حفظ حریم زمانی در شبکه‌های ارتباطی با استفاده از تئوری صف

ابوالفضل دیانت
ab.diyanat@gmail.com

مقدمه

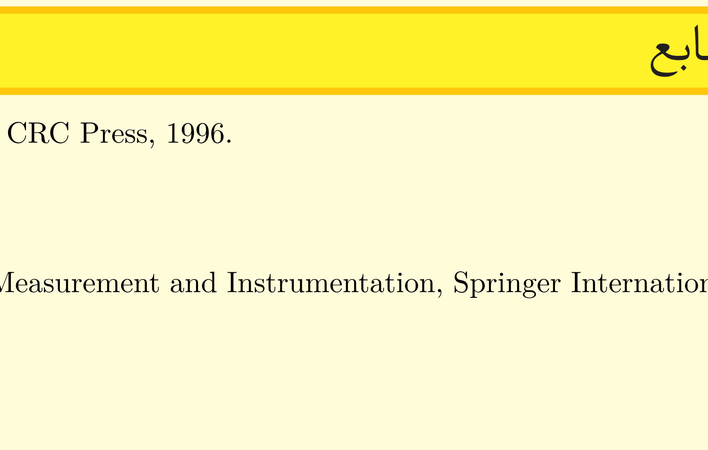
امنیت از مهم‌ترین واژه‌هایی است که در فکر و ذهن بشر، از نخستین لحظات زندگانی‌اش در جریان بوده‌است. هنگامی که ژولیوس سزار برای نخستین بار در ۵۰ سال قبل از میلاد، رمز ساده جانشینی حرفی خود را بکار گرفت، هیچ‌گاه فکر نمی‌کرد که حوزه‌ای که در آن گام نهاده، به یکی از بزرگترین حوزه‌های تحقیقاتی دنیا مبدل خواهد شد. امنیت در حوالی جنگ جهانی دوم رشد شگرفی را تجربه کرد. اما آن‌چه که ما اکنون بر آن گام می‌نهیم، مدیون دو انقلاب بزرگ در این حوزه است، مقاله ۱۹۴۹ شانون – Claude Elwood Shannon (April 30, 1916 – Feb 24, 2001) و دیگری بوجود آمدن مفهوم امنیت مبتنی بر کلید عمومی (Public Key).
تا مدت‌ها نگاه ما به امنیت به سه‌گانه CIA خلاصه می‌گشت، اما با گذر زمان مفاهیم جدیدی نظیر تازگی، انکارناپذیری، گمنامی و حفظ حریم خصوصی نیز مطرح گشت و جای خود را در این حوزه پیدا کرد. در این مجال، از دریای بی‌کران امنیت، به سراغ حفظ حریم‌خصوصی می‌رویم [۱].

امنیت مبتنی بر اطلاعات جانبی

حفظ حریم‌خصوصی در دو دسته [۴، صفحه ۲۰۲]:

- مبتنی بر داده (Data Oriented)
- مبتنی بر اطلاعات جانبی (ContextOriented)

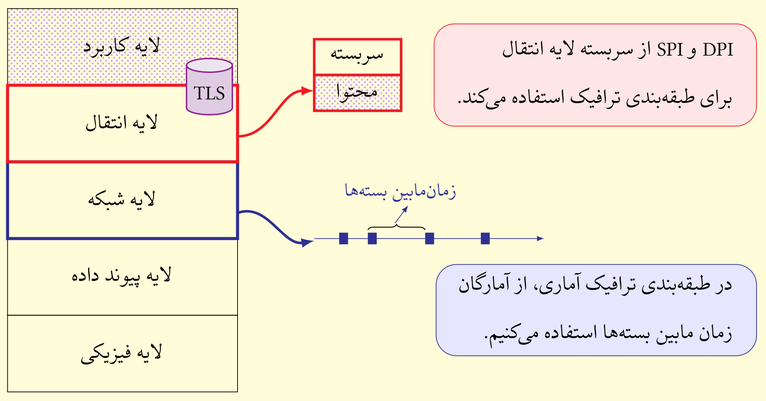
نقطه تمرکز حریم‌خصوصی مبتنی بر داده، بر روی محتوای داده است و بدین‌سان سازوکارهایی نظیر رمزنگاری و حفظ یکپارچگی برای تامین چنین نیازی کارا و کافی خواهد بود. در حریم‌خصوصی مبتنی بر اطلاعات جانبی، هدف غایی کسب اطلاعات جانبی از داده‌ها است. فرض کنید جلسه‌ای محرمانه بین دو نفر تشکیل شده است. در این نوع از حفظ حریم‌خصوصی، محتوای داده (صحبت‌هایی که در جلسه مطرح شده) برای ما اهمیت ندارد، بلکه اطلاعات جانبی آن نظیر این‌که چه‌کسانی، درکجا، کی، چگونه و چرا این جلسه را برگزار کردند، از اهمیت بیشتری برخوردار خواهد بود.
آن‌چه که ما به دنبال آن هستیم، نوعی از حریم‌خصوصی است که ما آن را حریم‌خصوصی زمانی و آماری (Temporal and Statistical Privacy) می‌نامیم. این نوع از حریم‌خصوصی، هر نوع اطلاعاتی از زمان رخداد یک حادثه چه به صورت قطعی و چه به صورت آماری (به عنوان نمونه نرخ و پراش زمان رخداد آن حادثه) ممکن است حریم‌خصوصی کاربر را به مخاطره بیافکند.



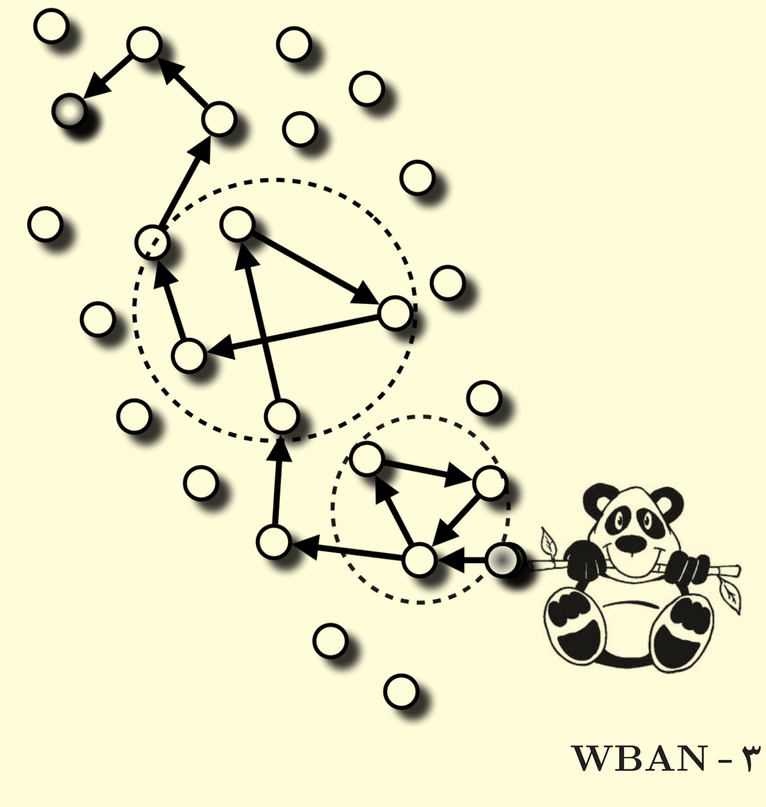
حفظ حریم زمانی و آماری از جنبه‌های بسیاری می‌تواند حائز اهمیت باشد. ما در نقش پدآفندی قرار داریم.

کاربردها

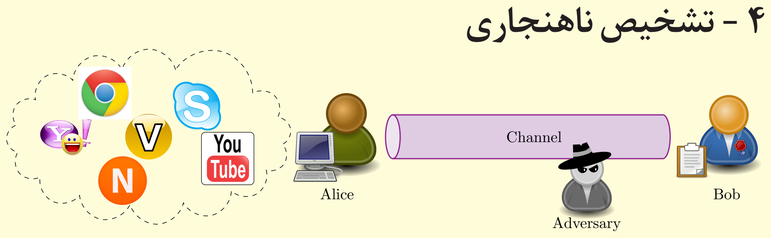
۱ - طبقه‌بندی ترافیک



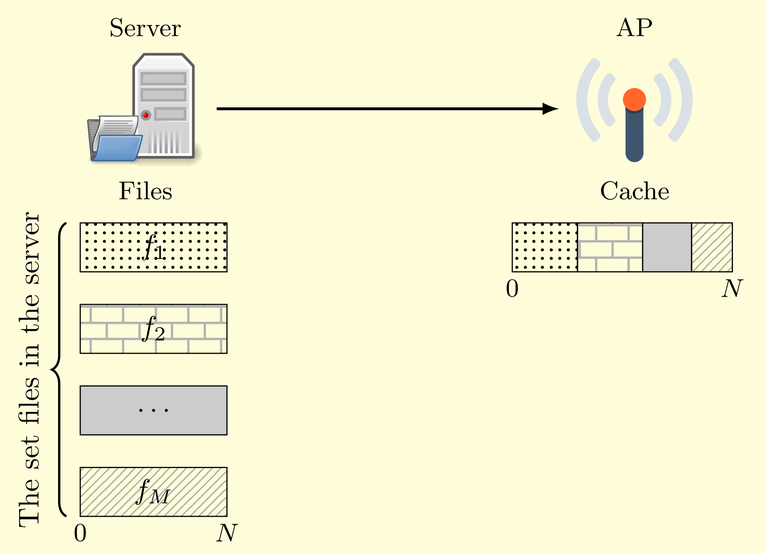
۲ - شبکه‌های حسگر بی‌سیم



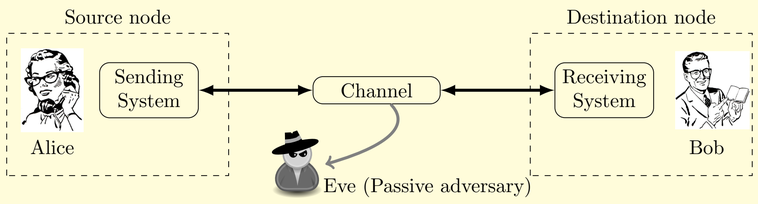
۴ - تشخیص ناهنجاری



۵ - سامانه‌های ذخیره‌سازی



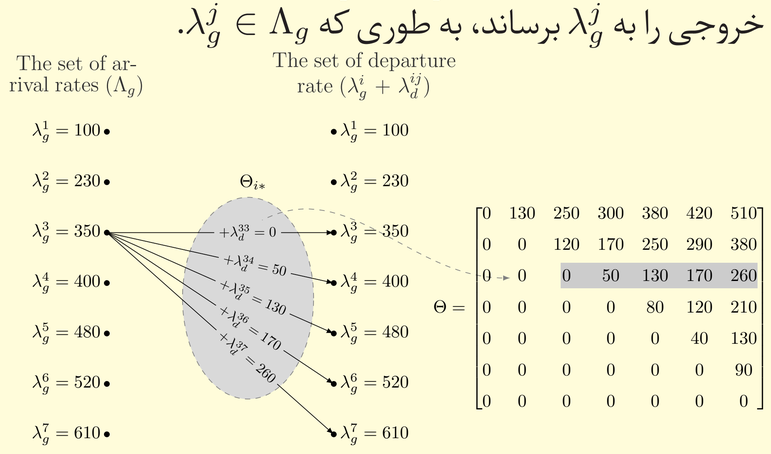
مثال انگیزه‌بخش



Alice (گره مبدا) قصد تبادل اطلاعات با Bob (گره مقصد) را دارد. فرض کنید که Alice در هر بازه زمانی، یک کاربرد از مجموعه هفت کاربرد موجود بر روی سامانه خود را اجرا می‌کند. اجازه دهید که نرخ تولید بسته‌ها توسط کاربرد iام $(1 \leq i \leq 7)$ را با $\lambda_g^i \in \Lambda_g$ نشان دهیم، که Λ_g بیانگر مجموعه نرخ‌های این هفت کاربرد است. در ادامه Λ_g را به صورت زیر در نظر بگیرید.

$$\Lambda_g = \{100, 230, 350, 400, 480, 520, 610\} \text{ [kbps]}.$$

در این میان Eve به عنوان یک مهاجم، به شنود کانال ارتباطی بین Alice و Bob می‌پردازد. او قصد دارد بداند که Alice کدام یک از این هفت کاربرد را در آن بازه زمانی اجرا نموده است. به دلیل استفاده از سازوکارهای امنیتی (نظیر رمزنگاری) به نظر می‌رسد Eve نتواند به محتوای بسته‌های ارسالی دست یابد و به ناچار دست به دامان قانون پایستگی جریان (Flow Conservation Law) [۲، قضیه ۵.۴.۳] می‌شود. برطبق این قانون نرخ خروج بسته‌های ارسالی از سوی Alice، برابر با نرخ تولید بسته‌ها خواهد بود. بدین‌سان و با علم به نگاشت هر نرخ به کاربرد متناظرش، می‌تواند به مقصود خود نایل گردد.
به دنبال آن هستیم که راه‌کاری پیش پای Alice برای حفظ حریم‌خصوصی نرخ بگذاریم. خواهید دید که اضافه کردن بسته‌های Dummy جزو مواردی است که قانون پایستگی جریان را نقض می‌کند. بدین‌سان Alice برای حفظ حریم‌خصوصی کاربرد i با نرخ λ_g^i، سعی می‌کند با اضافه کردن جریانی از بسته‌ها با نرخ $\lambda_d^{ij} = \lambda_g^j - \lambda_g^i$، نرخ بسته‌های خروجی را به λ_g^j برساند، به طوری که $\lambda_g^j \in \Lambda_g$.



نوآوری

درجه حریم‌خصوصی: به احتمال خطای بهترین تخمین مهاجم از شناسه کاربرد، درجه حریم‌خصوصی گره مبدا می‌گوییم.
ذکر خواهد شد که نامساوی Fano [۳، قضیه 2.10.1] ما را یاری می‌رساند تا بتوانیم یک کران پایین برای خطای مهاجم (P_e) در بهترین تخمینش بیابیم.

- ارایه یک روش پیشنهادی (اضافه نمودن بسته‌های ساختگی) به صورت کامل ارایه خواهد شد.
- توصیف رفتار Alice در اضافه نمودن بسته‌های ساختگی، مبتنی بر یک مدل ریاضیاتی بر مبنای Preemptive Resume Priority Queue.
- شروطی نیز بر روی نحوه ارسال بسته‌های ساختگی، چراکه اضافه‌کردن بسته‌های ساختگی، ممکن است موجب سوق داده شدن سامانه به ناحیه غیرپایدار است.

منابع

[1] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications, CRC Press, 1996.

[2] G. Kesidis. *An Introduction to Communication Network Analysis*. Hoboken, NJ, USA: John Wiley & Sons, Inc., June 2007.

[3] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, 2006.

[4] A. Mason, S. Mukhopadhyay, and K. Jayasundera. *Sensing Technology: Current Status and Future Trends III*. Smart Sensors, Measurement and Instrumentation, Springer International Publishing, 2014.