دانشگاه تهران
پردیس دانشکده های فنی
دانشکده مهندسی برق و کامپیوتر

بررسی و ارزیابی حفظ حریم زمانی در شبکه‌های ارتباطی با استفاده از تئوری صف

رساله برای دریافت درجه دکترای تخصصی

در رشته مهندسی کامپیوتر گرایش نرم‌افزار

ابوالفضل دیانت

استاد راهنما:

دکتر احمد خونساری

دی‌ماه ۱۳۹۵


بسم الله الرحمن الرحيم

دانشگاه تهران

پردیس دانشکده های فنی

رساله برای دریافت درجه‌ی دکتری تخصصی در رشته مهندسی کامپیوتر گرایش نرم‌افزار

عنوان: بررسی و ارزیابی حفظ حریم‌زمانی در شبکه‌های ارتباطی با استفاده از تئوری صف

نگارش: ابوالفضل دیانت

این پایان‌نامه در تاریخ ۱۳۹۵/۱۱/۲۰ در مقابل هیات داوران دفاع گردید و مورد تصویب قرار گرفت.

رییس دانشکده‌ی مهندسی برق و کامپیوتر: دکتر مجید نیلی احمدآبادی

معاون پژوهشی و تحصیلات تکمیلی دانشکده مهندسی برق و کامپیوتر: دکتر بابک نجار اعرابی

استاد راهنما: دکتر احمد خونساری

عضو هیات داوران: دکتر بابک خلج

عضو هیات داوران: دکتر فرید آشتیانی

عضو هیات داوران: دکتر مهدی کارگهی

عضو هیات داوران: دکتر بهنام بهرک

تعهدنامه‌ی اصالت اثر

باسمه تعالی

این‌جانب ابوالفضل دیانت تایید می‌کنم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی این‌جانب است و به دستاوردهای پژوهشی دیگران که در این نوشته از آن‌ها استفاده شده است، مطابق مقررات ارجاع گردیده است. این پایان‌نامه قبلا برای احراز هیچ مدرک هم‌سطح یا بالاتر ارایه نشده است.

نام و نام‌خانوادگی دانشجو: ابوالفضل دیانت

امضای دانشجو:

تقدیم به همه آنهایی که

می خواهند بیشتر بدانند

سپاس‌گزاری...

در ابتدا از زحمات پدر و مادر گرامی‌ام، همسر مهربانم و خانواده دلسوزم که در دوران تحصیل مشوق و پشتیبان این‌جانب بوده، کمال تشکر و امتنان را دارم. در ضمن بر خود واجب می‌دانم از زحمات استاد راهنمای خود، جناب آقای دکتر احمد خونساری ، صمیمانه تشکر و قدردانی کنم که قطعاً بدون راهنمایی‌های ایشان، این رساله به انجام نمی‌رسید. هم‌چنین از آقای سید پویا شریعت‌پناهی که هم در زمینه علمی و هم اخلاقی مشاور خوبی برای من بوده و هستند، کمال سپاس‌گزاری را دارم.

لازم می‌دانم از پدید آورندگان بسته زی‌پرشین (XƎPersian)، مخصوصاً جناب آقای وفا خلیقی، که این پایان‌نامه با استفاده از این بسته، آماده شده است و نیز از تمای اعضای گروه پارسی‌لاتک به خاطر پاسخ‌گویی به سوالاتم در مورد LaTeX، کمال قدردانی را داشته باشم.

خدایا...

به من زیستنی عطا کن که در لحظه مرگ، بر بی‌ثمری لحظه‌ای که برای زیستن گذشته است، حسرت نخورم و مُردنی عطا کن که بر بیهودگیش، سوگوار نباشم. بگذار تا آن را، خود انتخاب کنم، اما آنچنان که تو دوست می‌داری.

تو می‌دانی و همه می‌دانند که شکنجه دیدن بخاطر تو، زندانی کشیدن بخاطر تو و رنج بردن به پای تو تنها لذت بزرگ زندگی من است، از شادی توست که من در دل می‌خندم، از امید رهایی توست که برق امید در چشمان خسته‌ام می‌درخشد و از خوشبختی توست که هوای پاک سعادت را در ریه‌هایم احساس می‌کنم. نمی‌توانم خوب حرف بزنم. نیروی شگفتی را که در زیر کلمات ساده و جمله‌های ضعیف و افتاده، پنهان کرده‌ام دریاب، دریاب.

تو می‌دانی و همه می‌دانند که زندگی از تحمیل لبخندی بر لبان من، از آوردن برق امیدی در نگاه من، از برانگیختن موج شعفی در دل من، عاجز است.

تو، چگونه زیستن را به من بیاموز، چگونه مردن را خود خواهم آموخت.

به من توفیق تلاش در شکست، صبر در نومیدی، رفتن بی‌همراه، جهاد بی‌سلاح، کار بی‌پاداش، فداکاری در سکوت، دین بی‌دنیا، مذهب بی‌عوام، عظمت بی‌نام، خدمت بی‌نان، ایمان بی‌ریا، خوبی بی‌نمود، گستاخی بی‌خامی، قناعت بی‌غرور، عشق بی‌هوس، تنهایی در انبوه جمعیت، و دوست داشتن بی‌آنکه دوست بداند، روزی کن [1].

---

[1] مناجاتی از دکتر علی شریعتی.

چکیده

امروزه نشان داده شده که حتی در صورت استفاده از سازوکارهای تامین امنیت محتوای داده، نظیر رمزنگاری داده‌ها، یک مهاجم باهوش می‌تواند اطلاعات مفیدی را با تحلیل رفتار تولید داده‌ها، بدست آورد. این بدان علت است که با استفاده از سازوکارهای سنتی رمزنگاری، حریم‌خصوصی بسیاری از جنبه‌های تولید داده نظیر میانگین و پراش زمان تولید داده‌ها، در برابر یک مهاجم باهوش قابل حفظ نخواهد بود. بدین‌سان علاوه بر استفاده از سازکارهای تامین امنیت محتوای داده و به عنوان مکمل آن، نیاز به ارایه راه کارهایی به منظور حفظ حریم خصوصی این جوانب نیز وجود دارد. به عبارت‌بهتر و از دیدگاه علم شبکه‌های رایانه‌ای، مهاجم بدون داشتن اطلاعاتی در مورد لایه کاربرد و لایه انتقال، و فقط با داشتن اطلاعات زمانی ارسال بسته‌ها در لایه شبکه، حریم خصوصی کاربر را به خطر بیاندازد.

در این رساله، با استفاده از نظریه صف و نظریه اطلاعات این جنبه از حریم خصوصی را مورد بررسی قرار خواهیم داد. ما در ابتدا به سراغ نرخ تولید داده در گره مبدا می‌رویم. خواهیم گفت که یک مهاجم باهوش می‌تواند با بهره‌گرفتن از قانون پایستگی جریان و با استفاده از نرخ، حریم‌خصوصی زمانی و آماری کاربر را به خطر بیاندازد. البته در ادامه خود را محدود به نرخ نخواهیم کرد و از یک ویژگی به صورت کلی سخن به میان خواهد آمد. برای ویژگی نرخ راه‌کاری نیز مبتنی بر اضافه نمودن بسته‌های ساختگی ارایه می‌گردد. در ضمن گذری نیز بر حریم‌خصوصی زمانی و آماری در سامانه‌های ذخیره‌سازی خواهیم داشت. مهاجم باشنود کانال در مرحله تحویل در سامانه‌های ذخیره‌سازی، می‌تواند حریم خصوصی کاربران را به خطر بیاندازد، بدین‌سان که می‌تواند دریابد که با احتمال زیادی یک کاربر، چه فایلی را درخواست کرده‌است.

روش‌های پیشنهادی در کل این رساله، می‌بایست به نحوی باشد که ضمن حفظ حریم‌خصوصی زمانی و آماری، QoS کاربر را نیز حفظ نماید. تمامی روش‌های پیشنهادی ارایه شده در این رساله، بر پایه تعدادی مساله بهینه‌سازی، استوار است که بده‌بستان بین حریم خصوصی و هزینه را مدیریت می‌نماید. از سوی دیگر به منظور مدل‌سازی هرچه بهتر مفهوم حریم خصوصی، به سراغ یافتن یک‌سری کران پایین برای احتمال خطای بهترین تخمین مهاجم خواهیم رفت. در این راه از باندهای پیشنهاد شده در مبحث کانال‌های مخابراتی که در علم نظریه اطلاعات مورد بحث قرار می‌گیرد، استفاده کرده‌ایم. در نهایت نیز یک مدل ریاضیاتی برای سامانه‌های ذخیره‌سازی و بالابردن حریم خصوصی در این نوع از سامانه‌ها با درنظر گرفتن میزان ترافیک مبادله شده پیشنهاد خواهیم داد.

کلمات کلیدی: حریم خصوصی مبتنی بر اطلاعات جانبی، بسته ساختگی، احتمال خطای بهترین تخمین مهاجم، نظریه اطلاعات، سامانه ذخیره‌سازی.

فهرست مطالب

فهرست تصاویر

فهرست جداول

A

AP . . . . . Access Point

C

C-I-A . . . . . Confidentiality، Integrity and Availability

D

DPI . . . . . Deep Packet Inspection

E

ECG . . . . . Electrocardiography

EEG . . . . . Electroencephalography

F

FTP . . . . . File Transfer Protocol

Q

QoE . . . . . Quality of experience

QoS . . . . . Quality of Service

S

SPI . . . . . Stochastic Packet Inspection

W

WBAN . . . . . Wireless Body Area Network

WBSN . . . . . Wireless Body Sensor Network

فصل ۱

مقدمه

در این فصل انگیزه و هدفمان را، در انتخاب موضوع این رساله بیان خواهیم کرد. بدین‌منظور نخست در بخش ۱.۱ به سراغ مفهوم امنیت[۱] خواهیم رفت. خواهیم گفت که امروزه، حریم خصوصی[۲] مبتنی بر اطلاعات جانبی[۳] اهمیت بی‌بدیلی در حوزه امنیت یافته است. از دریای بی‌کران موضوعات مربوط به حریم خصوصی مبتنی بر اطلاعات جانبی، به سراغ مبحث حریم‌خصوصی زمانی و آماری[۴] خواهیم رفت. برای جلب توجه خواننده به اهمیت موضوع در بخش ۲.۱، برخی از کاربردهای مطرح در این حوزه مورد بررسی قرار خواهد گرفت. در نهایت در بخش ۳.۱ و بخش ۴.۱ به ترتیب دستاوردهای حاصل گشته و ساختار رساله ارایه می‌گردد.

[1] Security
[2] Privacy
[3] Context Oriented
[4] Temporal and Statistical Privacy

۱.۱ از امنیت تا حریم‌خصوصی زمانی و آماری

امنیت از مهم‌ترین واژه‌هایی است که در فکر و ذهن بشر، از نخستین لحظات زندگانی‌اش در جریان بوده‌است. هنگامی که ژولیوس سزار[۵] 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[۶] [۱] و دیگری بوجود آمدن مفهوم امنیت مبتنی بر کلید عمومی[۷] [۲].

تا مدت‌ها نگاه ما به امنیت به سه‌گانه C-I-A[8] خلاصه می‌گشت، اما با گذر زمان مفاهیم جدیدی نظیر تازگی[۹]، انکارناپذیری[۱۰]، گمنامی[۱۱] و حریم خصوصی نیز مطرح گشت و جای خود را در این حوزه پیدا کرد [۲]. در این مجال، از دریای بی‌کران امنیت، به سراغ حریم خصوصی می‌رویم.

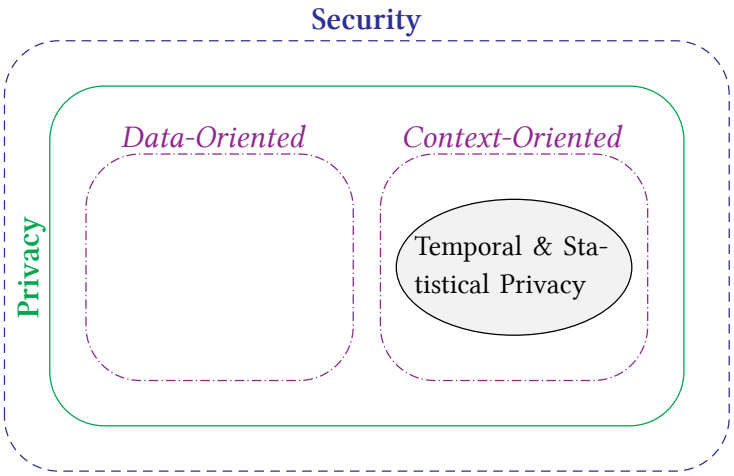
حریم خصوصی را می‌توان در دو دسته مبتنی بر داده[۱۲] و مبتنی بر اطلاعات جانبی طبقه‌بندی نمود [۳، بخش 12.4.1]، [۴، صفحه ۲۰۲]. نقطه تمرکز حریم خصوصی مبتنی بر داده، بر روی محتوای داده است و بدین‌سان سازوکارهایی نظیر رمزنگاری[۱۳]، یکپارچگی[۱۴] و غیره برای تامین چنین نیازی کارا و کافی خواهد بود. اما در این رساله به سراغ دسته دوم یعنی حریم خصوصی مبتنی بر اطلاعات جانبی می‌رویم. در این دسته بالعکس دسته نخست، هدف غایی کسب اطلاعات جانبی از داده‌ها است. فرض کنید جلسه‌ای محرمانه بین دو نفر تشکیل شده است. در این نوع از حریم خصوصی، 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 در این رساله به دنبال آن هستیم، نوعی از حریم خصوصی مبتنی بر اطلاعات جانبی است، که ما آن را حریم‌خصوصی زمانی و آماری می‌نامیم. در شکل ۱.۱ نسبت موضوع انتخاب گشته (یعنی حریم‌خصوصی زمانی و آماری) به نسبت کل حوزه امنیت به خوبی نشان داده شده است. خواهید دید که در حریم‌خصوصی زمانی و آماری، هر نوع اطلاعاتی از زمان رخداد یک حادثه چه به صورت قطعی و چه به صورت آماری (به عنوان نمونه نرخ و پراش[۱۵] زمان رخداد آن حادثه) ممکن است حریم خصوصی کاربر[۱۶] را به مخاطره بیافکند. در ادامه برخی از کاربردهای این نوع از حریم خصوصی را ذکر خواهیم کرد.

۲.۱ کاربردهای حریم‌خصوصی زمانی و آماری

حریم‌خصوصی زمانی و آماری از جنبه‌های بسیاری می‌تواند حائز اهمیت باشد. در ادامه ما به چند نمونه از این کاربردها اشاره خواهیم نمود. البته کاربردهای مساله یاد شده، به موضوعات مورد اشاره محدود نمی‌شود، و موارد اشاره شده تنها

[5] Gaius Iulius Caesar
[6] Claude Elwood Shannon (April 30, 1916 – Feb 24, 2001)
[7] Public Key
[8] Confidentiality, Integrity and Availability
[9] Freshness
[10] Non-repudiation
[11] Anonymity
[12] Data Oriented
[13] Encryption
[14] Integrity
[15] Variance
[16] User



شکل ۱.۱: حفظ حریم خصوصی، یکی از مهم‌ترین ابعاد حفظ امنیت یک سامانه است. حریم خصوصی به نوبه خود به دو بخش مبتنی بر داده و مبتنی بر اطلاعات جانبی تقسیم می‌گردد. در این رساله ما به دنبال پویش در حوزه حریم‌خصوصی زمانی و آماری (از زیرمجموعه حریم خصوصی مبتنی بر اطلاعات جانبی) هستیم.

نمونه‌هایی از کاربردهای این حوزه هستند.

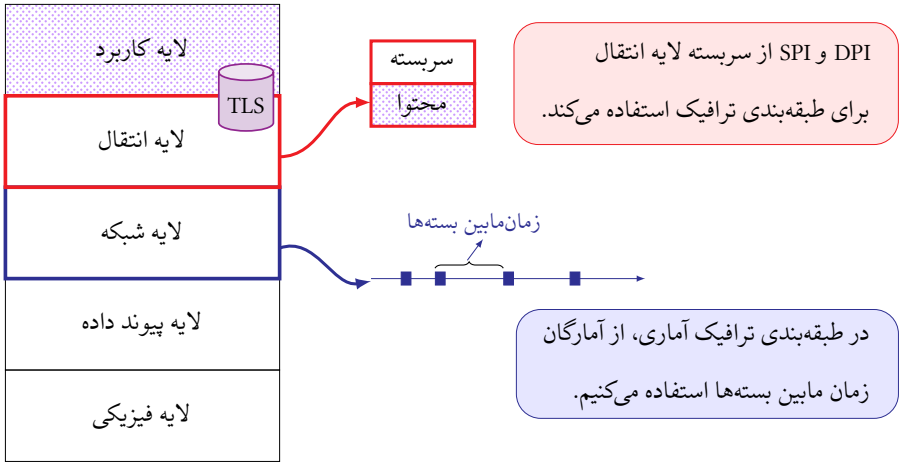
۱.۲.۱ حریم خصوصی کاربر در حوزه طبقه‌بندی ترافیک

تا چند سال پیش، تقریبا همه کاربرد[۱۷]هایی که بر روی رایانه‌ها اجرا می‌شدند، از پروتکل‌های شناخته شده با شماره درگاه[۱۸] مشخص استفاده می‌کردند؛ به مانند کاربرد FileZilla که از پروتکل FTP[19] و شماره درگاه 20 و 21 استفاده می‌کند. اما امروزه تعداد کاربردهای با پروتکل نامعلوم و اختصاصی، با شماره درگاه‌های غیراستاندارد و تصادفی بسیار فراگیر شده است. به عنوان نمونه‌ای از این کاربردها می‌توان از Skype، BitTorrent و VPN نام برد. در ضمن استفاده از سازوکارهای امنیتی در بسته‌ها[۲۰]ی تولید شده توسط کاربردهای یاد شده، موجب می‌شود که از محتوای بسته، نتوان پی به کاربرد تولید کننده آن برد.

یک مهاجم[۲۱] بنا به جهات بسیاری تمایل دارد که دریابد که در گره مبدا[۲۲] چه کاربردی اجرا شده است. این موضوع در حوزه‌ای از تحقیقات به نام طبقه‌بندی ترافیک[۲۳] و یا بازرسی بسته[۲۴] مورد بررسی قرار می‌گیرد. روش‌های مختلفی برای کمک به مهاجم در این زمینه وجود دارد که دو نمونه از مهم‌ترین این روش‌ها به شرح زیر است [۵] (شکل ۲.۱):

✍ **طبقه‌بندی ترافیک بر مبنای محتوا**[۲۵]: در این روش محتوای سربسته[۲۶] لایه انتقال[۲۷] مورد بازرسی قرار می‌گیرد. در حالت کلی این روش دسته‌بندی، به دو صورت DPI[28] و SPI[29] انجام می‌پذیرد.

[17] Application
[18] Port Number
[19] File Transfer Protocol
[20] Packet
[21] Adversary
[22] Source Node
[23] Traffic Classification
[24] Packet Inspection
[25] Payload
[26] Header
[27] Transport Layer
[28] Deep Packet Inspection
[29] Stochastic Packet Inspection



شکل ۲.۱: در DPI و SPI از محتوای سربسته لایه انتقال استفاده می‌شود، در حالی‌که در طبقه‌بندی ترافیک آماری از آمارگان زمان مابین خروج بسته‌ها استفاده می‌گردد.

- در DPI، سعی می‌شود که محتوا با یک امضای ثابت مقایسه گردد. دسته‌بندی بر مبنای پروتکل و شماره درگاه، به عنوان یکی از زیردسته‌های DPI محسوب می‌گردد. DPI به صورت گسترده در نرم‌افزارها و دیوارهای آتش[۳۰] مورد استفاده قرار می‌گیرد [۶].
- در SPI، ویژگی‌های آماری سربسته و محتوای بسته لایه انتقال، مورد پویش قرار می‌گیرد [۷].

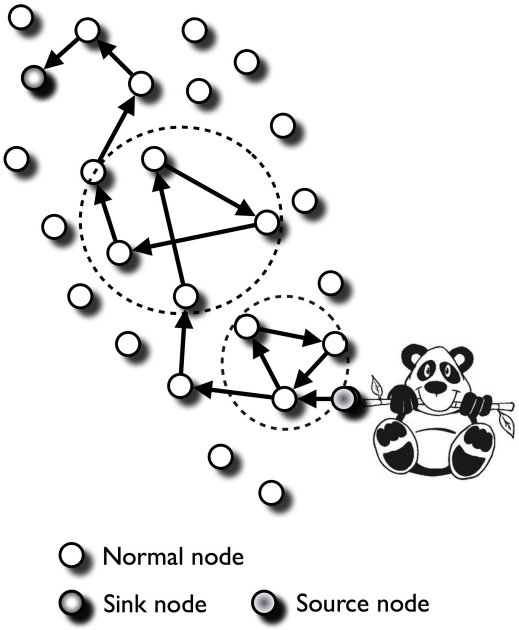
✍ **طبقه‌بندی ترافیک آماری[۳۱]ی:** در این شیوه به ویژگی‌های آماری زمان مابین خروج[۳۲] و طول بسته‌ها در لایه شبکه[۳۳] توجه می‌شود. لازم به ذکر است که در دسته‌بندی آماری بر خلاف SPI نیازی به بازگشایی بسته وجود ندارد، بدین‌سان در این نوع از دسته‌بندی حجم پردازش و محاسبات، به مراتب کمتر از SPI است.

با زیاد شدن پروتکل‌ها، مخفی ماندن جزئیات کارکرد آن‌ها به دلایل تجاری و استفاده از سازوکارهای امنیتی نظیر IPSec، روش‌های DPI و SPI دیگر به خوبی نمی‌توانند جواب‌گوی ما در این مساله باشند، و بدین‌سان امروزه شاهد یک اقبال عمومی به روش‌های طبقه‌بندی ترافیک آماری هستیم [۸، ۹]. پرواضح است که هیچ‌کدام از ما دوست نخواهیم داشت که کسی بداند که چه کاربردی را در هر بازه زمانی بر روی رایانه خود اجرا می‌کنیم. این امر به نوعی جزوی از حریم خصوصی ما محسوب می‌گردد. در این رساله یک چارچوب کلی برای حفظ حریم خصوصی در مقابل این نوع از حملات ارایه می‌گردد.

۲.۲.۱ حریم‌خصوصی زمانی و آماری در شبکه‌های حسگر بی‌سیم

Ozturk در [۱۱]، مساله‌ای به نام Panda-Hunter را معرفی کرده است که برطبق آن تعداد زیادی حسگر[۳۴]، در منطقه‌ای به منظور تشخیص وجود پانداها قرار داده شده است (شکل ۳.۱). هر زمان که وجود پاندایی توسط حسگر تشخیص داده

[30] Firewall
[31] Statistical
[32] InterDeparture Time
[33] Network Layer
[34] Sensor



شکل ۳.۱: حسگرها به محض حس یک پاندا، گزارشی به صورت چندگامه ارسال می‌کنند [۱۰].

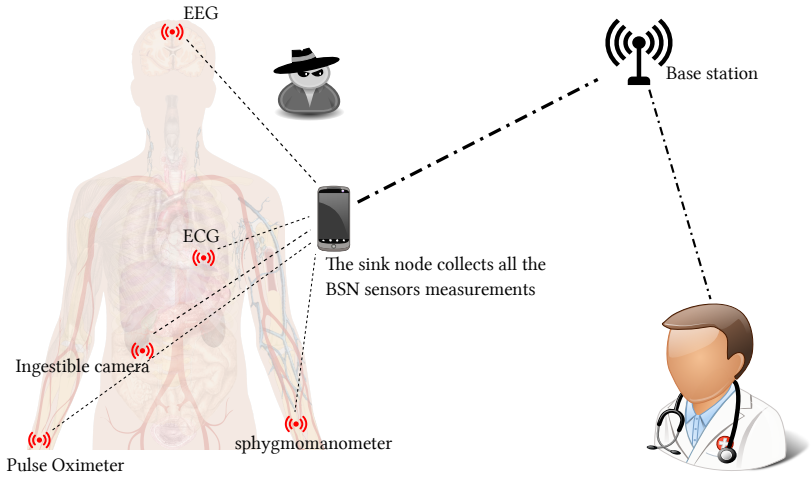
شود، سیگنالی به مرکز جمع‌آوری داده ارسال می‌گردد. حسگرها توسط پروتکل‌های مسیریابی[۳۵] چندگامه[۳۶]، داده خود را به دست مرکز جمع‌آوری می‌رسانند. شکارچی نیز وجود دارد که قصد دارد توسط اطلاعات ارسالی از حسگرها به محل پاندا پی ببرد. به همین علت شکارچی به شنود کانال منتهی به مرکز جمع‌آوری مبادرت می‌ورزد.

با رسیدن سیگنال یک حسگر به مرکز، شکارچی در می‌یابد که اتفاقی افتاده، و بدین‌سان سعی می‌کند که مکانی که اتفاق مورد نظر رخ داده است را بیابد. از سوی دیگر، شکارچی با بدست آوردن این اطلاعات، می‌تواند نحوه رفتار حرکت پانداها را تخمین بزند، و دریابد که به احتمال زیاد در هر ساعت از شبانه‌روز، پانداها در کدام محل قرار گرفته‌اند. به نظر می‌رسد که در هر دو حالت یاد شده، مبحث حریم‌خصوصی زمانی و آماری از اهمیت ویژه‌ای برخوردار باشد.

۳.۲.۱ حریم‌خصوصی زمانی و آماری در WBAN

در WBAN[37] تعدادی حسگر به منظور سنجش ضربان قلب، وضعیت مغز، قند، فشار، چربی و غیره، بر روی بدن بیمار نصب می‌گردد [۱۲]. بسته به نوع بیماری فرد، این حسگرها با نرخ‌های مختلفی سنجش‌های مذکور را انجام می‌دهند. به عنوان مثال فرض کنید که مریضی به علت بیماری دیابت در بیمارستان بستری شده است. پرواضح است که برای تنظیم میزان انسولین تزریقی به بیمار، نیاز است در طول روز، حداقل چهار بار میزان قند خون او سنجیده شود، در حالی‌که این تعداد اندازه‌گیری برای سنجش چربی خون و ضربان قلب نیاز نخواهد بود. در هر بار سنجش، حسگر سیگنالی را به گره مرکزی ارسال و سپس از آن‌جا این اطلاعات در صورت نیاز به پزشک معالج نیز ارایه می‌گردد.

[35] Routing
[36] Multi-Hop
[37] Wireless Body Area Network



شکل ۴.۱: حسگرهای نصب شده بر روی بدن بیمار در WBAN، در زمان‌های مشخص به اندازه‌گیری علایم حیاتی او می‌پردازد. یک مهاجم باهوش می‌تواند با بدست‌آوردن اطلاعات مربوط به زمان‌های اندازه‌گیری حسگرها، پی به بیماری فرد ببرد.

همان‌طور که در شکل ۴.۱ نشان داده شده، فرض کنید که یک مهاجم دستگاهی را در کنار تخت بیمار کار گذاشته است که هنگام ارسال سیگنال توسط هر حسگر به گره مرکزی، متوجه ارسال سیگنال می‌گردد. گرچه به علت استفاده از سازوکارهای رمزنگاری، شاید نتواند به میزان سنجه مورد اندازه‌گیری پی ببرد. اما یک مهاجم باهوش می‌تواند با تحلیل اطلاعات مربوط به زمان‌های ارسال سیگنال توسط هر حسگر، پی به نوع بیماری فرد ببرد. با کمی دقت می‌توان دریافت که این موضوع، به طور قطع ناقض حریم خصوصی بیمار است.

۴.۲.۱ تشخیص ناهنجاری

فرض کنید که یک بدافزار[۳۸] به رایانه شما نفوذ کرده است. نرم‌افزارهایی که برای نابودی بدافزارها بکار گرفته می‌شوند، دو ایده کلی را دنبال می‌کنند؛ یا آن‌ها با فعالیت و نحوه تاثیر بدافزار آشنا هستند، و یا در صورت ناآشنا بودن با آن، به رهگیری رفتارهای غیر معمول در سیستم‌عامل[۳۹] می‌پردازند، و در صورت بروز چنین رفتارهایی، عامل آن رفتار را به عنوان بدافزار تشخیص می‌دهند [۱۳]. این‌که بدافزار به چه قسمتی از رایانه، در چه زمانی و با چه آمارگانی دسترسی پیدا می‌کند، رفتار یک بدافزار را تشکیل می‌دهد.

بازهم ادعا می‌کنیم که چارچوب ارایه شده می‌تواند هم به بدافزار و هم به نگهبان رایانه شما یاری رساند. از یک سو چارچوب ارایه شده برای بدافزار می‌تواند مفید باشد چرا که کمک می‌کند تا اطلاعات زمانی و آماری نحوه دسترسی بدافزار مخفی گردد. از سوی دیگر به شما کمک می‌کند تا بتوانید ویژگی‌های زمانی و آماریی از بدافزار استخراج نمایید که نسبت به بسیار از اتفاقاتی که در سیستم‌عامل رخ می‌دهد، مقاوم باشد.

[38] Malware
[39] Operating System

۳.۱ نوآوری‌ها

در ادامه به صورت مختصر دستاوردها و نوآوری‌های بدست‌آمده در این رساله را ذکر می‌کنیم. گرچه لازم به ذکر است که هر یک از دستاوردها متناظر با فصلی از رساله است که در جای خویش به تشریح بیان خواهد شد.

- در فصل ۳، روشی پیشنهاد خواهیم داد که در آن با استفاده از اضافه کردن تعدادی بسته که ما از آن‌ها با عنوان بسته‌های ساختگی[۴۰] یاد می‌کنیم، سعی داریم که حریم خصوصی نرخ[۴۱] را حفظ کنیم. لازم به ذکر است که در روش پیشنهادی به منظور حفظ QoS[42]، تنها تعدادی بسته اضافه خواهد گشت و بسته‌ای حذف نخواهد شد. در همان فصل خواهید دید که با استفاده از نامساوی Fano[۴۳] [۱۴، قضیه 2.10.1]، معیاری برای توصیف ریاضیاتی حریم خصوصی پیشنهاد خواهیم داد. سپس با یاری‌جستن از یک مساله بهینه‌سازی[۴۴]، بده‌بستان[۴۵] بین حریم خصوصی و هزینه ارتباطی[۴۶]ناشی از ارسال بسته‌های ساختگی، مدیریت خواهد شد. در ؟؟، به صورت جزئی‌تر به تشریح دستاوردهای حاصل گشته در این قسمت، مبادرت خواهیم ورزید. در ضمن مطالب بیان شده، در مقاله زیر نیز ارایه گشته است.

  A. Diyanat, A. Khonsari, and S. P. Shariatpanahi, "A Dummy-Based Approach for Preserving Source Rate Privacy," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1321–1332, Jun. 2016.

- در فصل ۴، توسعه‌ای همه‌جانبه بر مطالب فصل ۳ خواهیم داشت. اولا خود را محدود به نرخ نخواهیم کرد، و به صورت کلی در مورد حفظ حریم خصوصی یک ویژگی[۴۷] صحبت خواهیم نمود. ثانیا نگاشت[۴۸] بین ویژگی‌ها به صورت کلی در نظر گرفته می‌شود؛ به عبارت‌بهتر اگر ویژگی را همان نرخ در نظر بگیریم، هم می‌توان با اضافه کردن بسته‌های ساختگی، به نرخ اضافه کرد و هم با حذف برخی از بسته‌ها، از نرخ کاست. در ضمن فرضی نیز بر روی توزیع اجرای کاربردها نخواهیم داشت. از سوی دیگر سه کران پایین[۴۹] به منظور توصیف احتمال خطای بهترین تخمین مهاجم[۵۰] با بهره‌گیری از علم نظریه اطلاعات[۵۱] بکار گرفته می‌شود. ضمن تشریح نوآوری بدست آمده در این فصل در ؟؟، این مطالب در مقاله زیر نیز ارایه گشته است.

  A. H. RezaeiTabar, A. Diyanat, and A. Khonsari, "On the Perfect Privacy: a Statistical Analysis of Network Traffic Approach," *IEEE Communications Letters*, pp. 1–4, 2016.

- در فصل ۵، به سراغ سامانه‌های ذخیره‌سازی[۵۲] خواهیم رفت. در آن‌جا ذکر خواهد شد که اگر یک مهاجم باهوش،

[40] Dummy Packet
[41] Rate
[42] Quality of Service
[43] Fano's Inequality
[44] Optimization Problem
[45] Trade-Off
[46] Communication Cost
[47] Feature
[48] Mapping
[49] Lower Bound
[50] Adversary's Best Estimation Error Probability
[51] Information Theory
[52] Caching System

به شنود پیوند[۵۳] ارتباطی بین AP[54] تا خدمت‌گزار[۵۵] بپردازد، می‌تواند در مرحله تحویل[۵۶] داده، پی ببرد که کاربر کدام فایل را درخواست کرده، و بدین‌سان حریم خصوصی کاربر نقض خواهد شد. در فصل مذکور با طرح یک مساله بهینه‌سازی خواهیم گفت که چگونه می‌توان سیاست‌گذاری[۵۷] بهینه[۵۸]ای برای نحوه پر کردن ذخیره‌سازها[۵۹] یافت به‌گونه‌ای که هم حریم خصوصی حفظ شود و هم میزان ترافیک مبادله شده در مرحله تحویل کاهش یابد. از سوی دیگر کمی نمودن حریم خصوصی‌در سامانه‌های ذخیره‌سازی نیز از جمله نوآوری‌های مهم در این فصل خواهد بود. نوآوری‌های ارایه شده در این قسمت به صورت دقیق‌تر در بخش ۲.۵ و مقاله زیر تشریح شده است.

A. Diyanat, A. Khonsari, and S. P. Shariatpanahi, "An Information Theoretic Approach to Evaluate and Preserve Privacy in a Network Caching System," *Submitted in ACM MobiHoc 2017*, 2016.

- در فصل ۶، به سراغ یک شبکه WBSN[60] خواهیم رفت. بیان خواهد شد که مهاجم با دست‌یابی به اطلاعات جانبی داده‌ها بین گره کنترل‌کننده و حسگرها در یک شبکه WBSN، می‌تواند حریم خصوصی بیمار را به خطر بیافکند. در ضمن همان‌طور که خواهد گذشت، ما برای حل این چالش، ایده‌ای مبتنی بر صف‌های اولویت‌دار زمانی[۶۱] ارایه خواهیم داد. در ضمن شایان ذکر است که مفهوم صف‌های اولویت‌دار زمانی نیز برای توابع اولویت[۶۲] عمومی گسترش خواهد یافت. مطالب بیان شده در این فصل در مقاله زیر ارایه شده است.

A. Diyanat, A. Khonsari, and S. H. Shafiei, "Preservation of Temporal Privacy in Body Sensor Networks," *Journal of Network and Computer Applications - Elsevier*, 2017.

۴.۱ ساختار رساله

حاصل کار پژوهشی این رساله در شش فصل و یک پیوست جمع‌آوری شده است. بعد از مطالب مقدماتی که در این فصل ذکر شد، در فصل ۲، گذری بر کارهای تحقیقاتی خواهیم داشت که از جنبه‌های مختلف با موضوع رساله در ارتباط هستند. در فصل ۳، چارچوبی ارایه می‌گردد که توسط آن می‌توان حریم خصوصی نرخ را حفظ نمود. فصل ۴ به نوعی گسترش و توسعه همه‌جانبه مطالب فصل ۳ خواهد بود. در فصل ۵ نیز به سراغ حریم خصوصی سامانه‌های ذخیره‌سازی خواهیم رفت. در فصل ۶ نیز حریم خصوصی در WBSN بررسی می‌گردد. در نهایت نیز در فصل ۷، نتیجه رساله به همراه پیشنهاداتی برای کارهای آتی ذکر خواهد شد.

---

[53] Link
[54] Access Point
[55] Server
[56] Delivery
[57] Policy
[58] Optimal
[59] Cache
[60] Wireless Body Sensor Network
[61] Time-DependentPriorityQueue
[62] Priority Function

فصل ۲

کارهای پیشین

۱.۲ حریم‌خصوصی زمانی و آماری

فصل ۳

حفظ حریم خصوصی نرخ

۱.۳ مثال انگیزه‌بخش

۲.۳ مدل سامانه

در این بخش به بیان مدل سامانه[1] خواهیم پرداخت. مدل گره مبدا (Alice) و مهاجم (Eve) به ترتیب در ؟؟ و ؟؟ ارایه می‌شود. در ضمن مجموعه‌ای از نمادهای پر کاربرد در این فصل در جدول ۱.۳ ارایه شده است.

[1] System Model

جدول ۱.۳: فهرستی از نمادهای بکار رفته در این فصل

نماد	توضیح
$\Pr\{A\}$	احتمال رخداد رویداد A
$\mathbb{E}\{\Re\}$	امید ریاضی* متغیر تصادفی $\Re$
$\mathrm{H}(\Re)$	اِنتروپی متغیر تصادفی $\Re$
$f_{\Re}$	تابع چگالی احتمال متغیر تصادفی $\Re$
$\mathbb{R}^{++}$	مجموعه اعداد حقیقی مثبت بدون حضور صفر
$\mathbb{R}^{+}$	مجموعه اعداد حقیقی مثبت با حضور صفر
$\mathbb{N}$	مجموعه اعداد طبیعی
λ_g^i	نرخ ورودی بسته‌های کاربرد i ام
λ_g	متغیر تصادفی گسسته که نمونه‌های آن متعلق به مجموعه Λ_g است.
$\hat{\lambda}_g$	تخمین مهاجم از λ_g
λ_d^{ij}	نرخ بسته‌های ساختگی اضافه شده برای نگاشت کاربرد i ام به j ام
μ_g^i	نرخ خدمتگزاری بسته‌های اصلی کاربرد i ام.
γ^j	نرخ خروجی j ام که در این فصل آن را به صورت $\gamma^j = \lambda_g^j$ در نظر می‌گیریم.
γ	متغیر تصادفی گسسته نرخ خروجی بسته‌ها که نمونه‌های آن متعلق به مجموعه Λ_g است.
t_l	زمان ورود بسته l ام
τ_l	انتقال داده شده t_l به‌گونه‌ای که $\tau_0 = 0$ باشد.
d_l	زمان خروج بسته l ام
N	تعداد کل کاربردهای اجرا شده بر روی گره مبدا
Λ_g	مجموعه مرتب‌شده از تمامی λ_g^i ها و نیز داریم $\lvert\lambda_g^i\rvert = N$.
Θ_{i*}	مجموعه تمامی نرخ‌های ساختگی (λ_d^{ij}) برای کاربرد i ام به گونه‌ای که $\lambda_g^i + \lambda_d^{ij} \in \Lambda_g$.
P_e	احتمال خطای مهاجم که به صورت $\Pr\{\hat{\lambda}_g \neq \lambda_g\}$ تعریف می‌شود.
M	فرایند نقطه‌ای نشان‌دار مانا که به صورت $\{t_l, s_l\}_{l=-\infty}^{\infty}$ تعریف می‌شود.
M_0	فرایند نقطه‌ای نشان‌دار مانای همگام که به صورت $\{\tau_l, s_l\}_{l=-\infty}^{\infty}$ در نظر گرفته می‌شود.
p_{ij}	احتمال نگاشت نرخ کاربرد i ام به نرخ کاربرد j ام
ξ	کران پایین برای احتمال خطای بهترین تخمین مهاجم‌که از نامساوی Fano بدست می‌آید.
α	پارامتر وزن در بده‌بستان بین هزینه ارتباطی و درجه حریم خصوصی
ψ_{ij}	هزینه ارسال بسته‌های ساختگی که به صورت تابعی از λ_d^{ij} تعریف می‌شود ($\psi_{ij} = f(\lambda_d^{ij})$).

فصل ۴

حفظ حریم خصوصی ویژگی‌ها

۱.۴ انگیزه

فصل ۵

حریم خصوصی در سامانه‌های ذخیره‌سازی

افزایش روزافزون کاربردهای چند رسانه‌ای[۱]، موجب رشد فزاینده‌ی ترافیک در شبکه‌های کنونی گشته است. انتقال این حجم عظیم از داده در ساعات اوج مصرف، همواره یکی از چالش‌های بزرگ طراحان شبکه بوده است؛ چراکه در این حالت، بسیاری از پیوندهای شبکه به مرز اشباع خود می‌رسند، که این خود موجب افزایش چشمگیر تاخیر[۲] و کاهش QoE[3] کاربران می‌گردد. استفاده از سامانه‌های ذخیره‌ساز شبکه‌ای[۴]، یکی از روش‌های موثر برای حل این معضل محسوب می‌گردد [۱۵].

همان‌طور که در شکل ۱.۵ مشاهده می‌کنید، کاربری در پوشش[۵] یک AP قرار گرفته است. AP نیز به خدمت‌گزار اصلی شبکه متصل است. هدف غایی این شبکه، ارسال محتوا[۶]ی مورد نیاز کاربر از خدمت‌گزار به اوست. در سامانه‌های ذخیره‌ساز شبکه‌ای در طول ساعات کم‌ترافیک، مرحله جایگذاری[۷] صورت می‌پذیرد. در طول این مرحله برخی از محتواهایی که کاربران ممکن است در ساعات اوج ترافیک بدان نیاز داشته‌باشند، در ذخیره‌ساز AP قرار می‌گیرد. در ساعات اوج مصرف با رسیدن درخواست کاربر، ابتدا AP چک می‌کند که محتوای مورد نظر در ذخیره‌ساز وجود دارد یا نه؟ در صورت وجود، AP بدون رهسپار نمودن درخواست به خدمت‌گزار اصلی، خود به سرعت محتوای موردنظر را برای کاربر ارسال می‌کند. در غیر این صورت AP درخواست کاربر را به خدمت‌گزارا صلی می‌دهد. به این مرحله که عموما در ساعات اوج ترافیک صورت می‌پذیرد، اصطلاحا مرحله تحویل گفته می‌شود

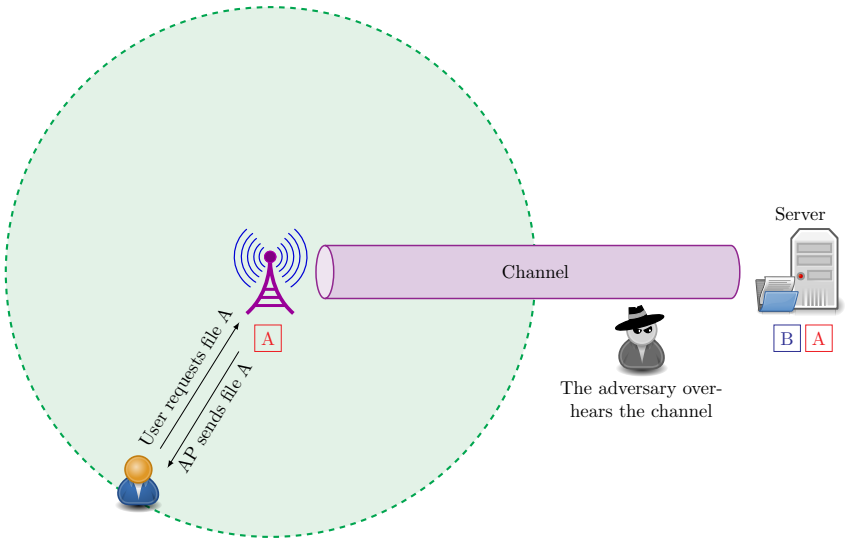
[1] Multimedia Application
[2] Delay
[3] Quality of experience
[4] Network Caching System
[5] Coverage
[6] Content
[7] Replacement

[۱۶]. این مرحله به خوبی در شکل ۱.۵ نشان داده شده است.

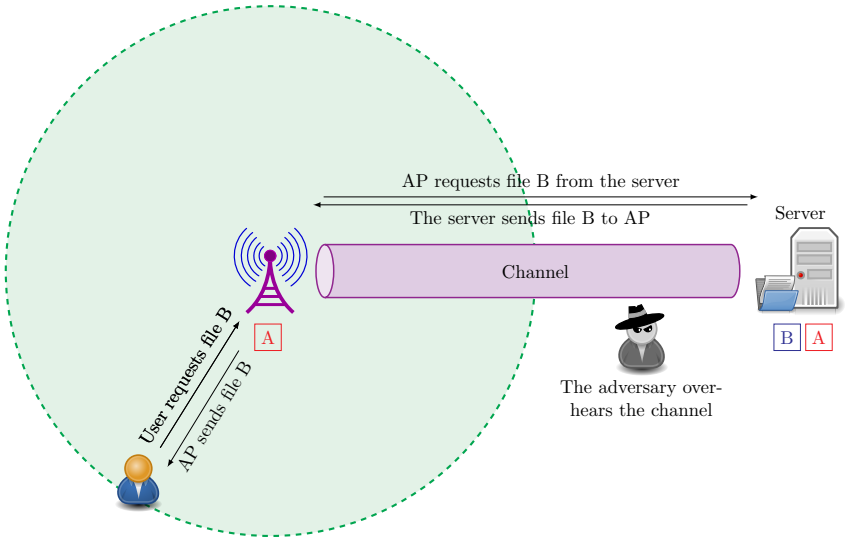
بیشتر کارهای تحقیقاتی موجود در حوزه سامانه‌های ذخیره‌سازی، بر روی تعین سیاست‌گذاری بهینه برای نحوه پر کردن ذخیره‌سازها، ظرفیت[۸] این سامانه[۹] و حریم خصوصی محتوای داده مبادله شده، تمرکز کرده‌اند [۱۶، ۱۷، ۱۸، ۱۹]. باتوجه به مطالعات صورت‌پذیرفته، تاکنون کاری در مورد حفظ حریم خصوصی مبتنی بر اطلاعات جانبی در سامانه‌های ذخیره‌سازی صورت نگرفته است. ما بر آنیم تا در این فصل بر روی این موضوع متمرکز شویم.

در بخش ۱.۵ نخست سعی داریم تا با یاری جستن از یک مثال ساده، خلا حریم خصوصی مبتنی بر اطلاعات جانبی، در سامانه‌های ذخیره‌سازی را متذکر شویم. در بخش ۲.۵، به تشریح نوآوری‌های بدست آمده، خواهیم پرداخت. بخش ۳.۵ را به بیان مدل سامانه تخصیص می‌دهیم. روش پیشنهادی به همراه تحلیل ریاضیاتی آن در بخش ۴.۵ خواهد آمد. در نهایت نیز شبیه‌سازی[۱۰] و تحلیل عددی[۱۱] روش پیشنهادی، در بخش ۵.۵ بیان خواهد شد.

[8] Capacity
[9] System
[10] Simulation
[11] Numerical Analysis



(آ)



(ب)

شکل ۱.۵: (آ) کاربر از AP درخواست فایل A را می‌کند. چون AP در ذخیره‌ساز خود این فایل را دارد، بدون درخواست از خدمت‌گزار اصلی، این فایل را به کاربر در مدت زمانی اندک ارسال می‌کند. (ب) کاربر از AP درخواست فایل B را می‌کند. چون AP در ذخیره‌ساز خود این فایل را ندارد، مجبور است از خدمت‌گزار اصلی بخواهد که این فایل را برای او ارسال کند. با دریافت این فایل توسط AP او آن را به کاربر می‌دهد.

۱.۵ مثال انگیزه‌بخش

۲.۵ نوآوری‌ها

۳.۵ مدل سامانه

۴.۵ روش پیشنهادی

۵.۵ شبیه‌سازی و تحلیل عددی

فصل ۶

حریم خصوصی در شبکه‌های WBSN

امروزه شبکه‌های WBSN، نقش بی‌بدیلی در سامانه‌های پویش سلامت[۱] ایفا می‌نماید. حسگرهای پویش علایم حیاتی نصب شده بر بدن بیمار، موجب افزایش در کیفیت خدمات سلامت گشته است. حسگرهایی نظیر EEG[2]، ECG[3]، فشارخون، اندازه‌گیری قندخون و ....، می‌توانند در هر زمان، پارامترهای حیاتی بیماران را به صورت منظم اندازه‌گیری نمایند و آن را برای یک گره جمع‌کننده[۴] ارسال کنند. در این فصل خواهیم گفت که یک مهاجم باهوش می‌تواند تنها با علم به نوع و زمان اندازه‌گیری هر حسگر و بدون اطلاع از محتوای پیام‌های مبادله گشته، پی به اطلاعاتی در مورد بیماری فرد ببرد.

[1] Medical Monitoring System
[2] electroencephalography
[3] electrocardiography
[4] Sink Node

۱.۶ مثال انگیزش‌بخش

فصل ۷

نتیجه‌گیری و کارهای آینده

در این فصل، نخست در بخش ۱.۷، چکیده و نتیجه این رساله به صورت خلاصه ذکر می‌گردد. سپس در ؟؟، ایده‌هایی مطرح می‌گردد که می‌تواند به عنوان ادامه پژوهش بر روی مبحث بیان شده در این رساله، در نظر گرفته شود.

۱.۷ نتیجه‌گیری

پیوست آ

اثبات قضایا و لم‌ها

آ.۱ اثبات ؟؟

برای اثبات این لم، بدترین شرایط را در نظر گرفته و ثابت می‌کنیم که سامانه پایداری خود را در این شرایط نیز از دست نمی دهد. پارامتر آزاد مساله λ_d^{ij} است و با توجه به (؟؟) هر چه مقدار این پارامتر بزرگتر باشد، سامانه به سمت ناپایداری بیشتر سوق پیدا می‌کند. بنابراین بدترین شرایط زمانی که λ_d^{ij} بیشترین مقدار خود را داشته‌باشد، و این حالت زمانی رخ می‌دهد که کاربرد i به کاربرد N ام (کاربرد با بیشترین نرخ) نگاشته شود. به عبارت‌دیگر $\lambda_d^{ij} = \lambda_g^N - \lambda_g^i$. با قراردادن (؟؟) در (؟؟) خواهیم داشت:

$$\frac{\lambda_g^i}{\mu_g^i} + \frac{\lambda_d^{ij}}{\mu_d^{ij}} = \frac{\lambda_g^i}{\mu_g^i} + \frac{\lambda_d^{ij}}{\frac{\mu_g^i}{\mu_g^i - \lambda_g^i}\lambda_d^{ij} + \varepsilon} \overset{\lambda_d^{ij} = \lambda_g^N - \lambda_g^i}{\Longrightarrow} \frac{\lambda_g^i}{\mu_g^i} + \frac{\lambda_g^N - \lambda_g^i}{\frac{\mu_g^i}{\mu_g^i - \lambda_g^i}(\lambda_g^N - \lambda_g^i) + \varepsilon} \tag{آ.۱}$$

بعد از مقداری ساده‌سازی (آ.۱) به صورت زیر در خواهد آمد.

$$\begin{aligned} \frac{\lambda_g^i}{\mu_g^i} + \frac{\lambda_g^N - \lambda_g^i}{\frac{\mu_g^i}{\mu_g^i - \lambda_g^i}(\lambda_g^N - \lambda_g^i) + \varepsilon} &= \frac{\lambda_g^i}{\mu_g^i} + \frac{\mu_g^i - \lambda_g^i}{\mu_g^i + \varepsilon'} \\ &< \frac{\lambda_g^i}{\mu_g^i} + 1 - \frac{\lambda_g^i}{\mu_g^i} = 1. \end{aligned} \tag{آ.۲}$$

مراجع

[1] C. Shannon, "Communication theory of secrecy system," *Bell System Technical Journal*, vol.28, no.4, pp.656–715, 1949.

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

[3] M. Guizani, H. Chen, and C. Wang. *The Future of Wireless Networks: Architectures, Protocols, and Services*. Wireless Networks and Mobile Communications, CRC Press, 2015.

[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.

[5] S. Valenti, D. Rossi, A. Dainotti, A. Pescapè, A. Finamore, and M. Mellia, "Reviewing Traffic Classification," in *Data Traffic Monitoring and Analysis SE - 6* (E. Biersack, C. Callegari, and M. Matijasevic, eds.), vol.7754 of *Lecture Notes in Computer Science*, pp.123–147, Springer Berlin Heidelberg, 2013.

[6] T. Abuhmed, A. Mohaisen, and D. Nyang, "A Survey on Deep Packet Inspection for Intrusion Detection Systems," *Magazine of Korea Telecommunication Society*, vol.24, no.11, pp.25–36, 2008.

[7] A. Finamore, M. Mellia, M. Meo, and D. Rossi, "Kiss: Stochastic packet inspection classifier for udp traffic," *Networking, IEEE/ACM Transactions on*, vol.18, no.5, pp.1505–1515, 2010.

[8] J. Muehlstein, Y. Zion, M. Bahumi, I. Kirshenboim, R. Dubin, A. Dvir, and O. Pele, "Analyzing HTTPS encrypted traffic to identify user operating system, browser and application," *CoRR*, vol.abs/1603.04865, 2016.

[9] M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli, "Traffic classification through simple statistical fingerprinting," *ACM SIGCOMM Computer Communication Review*, vol.37, jan 2007.

[10] M. Conti, J. Willemsen, and B. Crispo, "Providing Source Location Privacy in Wireless Sensor Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol.15, no.3, pp.1238–1280, 2013.

[11] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks - SASN '04*, SASN '04, (New York, New York, USA), pp.88–93, ACM Press, 2004.

[12] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol.36, no.3, pp.1065–1094, 2012.

[13] M. M. B. Salem, S. Hershkop, and S. J. S. Stolfo, "A Survey of Insider Attack Detection Research," in *Advances in Information Security*, pp.pp 69–90, Springer, 2008.

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

[15] S. Borst, V. Gupta, and A. Walid, "Distributed caching algorithms for content distribution networks," in *Proceedings - IEEE INFOCOM*, 2010.

[16] M. A. Maddah-Ali and U. Niesen, "Fundamental Limits of Caching," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp.1077–1081, 2013.

[17] U. Niesen and M. A. Maddah-Ali, "Coded Caching for Delay-Sensitive Content," *arXiv preprint arXiv:1407.4489*, 2014.

[18] A. Sengupta, R. Tandon, and T. Clancy, "Fundamental limits of caching with secure delivery," in *Communications Workshops (ICC), IEEE International Conference on*, pp.771–776, June 2014.

[19] A. Sengupta, R. Tandon, and T. Clancy, "Decentralized caching with secure delivery," in *Information Theory (ISIT), IEEE International Symposium on*, pp.41–45, June 2014.

واژه‌نامه انگلیسی به فارسی

A

Adversary . . . . . مهاجم

Adversary's Best Estimation Error Probability . . . . . احتمال خطای بهترین تخمین مهاجم

Adversary's Error Probability . . . . . احتمال خطای مهاجم

Anonymity . . . . . گمنامی

Application . . . . . کاربرد

Arrival Rate . . . . . نرخ ورودی

Arrival Time . . . . . زمان ورود

C

Cache . . . . . ذخیره‌ساز

Caching System . . . . . سامانه ذخیره‌سازی

Capacity . . . . . ظرفیت

Communication Cost . . . . . هزینه ارتباطی

Content . . . . . محتوا

Context Oriented . . . . . مبتنی بر اطلاعات جانبی

Cost . . . . . هزینه

Coverage . . . . . پوشش

D

Data Oriented . . . . . مبتنی بر داده

Delay . . . . . تاخیر

Delivery . . . . . تحویل

Departure Rate . . . . . نرخ خروجی

Departure Time . . . . . زمان خروج

Dummy Packet . . . . . بسته ساختگی

Dummy Rate . . . . . نرخ ساختگی

E

Encryption . . . . . رمزنگاری

Entropy . . . . . اِنتروپی

Expected Value . . . . . امید ریاضی*

F

Fano's Inequality . . . . . نامساوی Fano

Feature . . . . . ویژگی

Firewall . . . . . دیوار آتش

Freshness . . . . . تازگی

H

Header . . . . . سربسته

I

Information Theory . . . . . نظریه اطلاعات

Integrity . . . . . یکپارچگی

زمان مابین خروج . . . . . InterDeparture Time

L

پیوند . . . . . Link

کران پایین . . . . . Lower Bound

M

بدافزار . . . . . Malware

نگاشت . . . . . Mapping

سامانه پویش سلامت . . . . Medical Monitoring System

چندگامه . . . . . Multi-Hop

کاربرد چندرسانه‌ای . . . . . Multimedia Application

N

سامانه ذخیره‌ساز شبکه‌ای . . Network Caching System

لایه شبکه . . . . . Network Layer

انکارناپذیری . . . . . Non-repudiation

تحلیل عددی . . . . . Numerical Analysis

O

سیستم‌عامل . . . . . Operating System

بهینه . . . . . Optimal

مساله بهینه‌سازی . . . . . Optimization Problem

بسته اصلی . . . . . Original Packet

P

بسته . . . . . Packet

بازرسی بسته . . . . . Packet Inspection

محتوا . . . . . Payload

سیاست‌گذاری . . . . . Policy

شماره درگاه . . . . . Port Number

تابع اولویت . . . . . Priority Function

حریم خصوصی . . . . . Privacy

درجه حریم خصوصی . . . . . Privacy Degree

تابع چگالی احتمال . . . . Probability Density Function

کلید عمومی . . . . . Public Key

R

متغیر تصادفی . . . . . Random Variable

نرخ . . . . . Rate

جایگذاری . . . . . Replacement

مسیریابی . . . . . Routing

S

امنیت . . . . . Security

حسگر . . . . . Sensor

خدمت‌گزار . . . . . Server

نرخ خدمتگزاری . . . . . Service Rate

شبیه‌سازی . . . . . Simulation

گره جمع‌کننده . . . . . Sink Node

گره مبدا . . . . . Source Node

فرایند نقطه‌ای نشان‌دار مانا . . Stationary Marked Point Process

آمار . . . . . Statistical

فرایند نقطه‌ای نشان‌دار مانای همگام . . . . Synchronous Stationary Marked Point Process

سامانه . . . . . System

مدل سامانه . . . . . System Model

T

حریم‌خصوصی زمانی و آماری . Temporal and Statistical Privacy

صف اولویت‌دار زمانی . . Time-DependentPriorityQueue

بده‌بستان . . . . . Trade-Off

طبقه‌بندی ترافیک . . . . . Traffic Classification

لایه انتقال . . . . . Transport Layer

U

کاربر . . . . . User

V

پراش . . . . . Variance

واژه‌نامه فارسی به انگلیسی

ا

آمار . . . . . Statistical

احتمال خطای بهترین تخمین مهاجم . Adversary's Best Estimation Error Probability

احتمال خطای مهاجم . . Adversary's Error Probability

امنیت . . . . . Security

امید ریاضی* . . . . . Expected Value

اِنتروپی . . . . . Entropy

انکارناپذیری . . . . . Non-repudiation

ب

بازرسی بسته . . . . . Packet Inspection

بدافزار . . . . . Malware

بده‌بستان . . . . . Trade-Off

بسته . . . . . Packet

بسته اصلی . . . . . Original Packet

بسته ساختگی . . . . . Dummy Packet

بهینه . . . . . Optimal

پ

پراش . . . . . Variance

پوشش . . . . . Coverage

پیوند . . . . . Link

ت

تابع اولویت . . . . . Priority Function

تابع چگالی احتمال . . . . Probability Density Function

تاخیر . . . . . Delay

تازگی . . . . . Freshness

تحلیل عددی . . . . . Numerical Analysis

تحویل . . . . . Delivery

ج

جایگذاری . . . . . Replacement

چ

چندگامه . . . . . Multi-Hop

ح

حریم خصوصی . . . . . Privacy

حریم‌خصوصی زمانی و آماری . Temporal and Statistical Privacy

حسگر . . . . . Sensor

خ

خدمت‌گزار . . . . . Server

د

درجه حریم خصوصی . . . . . Privacy Degree

دیوار آتش . . . . . Firewall

ذ

ذخیره‌ساز . . . . . Cache

ر

رمزنگاری . . . . . Encryption

ز

زمان خروج . . . . . Departure Time

زمان مابین خروج . . . . . InterDeparture Time

زمان ورود . . . . . Arrival Time

س

سامانه . . . . . System

سامانه پویش سلامت . . . . Medical Monitoring System

سامانه ذخیره‌ساز شبکه‌ای . . Network Caching System

سامانه ذخیره‌سازی . . . . . Caching System

سربسته . . . . . Header

سیاست‌گذاری . . . . . Policy

سیستم‌عامل . . . . . Operating System

ش

شبیه‌سازی . . . . . Simulation

شماره درگاه . . . . . Port Number

ص

صف اولویت‌دار زمانی . . Time-DependentPriorityQueue

ط

طبقه‌بندی ترافیک . . . . . Traffic Classification

ظ

ظرفیت . . . . . Capacity

ف

فرایند نقطه‌ای نشان‌دار مانا . . Stationary Marked Point Process

فرایند نقطه‌ای نشان‌دار مانای همگام . . . . Synchronous Stationary Marked Point Process

ک

کاربر . . . . . User

کاربرد . . . . . Application

کاربرد چندرسانه‌ای . . . . . Multimedia Application

کران پایین . . . . . Lower Bound

کلید عمومی . . . . . Public Key

گ

گره جمع‌کننده . . . . . Sink Node

گره مبدا . . . . . Source Node

گمنامی . . . . . Anonymity

ل

لایه انتقال Transport Layer

لایه شبکه Network Layer

م

مبتنی بر اطلاعات جانبی Context Oriented

مبتنی بر داده Data Oriented

متغیر تصادفی Random Variable

محتوا Payload

مدل سامانه System Model

مساله بهینه‌سازی Optimization Problem

مسیریابی Routing

مهاجم Adversary

ن

نامساوی Fano Fano's Inequality

نرخ Rate

نرخ خدمتگزاری Service Rate

نرخ خروجی Departure Rate

نرخ ساختگی Dummy Rate

نرخ ورودی Arrival Rate

نظریه اطلاعات Information Theory

نگاشت Mapping

و

ویژگی Feature

ه

هزینه Cost

هزینه ارتباطی Communication Cost

ی

یکپارچگی Integrity

نمایه

Abstract

Recent investigations have clarified that not only insensitive data with no encryption methods, but amazingly also encrypted sensitive data may translate into invaluable information by an intelligent adversary. In the latter case, in spite of the protection that data encryption might provide, there are many aspects related to the creation and delivery of messages that remain unprotected by conventional security mechanisms. Complement to the data encryption methods, other techniques are required to protect such contextual information to preserve the privacy of the sources and have been the focus of attention of many research studies during the past few years. The former is known as data-oriented privacy and employs encryption methods to protect data, while the latter is known as context-oriented privacy, which focuses on preservation of the contextual information such as the location and the time when a message is generated i.e., location and temporal privacy, respectively. Inhibiting the adversary of being able to extract information from the traffic rate of source nodes is a complicated task unless taking into consideration the *flow conservation law* effect of the transmitter queue. A reliable method of preserving the privacy that copes with the *flow conservation law*. Augmenting dummy packets, however, bears redundancy and hence requires extra resources in terms of bandwidth and buffer requirements and more importantly suggests higher transmitting energy consumption. Grounded on the queueing and information theories, in this paper we present an efficient method that minimally augments dummy packets to preserve the source rate privacy at a given degree while preserving the delay distribution of the original packets intact, and thus does not affect the QoS parameters of the transmitted data in terms of delay and jitter. Then we extend our proposed approach to preserve privacy of a general feature. We present an approach that mixes the features of applications in the source node such that maximizes the ambiguity of adversary. Finally, we formulate a mathematical model for privacy preserving of a caching system and then present a method so as to cache files in an efficient manner such that maximizes the degree of privacy preservation while maintains the average delivery load at a given level.

University of Tehran

College of Engineering

School of Electrical and Computer Engineering

Analysis of privacy preserving in the communication networks using queuing theory

By:

Abolfazl Diyanat

Supervisor:

Dr. Ahmad Khonsari

A thesis submitted to the Graduate Studies Office in partial fulfillment of the requirements

for the degree of doctor in

Computer Engineering - Software

December 2016