان می‌کنیم.

۴-۱- بهبود فرض

در حمله‌ی افشای آماری، در هر دور b کاربر اقدام به ارسال پیام می‌کنند. کاربر A مخاطب خود را به طور یکنواخت از یک مجموعه‌ی m عضوی انتخاب می‌کند. دیگر کاربران سیستم نیز مخاطب خود را به طور مستقل و یکنواخت از مجموعه‌ی N عضوی (کل کاربران) انتخاب می‌کنند.

بردار $\vec{v}$ نشان دهنده‌ی الگوی مورد استفاده‌ی A برای انتخاب مخاطبانش است و هدف از حمله، کشف این بردار است. بقیه‌ی کاربران شرکت کننده در هر دور از بردار $\vec{u}$ برای انتخاب مخاطب خود استفاده می‌کنند.

به منظور واقعی‌تر شدن فرض‌های مسئله، نخست این محدودیت را که هر کاربر با احتمال مساوی مخاطب خود را از مجموعه‌ی مخاطبان انتخاب می‌کند، از بین می‌بریم. بدین معنی که در مجموعه‌ی مخاطبان، یک عضو می‌تواند احتمال بیشتر و یا کمتری برای انتخاب شدن داشته باشد. همچنین برای هر کاربر سیستم گمنامی، یک بردار ارسال خاص در نظر می‌گیریم. کاربر iام، بردار ارسال خاص خودش را دارد که آن را با $\vec{v_i}$ نمایش می‌دهیم. در هر دور، کاربر iام مخاطب خود را براساس بردار $\vec{v_i}$ انتخاب می‌کند.

در روش جدید، برخلاف حمله‌ی افشای آماری، مهاجم تمامی دورهای اجرای پروتکل را زیر نظر می‌گیرد. مهاجم پس از انجام هر مشاهده از اجرای پروتکل، بردار $\vec{o_i}$ را تشکیل می‌دهد. در این بردار به ازای کاربران مشاهده شده در مجموعه‌ی گیرندگان، مقدار $\frac{1}{b}$ و به ازای دیگر کاربران مقدار صفر منظور می‌شود. بدین ترتیب مهاجم پس از t مشاهده، بردارهای $\vec{o_1}, \vec{o_2}, ..., \vec{o_t}$ را در اختیار دارد.

هدف از حمله، کشف بردار $\vec{v}$ است. به منظور استفاده از قانون اعداد بزرگ برای میل دادن میانگین مشاهدات به میانگین رفتار کاربران در هر دور، نیازمند تخمینی از رفتار دیگر کاربران هستیم. در حمله‌ی افشای آماری از بردار $\vec{u}$ برای مدل کردن رفتار کاربران سیستم غیر از A، استفاده می‌شود. اما در مدل ما باید براساس مشاهدات انجام شده، بتوانیم تخمینی از رفتار دیگر کاربران بدست آوریم.

برای این منظور، مشاهداتی را که A در آنها ارسالی انجام نداده است، در نظر می‌گیریم؛ از میانگین این مشاهدات می‌توان به عنوان تخمینی برای رفتار کاربران سیستم، غیر از A استفاده کرد. بنابراین اگر فرض کنیم تعداد چنین مشاهداتی برابر با s باشد، بردار $\overrightarrow{others}$ را از رابطه‌ی(۳) بدست می‌آوریم.

$$\overrightarrow{others} = \frac{1}{s}\sum_{i=1}^{t}(\vec{o_i} \mid i \text{ is not A's round}) \qquad (۳)$$

حال با داشتن بردار $\overrightarrow{others}$، می‌توانیم از قانون اعداد بزرگ استفاده کنیم. اگر تعداد دورهایی که A در آنها پیام ارسال کرده است برابر با t' باشد، رابطه‌ی(۴) را می‌توان نوشت و از آن به رابطه‌ی(۵) رسید. بدین ترتیب مهاجم می‌تواند بردار

$\vec{v}$ را محاسبه کند. پس از محاسبه‌ی بردار $\vec{v}$ مولفه‌هایی که بیشترین مقدار را دارند، به عنوان مخاطبان A شناسایی می‌شوند.

$$\frac{\sum_{i=1}^{t}(\vec{o_i} \mid i \text{ is A's round})}{t'} = \frac{\vec{v} + (b-1)\overrightarrow{others}}{b} \quad (۴)$$

$$\vec{v} = \frac{b\sum_{i=1}^{t}(\vec{o_i} \mid i \text{ is A's round})}{t'} - (b-1)\overrightarrow{others} \quad (۵)$$

همانطور که در بخش ۵ اشاره خواهیم کرد، در روش پیشنهادی، بردار $\overrightarrow{others}$ تخمین مناسب‌تری به نسبت بردار $\vec{u}$ بدست می‌دهد؛ در نتیجه دقت حمله بالاتر خواهد رفت.

۴-۲- بکارگیری دانش پس زمینه

در یک شبکه‌ی ارتباطی با تعداد زیادی کاربر، طبیعی است که هر کاربر علایق و الگوی رفتاری خاص خود را داشته باشد. چنانچه کاربران این شبکه به منظور برقراری ارتباط با یکدیگر از سیستم گمنامی استفاده کنند، می‌توان از منابع اطلاعاتی دیگر در کنار مشاهدات برای مرتبط کردن کاربران به یکدیگر استفاده کرد. اگر علایق هر کاربر را توسط مجموعه‌ای از موضوعات نمایش دهیم، می‌توان به کمک روش‌هایی میزان شباهت علایق کاربران به یکدیگر را سنجید. موضوعاتی همانند ورزش، سیاست، موسیقی، تجارت و غیره می‌توانند در مجموعه‌ی علایق کاربران قرار گیرند. چنین مجموعه‌هایی از روی شبکه‌های اجتماعی که کاربران در آنها عضویت دارند قابل استخراج است.

در این مقاله، فرض می‌کنیم که مجموعه‌ی علایق کاربران سیستم گمنامی به صورت استاندارد و سازگار با هم به عنوان ورودی در اختیار است. می‌توان پذیرفت که در یک شبکه‌ی ارتباطی، کاربرانی که سلیقه‌های شبیه‌تری دارند، با احتمال بیشتری به یکدیگر پیام ارسال می‌کنند.

به منظور تعیین میزان شباهت دو مجموعه از اقلام، ضریب جکارد[1] معیار مناسبی است. ضریب جکارد میزان شباهت دو مجموعه را به صورت عددی بین 0 و 1 بیان می‌کند. اگر دو مجموعه‌ی A و B از اقلام داشته‌باشیم، ضریب جکارد A و B از رابطه‌ی(۶) بدست می‌آید. هر چه این ضریب به 1 نزدیک‌تر باشد، دو مجموعه‌ی A و B به هم شبیه‌تر هستند.

$$\text{Jacc}(A,B) = \frac{|A \cap B|}{|A \cup B|} \quad (۶)$$

بدین ترتیب با داشتن مجموعه علایق کاربران، می‌توان اطلاعات پس زمینه‌ای را به منظور افزایش دقت حمله به کار ببریم. برای این منظور پس از انجام مشاهدات و بدست آوردن بردار $\vec{v}$، اطلاعات حاصل از شباهت مجموعه علایق را برای بهبود دقت بردار $\vec{v}$ بکار می‌گیریم.

همانطور که اشاره شد، بردار $\vec{v}$ دارای N مولفه می‌باشد که مولفه‌ی iام آن بیانگر احتمال مخاطب قرار گرفتن کاربر iام از سوی A است. بنابراین اگر مولفه‌ی iام از بردار $\vec{v}$ را با p_i نمایش دهیم، براساس رابطه‌ی(۷) مولفه‌ی iام آن را به روز می‌کنیم.

$$p_i = \alpha p_i + (1-\alpha)\, jacc_i \quad (۷)$$

در رابطه‌ی مذکور، $jacc_i$ بیانگر ضریب جکارد بین مجموعه علایق کاربر iام و A است. متغییر α تعیین کننده‌ی وزنی است که به نتیجه‌ی حاصل از مشاهدات می‌دهیم.

واضح است دقت مجموعه علایق کاربران تاثیر زیادی در دقت نتایج خواهد داشت. به همین دلیل مناسب است که به نتایج حاصل از مشاهدات وزن بیشتری داده شود. البته در صورت اطمینان از دقت مجموعه‌ی علایق می‌توان سهم آن را بیشتر کرد. در شبیه سازی‌ها مقدار α برابر با 0.8 در نظر گرفته شده است؛ با این وجود این روش تاثیر چشم‌گیری در بهبود نتایج حاصل از حمله داشته است.

۵- شبیه‌سازی

به منظور ارزیابی روش جدید و مقایسه‌ی دقت آن با حمله‌ی افشای آماری، از نرم‌افزار MATLAB نسخه‌ی 7.9 استفاده کردیم. روند کلی شبیه‌سازی اینگونه است که ابتدا مشاهدات را ایجاد کرده و سپس حملات افشای آماری و روش جدید را بر روی این مجموعه مشاهدات اعمال می‌کنیم. در حملات اشتراک‌گیری، گلوگاه تعداد مشاهدات لازم از کاربر A است. به همین دلیل درصد موفقیت هر یک از حملات بر روی مجموعه‌ی یکسانی از مشاهدات را به عنوان معیاری برای مقایسه قرار دادیم.

۵-۱- راه‌اندازی

در شبیه‌سازی، تعداد کل کاربران (N) را برابر با 20000، اندازه‌ی دسته (b) را برابر 50 و تعداد مخاطبان A (m) را برابر 20 قرار دادیم. در یک فایل جداگانه ابتدا مشاهدات را برای تعداد دورهای متفاوت (t) ایجادکردیم.

در شکل۲ شبه کدهای مربوط به ایجاد مشاهدات و حمله‌ها آورده شده است. نحوه‌ی ایجاد مشاهدات بدینگونه است که ابتدا برای هر کاربر، به صورت تصادفی مجموعه‌ای حداکثر 100 عضوی از کاربران سیستم را به عنوان مخاطب تعیین می‌کنیم. مخاطبان هر کاربر از این مجموعه انتخاب خواهند شد. سپس برای هر دور یک نمونه‌ی تصادفی به اندازه‌ی b از کل کاربران می‌گیریم؛ این مجموعه فرستندگان آن دور را تشکیل می‌دهد. سپس برای هر یک از اعضای مجموعه فرستندگان، گیرنده‌ی پیام تعیین می‌شود.

[1] Jaccard Coefficient

```
#Generate Observations
for i = 1 .. t
senderSet ← a sample of size b from N
foreach k in senderSet do
        Choose a receiver from k's partners and insert
it
        into receiverSet
end
end

# Statistical Disclosure Attack
rounds ← rounds that A participated in it
t ← | rounds|
foreach r in rounds
    foreach k in receiverSet(r)
        O(k) += 1/b
    end
end
O̅ ← ∑O(k)/t
v⃗ ← b. O̅ - (b-1).u

# Improved SDA
Calculate O vectors for all rounds
nonARounds ← rounds that Al did not participate in
ARounds ← rounds that A participated in
s ← | nonARounds |
t' ← | ARounds |
others ← ∑(O(k)| k is in nonARounds )/s
v⃗ ← (b/t') . ∑(O(k)| k is in ARounds )- (b-1)others

# Incorporate interests
for i = 1 .. N
    jacc(i) ← Jaccard( IntrestSet(A), IntrestSet(i) )
    v(i) ← α . v(i) + (1-α) . jacc(i)
end
```

شکل۲-شبه کد شبیه‌سازی

پس از ایجاد مجموعه فرستندگان و گیرندگان برای هر دور، نوبت به محاسبه‌ی بردارهای مشاهده می‌رسد. برای هر دور یک بردار $\vec{o}$ با N مولفه ایجاد می‌شود که به ازای هر بار ظاهر شدن یک کاربر خاص در مجموعه گیرندگانِ آن دور، مولفه‌ی متناظر آن کاربر در بردار $\vec{o}$ به اضافه‌ی $\frac{1}{b}$ می‌شود. در حمله‌ی افشای آماری فقط به دورهایی که A در آنها شرکت کرده است، توجه می‌شود؛ پس از محاسبه‌ی بردار مشاهدات به کمک رابطه‌ی (۲) بردار $\vec{v}$ محاسبه می‌شود. در روش بهبود یافته، به کمک دورهایی که A در آنها شرکت نکرده است، تخمینی از رفتار دیگر کاربران بدست می‌آوریم و سپس به کمک رابطه‌ی (۵) بردار ارسال A را محاسبه می‌کنیم. اگر مجموعه علایق کاربر iام به صورت IntrestSet(i) نمایش داده شود، پس از بدست آوردن ضریب جکارد میان مجموعه علایق A و دیگر کاربران، به کمک رابطه‌ی (۷) بردار $\vec{v}$ به‌روز می‌شود.

۵-۲-نتایج شبیه‌سازی

همانطور که اشاره شد، گلوگاه در حملات اشتراک‌گیری تعداد مشاهدات مورد نیاز از کاربر A است. بنابراین تعداد مشاهدات مورد نیاز برای رسیدن به حد مشخصی از نرخ خطا[1] می‌تواند معیار مناسبی برای مقایسه باشد. در شبیه‌سازی‌های خود تاثیر پارامترهای N، m و b را بر تعداد مشاهدات مورد نیاز برای موفقیت مهاجم سنجیدیم. بدین معنی که مقادیر این سه پارامتر را به صورت (N=20000, b =50, m=20) قرار داده و هربار با ثابت نگهداشتن دو پارامتر، پارامتر سوم را تغییر داده و تاثیر آن بر تعداد مشاهدات مورد نیاز را سنجیدیم.

در شکل۳ تعداد مشاهدات مورد نیاز برای هر یک از حملات با توجه به تغییر پارامترها مشاهده می شود. در شکل۳-الف تاثیر تغییر اندازه‌ی دسته (b) را بر تعداد مشاهدات مورد نیاز نمایش داده شده است. شکل۳-ب تاثیر تغییر اندازه‌ی تعداد کل کاربران سیستم (N)، و شکل۳-ج تاثیر تغییر تعداد مخاطبان (m) را بر تعداد مشاهدات مورد نیاز برای رسیدن به نتیجه‌ی مناسب نمایش داده شده است. به منظور تبیین تاثیر هر یک از نوآوری‌های این مقاله یک بار حمله‌ی جدید را بدون در نظر گرفتن علایق و یک بار با در نظر گرفتن علایق اجرا کرده و نتایج را به صورت نمودارهای جداگانه نمایش دادیم. قابل ذکر است که شرط توقف حملات رسیدن به نرخ خطای 0.5% قرار داده شد.

این شکل‌ها نشان می‌دهند که بهبود فرض تاثیر بسزایی در بهبود دقت حمله دارد. همچنین به کارگیری اطلاعات پس-زمینه، به مراتب از تعداد مشاهدات مورد نیاز می‌کاهد. همانگونه که مشخص است حمله‌ی جدید نسبت به حمله‌ی افشای آماری به تعداد مشاهدات کمتری نیازمند است.

۶- نتیجه‌گیری

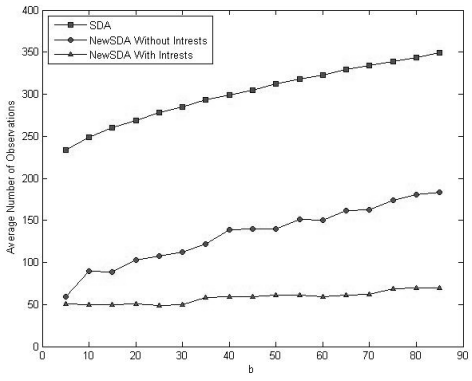
در این مقاله بهبودی بر حمله‌ی افشای آماری در پروتکل های گمنامیِ مبتنی بر میکس ارائه کردیم. در این حمله بدون توجه به مکانیزم درونی سیستم گمنامی، تنها از طرق مشاهده‌ی پیام‌های ورودی و خروجی، می‌توانیم مخاطبان یک کاربر خاص را شناسایی کنیم. روش بهبود یافته برای موفقیت نسبت به حمله‌ی افشای آماری به تعداد مشاهدات کمتری نیاز دارد. در این روش با استفاده از اطلاعات حاصل از دورهایی که قربانی در آنها شرکت نکرده تخمین بهتری از رفتار دیگر کاربران بدست می‌آوریم؛ از سوی دیگر با بهره‌گیری از اطلاعات ناشی از سلیقه‌ی کاربران می‌توانیم با مشاهدات کمتر به جواب دقیق‌تر دست یابیم. تعیین حدی برای حداقل تعداد مشاهدات مورد نیاز

[1] Error Rate

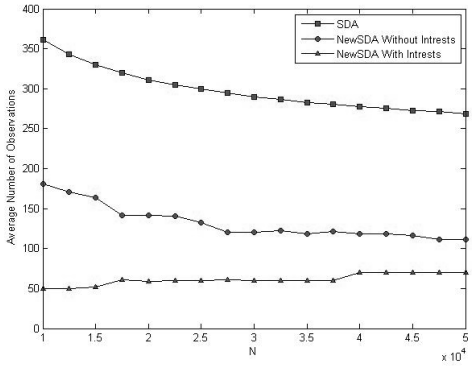
برای رسیدن به میزان مشخصی از نرخ خطا به صورت تحلیلی می‌تواند به عنوان کارهای آینده مطرح باشد.

سپاسگزاری

بخش‌هایی از این تحقیق با حمایت مالی مرکز تحقیقات مخابرات ایران انجام شده است که در اینجا از آن مرکز محترم قدردانی می‌شود.



شکل۳-الف: تاثیر تغییر پارامتر b بر تعداد مشاهدات



شکل۳-ب: تاثیر تغییر پارامتر N بر تعداد مشاهدات

شکل۳-ج: تاثیر تغییر پارامتر m بر تعداد مشاهدات

مراجع

[1] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the ACM, 4(2):84–88, 1981.

[2] D. Chaum, “The dining cryptographers problem: Unconditional sender and recipient untraceability,” Journal of Cryptology, vol. 1, 1988, pp. 65–75.

[3] G. Danezis, “Better Anonymous Communications,” Ph.D. Thesis, University of Cambridge, 2004.

[4] G. Danezis and L. Sassaman, "Heartbeat traffic to counter (n-1) attacks: red-green-black mixes," in Proceedings of the 2003 ACM workshop on Privacy in the electronic society, 2003, p. 93.

[5] G. Danezis, “Statistical disclosure attacks: Traffic Confirmation in Open Environments,” Proceedings of Security and Privacy in the Age of Uncertainty, (SEC2003), 2003, pp. 421-426.

[6] M. Edman and B. Yener, “On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems.” ACM Computing Surveys (CSUR), 2009, pp 1-35.

[7] D. Kesdogan, D. Agrawal, “Measuring anonymity: the disclosure attack,” Security & Privacy, IEEE, vol. 1, 2003, pp. 27-34.

[8] A. Pfitzmann and M. Kohntopp, “Anonymity, unobservability, and pseudonymity-a proposal for terminology,” Draft status, February 2008. Available electronically at http://dud.inf.tu-dresden.de/literatur/Anon- Terminology v0.31.pdf

[9] J.F. Raymond, “Traffic analysis: Protocols, attacks, design issues, and open problems,” In H. Federrath, editor, Designing Privacy Enhancing Technologies: Workshop on Design Issue in Anonymity and nobservability, LNCS 2009, 2000, pp 10–29.

[10] M.G. Reed, P.F. Syverson, and D.M. Goldschlag, “Anonymous connections and onion routing,” IEEE Journal on Selected areas in Communications, vol. 16, 1998, pp. 482–494.

[11] M.K. Reiter and A.D. Rubin, “Crowds: Anonymity for web transactions,” ACM Transactions on Information and System Security (TISSEC), vol. 1, 1998, pp. 66–92.

[12] A. Serjantov, R. Dingledine, P. Syverson, and others, “From a trickle to a flood: Active attacks on several mix types,” In Proceedings of Information Hiding Workshop (IH 2002), F. Petitcolas, Ed. Springer-Verlag, LNCS 2578, 2002, pp 36-52.

[13] V. Shmatikov and M.H. Wang, “Timing analysis in low-latency mix networks: Attacks and defenses,” Computer Security–ESORICS 2006, 2006, pp. 18–33.