امنیت در شبکه های AD-HOC

نویسندگان :

مهندس حمید یزدانی enj.hamid.yazdani@gmail.com
محسن حسن زاده تخت mohsen31344@yahoo.com
ساسان رجبی جوشقانی rajabi_sasan@yahoo.com

چکیده

شبکه‌های ویژه ، الگوی شبکه‌بندی جدیدی هستند با یک مکان‌شناسی و فقدان زیربنایی از پیش مشخص شده. در نتیجه، شبکه‌های ویژه نسبت به شبکه‌های سنتی در حمله‌ها آسیب پذیر هستند. تابحال راهکارهای به کار رفته برای پشتیبانی کردن از این شبکه‌ها به ثبوت رساندن و کدگذاری بوده است. به هرحال، به نظر می‌رسد در مقابل انداختن بسته مخرب و افکار حمله این خدمات ناکارآمد باشند. این شبکه مشکل انداختن بسته مخرب را در نظر می‌گیرد و راهکاری در جهت رفع آن را ارائه می‌دهد. در حقیقت یک مدل مطمئن بر مبنای مفهوم محاسباتی بوجود می‌یابد. این راهکار دو شیوه را ارائه می دهد :

بررسی رفتار گره‌های مجاور در شبکه و محاسبه مقادیر محاسباتی آنها بر پایه اطلاعات ارائه شده و همچنین به طور مفصل چگونگی مدیریت اطلاعات محاسباتی در شبکه را مورد بحث قرار می‌دهد راهکار پیشنهاد شده با مقداری کار شبیه سازی معتبر می‌شود. سیستم های مبتنی بر محاسبات نمونه جدیدی از بالا بردن ایمنی در شبکه های تک موردی هستند. این راه کارها می توانند بخصوص در مواجه شدن با نا مرتبی بین گره ها بکار رود. بسته پیشرو ایمنی در شبکه های تک موردی (SAFE) مثالی از این مقوله است. هنگامیکه این سیستم ها بکار می روند، هر گره در

شبکه نشر بسته در گره های همسایه را بررسی می کند و به آنها برخی مقادیر محاسبه شده طبـق آن تخصیص می دهد. در حقیقت، رهیافت های مختلفی برای بـازبینی (نظـارت) وجـود دارد و هـر رهیافتی دارای اثر خود روی عملکرد سیستم مبتنی بر محاسبات دارد. بر مبنای برخی نتایج ، شبیه سازی اثر دو روش نظارت روی عملکرد راه کار SAFE را مقایسه می کند.

فصل اول

ایمن کردن ارسال بسته در شبکه‌های ویژه

۱–۱شبکه‌های ویژه الگوی شبکه‌بندی

شبکه‌های ویژه الگوی شبکه‌بندی جدیدی را در حالیکه ارتباط‌ها بین دستگاه‌های بـدون پشـتیبانی یک زیربنای مرکزیت یافته برقرار می‌شوند را ارائه می‌دهد. این الگوی جدید یک مکمل جالب (اگـر نه یک گزینه) برای شبکه‌های سنتی است. بخصوص که دستگاه‌ها می‌توانند به آسانی افزوده شده یا برداشته شوند و شبکه زیرکانه خود را بعد از هر پیکربندی می‌کند متأسفانه نبودن زیربنـا و قابلیـت دسترسی باز شبکه‌های ویژه آنها را در مقابله با شبکه‌های سـیم دار (سـیم کشـی شـده) در مقابـل حمله‌ها آسیب پذیرتر می‌کند. معمولاً ایمنی در شبکه‌های ویژه از طریق کدگذاری و بدست می‌آید. این روش‌ها می‌توانند به عنوان خط اول در نظر گرفته شوند چون آنها نمی‌توانند از گره مخـرب کـه قبلاً برای افکار برخی حمله‌های سازمان یافته به شبکه ملحق شده‌اند بگیرند، این شکل بـه توسـعه سیستم‌های محاسباتی منجر شده تا گره‌های مخرب را کشف و آنها را از شبکه به دور اندازد.

در این کار، ما با دو نوع سوء استفاده (سوءرفتار) سروکار خواهیم داشـت: انـداختن بسـته مخـرب و ترویج اتمام کاذب، در شبکه‌های ویژه، هر گره فرض می‌شود برای دیگر مسـیر باشـد، بهرحـال ایـن گره‌ها معمولاً دارای توانایی‌های محدودی هستند که توسط برخی از آنها بعنوان توجیه بـرای رفتـار خودپسندانه در نظر گرفته می‌شوند. در حقیقت، گره‌های خودپسند به سایر گره‌ها در شبکه برای به جلو فرستادن بسته‌های آنها متکی هستند. بهرحال آنها می‌توانند مقدار معینی از بسته‌های دریافـت شده را بفرستند تا بتوانند منابع خود را حفظ کنند. انداختن بسته مخـرب ممکـن اسـت همچنـین برای قطع کردن عملکرد شبکه و تنزل عملکرد آنها انجام شود. برخی از گره‌های مخرب دیگر ممکن است بسته‌ها را نیاندازند، بهرحال آنها اتهام کاذب برای منزوی کردن برخی از گره‌های دیگر خواهند فرستاد تا عملکرد شبکه را مختل کنند.

ما یک سیستم محاسباتی که گره‌های سوءاستفاده کننده را کشف مـی‌کنـد و آنهـا را از شـبکه دور می‌اندازد را توسعه می‌دهیم. راهکار ما ایجاد اطمینان بین گره‌ها در شبکه با همگون سازی همکاری

بین آنها و دلسرد کردن مخرب‌ها از انجام دادن حمله‌ها و دغلکاری است. در طرح مـا، هـر گـره در شبکه رفتار همسایگی خود را دیده‌بانی می‌کند و اگر سوءرفتاری کشف شود دیگر گره‌های همسـایه آگاه می‌شوند تا در پشتیبانی به آنها کمک شود.

استفاده از راهکارهای محاسباتی برای ایمنی ارسال بسته توسط بسیاری پیشنهاد شد برای مثال، در [۱]، [۲]، رفتارهای خودپسندانه و ناموفق مطالعه می‌شوند و محاسبات اینجا به سادگی محـدود بـه این است که مسیریاب‌های خوبی گره‌ها هستند. برای دقیق تر بودن، یک گره خوب به گره‌ای ارجاع می‌شود که بسته‌ها را گره بعدی در مسیری که علاقه‌ای به ایـن فعـل و انفعـال نـدارد مـی‌فرسـتد. برمبنای تعداد فعل و انفعالات موفقیت آمیز فرستادن، مقدار محاسبات تعیین می‌شود.

دو سیستم محاسباتی که به همین طریق کار می‌کنند برای کمک بـه حمایـت فرسـتادن بسـته در شبکه‌های ویژه پیشنهاد شده‌اند: راهکار محاسباتی همکاری کننده (هسـته) [۳]، و بـی کاسـتی در پروتوکل شبکه‌های ویژه پویا [۴].

طرح هسته از مقادیر محاسباتی کلی که حد آنها از مقدار ۱+ از طریق مقدار ۰ به مقدار ۱- استفاده می‌کند. این راهکار توجه بیشتری به مشاهدات گذشته که ممکن اسـت رفتارهـای بـد ناپیوسـته را تحمل کند نشان میدهد. در این مورد، یک گره مخرب می‌تواند محاسبات خوبی انجام دهد، یک گره عاملی کُندی می‌شود و سپس شروع به رفتار مخربانه می‌کنـد کـه در ایـن مـورد اثـر عمیقـی روی عملکرد شبکه باقی می‌گذارد.

راه کار شبکه های ویژه پویا پروتوکل‌های مسیریابی واکنشی را گسترش می‌دهـد و فقـط از مقـادیر منفی برای محاسبات استفاده می‌کند. طرح شبکه های ویژه پویا از پیامـدهـای هشـدار بـرای آگـاه کردن سایر گره‌ها در شبکه درباره یک سوءرفتار در شبکه استفاده می‌کند. این اطلاعات به فهرسـت دوستان فرستاده می‌شود این محدود کننده و پیچیده است چون درست بودن یک گره بایـد معـین شود و اطلاعات متناظر باید حفظ شود.

شبکه‌های ویژه پویا به گره‌های مخرب اجازه می‌دهد که از طریق وقفه هنگامیکـه تمامیـت آنهـا در فهرست سیاه منقضی می‌شود و حذف می‌شوند بازیابی داشته باشد. این روش مجاز دانستن بازیافت گره‌ها آسیب پذیری جدیدی ارائه می‌کند که قادر کردن گره‌های مخرب به ملحق شدن دوبـاره بـه شبکه است و تکرار حمله‌هایشان.

در مورد SAFE، این همچنین پروتوکل‌های مسیریابی واکنشی را گسترش می‌دهد. این راهکـار از مقادیر محاسباتی مثبت متغیر بین ۰ و ۱ استفاده می‌کند. ایـن اجـازه مـی‌دهـد بـه طریقـی سـاده نسبت‌های بسته‌های فرستاده شده توسط هر گره در شبکه توضیح داده شود. برخلاف هسته، راهکار SAFE روی جدیدترین مشاهدات بیشتر حساب مـی‌کنـد، امـا بـدون نادیـده انگاشـتن مشـاهدات گذشته. این روش حساب کردن محاسباتی روش مناسبتر و یکپارچه‌تری در طبقه‌بندی سایر گره‌هـا عرضه می‌کند. SAFE همچنین اجازه مبادله اطلاعـات بـدرفتاری بـین گـره‌هـای همسـایه بـدون محدودیت را می‌دهد که راهکار قوی‌تری برای حفاظت از کـل شـبکه تـأمین مـی‌کنـد. راهکـار مـا همچنین مستعد بازیافت گره‌ها است. بهرحال، هنگامیکه گره‌های بازیافـت شـده دوبـاره بـه شـبکه ملحق می‌شوند، به آنها مقادیر محاسباتی بحرانی تخصیص داده می‌شود که آنها را وادار می‌کنـد بـه درستی رفتار کنند، در غیر اینصورت آنها دوباره از شبکه دور انداخته می‌شوند.

۱–۲ طرح SAFE

برقراری اطمینان در شبکه‌های ویژه احتیاج دارد که مداخله‌ها کشف شـوند و از شـبکه دورانداختـه شوند. بهرحال، اگر ما فقط به کشف خودبخود سوءرفتارها متکی باشیم، این می‌توانـد کـافی نباشـد چون یک گره که در حال حاضر هیچ نیرنگی را کشف نمی‌کند، نمی‌توان مطمئن شـد کـه کلیـه‌ی همسایگی در یک قدمی قابل اطمینان هستند، در واقـع، یـک گـره واقعـاً بسـته‌هـایی نمـی‌فرسـتد نمی‌تواند گره‌های خودآگاه در همسایگی خود را کشـف کنـد. در نتیجـه، همکـاری بـین گـره‌هـای همسایه اجباری است تا راهکاری کلی برای حفاظت کلیه‌ی شبکه عرضه کنـد. بـرای بدسـت آوردن

این، هر گره در شبکه فرستادن شبکه در همسایگی خود را دیده‌بانی می‌کند و به محض کشف یک سوءرفتار از یکی از آنها، این اطلاعات را به سایرین پخش می‌کند. مقادیر محاسباتی که هر گره محاسبه می‌کند بر مبنای نتایج دیده‌بانی به عهده گرفته شده است و مقدار اطمینانی را که این گره روی آنهایی که برای فرستاده گره‌ها به آنها متکی است را نشان خواهد داد. همچنین ۵ همسایگی یک گره آ به گره‌هایی ارجاع می‌شود که فقط در یک قدمی گره آ هستند. این به سادگی به معنی این است که اتهامات فقط به اندازه‌ی یک قدم دورتر فرستاده می‌شوند و اطلاعات محاسباتی جمع آوری شده از گره‌ها که فقط به اندازه یک قدم از درخواست کننده گره دور هستند.

ایجاد اطمینان بین گره‌ها در یک شبکه ویژه احتیاج دارد که گره‌ها صاحب مشخصات معتبر طی دوره معقولی از زمان باشند. هر قدر این مشخصات در مقابل سراسیمگی مقاوم باشند سیستم محاسباتی قوی‌تر خواهد بود. راهکار ما به سادگی از آدرس‌های آی ـ پی برای مشخص کردن گره‌ها استفاده می‌کند و می‌تواند همراه با هر مکانیسم دیگری بکار رود، برای مثال پروتوکل مسیریابی امن برای سروکار داشتن با سراسیمگی آی ـ پی.

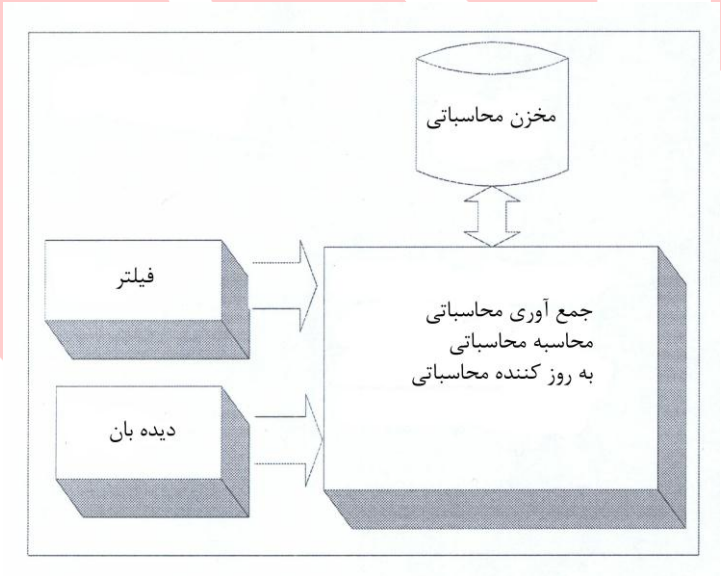
در شبکه‌های ویژه انداختن بسته، دارای دلیل‌های متنوع پشت سر آن است. یک گره ممکن است بسته را بخاطر حفظ منابع خودش بیاندازد یا افکار حمله سازمان یافته را انجام دهد. بهرحال، ممکن است یک گره بسته‌ها را به خاطر اینکه منابع کافی برای حفظ کردن ندارد می‌اندازد. SAFE انداختن بسته‌های اضافی را بعنوان یک سوءرفتار علی رغم منظور پشت سر آن در نظ ر می‌گیرد. یک گره مخرب به معنی این است که به این گره مقدار محاسباتی کمتر از یک مدخل مشخص شده تخصیص داده شده. این مقادیر محاسباتی شدیداً به تعداد بسته‌های افتاده شده‌ای یک گره محدود هستند. بدین ترتیب، هنگامیکه یک مدخل رسید، انداختن بسته یک تهدید جدی می‌شود و گره مسئول این انداختن باید پرهیز شود.

SAFE همچنین از همکاری زیرکانه بین گره‌ها در یک شبکه طرفداری می‌کند. روش‌های مناسب برای اجرای چنین همکاری الگوریتم‌های همه‌گیر مقرر می‌کند. [۶]، بدین ترتیب هنگامیکه گره‌ها

در ارتباط مستقیم هستند، شبیه انتقال یک بیماری واگیردار بین افراد اطلاعات پخش می‌کننـد. در حقیقت، هنگامیکه یک سوءرفتار در ر ابطه با یک گره آ کشف می‌شود، این اطلاعـات بـه گـره‌هـای همسایه پخش می‌شود، که آنرا برای دوره‌ای از زمان نگه می‌دارد. اگر این گره‌ها بـه شـبکه دیگـری رفت و این اطلاعات سوءرفتار به دلایلی از قبیل الحاق اخیراً گره آ به این شـبکه جدیـد لازم اسـت، این اطلاعات می‌تواند برای کمک در کشف کردن و دورانداختن گره آ بکار رود. روشی که مخزن‌های محاسـباتی در SAFE سـاخته شـده‌انـد، همچنـین بـر مبنـای برخـی روش‌هـای بکـار رفتـه در الگوریتم‌های هم گیر [۶] هستند، که باعث می‌شود آنها برای شبکه‌های بسیار پویا مناسب تر باشند.

۱-۲-۱ بلوک‌های سازنده

SAFE از طریق یک تمامیت، به اسم عامل SAFE اعتبار ایجاد می‌کند، که روی هر گره در شبکه ویژه عمل می‌کند. هر گره مسئول کشف سوءرفتارهای کلی بصورت مستقل است. بهرحال، همکاری بین کلیه‌ی گره‌ها برای امن کردن تمام شبکه لازم است. معماری عامل SAFE در شـکل ۱ نشـان داده شده است و شامل کارکرد پذیری‌های ذیل است.



شکل ۱-۱ معماری مدیریت اداره کردن اعتبار

دیده‌بان: دیده‌بان مسئول مشاهده صدور بسته همسایگی گره‌ها است. برای مثال، اگر گـره آ رفتـار گره بی را دیده‌بانی می‌کند، گره آ نسبتی از تعداد بسته‌هایی که گـره بـی فرسـتاده اسـت و تعـداد بسته‌هایی که گره آ به گره بی فرستاده که آنها را دورتر بفرستد نگه می‌دارد. نتایج دیده‌بانی مرتباً به مدیر محاسباتی فرستاده می‌شود، که مقدار محاسباتی گره دیـده‌بـانی شـونده را بـه روز کنـد و در مخزن محاسباتی ذخیره می‌کند.

فیلتر: راهکار SAFE یک سرساز محاسباتی به پروتوکل مسیریابی اصلی به منظور تسـهیل کـردن مبادله اطلاعات محاسباتی بین عوامل مختلف SAFE اضافه می‌کند. این فیلتر می‌تواند بـه عنـوان یک مدول مکمل که در تشخیص دادن بسته‌های حاوی برخی اطلاعات محاسباتی از بقیه بسـته‌هـا دریافت شده کمک می‌کند در نظر گرفته شود. در حقیقت، هنگامی که یک بسته توسط یـک گـره دریافت می‌شود، ابتدا آن را از فیلتر عبور می‌دهد که بررسی کند که آیا در سرساز محاسباتی شامل است. اگر اینطور است، این بسته به مدیر محاسباتی فرستاده می‌شود. در غیراینصورت، به عنوان یک بسته معمولی پردازش می‌شود.

مدیر محاسباتی: مدیر محاسباتی مؤلفه اصلی عامل SAFE است این مدول به طور کلی مسـئول اداره کردن اطلاعات محاسباتی است. برای دقیقتـر بـودن، مـدیر محاسـباتی، اطلاعـات محاسـباتی مرتبط با همسایگی را جمع آوری، محاسبه و حفاظت می‌کند. مدیر محاسباتی ورودی را یا از فیلتـر می‌گیرد. مورد ارسال منعکس می‌کند که یک گره بخصـوص ارسـال کننـده بسـته دارد دیـده‌بـانی می‌شود. بنابراین، برای به روز کردن اطلاعات محاسباتی متناظر باید با مدیر محاسباتی ارتباط برقرار شود. بهرحال، در رابطه با یک گره مخرب رمـتهم ورودی دریافـت شـده از فیلتـر بـه چنـد مبادلـه اطلاعات محاسباتی بین چند گره همسایه مرتبط است. مـدیر محاسـباتی بـا اسـتفاده از معیارهـای متری توضیح داده شده **است**.

مخزن محاسباتی: SAFE فرض می‌کند هر گره در شبکه یک مخزن محاسباتی همسایگی طبق معیارهای متری توضیح داده شده در بخش III-B ذخیره می‌شوند. این مخازن پر از مقادیر محاسبه شده از طریق یک دیده‌بانی مستقیم یا از طریق اتمام فرستاده توسط چند گره در شبکه محاسبه می‌شوند. برای عینیت بیشتر، SAFE اطلاعات محاسباتی را به شکل (مقدار کلیدی) جفت‌ها ذخیره می‌کند. زمینه‌ی کلیدی به آدرس IP گره که محاسبات برای آن انجام می‌گیرند دلالت می‌کند. بهرحال، مقدار زمینه به بردار شامل REP-VAL دلالت می‌کند که مقدار محاسباتی گره دیده‌بانی شونده است و تی ـ تی ـ ال که مقدار زمان دوام آوردن است. تی ـ تی ـ ال دوره‌ی زمانی را که ورودی بهتر است را نشان می‌دهد و هنگامی که به سر رسید، سرعت از مخزن محاسباتی برداشته می‌شود. تی ـ تی ـ ال برای دو هدف بکار گرفته می‌شود:

- اندازه مخزن را محدود می‌کند بخصوص برخی گره‌ها ممکن است بخواهد شبکه را ترک کنند و دوباره به مدت طولانی ملحق نشوند، بنابراین بی‌فایده است که تمامی آنها را در مخزن‌های محاسباتی نگه داشت اگر آنها به کار نمی‌روند.
- گره‌هایی که از شبکه دور انداخته می‌شوند، گره‌های اضافی بسته‌های انداخته شده هستند. به هر دلیلی که پشت سر آن است می‌تواند بازیافته و دوباره به شبکه ملحق شود. گره‌هایی که به خاطر مشکلات فیزیکی نتوانند بسته‌ها را به جلو بفرستند، دوباره به شبکه ملحق خواهند شد و در عمل فرستادن بسته به طور فعال شرکت خواهند کرد. گره‌های مخرب هم می‌توانند بعد از دور انداخته شدن به شبکه ملحق شوند. بهرحال، هر گره که به شبکه ملحق می‌شود به آن یک مقدار محاسباتی تخصیص داده می‌شود که نزدیک به مدخل از بیش مشخص شده است این گره‌های مخرب را وادار می‌کند که به درستی رفتار کنند، در غیراینصورت محاسبات آنها پائین خواهد رفت و به مدخل ذکر شده خواهد رسید و بدین ترتیب دوباره از شبکه دور انداخته می‌شوند.

۱–۳ توصیف پروتوکل

هر چند طرح SAFE برخی خصوصیات جدید ارائه می‌دهد که می‌توانند به راحتی با پروتوکل مسیریابی اصلی تلفیق شوند، این طرح هنوز کم اهمیت است و می‌تواند بیشتر با یک پروتوکل از قبیل پروتوکل مسیریابی امن برای سروکار داشتن با بازیافت مسیر امن یکپارچه شود. در این مورد، شبکه امن‌تر است چون قادر است مجموعه گسترده‌تری از حمله‌ها را کشف کند.

A. مبادله اطلاعات محاسباتی

SAFE روش جدیدی برای مبادله اطلاعات محاسباتی بین گره‌ها و همسایه در شبکه عرضه کند. این مبادله از طریق سرساز در شکل زیر نمایش داده شده است.

فرم محاسباتی	مشخصات اتهام	مقدار محاسباتی

مبادله اطلاعات محاسباتی در دو وضعیت انجام می‌گیرد: ابتدا، هنگامیکه یک گره سوءرفتاری از یک گره دیگر از طریق دیده‌بانی مستقیم کشف می‌کند در این مورد، گره کشف کننده فریبکار مجبور است این اطلاعات را به همسایه خود برای کمک به آنها در حفاظت از خود بفرستد. وضعیت دوم هنگامیکه یک گره آ اتهامی درباره گره بی از گره دیگر در همسایگی دریافت می‌کند انجام می‌گیرد. گره آ مقدار محاسباتی را مستقیماً با اطلاعات دریافتی از متهم کننده به روز نمی‌کند، بهرحال، گره دیگر در همسایگی را برای عقیده شان در مورد گره متهم شده استعلام می‌کند. بر مبنای این اطلاعات دریافت شده، مقدار محاسباتی گره مشکوک به روز خواهد شد. خصوصیات ذکر شده توسط گره آ به افزوده شدن یک سرساز شامل زمینه‌های نشان داده شده در شکل بالا احتیاج دارد بیتی ساز گره آ در سرساز پروتوکل اصلی بعنوان یک آی ـ پی اضافی یا بعنوان سرساز جداگانه اضافه شده بعد از سرساز آی ـ پی و قبل از پروتوکل لایه بالاتر تلفیق می‌شود. سرساز SAFE شامل سه مقدار است: نوع محاسبات، آدرس آی ـ پی گره که محاسبات آن گزارش می‌شود و مقدار محاسباتی خود. در زیر، شرحی از این مقادیر متفاوت ارایه می‌شود:

- **نوع محاسبات:** پیام‌های مختلف SAFE به کمک نوع محاسبات (REP-TYPE) تشخیص داده مس شود. آخرین پیام یکی از مقادیر ذیل را دارد:
  - REP-TYPE (اتهام محاسباتی): این مقدار هنگامی بکار می‌رود که یک گره سوءرفتاری کشف می‌کند و مایل است این اطلاعات را با همسایگی خود سهیم باشد.
  - REP-REQUEST: این مقدار هنگامی به کار می‌رود که یک گره اتهامی در مـورد گـره دیگر دریافت می‌کند و مایل است همسایگی خود را درباره عقایدشان استعلام کند.
  - REP-RESPONSE(پاسخ محاسـباتی): هنگـامی کـه یـک گـره پیـامی از SAFE بـا درخواست عقیده درباره یک گره مشخص دریافت می‌کند، مقدار REP-RESPONSE برای جواب به این نوع درخواست به کار می‌رود.
- ACCUSED-ID (مشخصات – اتهام) : این زمینه شامل آدرس آی ـ پی گره متهم است.
- REP-VALUE (مقدار محاسباتی): این زمینه شامل مقدار محاسباتی گره متهم است.

B. ارزیابی محاسباتی

مقادیر محاسباتی به کار رفته در این کار، تعریف شده‌اند که اعداد واقعی بین ۰ تا ۱ باشند. در ادامه، ما بین مقدار محاسباتی نشان داده شده با r_{direct}، و که پیامد دیده‌بانی کردن بسته فرستاده اسـت و مقدار محاسباتی باقیمانده که مجموعه r_{direct} و مقدار محاسباتی قبلاً موجود در مخـزن محاسـباتی (نشان داده شده با r_{reptab}) گره‌ای که درجه‌بندی را انجام می‌دهد تفـاوت قائـل مـی‌شـویم. مقـادیر محاسباتی مستقیم به طور کلی به تعداد بسته‌های فرستاده شده طی یک فعـل و انفعـالات مـرتبط هستند. برای مثال، اگر طی زمان مفروضی، یگ گره ۱۰ بسته دریافت می‌کرده است، فقط ۷ بسـته را می‌فرستد، به این گره مقدار محاسباتی 0.7 تخصیص داده می‌شود.

محاسبات یک گره طبق رفتار آن تغییر می‌کند، ممکن است افزایش یابد یا کاهش یابد که به تعداد بسته‌های فرستاده شده بستگی دارد.

۱–۴ مقدار محاسباتی اصلی

اگر دو گره درمحدوده انتقال یکدیگر هستند درست بعد از فاز بازیافت، هر یک از آنها یک ورودی در مخزن محاسباتی خود برای دیگری بوجود می‌آورد و بـه آن مقـدار λ_{init} تخصـیص مـی‌دهـد. ایـن مقداریکی بیشتر از مقدار مدخل λ_{thre} است. آخری سادگی تصریح می‌کند که اگر یـک گـره دارای محاسباتی کمتر از این مقدار است، اعلام می‌شود که این گره مخرب است. برای تمرکز بیشـتر اگـر مقدار مدخل ۰.۸ است مقدار محاسباتی اولیه برای مثال ۰.۸۲ خواهد بود.

محاسبه کردن محاسبات با استفاده از دیده‌بانی مستقیم

دیده‌بانی فرستادن بسته‌های یک گره طبق تعداد بسته‌هایی کـه ایـن گـره فرسـتاده اسـت بدسـت می‌آید. به گفته دیگر، اگر گره آ به گره بی متکی است تا بسته‌های خود را بفرستد، گره آ با استفاده از معیار متری ذیل محاسبات گره بی را محاسبه می‌کند.

(۱)

$$r_{direct}(A,B) = \frac{\#forwarded}{\#sent}$$

مقدار محاسباتی منتج از فرمول (۱) با مقدار محاسباتی قبلاً موجود در مخزن A در رابطه با گره B تر کیب می‌شود. این می‌تواند از طریق فرمول زیر بدست آید:

(۲)

$$r(A,B) = (1-\alpha).r_{reptab}(A,B) + \alpha.r_{direct}(A,B)$$

α تعدادی در حدود ۰ و ۱ است. این فرمول از مجموعه شامل دو بخش بوجود مـی‌آیـد بخـش اول مقدار محاسباتی گره بی قبلاً مورد احتیاج مخزن محاسباتی گره آ را توصیف می‌کند. اگر گره آ قبلاً با گره بی مواجه نشده، مقدار محاسباتی به مقدار $r_{reptab}(A,B)$ قرار می‌شود همانطور که قبلاً ذکـر شد. منعکس می‌کند که برخی در رابطه با محاسبات گره بی انجام گرفت و مقدار محاسباتی متناظر

لازم است به روز شوند. بنابراین گره A مقدار مقدار محاسباتی گره بی را محاسبه می‌کند و آنـرا بـه مقدار قبلی اضافه می‌کند. ($r_{reptab}(A,B)$) بطریقی که در فرمول (۲) توصیف شده قبـل از ذخیـره کردن مجموع درمخزن محاسباتی. با بحساب آوردن پیشینه محاسباتی یـک گـره، ارزیـابی متـداوم خواهد بود. در واقع، یک مسیریاب خوب که بمدت کوتاهی با شکل فیزیکی مواجه می‌شـود، تنبیـه نخواهد شد و دور انداخته نخواهد شد چون محاسبات آن افزایش خواهد یافت اگر دوباره به آن برای فرستادن بسته‌های داده‌ها متکی باشیم و از طرف دیگر، محاسبات یک گره یکپارچه تغییر کند. اگر محاسبات، برای مثال، به طور موجی حرکت کند، اغلب یک مسیر راهیابی جدید مطالعه می‌شـود و نیروی گره به سرعت مصرف می‌شود. علیـرغم مسـاعدت محاسـبات پیشـینه‌ای، جدیـدترین مقـدار محاسباتی همواره بیشتر در نظر گرفته می‌شود.

۱–۴–۱محاسبه‌ی محاسباتی با استفاده از اتهامات

در این متن، به اتهام‌ها به اطلاعات محاسباتی که یک گره در شبکه در رابطه با گره دیگـر فرسـتاده دلالت می‌کند. این اتهام‌ها ممکن است درست باشد اگر فرستنده واقعاً سوءرفتاری کشف کرده بود و مایل بود این اطلاعات را با همسایگی خود سهیم شود. بهرحال، فرستادن اتهامات نادرست، می‌تواند برای قطع کردن عملکرد شبکه بکار رود یک گره مخرب به جـای انـداختن بسـته‌هـا ممکـن اسـت اتهامات کاذب بفرستد تا برخی گره‌ها را از شبکه دور اندازد و متعاقباً عملکرد آن را کاهش دهد.

برای جلوگیری از اینکه یک مخرب اتهام‌های کاذب آورد، راهکارهای SAFE معیارهای ذیل را ارائه میدهد:

اتهام‌ها از گره مخرب در نظر گرفته می‌شوند. این به معنی این است که یـک اتهـام فرسـتاده شـده توسط یک گره که دارای مقدار محاسباتی کمتر از مدخل است نادید ه گرفته بشود.

اگر گره آ در رابطه به گره بی اتهامی دریافت کند. گره آ ابتـدا همسـایه‌هـای او را بـرای عقایدشـان درباره گره متهم شده استعلام می‌کند. اگر گره‌های استعلام شده دارای هر اطلاعاتی در رابطه با گره متهم هستند، آنها را به گره آ خواهند فرستاد. اینجا هم یک عدد اتهام مدخل θ_{accu} ارائه مـی‌شـود. این معنی این است که اگر تعداد اتهام‌های دریافت‌های توسط گره آ کمتـر از مقـدار مـدخل θ_{accu} است، اتهام بر علیه گره بی نادیده گرفته خواهد شد، در غیراین صورت محاسـبات گـره بـی بـه روز می‌شود. برای دقیق تر بودن، اجازه دهید فرض کنیم که ($p>\theta_{accu}$) اتهام‌ها در رابطـه بـا گـره بـی دریافت شده توسط گره آ از گره‌های $N_1, \ldots, N_p$. در این مورد، مقدار محاسباتی گره بی به صورت ذیل به روز خواهد شد:

(۳)

$$r(A,B) = \tau . r_{reptab}(A,B) + (1-\tau) . \frac{\sum_{i=1}^{p} r_{reptab}(A,N_i) . r_{reptab}(N_i,B)}{\sum_{i=1}^{p} r_{reptab}(A,N_i)}$$

اجازه دهید توجه کنیم که گره با پاسخ‌های دریافت شده بـر مبنـای اطمینـان خـود بـه گـره‌هـای فرستنده رفتار می‌کند. این گره‌های واقع در شبکه را وادار می‌کند بدرستی رفتار کننـد، چـون ایـن گره قابل اطمینان تر است، پاسخ آن معتبرتر است. محاسبات تاریخی دوباره در اینجا از طریق مقدار $r_{reptab}(A,B)$ در نظر گرفته می‌شود. بهرحال اثر τ برای مؤثرتر کردن محاسبات انجام شده در حال حاضر اثر τ به اندازه کافی کوچک در نظر گرفته خواهد شد.

۱–۵ شبیه سازی

شبیه ساز ۲ –ns شبکه [۹] رای همگون کردن معماری عامل SAFE توصیف شده در بخش II-B بکار رفت. شبیه ساز ns-2 شبکه یک همگون ساز شبکه سازگار با هدف و ناشی از پیامـد مجـزا است، که در سال‌های اخیر ابزاری نیرومند، پروتوکل‌ها و مول‌هایی از زمینه شبکه‌های ویـژه بوجـود آورده است. با در نظر گرفتن شبیه ساز ns-2 ماننـد معمـاری تعـدیلی عامـل SAFE محـدودیت ندارد، استفاده از هر شبیه ساز شبکه دیگری را مجاز می‌کند.

هر میزبان متحرک دارای یک آنتن همه سویه با بازده یکسان است. هم کنشگر بی سیم ماننـد یـک رسانه رادیویی مشترک بانسبت بیت 2Mb/s و حد رادیویی صدی ۲۵۰mm مدل بندی شده است [۱۰]. هر گره فرض شده که دارای یک بیانگر (بافر) از بسته‌هـای انـدازه ۶۴ باشـد. مطالعـه شـبیه سازی با در نظر گرفتن پارامتر زمان مکث (وقفه) کـه تحـرک عامـل در شـبکه‌هـای ویـژه را نشـان می‌دهد انجام شد. برای مثال، هنگامیکه زمان مکث افزایش می‌یابد گره‌ها تمایل بیشتری دارند کـه بدون حرکت باقی بمانند. در غیر این صورت، گره‌ها مـداوماً بـا زمـان‌هـای مکـث کوتـاه در حرکـت هستند (یعنی حرکت کمی هنگامیکه زمان مکث ۰ است) مدل مدخل ورودی تصادفی [۱۱] بعنوان مدل متحرک در زمینه مستطیلی انتخاب می‌شود (متر ۳۰۰×۶۰۰). زمینه حرکت فایل‌ها بـا زمـان مکث پارامتر مشخص می‌شوند p از صفر تا۲۰، ۳۰، ۵۰، ۱۰۰، ۲۰۰، ۳۰۰، ۴۰۰ تا ۵۰۰ ثانیه تغییر می‌کند. حرکت گره‌ها به طور یکنواخت بین صفر و حداکثر مقدار $10\ m.s^{-1}$ توزیع می‌شود.

برای ارزیابی راهکار SAFE، در کل **۱۵** گره در زمینه‌ای مستطیلی به کار گرفته می‌شوند، جائیکه منبع و مقصد در طرف‌های مخالف قرار دارند و یک گره مخرب در وسط اتصال است. بقیه گره‌ها به طور تصادفی دراین زمینه حرکت می‌کنند. گره منبع بسته‌ها را با نسبت فرستادن 4 pkts/s فرستاده می‌شوند و اندازه بسته ۶۴ بیتی.

مسیریابی منبع پوویا [۱۲] بعنوان پروتکل اصلی به کار می‌رود که بخاطر کارایی و کامل بودن آن است و شبیه‌سازی‌ها طی ۹۰۰ ثانیه با بحساب آوردن زمان‌های مکث بالا رانده می‌شوند.

گره مخرب با استفاده از ماشین زنجیره مارکوف دو مرحله‌ای ایجاد می‌شود. در یک مرحله خوب، گره‌های بالا بدون انداختن هیچ بسته رسیده‌ای رفتار می‌کنند. بهرحال، در مرحله بد، گره‌های مخرب انداختن بسته‌ها بر مبنای تابع انداختن بسته است. آخری به عنوان یک عدد اتفاقی بین یک حداکثر (نسبت ـ حداکثر) و یک حداقل نسبت‌های انداختن تعریف می‌شود. ماشین زنجیره مارکوف بین دو حالت طی یک دوره زمانی (r_{trans}) که می‌تواند ثابت یا اتفاقی باشد نوسان می‌کند.

در این کار شبیه‌سازی نسبت تحویل بسته، سرجمع ارزیابی تأخیر سراسری و کامل را ارزیابی می‌کنیم (برای جزئیات بیشتر به [۱۰]، [۱۱] نگاه کنید.) نسبت به تحویل بسته کسری از بسته‌های داده‌های تحویل داده شده به مقصد را ارائه می‌دهد. از طرف دیگر، تعداد کل مسیریابی بسته‌های فرستاده شده بعنوان یک اتصال به حساب می‌آید. حداکثر ظرفیت به عملکرد اندازه‌گیری شده واقعی یک سیستم هنگامیکه تأخیر در نظر گرفته می‌شود دلالت می‌کند. در نتایج شبیه‌سازی، معیارهای اندازه‌گیری حداکثر توانایی به مقدار میانگین هر گره مرتبط است. سرانجام، میانگین تأخیر، میانگین باقیمانده یک طرفه مشاهده شده بین یک بسته فرستاده شده و دریافت شده را نشان می‌دهد. مهم است ذکر کرد که برای هر پیکربندی، اندازه‌گیری‌هایی گزارش شده، میانگینی حداقل ۲۰ رانش با سرعت‌های اتفاقی مختلف هستند.

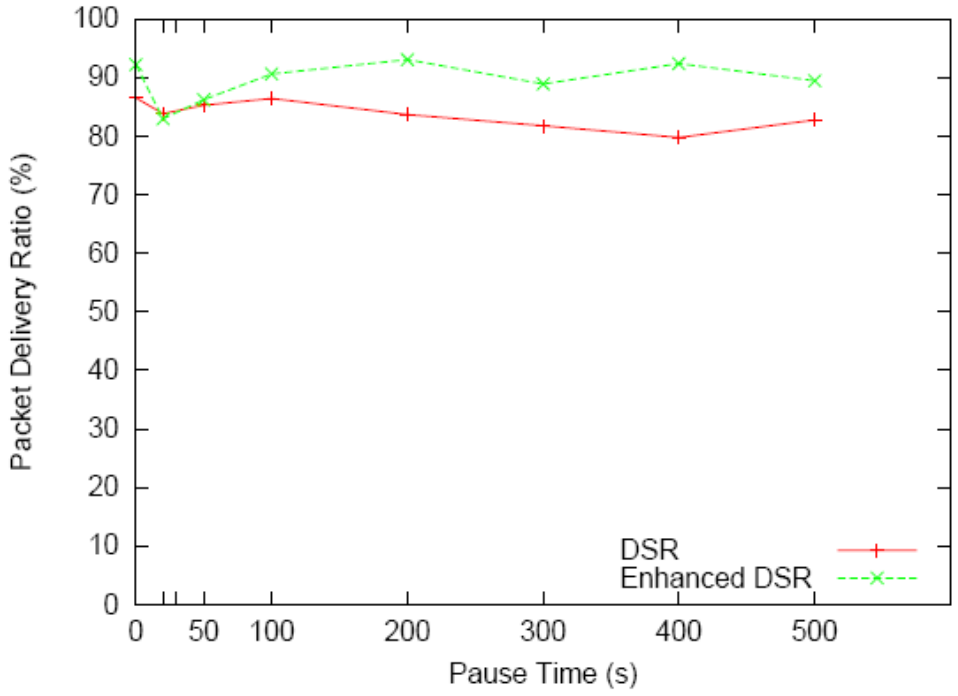
این کار شبیه‌سازی به دو قسمت تقسیم شده است. اولی بین عملکرد دی ـ اس ـ آر و دی ـ اس ـ آر بهبود یافته با راهکار SAFE مقایسه می‌شود. بهرحال، بخش دوم بهبودی بدست آمده توسط

دی ـ اس ـ آر بهتر شده هنگامی که از شاخص توزیع شده ایستا II (PDI) استفاده شـده اسـت را مورد بحث قرار می‌دهد.

در بقیه ، معیارهـای انـدازه گیـری مـرتبط بـا دی ـ اس ـ آر اصـلی بـا دی ـ اس ـ آر نشـان داده می‌شوند، که نشان می‌دهد که پروتکل بدون راهکار SAFE عمل می‌کنند. هنگامیکه کار آخر فعال می‌شود. اندازه گیری‌های بعنوان دی ـ اس ـ آر بهتر شده مشخص می‌شوند.

۱–۵–۱ ارزیابی عملکرد SAFE

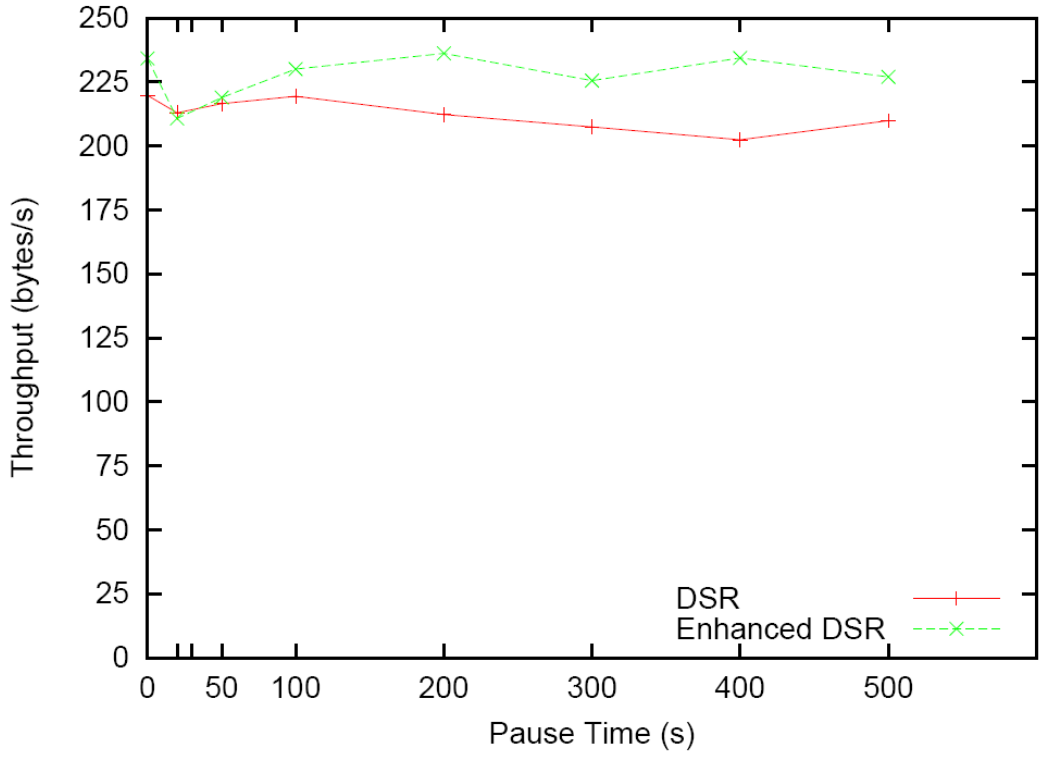
شکل ۲ نسبت تحویل دادن برای زمینه شبیه‌سازی بالا را نشان می‌دهد. ضمن اینکـه زمـان تـأخیر افزایش می‌یابد، درصد بسته داده‌ها بطور یکنواختی بهبود می‌یابد. برای مثال، برای زمان تأخیر بیش تر از ۱۰۰ ثانیه نسبت تحویل بدست آمده برای دی ـ اس ـ آر افزایش یافته در حدود ۱۰٪ بهتـر از حالت معمولی دی ـ اس ـ آر است. هنگامیکه زمینـه‌هـای بسـیاری پویـایی را در نظـر مـی گیـریم (PT≤100) عملکرد دی ـ اس ـ آر افزایش یافته مشابه D دی ـ اس ـ آر قبلی است.



شکل ۱–۲ مقایسه نسبت تحویل بسته

کارایی راهکار SAFE در رابطه با ظرفیت توانایی مشابه آن است که برای تحویل دادن مقدار بدست آمده نشان داده شده در شکل ۳ بدست آمد.

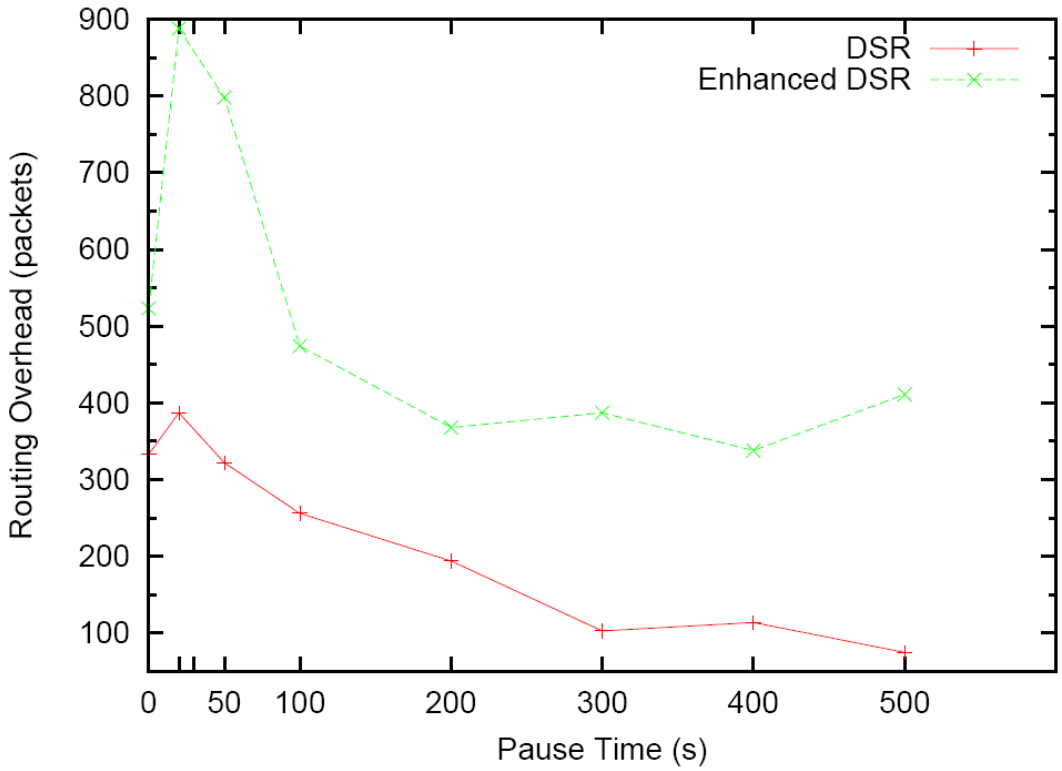
برای زمینه‌های متوسط و پایین تحرک (PT>300s: کم و 100s≤PT≤300s متوسط) میانگین ظرفیت حداکثر نزدیک به ۲۳۵ بیت بر ثانیه byte/s برای دی ـ اس ـ آر و ۲۱۵ byte/s برای دی ـ اس ـ آر بدون افزایش است. بدین ترتیب، راهکار SAFE کشف رفتار بد داده مخرب و برقراری مسیر جدید را برای پرهیز از گره مخرب مجاز می‌کند. این به معنی این است که درصد کمی از بسته‌های داده‌ها توسط گره‌های بد انداخته شدند هنگامیکه راهکار SAFE بکار گرفته شده بود. این موقعیت در شکل ۲ نشان داده شده است که نسبت تحویل افزایش یافته است.



شکل ۱-۳ ظرفیت پذیرش

بر مبنای دیده‌بانی سرجمع مسیریابی نشان داده شده در شکل ۴ تقریباً در همه موارد سرجمع مسیریابی در شبکه SAFE المثنی می‌شود این نسبتاً واضح است چون SAFE از چند بسته

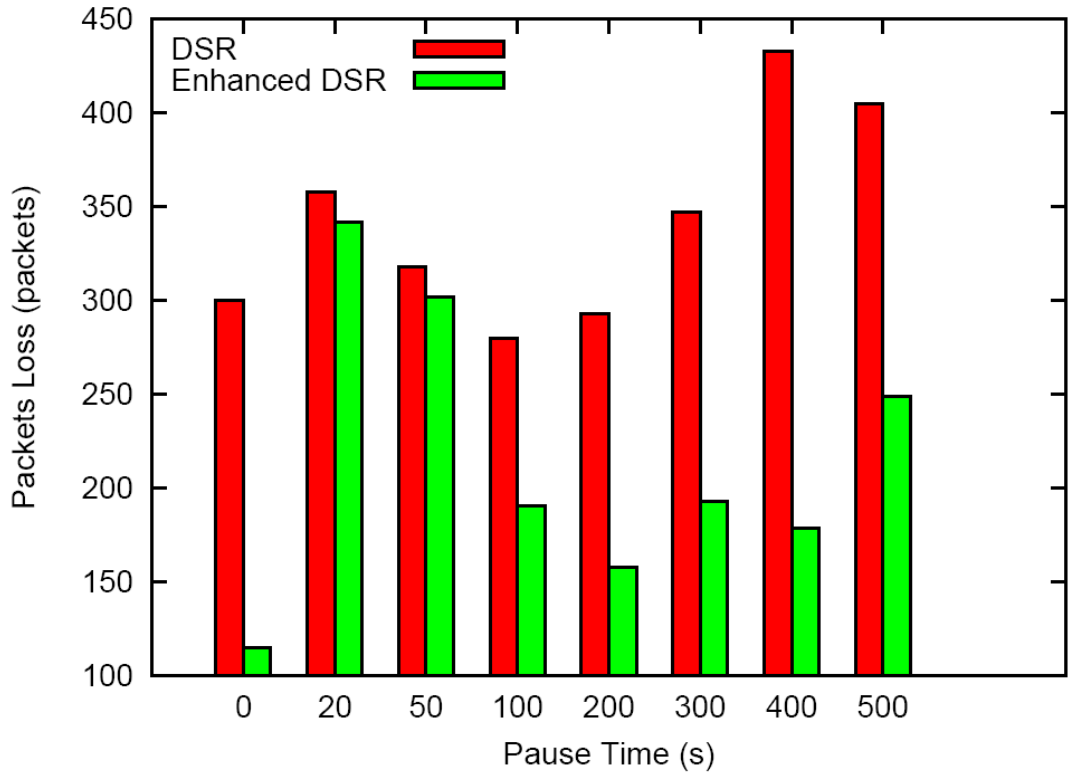
جدید استفاده می‌کند. بهرحال، راهکار SAFE همچنین کشف مکررتر گره‌های مخرب و حرکت سایر پارامترها از قبیل نسبت تحویل، ظرفیت توانایی و تأخیر را مجاز می‌کند. در پایان نشان خواهیم داد چطور سرجمع مسیریابی اضافی ایجاد شده توسط راهکار SAFE بدون هیچ بی‌توجهی به بهبودی‌های بدست آمده توسط این راه کار در طرف دیگر معیارهای اندازه گیری کاهش می‌یابد.



شکل ۱-٤ سرجمع

شکل ۵ تعداد کل بسته‌های انداخته شده توسط گره مخرب طی شبیه‌سازی را نشان می‌دهد. برای آر ـ اس ـ آر افزایش یافته، تعداد بسته‌های انداخته شده برای اکثریت زمان‌های مکث کاهش یافته (به استثنای PT=50s, PT=20s). این رفتار به توانایی راهکار SAFE در کشف گره‌های مخرب و جستجو برای مسیر ثانوی مربوط است ـ در حقیقت، برقراری یک مسیر جدید که گره مخرب پرهیز می‌کند احتیاج به برخی تعدیل‌ها در رابطه با پروتوکل اصلی دارد. این بخش هنوز کاملاً اجرا نشده است چون ما مایلیم اثر تحرک روی برقراری مسیری‌ها بعد از کشف یک سوءرفتار را ارزیابی کنیم.

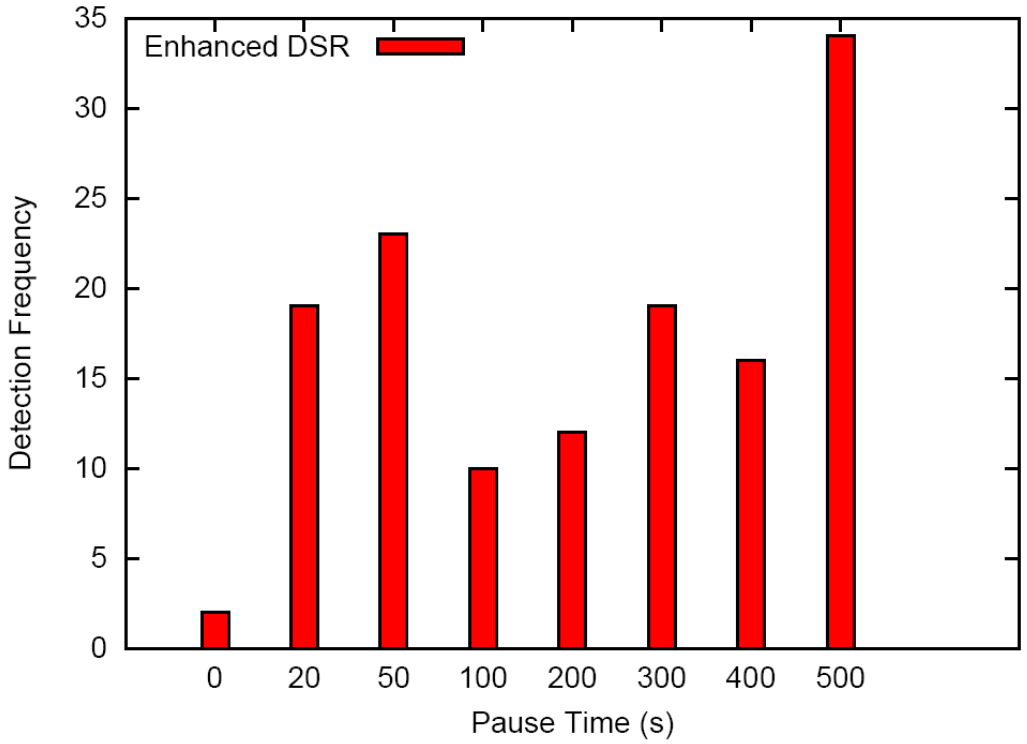
تابحال، راهکار SAFE اجازه می‌دهد که یک سوءرفتار برای اطلاع به گره منبع کشف شود. بسادگی مسیر تحویل دادن جدیدی راه خواهد انداخت. این روش شبیه به آن است که توسط دی ـ اس ـ آر برای برقراری مسیر جدید بکار رفت هنگامیکه یک قطع ارتباط کشف شده ضمن اینکه گرهها حرکت می‌کنند، ممکن است مسیر جدیدی دوباره یا با شامل کردن گره مخرب یا با مسیر قبلی دوباره مستقر شود.



شکل ۱- ۵ بسته های داده های انداخته شده توسط گره مخرب

نتایج شبیه‌سازی که در این شبیه‌سازی بدست آوردیم، نسبتاً جالب هستند و در زیر درباره آنها بحث می‌کنیم. تعداد دفعاتی که برای آنها کد مخرب کشف می‌شود در شکل ۶ نشان داده شده است. توجه کنید که برای یک حرکت کامل شبکه (PT=0)، کشف گره‌های مخرب در اثر تغییرات بسیار پویا در شبکه مشکل‌تر هستند. این بسادگی به این معنی است که گره مخرب خیلی سریع حرکت می‌کند و زمان کافی برای انداختن بسته‌ها ندارد. بهرحال، برای تحرک بالای پیکره‌بندی

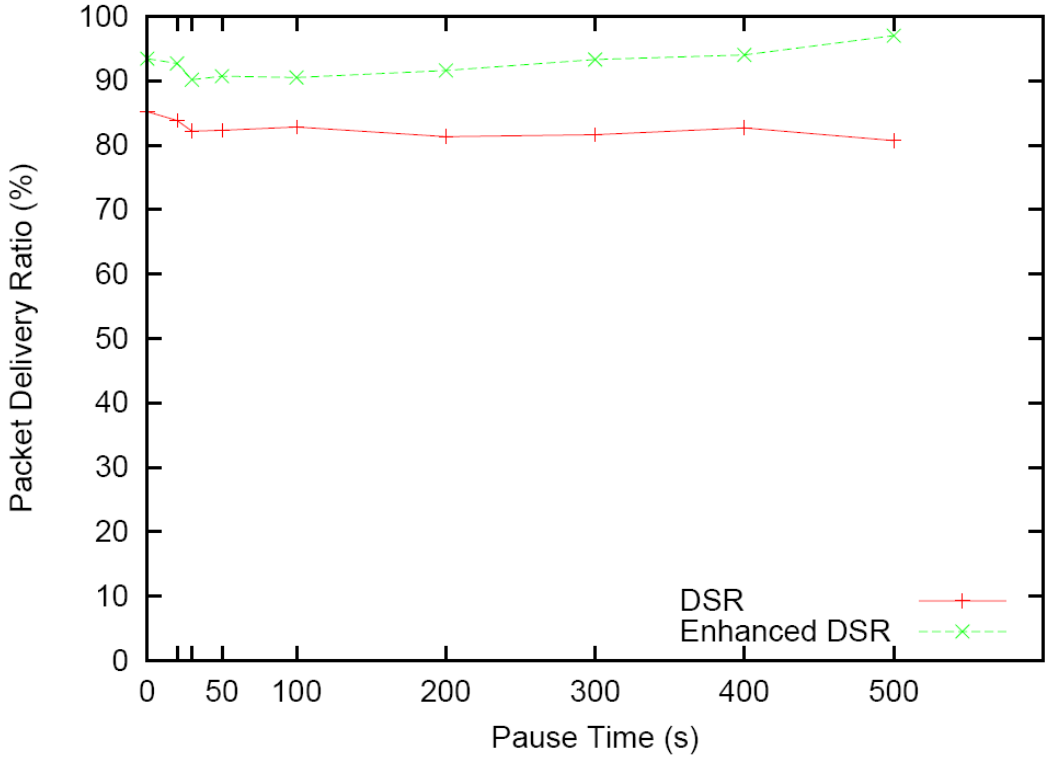
PT=50s, PT=100s، ما سطح بدست می آوریم کـه مـی‌توانـد در اثـر ایـن حقیقـت باشـد کـه هنگامیکه که گره مخرب کشف شده و هنگامیکه که مسیر جدیدی برقرار شد، گـره مخـرب دوبـاره بخشی از مسیر جدید است. نسبت پایینی تحویل بسته (به شکل ۲نگاه کنید) در نتیجه تعداد حلقه از کار افتاده است که به خاطر تغییرات بسیلر زیاد انجام گرفته در مکـان شناسـی شـبکه اسـت. در مورد زمینه تحرک کم (به استثنای PT=500s)، کشف‌های بدست آمده بین محـدوده (۱۸ و ۱۰) هستند. مثل پیکره بندی ایستا، گره مخرب مشخص شد، بهرحال، طی دوره کامل شبیه‌سـازی بـود که بخشی از مسیر بین منبع و مسافت بعنوان مکان شناسی شبکه تغییر نکرد. برای دقیقتـر بـودن، برای PT= 500s، گره‌ها طی زمان شبیه‌سازی ثابت باقی می‌ماند، و گره مخرب ۳۴ مرتبـه کشـف شد.



شکل۱- ۶ کثرت کشف گره مخرب

۱–۵–۲ عملکرد SAFE هنگام استفاده از شاخص گذاری توزیع انفعالی

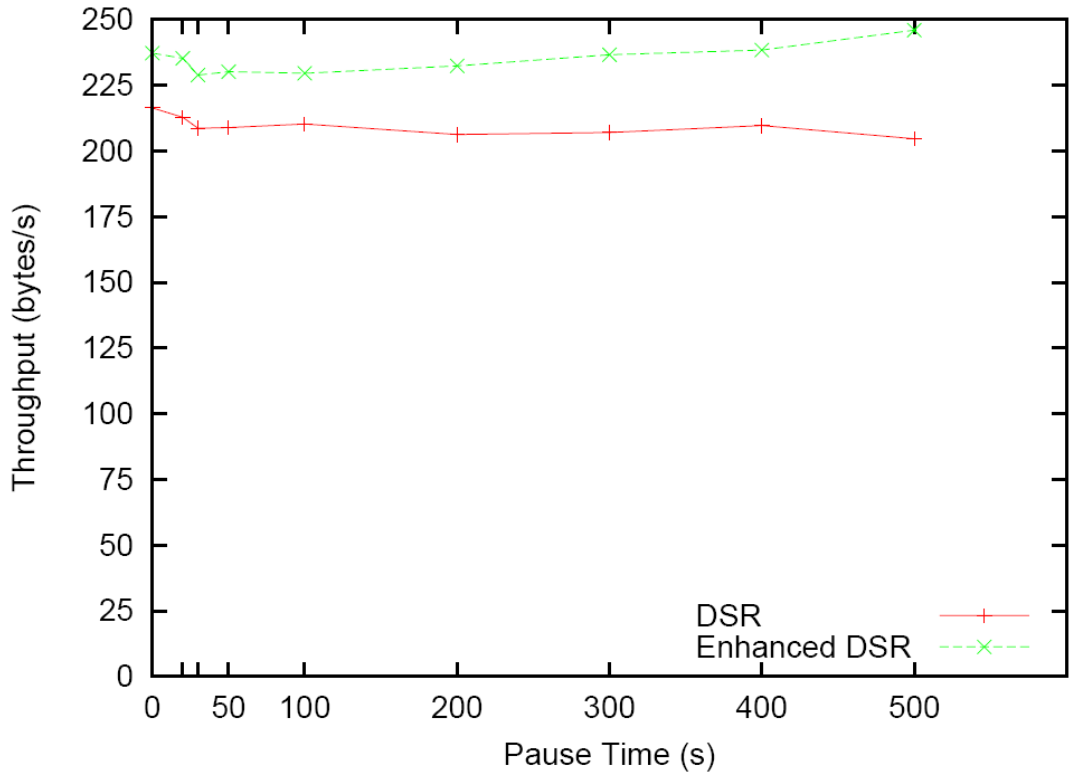
در این بخش، مخزن‌های محاسباتی حفظ شده توسط عامل‌های SAFE از طریق یک رویه شاخص‌گذاری همدیگر توصیف شده .اول شکل ۷ نشان می‌دهد که نسبت تحویل بسته هنگام استفاده از رویه ذکر شده بهبود یافته است. دی ـ اس ـ آر افزایش یافته، در این مورد، نسبت تحویل دادن با معیارهای اندازه گیری قبلی را با بیش از ۱۰٪ کلیه‌ی زمان‌ها و مکث از عملکرد باز می‌دارد. در مقایسه با معیارهای اندازه‌گیری سابق، برای مثال شکل ۲ درصد بسته‌های بدرستی دریافت شده توسط مقصد به طور قابل ملاحظه‌ای برای زمینه‌های تحرک زیاد افزایش یافته است.



شکل ۱–۷ مقایسه نسبت تحویل بسته

حداکثر ظرفیت در شکل ۸ نشان داده شده که نشان می‌دهد که برخی بهبودی‌ها همچنین برای زمینه‌های تحرک زیاد و کم بدست آمده بود. در اثر تأخیر کم ایجاد شده توسط SAFE هنگام

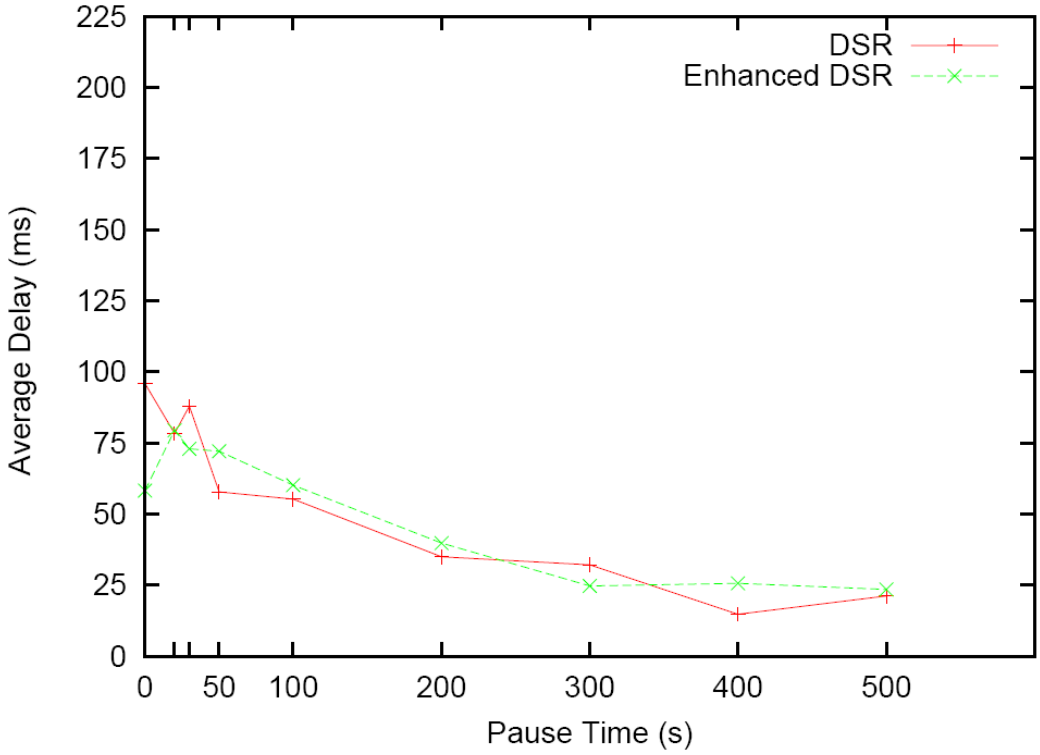
استفاده از الگوریتم‌های همدیگر حداکثر ظرفیت افزایش یافته دی ـ اس ـ آر در حدود بهینه (۷۰۰، ۲۴۹ بایت در ثانیه) نوسان می‌کند. با توجه به دی ـ اس ـ آر بـدون افـزایش، حـداکثر ظرفیـت بـه تعدادی کمتر از ۲۱۵ بایت بر ثانیه کاهش یافته است چون روشـی بـرای پرهیـز از انـداختن بسـته مخرب در محدوده معمولی دی ـ اس ـ آر وجود ندارد.



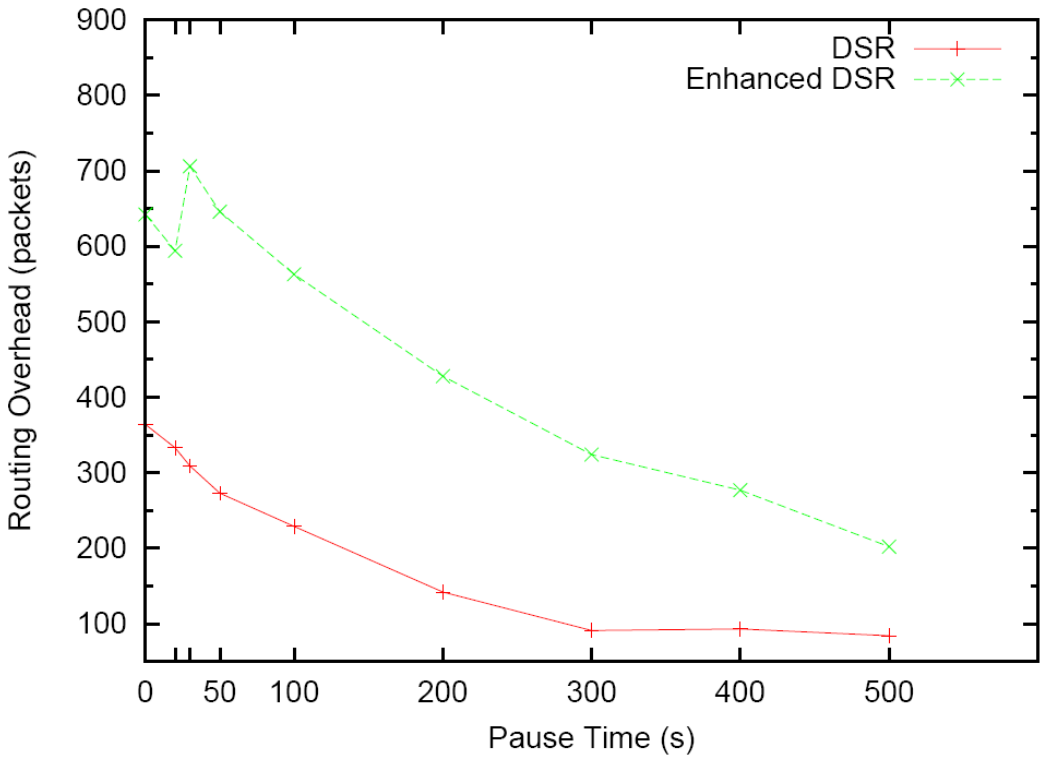
شکل ۱-۸ ظرفیت پذیرش

تأخیر میانگین بدست آمده به نظر می‌رسد شبیه به آن باشد که توسط دی ـ اس ـ آر معمولی ایجاد شده باشد همانطور که در شکل ۹ نشان داده شده است. این به معنی این است که راهکـار SAFE هیچ تأخیر اضافی برای دوره عدم فعالیت سرتاسری ایجاد نمی‌کند. شبیه شاخص‌گذاری توزیع شده انفعالی پی ـ دی ـ آر [۶] SAFE روش‌های مؤثر ارائه می‌دهد (بـه شـکل ۱۰ نگـاه کنیـد) کـه از

طریق دیده‌بانی کلی برای حریف شدن با شاخص قدیمی ورودی‌ها در اثر اتصال پـذیری ضـعیف، از کار افتادن گره و داده‌های تعدیل یافته است. این دیده‌بانی محلی به طور بالقوه نسـبت بـه ویـرایش قبلی سرجمع کمتری دارد، همانطور که نشان داده شده است. می‌توانیم ببینیم که سرجمع SAFE بدون هیچ افزایش پی ـ دی ـ آی بین 400ms و 500ms برای زمانه‌های مکـث P≥100s ثابـت باقی می‌ماند، بهرحال، با این افزایش (به شکل ۱۰ نگاه کنید). مخزن‌های محاسباتی بهینه می‌شوند. در نتیجه، برای زمان‌های مکث یکسان، یک بهبـودی بـین 200 ms و 650ms بـرای 100ms و 500 ms بترتیب مشاهده می‌شود.



شکل ۱-۹ تاخیر میانگین سرتاسری

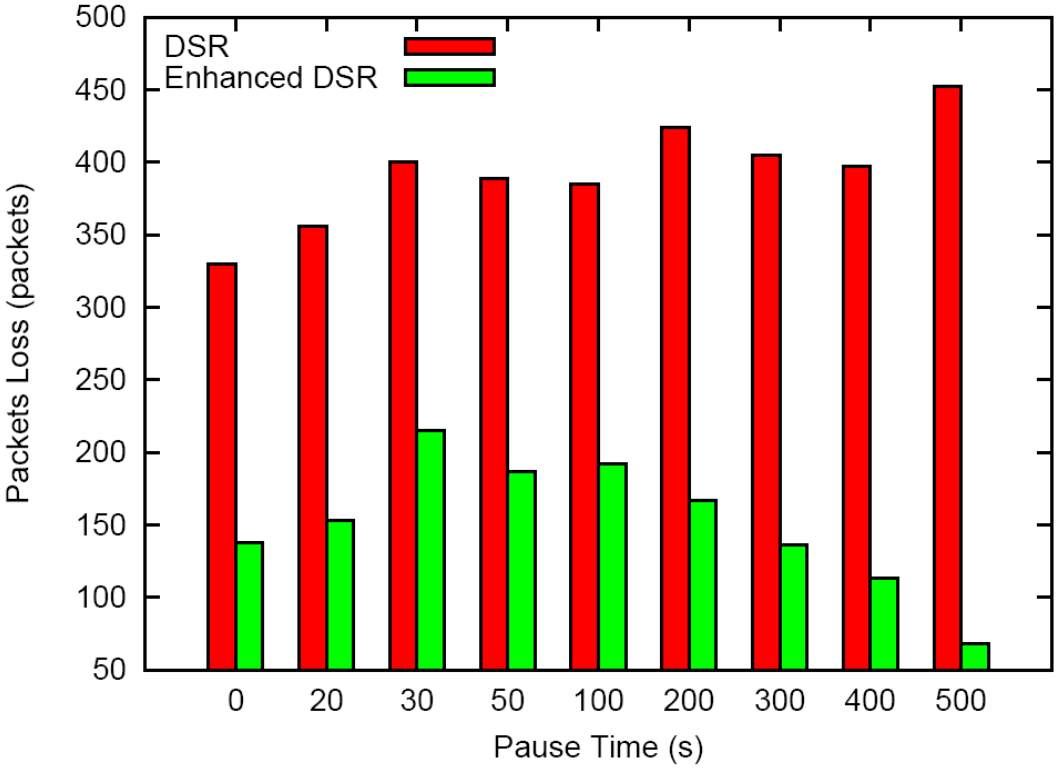


شکل ۱-۱۰ سرجمع

مهم است ذکر کرد که سرجمع مسیریابی برای زمینه تحرک بالا هم بهبود یافت. برای مثال، با استفاده از زمان‌های مکث 20s و 50s، سرجمع قبلی در حدود ۸۰۰ و ۹۰۰ بسته به ترتیب است، همانطور که در شکل ۴ نشان داده شده است) بهرحال، هنگامیکه SAFE از الگوریتم‌های همه‌گیر استفاده می‌کند، مقادیر سرجمع ۶۵۰ و ۷۰۰ بسته به ترتیب است همانطور که در شکل ۱۰ نشان داده شده است.

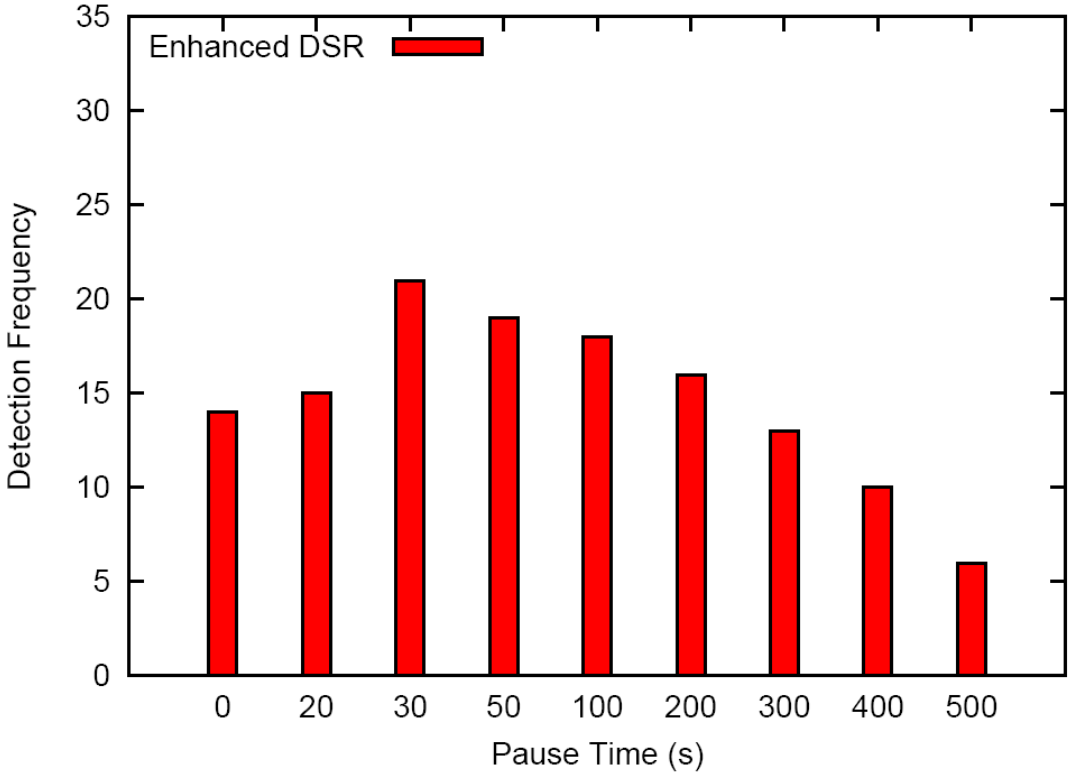
نتایج شبیه‌سازی همچنین کارایی رهیافت (شکل ۱۱) ما را در کاهش تعداد بسته‌های انداخته شده توسط گره مخرب را نشان می‌دهد. بطور کلی، نتیجه‌گیری می‌کنیم که تعداد بسته‌های انداخته شده برای تمام زمان‌های مکث تحلیل شده بیش از نصف کاهش یافته است. دوباره، هنگام مقایسه SAFE با افزایش پی ـ دی ـ آی و بدون افزایش، حرکت قابل ملاحظه ای برای تحرک زیاد پیکره‌بندی‌ها بدست می‌آوریم. برای مثال، برای زمان‌های مکث ۲۰ و ۵۰ ثانیه‌ای، گره مخرب در

مقایسه با نتایج SAFE نمایش داده شده در تصویر ۵، جائیکه این گره مخرب بترتیب ۳۴۵ و ۳۰۰ بسته انداخته است، این گره مخرب فقط ۱۵۰ و ۲۰۰ بسته بترتیب انداخته است (به شکل ۱۱ نگاه کنید).



شکل ۱-۱۱ بسته های داده ها و انداخته شده توسط گره مخرب هنگامیکه PDI بکار می رود

طبق شکل ۱۲، هنگامیکه SAFE با افزایش پی ـ دی ـ آی بکار رفته است نسبت به زمانی که SAFE بدون افزایش پی ـ دی ـ آی بکار رفته این گره مخرب در زمان‌های کمتری کشف شده است (در مورد پیکربندی های تحرک کم). برای مثال، در زمان مکث ۵۰۰ ثانیه‌ای، گره مخرب ۵ مرتبه مشخص شد همانطور که در شکل ۱۲ نشان داده شده. بدون افزایش پی ـ دی ـ آی، گره مخرب ۳۴ مرتبه کشف می‌شود.



شکل ۱-۱۲ کثرت کشف برای SAFE

با بکارگیری شاخص توزیع انفعالی پی ـ دی ـ آی [۶] SAFE بدون فرستادن پیام‌هایی خارج از محدوده‌های رادیو گره استعلام کننده بطور محلی استعلام‌های بیشتری انجام می‌دهد. نتایج شبیه‌سازی بهبودی در درصد داده‌های تحویل داده شده، ظرفیت پذیرش زیاد و تأخیر سراسری کم نشان می‌دهد. مشخصه اصلی SAFE کنترل محض روی چشم انداز تحویل اطلاعات و حداقل کردن سرجمع مسیریابی است.

در آینده موارد ذیل در نظر خواهند گرفت

- قبلاً ذکر کردیم که برقرای یک مسیر جدید که از یک گره مخرب هنگامیکه ایـن یکـی کشـف شود جلوگیری می‌کند، نسبتاً اجرا شده است. در اثر تحرک و توپولوژی اولیه شبکه، هنگامیکـه سعی می‌کنیم از گره مخرب اگر پروتوکل دی ـ اس ـ آر تعدیل نیافته جلوگیری کنیم، ممکـن است دوباره همان مسیر برقرار شود. به این دلیل، برای توانمند کـردن برقـراری دوبـاره کشـف مسیر برای جلوگیری از گره مخرب هنگام برقـرای مسـیری جدیـد، پروتوکـل دی ـ اس ـ آر را تعدیل کنیم.
- قابلیت گسترش راه کار SAFE را هنگامیکه شبکه بزرگتر است (یعنی ۵۰ / ۱۰۰ گره) و تعداد گره های مخرب بزرگتر است (۱۰، ۲۰، ...) ارزیابی خواهیم کرد.
- همچنـــین عملکـــرد راه‌کـــار SAFE را بـــا سیســـتم‌هـــای محاســـباتی از قبیـــل CORE و CONFIDANT مقایسه خواهیم کرد.

تا حالا، با استفاده از به تحقیق ثابت کردن و کد گذاری شبکه‌های ویژه ایمن هستند. این راه کارهـا به نظر می رسد در مقابل انواع حمله های دیگری از قبیل انداختن بسـته مخـرب و انکـار سـرویس ناکارآمد باشند. راه کاری که ما پیشنهاد کردیم. پروتوکل های مسـیریابی را قـادر کـرد حیلـه‌هـای انداختن بسته را کشف کند. در حقیقت، گره ها در شبکه بطور مستقل رفتار یکدیگر را دیـده بـانی می کنند، بهرحال، برای مشخص کردن مزاحم ها باید همکاری کنند. چون این راه کـار بـر مبنـای مفهوم محاسباتی است، کاروری‌هایی از قبیل جمع آوری اطلاعات محاسباتی و محاسبه محاسـباتی هم بحث می‌شوند. پیشنهاد ما همچنین با کار شبیه‌سازی نشان‌دهنده کنش پـذیری و عملکـرد آن اعتبار پیدا کرد.

۱–۶ همایش ویژه تکامل تثبیت خودگیری SAEF

یک گرد هم آیی ویژه بنام تکامل ثبیت خودگیری ("SAEF") وجود داشت، که با پیمایش جعبه میانی کنترل شده تکان شدید سر و کار داشت.

اطلاعات درباره این همایش می تواند اینجا پیدا شود.

این هماش نسبتاً خوب بود و با برخی بحث های سازنده داشتیم.

۱. توصیف این که چرا SAEF بیشتر احتمال دارد موفق شود جائیکه سایر پروتکل های آ ـ ای ـ تی ـ اف نات شکست خوردند

۲. متن منشور برای همایش آ ـ ای ـ تی ـ اف ونکور

۳. توضیح حمله امنیتی که با BOOTNONCE پرهیز می شود.

۴. اظهاریه های اجرا شدن از فروشندگان نات

۱–۶–۱ مرور "LOBSEC" (حذف شیء)

در زمینه برنامه ریزی سازگار با هدف، تئوری و عمل بطور قابل ملاحظه ای جدا رشد می کرده اند. زمان برنامه ریزی که طراحان و سازندگان همگردان ها با موضوعاتی مثل روش فایق آمدن، تکثیر بازمانده، الگو و غیره کشمکش می کنند که با خصوصیاتی که تئوریسن (نظریه پردازها) تئوری اصلی را توسعه می دادند وابستگی زیادی نداشت. البته، برخی از بینش های مهم سازگار بودن با هدف برای برنامه ریزی سازگار با هدف مزیت بزرگی بودند امّا برای برخی مطالب جائیکه کاروران می توانستند از کمک هایی استفاده کنند، پشتیبانی تئوریکی وجود نداشت. گیوزپ گاستاندا، نویسنده این کتاب توجه خود را به برخی از این زمینه های نادیده گرفته شده معطوف می کند. با تحقیق دکترای خود که در سال ۱۹۹۴ به پایان رساند، او مساعدت زیادی به تئوری برنامه ریزی سازگار با هدف با چندین پیشرفت مهم بخصوص در آن زمینه های نادیده گرفته شده کرد. این

کتاب نسخه تجدید نظر شده ای از پایان نامه دکترای او است. تلاش ویژه ای برای این که این کتاب برای تئوریسن ها و کارورها جالب و خواندنی باشد انجام گرفته است.

در این زمینه گاستاندا از روش های سنتی منحرف شد، اوّل از همه، عمدتاً با معطوف کـردن توجـه خود به طرف چند ریختی ویژه بجـای چنـد ریختـی پـارامتری [سـی ـ دبلیـو ۸۵]. چنـد ریختـی پارامتری هنگامی است که یک تابع بطور یکنواخت در محدوده ای از انواع کار مـی کنـد. در عمـل، چند ریختی پارامتری اغلب از طریق خصوصیاتی مانند انواع کوچک و الگو پشتیبانی می شود. چنـد ریختی ویژه هنگامیکه یک تابع روی چندین نوع مختلف کار می کند و ممکن است بـر روش هـای نامرتبط برای هر نوع رفتار کند بدست می آید. این شکل از چند ریختی اغلب از طریق خصوصیاتی مثل روش اضافه بار کردن و فایق آمدن با الـزام دیـر هنگـام در مـورد روش فراخـوانی هـا حمایـت می‌شود.

همانطور که قبلاً ذکر شد، اکثریت تئورسین هایی که روی زبان های برنامه ریزی سازگاری با هـدف (OO) کار می کنند روی چند ریختی پارامتری تمرکز می کنند. از اینرو، مشـکلات مخـتص چنـد ریختی ویژه حل نشده باقی مانده که بسیاری از آنها توسط گاستاندا به عهـده گرفتـه شـدند. آنچـه مخصوصاً برای کاروران OO (برنامه ریزی سازگار با هدف) سودمند است ایـن اسـت کـه گاسـتاندا توجه قابل ملاحظه ای به این سؤال که چطور تئوری توسعه یافتـه مـی توانـد عمـلاً در زبـان هـای برنامه‌ریزی OO بکار گرفته شوند می کند.

جنبه اصلی دیگری که گاستاندا از روش های سنتی منحرف شده، رهیافت او بطرف روش هـا اسـت در بسیاری از زبان ها، تصور این است که روش ها اهداف وابسته هستند. بر مبنای این چشـم انـداز ثابت شد رسمیت بخشیدن به روش فایق آمـدن مشـکل اسـت. بهرحـال، گاسـتاندا، بجـای چنـین رهیافت اصلی هدف، از رهیافت اصلی پیام استفاده کرد. در این رهیافت، فـرض مـی شـود روش بـه هدف وابسته نیست، بلکه به پیام وابسته است.

بعنوان شالوده ای برای رسمی سازگاری او، گاستاندا، کلکولسی به اسم & تعریف کرد. کلکـولس & یک نوع کلکولس از نوع ساده است که او آنرا با توابع گرانبار شده گسـترش داد. یـک تـابع گرانبـار حاوی چندین تابع عادی است که جهش خوانده می شوند. این می تواند به یک استدلال بـه همـان طریق که یک تابع اعمال شود. اثر چنین کاربرد تابع گرانبار آن است که جهشی که بهتـرین جفـت شدن با استدلال را دارد انتخاب می شود و به استدلال اعمال مـی شـود (عملکـرد تـابع معمـولی). ضابطه بهترین جفت شدن نوع زمان رانش استدلال است. به این طریق، مفهوم اصلی وابستگی نـوع در کلکولس تلفیق می شود. این مفهوم برای خصوصیات مرتبط با چند ریختی ویژه مثل روش فایق آمدن با الزام دیر هنگام اساسی است. این به گاستاندا اجازه داد این خصوصیات را با بازنمـایی پیـام های OO به توابع گرانبار و روش های منفرد به جهش های توابع گرانبار رسمی کند.

یک مزیت برای برنامه ریزی OO می تواند فوراً از این رسمی کردن بدسـت آیـد. همیشـه موضـوع مشکلی بوده است که محدودیت های نوعی باید روی روش عامل گرانباری و فـایق آمـدن گذاشـته شود. ممکن است تمایل این باشد که به برنامه ریز در حد امکان آزادی داده شود و هنوز امنیت نوع را حفظ کرد. یعنی از خطاهای زمان رانش مرتبط با تعیین نوع پرهیز کرد. از رسمی کردن گاستاندا این طور دنبال می شود که گرانباری و فایق آمدن دو طرف یک سکه هستند. علاوه بر این، قـوانین تعین نوع درست که الزامی و کافی هستند می تواند از قوانین تعین نوع کلکولس & و رسمی کردن پیام های OO بعنوان توابع گرانبار استنتاج شوند.

پتانسیل کلکولس & حتی از روش ساده گرانباری و فایق آمدن بهتر است. ایـن طـور از آب در مـی آید که روش های متعدد Clos (روشهایی که بیش از یک دریافت کننده دارند) همچنین می توانند با استفاده از کلکولس & رسمی شوند. دوباره قوانین تعین نوع درست برای روش گرانبـاری و فـایق آمدن در زمینه روش های متعدد می تواند استنتاج شود.

فقط کلکولس & و کار گاستاندا روی رسمی کردن زبان برنامه ریزی دارای پتانسیل منافع عملی به شکل خصوصیات پیشرفته در رابطه بـا چنـد ریختـی ویـژه، قابـل اطمینـان نـوع نیسـت. گاسـتاندا

همچنین یکبار و برای همه بین تئوریسن ها مباحثه ای درباره این که آیا باید از یک قـانون متغیـر برابر یا متفاوت برای تعیین نوع کوچک درباره انواع تابع استفاده کرد. مـن از جزئیـات ایـن مباحثـه چشم پوشی خواهم کرد، اما به من اطمینان داشته باشید که این باعث جـر و بحـث بیشـتری شـد. "متغیر برابر و متغیر نابرابر: منافات بدون سبب" (همچنین بعنوان یک مقاله مجله چـاپ شـد [۹۵ Cas] مشخصاً با این موضوع سر و کار دارد. گاستاندا خاطر نشان می کند که در کلکولس &، برای هر دوی متغیر برابر و متغیر نابرابر جا وجود دارد و هر یک نقش مهم امّا متفاوتی بازی می کند چند ریختی پارامتری در این کتاب نادیده گرفته نشده است. در بخش دوّم، چند ریختی ویـژه پـارامتری در یک کلکولس با سیستم نوع دوّم که توابع گرانبار را تلفیق می کند یکی شده اند. با این کلکولس "فقدان شکل اطلاعات" سبب الزام در برخی زبان ها برای ویرانی های شرم آور می تواند حل شـود. علاوه بر این، می تواند برای مطالعه فعل و انفعالات بین خصوصیات پیشرفته مرتبط با چند ریختـی های پارامتری مثل الگوی C^{++} و آنهایی که با چنـد ریختـی ویـژه مثـل روش هـای متعـدد مـورد استفاده قرار گیرد. چون این کتاب تحفه ای ارزشمند برای کاروران و تئوریسن های برنامه ریزی ۵۵ در زمینه نوع تئوری است. گاستاندا تلاش زیادی کرده است که این کتاب برای هر دو گروه علاقمند خواندنی باشد. او برای رسیدن به این از دو روش استفاده کرده است. اوّل از همه، برخی بخش ها بـا "خم شدن خطرناک" یا "کژ راهه" علامت گذاری شده اند که نشاندهنده این است که آن بخش ها شکل یا "از قلم انداختنی" هستند. دوّماً، کدامیک مناسب ترین روش های خواندن برای گروههـای علاقمند مختلف هستند (گاستاندا سه روش را مشخص می کنـد: کـاروران، معلمـان، و دانشـوران)، سرانجام شامل مروری عالی از کلیه کتاب برای خواننده عجول است. این همچنین مـی توانـد بـرای معین کردن این که کدام فصل را می شود با جزئیات بیشتر مطالعه کرد استفاده کرد. بطور خلاصه، این کتاب پلی بین تئوری و عمل در برنامه ریزی ۵۵ اسـت. بـدون انجـام دادن اعترافـات تئـوریکی گاستاندا می تواند مطالب تعین نوع زا برای کارورها و تئوریسن ها از طریق ارائه صریح و خوب قابل دسترسی کند. مساعدت های مهمی که او کرده، مرحله اصلی رو بجلو است.

۱–۷ موریس وان کولن

مدلی برای تحلیل یکنواخت مطالب اصلی برنامه ریزی OO (سازگار با هدف) ارائـه مـی دهـد. ایـن کتاب ویرایشی از پایاین نامه دکترای نویسنده است. این کتاب خودکفـا اسـت و مـی توانـد توسـط محقق ها، استادها و کارورها هم بکار رود. در یک ارائه کوتاه، نویسنده بـه خواننـده اشـاره هـایی در مورد مناسبترین روش خواندن می کند. اسم آن "تعیین نوع ساده" و بـه مـدل نویسـنده از برنامـه ریزی سازگار با هدف اختصاص یافته است. ، "برنامه ریزی سـازگار بـا هـدف". خصوصـیات هسـته مرکزی برنامه ریزی سازگار با هدف را از طریق زبان سازگار با هدف به اسم "زبان سازگار بـا هـدف هسته مرکزی" را مورد بحث قرار می دهد. این زبانی عملی است و از سبک سـیمولا را دنبـال مـی کند. این زبان شامل آن خصوصیات در نظر گرفته شده توسط نویسنده به عنوان شـالوده یکنواخـت برنامه ریزی سازگار با هدف است (طبقه ها، مدل ها، گرانباری، الـزام آوری دیـر، باقیمانـده، طبقـه های گسترده، آزمایش نوع). "کلکـولس &" مـدل مبتنـی بـر گرانبـاری را نشـان مـی دهـد. نمـاد (سمبول) & یک عامل است که برای چسبانیدن دو تابع به یکدیگر در یک عامل گرانبار بکار رفتـه است. بدین ترتیب، واژه M&N یک تابع گرانبار از دو جهش M و N را نشان می دهد. که یکی از آنها طبق نوع استدلال انتخاب خواهد شد. "متغیر متقابل و متغیر مخالف: کشمکش بـدون سـبب" نقش این عنوان ها را در نوع کوچکتر را روشن می کند. نویسنده از مدل ارائه شـده بـرای اسـتدلال این که متغیر متقابل و متغیر مخالف بطور مناسبی دو راه کار متمایز و مستقل را مشخص می کند. آنها بعنوان مفاهیم نامتضاد در نظر گرفته می شوند، که هر یک کاربرد خود را دارد: متغیـر متقابـل برای ویژه گری و متغیر مخالف برای جایگزینی. این فصل با سه "قانون طلایـی" کـه محتـوی آنـرا خلاصه می کند پایان می یابد: ۱ـ از متغیر مقابل (چپ) برای فلش نوع کوچـک بکـار نبریـد. ۲- از متغیر متقابل برای فایق آمدن به پارامترهایی که انتخاب روش پویا را می رانـد اسـتفاده کنیـد. ۳ـ هنگام فایق آمدن به روش باینری (یا M گانه) رفتار آنرا نه فقط برای طبقه بندی واقعی بلکه بـرای

پشتیبان هم مشخص کنید. یکدست کردن قوی، خصوصیات یکدست کردن را مطالعه می کند. این نشان می دهد که کلکولس قویاً یکدست نیست. دو شرط کافی داده شده که دارای یکدست کـردن قوی هستند و در سیستم نشانگر مشخص هستند که آنرا قانع می کنند. این سیستم به اندازه کافی نشانگر هستند که مدل برنامه ریزی سازگار با هدف باشند گرانباری بکـار رفتـه انـد، سـه سیسـتم مختلف را که مستقیماً از & حاصل شده اند را نشان می دهد: ۱- توسعه & با افزودن اضـطرارهای صریح، ۲- تعدیلی از کلکولس & با قانون کاهش جدیـد، ۳- یـک کلکـولس کـه در آن تـابع هـای معمولی و تابع های گرانبار با عامل جداسازی یکسان ارائه شده اند، که بنابراین آنها را یکنواخت می کند.۸ به تفسیر رسمی زبان کول در منزل مبتنی بر گرانباری ارائه شده اختصاص یافته است. در اثر این حقیقت که & برای مطالعه رسمی خصوصیات زبان های سازگار با هدف مناسب نیست، یک ابر زبان جدید به اسم Object (منظور) برای اثبات خصوصیات یک زبان سازگار با هدف ارائه می شود. زبان Object کلکولس & را با برخـی خصوصـیات جدیـد (دسـتورات بـرای تعریـف انـواع جدیـد، کارکردن روی ارائه آنها، اداره کردن سلسله مراتب انواع کوچک، تغییر دادن نوع یک واژه یا تعـدیل نظم و ترتیب گسیل داشتنی و غیره) که برای بازتولید سـاختارهای یـک زبـان برنامـه نویسـی لازم هستند و & فاقد آن است، غنی می کند. خصوصیات الزام آور و سایر چیزها در حالتی کمتر رسمی تر برخی از خصوصیات مورد علاقه عملی را که می تواند کول شامل باشند را نشان می دهـد. بـدین ترتیب، این زبان کارست پذیر می تواند با افزودن برخی فرمان های الزام آور به زبان سازگار با هدف واقع گرا ترفیع پیدا کند. همچنین می تواند بعه عنوان شکل منحصر بفردی از کاربرد برای تابع های معمولی و گرانبـار بکـار رود. سیسـتم نـوع کـول ممکـن اسـت بـرای اجـرای امضـاء تمـرین شـود. "معناشناسی" عمیقاً به داخل مشکلات ذیل مطرح شده توسط معناشناسانی کلکولس & مـی رود: ارتباط بیش از طبقه بندی بین انواع، محاسبه وابسته به نوع، الزام آوری دیر به استثناء پذیری ارائـه شده توسط تعریف نوع کوچک برای انواع گرانبار. تأکید می شود که برخی از این موارد نمی تواننـد در کلکولس & اداره شوند. این راه کار بر مبنای سیستم F چرا رد است که برای مناسـب بـودن در

اجرای الزام آوری دیر بارور می شود. هنوز خصوصیاتی وجود دارند که بصورت سر راست اداره نمـی شوند، از قبیل عالی و مقید. در فصل آخر "پسگفتار"، نویسنده کتاب خود را در چهارچوب سایر کار مربوط متمرکز می کند.

۱–۷–۱ تی بلاسنک

مرور "خبرنامه انجمن یوزنیکس"

پیشینه ناهنجار پیشروی زبان های برنامه ریزی سازگار با هدف از سیمولا به اسمال تاک، ایفل C^{++} Clos و جاوا شناخته شده است. اکثر این زبان ها سبک سیمولا را دنبـال مـی کننـد. امّـا Clos و چند تای دیگر چند گسیله هستند. این یعنی بحث برنامه ریزی سبک سیمولا وجود دارد امّا هیچک از زبان های چند گسیله وجود ندارنـد. آنچـه حتـی کمتـر شـناخته شـده اسـت روشـی اسـت کـه "گرانباری" توسعه یافت و کمبود تحقیق در مورد آن است. گاستاندا کار استادانه ای در مدل سازی مفاهیم درگیر در گرانباری همچنین آنهایی که برای مقایسه سبک های مختلف برنامه ریزی سازگار با هدف انجام داده است. این مطالعه ساده ای نیست، اما با آموختن چیزی بهتر خواهید شد.

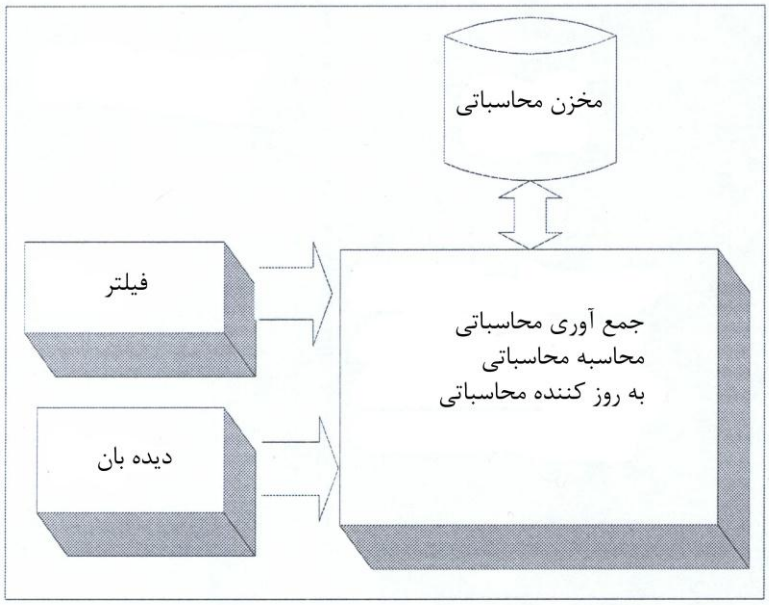
فصل دوم

پایش افت بسته داده ها

۲-۱ امنیت مخلص کلام است؟

سیستم های مبتنی بر محاسبات نمونه جدیدی از بالا بردن ایمنی در شبکه های تک موردی هستند. این راه کارها می توانند بخصوص در مواجه شدن با بی مرتبی ناشی از عناد و ترویج همکاری بین گره ها بکار رود. بسته پیشرو ایمنی در شبکه هـای تـک مـوردی (SAFE) مثـالی از ایـن مقولـه اسـت. هنگامیکه این سیستم ها بکار می روند، هر گره در شبکه نشر بسته در گره های همسایه را دیده بانی می کند و به آنها برخی مقادیر محاسبه شده طبق آن تخصیص می دهد. در حقیقـت، رهیافـت هـای مختلفی برای بازبینی (نظارت) وجود دارد و هر رهیافتی دارای اثر خود روی عملکرد سیسـتم مبتنـی بر محاسبات دارد. این مقاله، بر مبنای برخی نتایج شبیه سازی اثر دو روش نظـارت روی عملکـرد راه کار SAFE را مقایسه می کند.

راه کار SAEF را بررسی کنیم. برای جزئیـات بیشـتر،. SAFE از طریـق یـک تمامیـت بنـام عامـل SAFE که در هر گره در شبکه های تک موردی رانده می شـود، اطمینـان ایجـاد مـی کنـد. هرگـز مسئول کشف کردن سوء رفتارهای محلی بطور مستقل است. بهرحـال، بـرای ایمـن کـردن تمامیـت شبکه همکاری بین گره ها لازم است. معماری عامل SAFE در شکل ۱ نمـایش داده شـده و شـامل کاربرد پذیری های ذیل است.



شکل ۲-۱ معماری مدیر اداره کننده اعتبار

دیده بان: دیده بان مسئول مشاهده کردن صدور بسته همسایگی گره است. برای مثال: اگر گره آ رفتار گره بی را دیده بانی می کند، گره آ نسبتی از تعداد بسته های گره بـی فرسـتاده و تعـداد کـل بسـته هایی که گره آ به گره بی برای جلوتر فرستادن منتشر کرده نگه مـی دارد. نتـایج دیـده بـانی کـردن معمولاً با مدیر محاسبات ارتباط برقرار می کند که مقدار محاسبات گـره دیـده بـانی شـده را بـه روز خواهد کرد و آنرا در انبار ذخیره می کند. طریقی را که دیده بانی کردن بدست می آید .

فیلتر. در حقیقت، راه کار SAFE یک سر دسته برای تسهیل کردن مبادله اطلاعات محاسبات بـین عوامل SAFE مختلف به پروتکل مسیریابی اصلی اضافه می کند. این فیلتر مـی توانـد بعنـوان یـک مدول مکمل که به تشخیص دادن بسته های حاوی برخی اطلاعـات محاسـبات از سـایر بسـته هـای دریافت شده کمک می کند در نظر گرفته شود. در حقیقت، هنگامیکه بسته توسط یک گـره دریافـت شد، ابتدا از فیلتر عبور می کند که امتحان می کند خواه آن بسـته بـرای مـدیر محاسـبات فرسـتاده خواهد شد. در غیر اینصورت، بعنوان یک بسته معمولی پردازش می شود.

مدیر محاسبات: این مدول مسئول اداره کردن اطلاعـات محاسـبات اسـت. بـرای دقیـق تـر بـودن، محاسبات اطلاعات محاسبات مربوط به همسایگی را جمع آوری، محاسبه و نگه داری می کنـد. مـدیر محاسبات ورودی را از دیده بان یا فیلتر می گیرد. مورد اوّل منعکس می کند که صدور یک بسته گره بخصوص دارد دیده بانی می شود، بنابراین، برای به روز کردن اطلاعات محاسبات متناظر باید با مـدیر محاسبات ارتباط برقرار کرد. بهرحال، ورودی دریافت شده از این فیلتر به برخـی از مبادلـه اطلاعـات محاسبات بین برخی گره های همسایه در رابطـه بـا یـک گـره مـتهم / بـدخواه مـرتبط اسـت. مـدیر محاسبات مقدار محاسبات جدیدی گره تحت ملاحظه را با استفاده از برخی معیارهای مناسب حساب می کند و این مقدار را در انبار محاسبات خود ذخیره می کند.

انبار محاسبات: SAFE فرض می کند که هر گره در شبکه یک انبار محاسبات که در آنجـا مقـادیر محاسبات همسایه ذخیره می شوند نگه می دارد. این انبارها پـر از مقـادیر محاسـبات هسـتند کـه از طریق دیده بانی مستقیم یا از طریق اتهامات فرستاده شده توسط برخی از گره هـا در شـبکه حسـاب شده اند. برای بهم چسبیده تر بودن، SAFE اطلاعات محاسبات را شکل جفت (کلید، مقدار) ذخیره می کند. میدان کلیدی به آدرس آی ـ آر گره دلالت می کند که (رپ ـ وال) دلالت می کند که مقدار محاسبات گره دیده بانی شده و تی تی ال که مقدار زمان تا زندگی کردن است. تی تی ال دوره زمانی را نشان می دهد که ورودی معتبـر اسـت و هنگامیکـه سـپری شـد ورودی بطـور اتوماتیـک از انبـار محاسبات برداشته می شود.

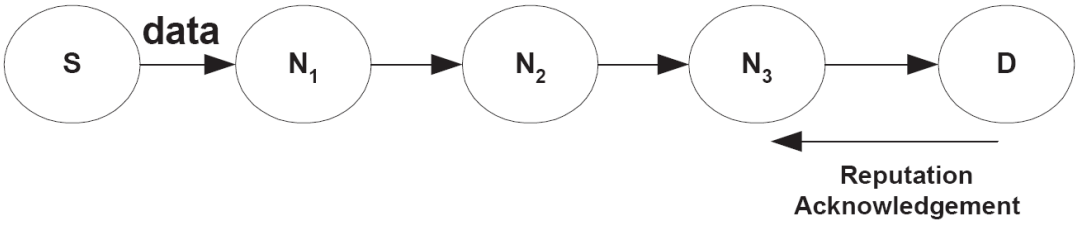
۲–۱–۱ روش های دیده بانی

اول. از همه، ما در طی این مقاله فرض می کنیم که گره های بی سیم را در نظر می گیریم مجهز به چند هم کنشگر IEEE ۸ .۲ .۱۱ هستند.

همانطور که قبلاً ذکر شد دیده بان مسئول مشاهده کردن صدور بسته های گره های همسایه است. این بسادگی یعنی این که اگر یک گره آ گره بی را دیه بانی می کند، دیده بان گره آ نسبت را نگه می دارد (تعداد بسته هایی که گره بی از گره آ دریافت کرده است و آنها را جلوتر فرستاده تقسیم بر تعداد کل بسته های دریافت شده از گره آ) و هنگامیکه سرحد از بیش تعریف شده رسید، این اطلاعات به مدیر محاسبات گره آ فرستاده می شود. در این بخش، دو روش دیده بانی را توضیح دادیم که توسط SAFE بکار گرفته شده بودند و اثرات متناظر آنها را روی این راه کار مقایسه کردیم.

۱- دیده بانی بر پایه تعداد توالی

این روش اجازه می دهد یک گره واسطه در یک مسیر اتلاف بسته انجام شده توسط گره بعدی (در مسیر) را به روشی مشابه راه کار تی ـ سی ـ پی محاسبه کند. به این منظور، برخی اعداد متوالی به بسته های فرستاده شده تخصیص داده می شوند. بدین ترتیب بسته های داده ها توسط منبع در طی مسیر فرستاده می شوند و اگر مقصد تشخیص داد که یک بسته گم شده است، پیامی به نام "اذعان محاسبات" خطرات منبع برای اطلاع دادن به گره ها در مسیر درباره این سوء رفتار می فرستد. در حقیقت، گره های واسطه جدیدترین تعداد توالی دریافت شده و همچنین تفاوت آن با آنکه قبلاً ذخیره می کند. هنگامیکه اذعان محاسبات فرستاده شده توسط گره های واسطه جدا می شوند و محاسباتی برای تأمین تعداد بسته اتلاف شده انجام می گیرند. برای نشان دادن این روش، اجازه دهید سناریوی توصیف شده در شکل ۲ را در نظر بگیریم.



شکل ۲-۲ زمینه

بخاطر سادگی بگیرد اجازه دهید فرض کنیم فقط یک داده از این مسیر عبور می کنـد. اجـازه دهیـد همچنین فرض کنیم که هر داده دارای یک آرایه است (از ۲ ورودی) جایی که جدیدترین عدد تـوالی بسته های دریافت شده و تفاوت آن با عدد توالی که قبلاً بود ذخیره می شود. در این مورد، الگـوریتم می تواند در طریق ذیل توضیح داده شود.

الگوریتم

اس ـ ام عدد توالی را نشان می دهد، دی تفاوت بین حد زیر عدد توالی دریافت شده و عدد قبل آن را در محلی را نشان می دهد.

مقادیر اصلی

اگر یکی از گره ها N۱ ، N۲ ، N۳ و D (برای مثال N۱) یک بسته جدید دریافت کند (با عدد توالی Smrecet) پس جایگزین عدد توالی بیشین می شود با گره جدید و جایگزین تفاوت با مقدار اختلاف می شود.

اگر این بسته تازه رسیده به گره دی برسد و اگر سرحد $\text{اس ـ ام}_{\text{جدید}} - \text{اس ـ ام}_{\text{قبلی}} >$

یک بسته گم شده و اذعان محاسبات باید فرستاده شود.

بعد از محاسبات به هنگام برای اولین بسته جدید مقدار تفاوت برای هر گره را دریافت کرد که توسـط این گره رسید مقدار تفاوت قبلی را بحساب نمی آورد.

تعداد توالی که در اینجا بکار می بریم در یک پروتکل اصلی بعنوان یک میدان جدید اضـافه شـده بـه پروتکل سردسته تلفیق می شود.

۲- دیده بانی بر پایه استراق سمع کردن

استراق سمع کردن بسادگی به دریافت یک بسته یا بخشی از یک بسته به گره دیگری فرستاده شـده دلالت می کند. هر چند این روش ([۵] ، [۶]) بهبود مهمی در عمل کرد شبکه نشان می دهد از قبیل نسبت تحویل دادن، میانگین تأخیر نهایی و کلی از برخی اشکالات از قبیل برخورد بسته و مصرف نیرو رنج می برد. استراق سمع بسته می تواند با استفاده از برخی کارت های PCMCH با حالت بی قاعده بدست آید. این آخری [۵] به حالت یک وفق دهنده شبکه بی سیم که در آن به همه ترافیک در یـک شبکه بی سیم در عوض فقط ترافیک به آن فرستاده شده گوش می دهد.

طریقی که استراق سمع بسته بکار می رود در مورد ما بطریق ذیل است: گـره آ دریافـت کننـده یـک بسته، آنرا بطرف گره بی می فرستد (طبق جدول مسیریابی آن) گره آ آن بسته را در انبار دیـده بـانی ذخیره می کند و سپس به صدورهای گره بی گوش می کند.

هنگامیکه گره بی یک بسته می فرستد. گره آ این بسته را استراق سمع می کند و آنرا با یکی که قبلاً در انبار دیده بانی ذخیره شده مقایسه می کند. اگر با هم جفت شوند، پس این بسته بطور اتوماتیک از نهانگاه برداشته می شود. اگر زمان قبلاً تعریف شده قبلاً سپری شده و گره آ هنوز سر جمع بسـته ای را که گره بی فرض شده بود بفرستد را ندارد نسبت (بسته های دریافت شده / تعـداد بسـته هـای فرستاده شده) به روز می شود. نسبت محاسبه شده بطور منظم به مدیر محاسبات فرستاده مـی شـود همانطور که قبلاً توضیح داده شد.

۲–۲ آی ـ وی شبیه سازی

***پیکربندی شبیه سازی**

شبیه ساز شبکه MS۲ (ویرایش ۲۸. ۲) برای راندن شبیه سازی های مختلـف، و اجـرای دی ـ اس ـ کیو تهیه شده، راه کار SAFE بکار رفت. راه کار SAFE بکار برنده حالـت بـی قاعـده (یعنـی روش استراق سمع، بخش IIIB) با SAFE + QM در بقیه این مقاله نشـان داده خواهـد شـد، بهرحـال، هنگامیکه روش تعداد توالی (بخـش IIIA) بکـار رفـت، راه کـار SAFE بـه عنـوان SAFE + SN منسوب خواهد شد.

چندین شبیه سازی با استفاده از سناریوهای مختلف و برای هر دوی SAFE + PM و SAFE + SN هدایت شدند. هر شبیه سازی حـداقل بمـدت ۲۰ دقیقـه رانـده شـد، و میـانگین تصـاویر همـه شبیه‌سازی ها برای تأمین نتایج معتبرتر بکار می روند. هر گره دارای باقی (میانگین) فرستاده به اندازه ۶۴ است (جائیکه بسته ها قبل از فرستاده شدن به صف می شوند) و از حد نسـبت اسـمی ۲۵۰ متـر استفاده می کند.

تحرک گره ها با مدل تحرک، سرعت و "زمان مکث" مشخص می شود. مدل تصادفی نقطـه ضـروری [۱۰] بعنوان یک مدل متحرک در یـک میـدان $۱۰۰۰\times۱۰۰۰m^۲$ مسـتطیلی انتخـاب مـی شـود. بـا استفاده از این مدل متحرک، هر حرکت یک خط مستقیم بین یک نقطه آغـاز و یـک نقطـه دریافـت است، که با سرعت ثابتی تحت پوشش قرار می گیرد. آخری (سرعت) بطور تصادفی با استفاده از توزیع یکنواخت بین و $۲۰m.s^{-۱}$ برای هر حرکت انتخاب می شود. بدین ترتیب، هر چه زمان مکث بیشـتر است، تحرک گره کم تر است. ما از ۵ زمان مکث مختلف اسـتفاده مـی کنـیم: ۰، ۱۰۰، ۳۰۰، ۶۰۰ و ۹۰۰ ثانیه.

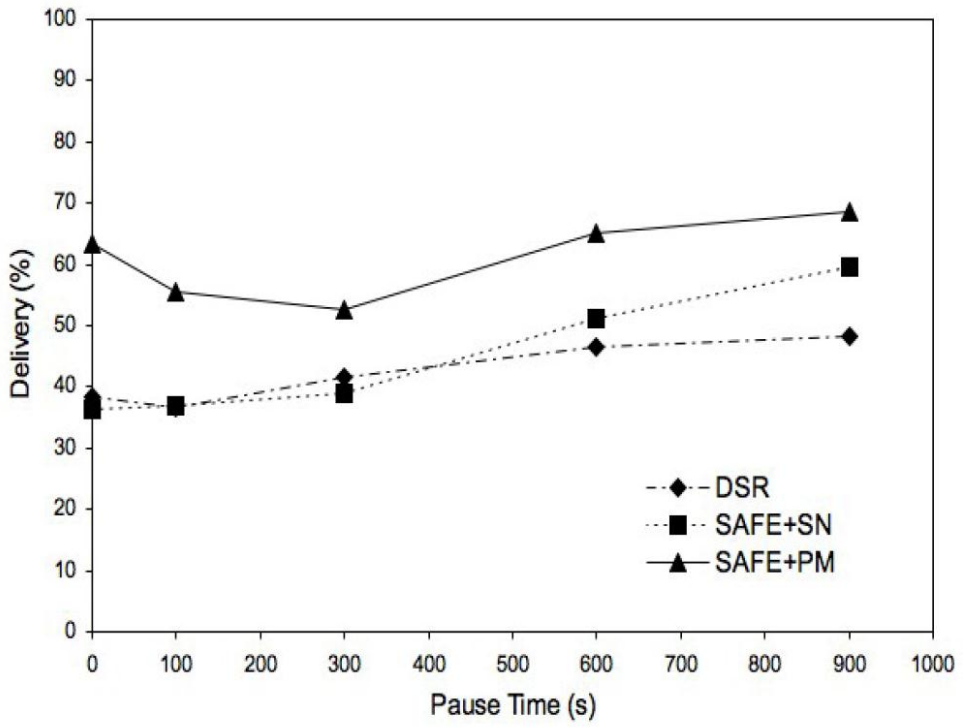
در کل ۵۰ گره وجود دارد، که از میان آنها ۱۵ گره مخـرب هسـتند. مـا از ۵ اتصـال CBR اسـتفاده می‌کنیم، بسته های ۶۴ بیتی با نسبت فرستادن $۴pkts.s^{-۱}$ می فرستیم: پهنای باند $۲Mb.s^{-۱}$ است

گره های مخرب به طریق ذیل اجرا می شود: آنها میانگین ۹۵٪ بسته های وصل شده CBR را کاهش می دهند، و منطقه دقیق کاهش بین یک حداکثر (نسبت حداکثر در مورد ما ۱۰۰٪) بطور تصادفی انتخاب می شود. و یک حداقل (نسبت حداقل، در مورد ما ۹۰ ٪) منطقه کاهش. منطقه های کاهش بعد از یک دوره بطور تصادفی انتخاب شده بین ۰ و ۲۵ ثانیه تغییر می کنند. بهرحال، گره های غرب بسته های مسیریاب DSR را رها نمی کنند. در واقع، یک گره مخرب کاهش دهنده همه بسته ها برای این شبکه بسیار کمتر خطرناک است. اگر گره مخرب بسته های مسیریابی را هم کاهش کاهش دهد، فرآیند پیدا کردن مسیر DSR هرگز قادر نخواهد بود هیچیک از آنها را در یک مسیر شامل کند، چون گره های مخرب هرگز به درخواست های مسیر پاسخ نخواهند داد. [۷]. بدین ترتیب هرگز قادر نخواهند بود هیچ بسته داده ای را رها کنند. به عنوان یک پیامد، اجرای گره های مخرب ما، به آنها اجازه نمی دهد بسته های مسیریابی را رها کنند، این راه کار SAFE بیشتری را چاش خواهد کرد.

برای ارزیابی SAFE + PM و SAFE + SN، ما معیارهای ذیل را در نظر می گیریم: نسبت تحویل بسته، سرجمع مسیریابی، تأخیر سر به سر میانگین و ظرفیت پذیرش ([۹] و [۱۰]). نسبت تحویل بسته کسری از بسته داده های تحویل شده به مقصد است. سرجمع مسیریابی نسبت فرستادن یا مسیریابی رو به جلو بسته ها از طریق بسته های داده های تحویل شده است (یعنی بسته های ایجاد شده توسط اتصال های CBR در مورد ما)، بدین ترتیب هزینه در مقایسه با نسبت افزایش. ظرفیت پذیرش به عملکرد اندازه گیری شده واقعی سیستم هنگامیکه تأخیر در نظر گرفته می شود است. در نتایج شبیه سازی، معیارهای ظرفیت پذیرش به مقدار میانگین طبق هر گره مرتبط است، سرانجام تأخیر میانگین مرحله پنهانی یک طرفه میانگین مشاهده شده بین یک بسته فرستاده شده و دریافت شده را نشان می دهد.

*** مطالعه مقایسه**

شکل ۳ نسبت تحویل برای سناریوی شبیه سازی بالا را نشان می دهد. راه کار SAFE+PM بهتر از DSR و SAFE+PM در رابطه با تعداد بسته های به درستی تحویل شده به مقصد عمل می کنـد. در مقایسه با DSR ، SAFE+PM نسبت تحویل بسته با تقریباً ۲۵٪ بهبود می یابد. از طرف دیگر، SAFE+SN عملکرد ضعیفی با در حدود درصد تحویل بسته بعنوان DSR اصلی، به استثنای شبکه های بسیار ایستا که در آنجا بهتر عمل می کند را نشان می دهد.

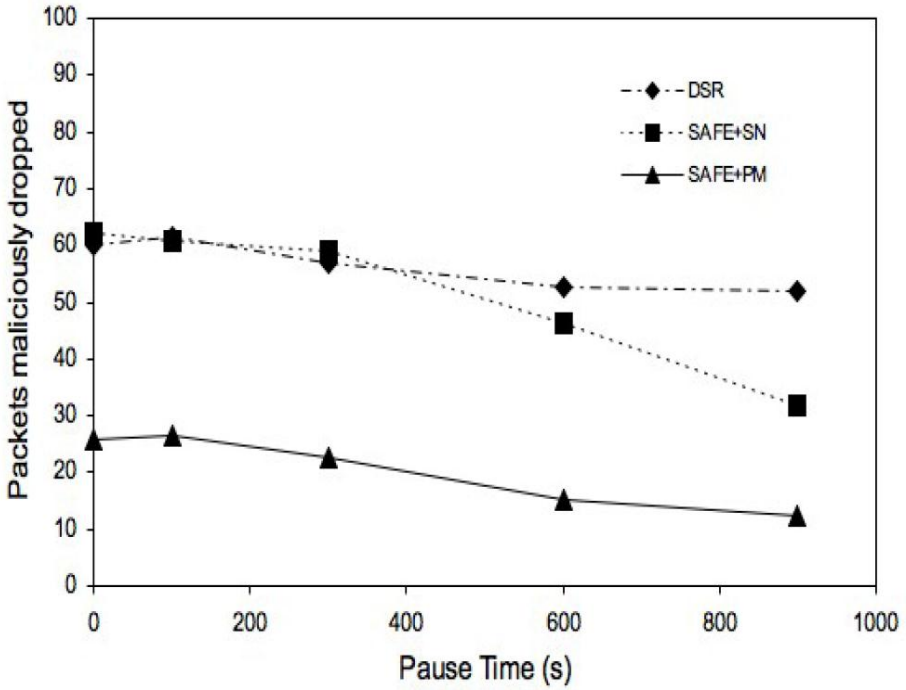


شکل ۲-۳ مقایسه نسبت تحویل بسته

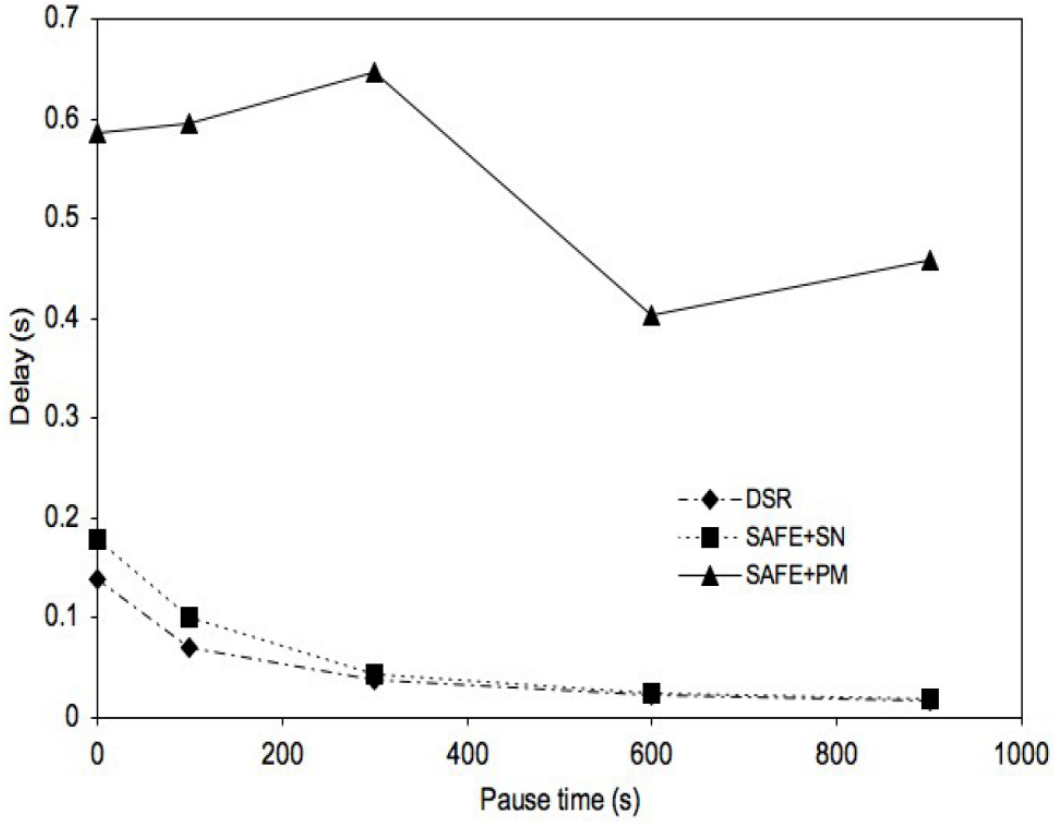
SAFE+SN هنگامیکه یک سیستم پایش سرتاسر را بکاری بود از مشکل ذکر شـده رنـج مـی بـرد ([۴] و [۳]). هر چه گره ها پویاتر باشند. مسیر داده ها بیشتر تغییر می کند، بـدین ترتیـب پـایش را منقطع می کند. دلیل دیگری برای آن، آن است که راه کـار SAFE+SN در اثـر سـاختار آن، الـزام دارد که برخی از داده ها از طریق گره های مخرب عبور کنند. برای مثال، اگر منطقـه رهـا کـردن در ۱۰۰٪ قرار گیرند، SAFE+SN تقریباً هیچ اثر مثبتی روی (تأخیر کوتاهتر، تحویل بالاتر، سر جمـع

کوچک تر...) عملکرد DSR نخواهد داشت. چون ما دارای منطقه رها کردن متغیـر بـین ۹۰ و ۱۰۰٪ داریم، اثرات مثبت SAFE+SN نسبتاً کاهش می یابند.

درصد بسته های رها شده توسط گره های مخرب اگر SAFE+PM بکار رود بطور زیادی کاهش می یابد، ما در حدود ۴۰٪ رها کردن بسته کمتر توسط گره های مخرب داریم، همانطور کـه در شـکل ۴ نشان داده شده است. بهرحال، کشف یک مسیر ثانوی که هنگامیکه دوباره رهـا مـی شـود تـا از کـره مخرب پرهیز کند، فاز کشف مسیر DSR هر دفعه فوراً پیشرفت نمی کند. اصولاً، اگر گره مخـرب در مسیر پاسخ دریافت شده توسط گره منبع شامل باشد، فاز کشف مسـیر تـا مسـیری کـه شـامل گـره مخرب نیست پیدا شود تکرار می شود. بعنوان یک پیامـد، در مـورد SAFE+PM همـانطور کـه در شکل ۵ نشان داده شده، تأخیر سرتاسر نسبتاً با اهمیت اسـت. پیامـد دیگـر ایـن کشـف هـای مسـیر متعدد، سرجمع مسیریابی SAFE+PM است. بنابراین، در ایـن مـورد سـرجمع و تـأخیر بسـته بـه کارآیی کشف مسیر در پرهیز از گره های مخرب پیامد منحصر بفردی است.



شکل ۲-٤ بسته های داده افتاده شده توسط گره مخرب

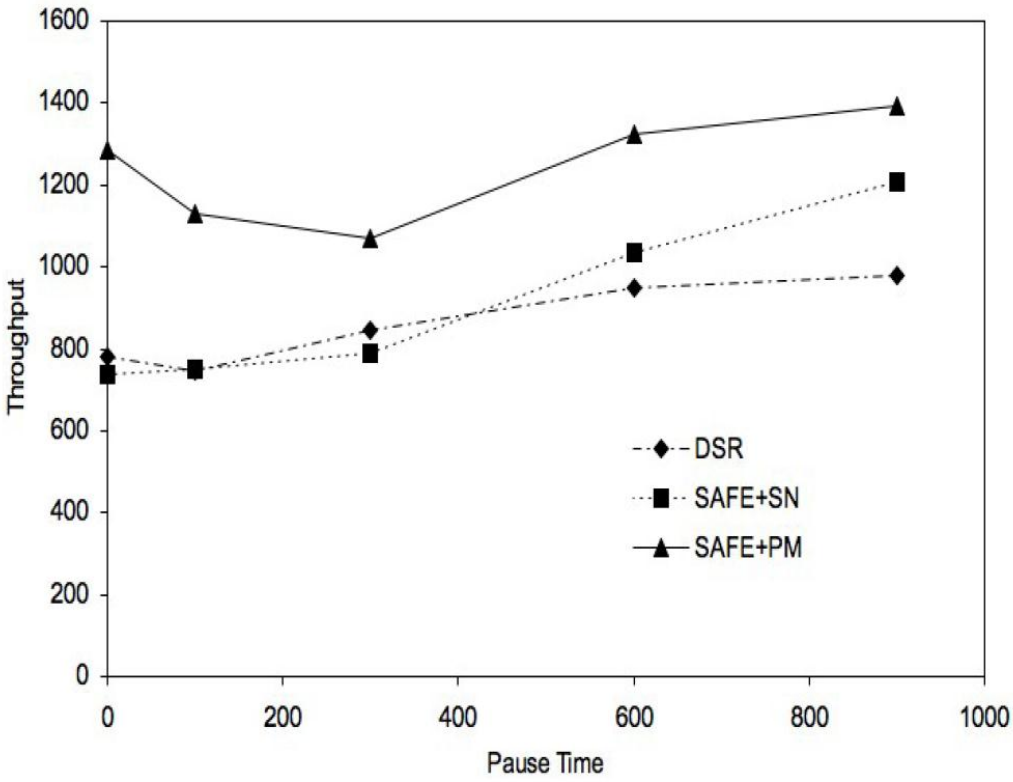


شکل ۲-۵ مقایسه تاخیر سرتاسر

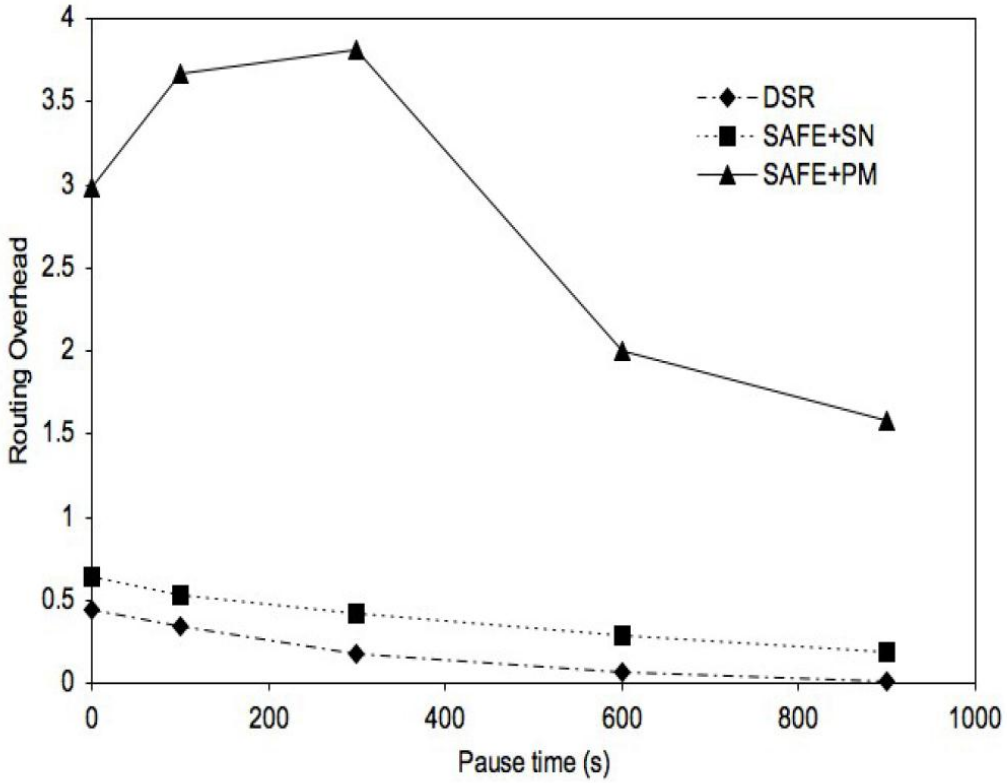
بـه روشـی مشـابه، ظرفیـت پـذیرش در شـکل ۶ رسـم شـده و سـرجمع در شـکل ۷، هنگامیکـه SAFE+PM اعمال می شود، ظرفیت پذیرش بطور واضح بهبود مـی یابـد. SAFE+PM فقـط در شبکه های بسیار ایستا عمل می کنند، به همان دلیل که مثلاً توضیح داده شد. مشاهده می کنیم که سرجمع مسیریابی خیلی بزرگتر از SAFE+SN بخصـوص در شـبکه هـای بسـیار پویـا اسـت. ایـن سرجمع اصولاً در اثر تعداد فرآیندهای کشف مسیر تحریک شده توسط راه کـار SAFE+PM بـرای تحقیق برای مسیری بدون گره های مخرب است.

راه کار SAFE پروتوکل های مسیریابی را قادر می کند حمله های رها کـردن بسـته را کشـف را در شبکه های ویژه کشف کنند. این کشف با استفاده از یک مدول دیده بانی که صدور بسـته گـره هـای

همسایه را نظارت می کند بدست می آید. دو روش دیده بـانی را ارائـه داد شـده و مطالعـه شـده کـه مبتنی بود بر برخی نتایج شبیه سازی اثر آنها روی عملکرد راه کار SAFE.



شکل ۲-۶ مقایسه ظرفیت پذیرش



شکل ۲-۷ مقایسه سر جمع

متکی بودن به مسافت امن برای بدست آوردن عضویت گروه قابل

۲–۳ تقسیم بندی در شبکه های ویژه

طراحی کاربردهای متحرک ویژه اغلب احتیاج به در دسترس بودن دیدگاههای پیگیر از حالت کاربر در میان میزبانان شرکت کننده دارد. چنین دیدگاههایی مهم هستند چون کارهای برنامه ریزی و ارزیابی را آسان می کند. ما استدلال می کنیم که جلوگیری از انجام گرفتن قطع شدن اعلام نشده برای ساختن و حفاظت دیدگاهی پیگیر در محیط متحرک ویژه اساسی است. با در نظر گرفتن این، ما مشخصاتی برای خدمات عضویت یک گروه قابل تقسیم بندی پشتیبان کاربردهای متحرک ویژه ارائه می دهیم و پروتوکلی برای اجرا کردن این خدمات پیشنهاد می کنیم. یک خصوصیات منحصر بفرد این عضویت گروه قابل تقسیم بندی آن است که پیام های فرستاده شده بین اعضای گروه تضمین می شوند که بطور موفقیت آمیزی با مفروض بودن فرضیات سیستم مناسب، تحویل داده شوند. این خصوصیت علیرغم حرکت و قطع شدن مکرر طی زمان حفاظت می شود. این پروتوکل گروهها را از هم جدا کرده و ترکیب می کند و یک نمودار اتصال منطقی بر مبنای اندیشه مسافت امن نگه می دارد. برای آزمایش کردن، اجرایی از پروتوکل در جاوا موجود است. این کار در اجرایی از لایم، یک میان افزار برای تحریک که از شریک بودن شفاف داده ها را در محیط های سیم کشی و بی سیم ویژه پشتیبانی می کند بکار می رود.

عضویت گروهی مشکل بزرگی در زمینه محاسبه تعمیم یافته مدارا کننده با کاستی بوده است و موضوع ارزیابی گسترده ای بوده است، حل کردن این مشکل به پیش بینی یک سرویس که نوعی موافقت بین مؤلفه های شرکت کننده درباره این که چه کسی در حال حاضر در گروه است برقرار و حفاظت می کند طی زمان و بین مؤلفه های شرکت کننده علیرغم حضور یا کاستی ها در سیستم تعمیم یافته متناظر احتیاج دارد. یک چنین سرویس عضویت گروهی توسعه بسیاری از کاربردهای تعمیم یافته اغماض کننده کاستی را ساده می کند و بطور گسترده ای برای حمایت معتبر ارتباطهای گروهی بکار می رود.

ما در محیط های متحرک ویژه در تلاش برای حمایت از محاسبه گروهی بـا شـکل عضـویت گروهـی مواجه شدیم. برای کاربردهای متحرک ویژه همکاری گروهی یـا فـرد بـه فـرد زمینـه هـای متـداولی هستند. هنگامیکه دو میزبان متحرک یا بیشتر برای تشکیل یک گروه کاری دور هم جمع می شـوند، بعضی مواقع برای کلیه آنها اساسی است که دارای دیدگاه یکسـانی دربـره حالـت محاسـباتی متصـل باشند هنگامیکه شروع به کار می کنند یا هنگامیکه برخی اعضا گروه را ترک مـی کننـد. یـک قطعـه مهم از اطلاعات وضعیت گروه، عضویت در گروه است، یعنی چه کسی در گـروه کـاری هسـت و چـه کسی نیست. هر موقعیتی که خواستار (به دلایل فنی یا قانونی) حضور دو یا تمامیت شخص یا بیشـتر است تا کاری انجام شود مورد احتیاج برای دیدگاه عضویت پیگیر را تحمیل کند. می توان پیش بینی تصور پیشروی از یک شـاهد الکترونیکـی از یـک معاملـه قـراردادی یـا شـرایطی کـه در آن حفاظـت روزمره ی هواپیمای تجاری الزام به واقعه نگاری امن بـا حضـور یـک بـازرس اف ـ آ ـ آ حامـل نشـان الکترونیکی مجاز دارد را داشت. الزام برای یک دیدگاه پیگیر در میان اعضای گروه همچنین در زمینه سیستم های اتصال باهوش بوجود می آید. راندن سیستم های کمکی علاوه بر شبکه ویـژه بـی سـیم متحرک برای هشدار تصادف و جلوگیری توسعه می یابند . در چنین سیستم هایی، دیدگاههای پیگیر درباره وسایل نقلیه شرکت کننده و تصمیم های پیگیر در میان اعضاء درباره سرعت، کـاهش سـرعت، تعبیر خط (مسیر) و غیره بحرانی است، اهمیت موافقت کردن درباره دیدگاه یکسـان دربـاره موقعیـت عضویت الزام برای خدمات عضویت گروهی را که دیدگاهی پیگیر درباره عضویت بین اعضای گروه نگه می دارید را ارائه می دهد.

مشکل عضویت گروهی که در محیط ویژه متحرک مواجه می شویم به مفهومی که دارای الزامات ویژه ای است که مخالف آنهایی هستند که قبلاً مطالعه شدند، جدید است. نه تنها احتیاج به موجود بودن و پیشرفت در حضور قسمت های شبکه است، مثل اکثر خدمات عضـویت گروهـی قابـل تقسـیم بنـدی هنگامیکه تقسیم بندی انجام می گیرد احتیاج به پیگیـری دارنـد کـه هیچیـک از خـدمات عضـویت گروهی قابل تقسیم بندی قبلی از آن پشتیبانی نمی کند . دلیل این که چرا خدمات عضویت گروهـی

قابل تقسیم بندی قبلی از پیگیری در حضور تقسیم بندی ها حمایت نمی کنند بنیادی است، چون مدل سیستم فرض شده غیر همزمان است و تعمیم یافته، موافقت و رضایت عمومی غیرممکن است. علاوه بر این، تقسیم بندی شبکه در یک شبکه ثابت معمولاً غیر مکرر و کم دوام است. این آزمایش دستی را انتخابی با دوام تر برای حل کردن هر بی ثباتی که ممکن است طی تقسیم بندی شبکه اتفاق افتد می کند. با این وجود، در مورد ما، تأکید می کنیم که الزام پیگیری چون تقسیم بندی شبکه در محیط های ویژه متحرک رویدادی مکرر است و هزینه بی ثباتی "کوتاه مدت" در زمینه های محاسباتی متحرک خیلی زیاد است. میزبان های متحرک در گستره وسیعی متقابلاً اثر می کنند، و بی ثباتی می تواند بطور بی نهایت گسترش پیدا کند و سبب صدمه غیر قابل جبران در عملکردهای بحرانی شود. پیگیری محض مشابه توسط کریستاین برای مشکل عضویت گروهی اولیه در سیستم های همزمان در نظر گرفته شده اند. امّا برای مشکل عضویت گروهی قابل تقسیم بندی ارزیابی شده‌اند.

هدف خدمات عضویت گروهی ما فقط ایجاد کردن دیدگاهی پیگیر از عضویت گروهی بین شرکت کننده ها نیست، امّا همچنین کمک به کاربرها و برنامه نویس های کاربرد برای پرهیز از پیچیدگی های ارائه شده با بی ثباتی بالقوه سبب شده توسط کاستی های حلقه القایی تحریک است.

کاستی های حلقه القایی متحرک به کاستی های ارتباطی بوجود آمده توسط واحدهای متحرک با خارج شدن از محدوده مخابراتی یکدیگر است مشخصه کلیدی یک کاستی حلقه القایی متحرک آن است که قابل بازیافت نیست و نسبت به کاستی های حلقه در شبکه های ثابت صدمه زننده تر است. برای مثال، یک پیام فرستاده شده در حالیکه یک تقسیم بندی شبکه فیزیکی در حال انجام شدن می تواند در حالت مشکوک تحویل دادن باشد. یعنی، یک طرف (فرستنده / گیرنده) فکر می کند "تحویل داده شده" و طرف دیگر (گیرنده / فرستنده) فکر می کند که تحویل داده نشده است. برای بدتر کردن موضوع، هیچ گاه راه کاری برای رفع ابهام از این موفقیت وجود ندارد. کاستی های حلقه انجام گرفته در شبکه های ثابت معمولاً قابل بازیافت هستند به این مفهوم که ارتباط برقرار کننده ها همیشه

می‌توانند از یک پروتوکل مبتنی بر دوباره فرستادن خبر وصول مثل تی ـ سی ـ پی برای اطمینان یافتن از این که یک تصور حلقه ناپایدار است چون در یک شبکه ثابت هر حلقه از کار افتاده ای "سرانجام باز می گردد". بازیافت ناپذیری قصور حلقه القاء شده متحرک می تواند منجر به بی ثباتی دائمی داده ها می شود و چالش بزرگی برای برنامه نویس های کاربرد متحرکی تحمیل می کنند. خدمات عضویت گروهی ما سعی در کمک کردن به برنامه نویس ها در این مورد با تضمین این که ارتباط بین اعضای گروه از قصول القاء شده متحرک رخ نخواهد برد.

الزامات شدید خدمات عضویت گروهی جدید اجرا در سیستم های نافرمان را غیر ممکن است. برای قابل حل شدن این شکل عضویت گروهی شدید در مدل سیستم خود سطحی از فرمانی را ارائه کردیم. فرض می کنیم که سرویس مخابرات در هر تقسیم بندی شبکه فیزیکی قابل اطمینان است و دارای زمان تحویل پیام t_d محدودی در تقسیم بندی است. علاوه بر این، همانطور که قبلاً ذکر کردیم یک پیام فرستاده شده در زمان $t < t_d$ بیش از این که یک طبقه بندی فیزیکی شبکه انجام گیرد می تواند در حالت مشکوک تحویل پیام باشد. با یک مفهوم کلیدی بنام مسافت امن برای حل این مشکل عرضه می کنیم. با جلوگیری از پیام گروه به افتادن در بسته ناثباتی شبکه سبب شده تقسیم بندی کار می کند. ما به اطلاعات موقعیت برای تصمیم درباره هنگامیکه یک میزبان در حدود ارتباط از یک گروه حذف شده یا توسط آن پذیرفته شده احتیاج داریم. سیاست عضویت گروهی در ماهیت محتاطانه است برای اطمینان از این که تغییرات در عضویت گروهی به نظر می رسد بسیار کوچک باشند یعنی فعل و انفعالات قابل طبقه بندی شدن هستند، الگوریتم، ادغام گروهها و تقسیم بندی یک گروه را در یک گروه از هم گسیخته متعدد گرد می آورد.

با ویرایشی از پروتوکل عضویت گروهی قابل تقسیم بندی قوی در جاوا را اجرا کرده ایم. از لایم یک افزار برای توسعه سریع کاربردهای متحرک پشتیبانی می کند. اگر فرضیات سیستم پروتوکل مواجه شوند اجرا بخوبی کار می کند. اعتبار فرضیات سیستم و چطور آنها می توانند اجرا شوند.

در بخش بعدی، ما رسماً الزامات سیستم و تعریف خـدمات عضـویت گروهـی را مشـخص مـی کنـیم. مفهوم مسافت امن را معرفی می کنیم و استراتژی راه حل خود را برای مشکل عضویت گروهـی ارائـه می دهیم. بخش ۴ اجرایی از پروتوکل ما را توضیح می دهـد. بخـش ۵ تحلیـل هـایی از رابطـه بـین مسافت امن، تأخیر شبکه، و سرعت میزبان متحرک ارائه می دهد.

۲–۳–۱ شناسایی مشکل

هدف نهایی ما تأمین توانایی حفاظت یک ساختار داده های جامع در یک زمینه که در آن میزبان های متحرک ضمن این که درگیر فعالیت های همکارانه موقت هستند می آیند و بـی رونـد بـرای توسـعه دهندگان کاربرد است. در این زمینه خدمات عضویت گروهی الزام به ارائه تصویری دقیـق و فـوری از دیدگاه خصوصیت کلیه اوقات دارد و یک پیام اطمینان حاصل کرده در یک دیدگاه باید تضـمن شـود به اعضاء در آن دیدگاه تحویل داده شود، علیـرغم تحـرک و قطـع شـدن هـای القـایی حرکـت، ایـن خصوصیت خدمات عضویت گروهی را برای بسیاری از کاربردهای متحرک سودمند می کنـد. از قبیـل آنهایی که قبلاً ذکر شدند. بعداً، ما در جستجوی مشخص کردن مشکل عضویت گروهی هستیم.

مشخصات عضویت

خدمات عضویت گروهی می توانـد بـا مشـخص کـردن حالـت محلـی متغیرهـا و ایمنـی و پیشـرفت خصوصیاتی که آن را قانع می کنند مشخص می شود. ما از واژگان و یادداشت شـبیه بـه آنهـایی کـه کریستان بکار برده [۲۷] برای مشخص کردن این خصوصیات اسـتفاده مـی کنـیم. اجـازه دهیـد کـه مجموعه ای از میزبان ها باشد که طی زمان وجـود دارنـد. فـرض مـی کنـیم هـر میزبـان دارای یـک شناساگر منحصر بفرد علامت گذاری شده با i است و کشیده شده از آن چه مجموعه اعداد Z^+ و همه گروههایی که طی زمان موجود هستند. شناساگر را از مجموعه G بکشید. هر میزبان در P متغیرهای حالت دو در ذیل را نگه مـی دارد: g و $g.\pi$ شناسـاگر گـروه اسـت و π زیـر مجموعـه P اسـت. π

همچنین دیدگاه عضویت Q خوانده می شود، یا "دیـدگاه" بطـور کوتـاه. اجـازه دهیـد $T=[۰,\infty)$، زمان باشد. دو تابع برای ساده کردن جمله بندی مشخصات معرفی می شوند.

$$\text{گروه}: P\times T\rightarrow G$$

$$\text{عضو}: P\times T\rightarrow ۲^{P}$$

(p,t) گروه شناساگر گروه برای میزبان p در زمـان محلـی t را ببـار مـی آورد؛ mem (p,t) دیـدگاه محلی p' عضو π در زمان t را ببار می آورد. ما یک گروه را g می خوانیم اگر شناساگر آن g باشد. g' را یک جایگزین گروه g می نامیم اگر یک عضو p از g وجود دارد بطوری که گـروه بعـدی p ملحـق شده بعد از ترک g، g' یک اسـت. مثـل [۲۷] succ (g , p) بـرای نشـان دادن جـایگزین گـروه g نسبت به میزبان p بکار می رود. pred (g , p) برای نشان دادن گروه پیشین g نسبت به p بکار می رود. با مفروض بودن این واژه ها، خدمات عضویت گروهی به حالت ذیل مشخص می شود:

- خودگیری: یک میزبان همیشه بخشی از دیدگاه عضویت آن است یعنی $p\in mem(p,t)$
- یکنواختی محلی: شناساگرهای گروهی نصب شده روی هر میزبـان در ترتیـب افزایشـی هسـتند. یعنی $pred(g,p)<g<succ(g,p)$
- دیدگاه عضویت اولیه: یک میزبان همیشه خود را بعنوان فقط عضو در دیدگاهخهود هنگامیکه آغاز کرد نصب می کند یعنی $mem(p,t_{init})=\{p\}$
- استدلال عضویت: اگر میزبان های p و q دارای شناساگر گروهی یکسان باشـند پـس آنهـا دارای دیدگاههای یکسان هستند: یعنی

$$\text{گروه}\ (p,t_p) = \text{گروه}\ (q,t_p) \Rightarrow mem\ \ (p,t_p)$$
$$= mem\ \ (q,t_p)$$

- عضویت توجیه را تغییر می دهد: جایگزین گروه g در رابطه با p یا زیر مجموعه مناسـب یـا زیـر مجموعه مناسب گروه g است.

- تحویل پیام دیدگاه یکسان: اگر میزبـان پیـام m_{pq} را ∞ میزبـان p در زمـان t بفرسـتد، و q در $mem(p,t)$ اسـت، پـس m_{pq} ضـمانت مـی شـود کـه بـه q در زمـان t' تحویـل داده شـود و $mem(q,t')=mem(p,t)$. توجه کنید که این خصوصیت بطور سنتی در خدمات ارتبـاطی گروه شامل است ([۱۰]، [۱۸]) بجای خدمات عضویت گروهی ([۱۰]، [۱]). ما بعداً توضـیح مـی دهیم چرا آنرا اینجا شامل کردیم.
- یکپارچگی محدود شرطی: p را متعلق به گروه g_1 و q را متعلق به گروه g_2 قـرار دهیـد. فـرض کنید g_1 و g_2 تنها دو گروه اقناع کننده معیار ادغام در زمان T است (مبدأ توصـیف مـی شـود). ثابت زمانی T_c این دو گروه به یک گروه ادغام می شوند، یعنی

$$\exists t_p, t_q \in [T, T+T_c], mem(q,t_q)=mem(p,t_p)$$

- انشعاب گروه شرطی: یک گروه فقط وقتی لازم باشد انشعاب می کنـد. یعنـی هنگامیکـه شـرایط انشعاب مواجه شود (بعداً توضیح داده می شود)

دو الزام ایمنی اوّل برای اکثر مشخصات عضویت گروهی قابل تقسیم بندی متداول هستند الزام سـوّم در مشخصات ما، الزام دیدگاه عضویت اولیه از اکثر آنها در توضیحات متفاوت هستند [و نسبتاً منحصر بفرد است، فراهم شده برای محیط های متحرک ویژه: یک میزبان متحرک ممکن است بدون آگاهی از سایر میزبان ها در جهان آغاز کند. توجیه تعبیر عضویت برای اطمینان از تداوم در خصوصـیات تغییـر دیدگاه ارائه شده است.

الزام تحویل پیام دیدگاه یکسان برای افزودن قابلیت پیش بینی بیشتر بـه خـدمات عضـویت گروهـی برای برخی کاربردها عرضه شد . ما این خصوصیت منحصر بفرد، توسعه دهندگان کاربرد با استفاده از خدمات اطمینان می دهند که تحویل پیام در قلمرو ایـن دیـدگاه معتبـر اسـت. بـه گفتـه دیگـر، در محدوده دیدگاه دیگر لازم نیست برنامه نویس ها درباره پیچیدگی بالقوه ناسازگاری های سـبب شـده توسط اتلاف پیام در اثر تحرک نگران باشند. توجه کنید که این خصوصیت (یا یکی شـبیه آن) بطـور سنتی در خدمات ارتباط گروهی بجای خدمات عضویت گروهی شامل است. دلیل این که آنرا این هـا

شامل می کنیم بالا بردن خدمات عضویت گروه با خصوصیت لازم توسـط کاربردهـای هـدف کـه بـه خدمات ارتباط گروهی احتیاج ندارد.

یکپارچگی نهایی شرطی و انشعاب گروهی شرطی برای پرهیز از شـکل کلاسـیک "انشـعاب دِمُـدی" عرضه شده اند. بدون احتیاج به یکپارچگی محدودیت، اجرای عضویت گروهی می تواند بسادگی هـیچ ادعای از گروهها انجام ندهد و با این حال با نگه داشتن همه گروهها بصورت منفرد مشخصات را قـانع کند. توجه کنید که در این مشخصات ما صریحاً نگفتـیم کـه ضـوابط ادغـام و ضـوابط انشـعاب چـی هستند. ضوابط ادغام و انشعاب، بطور کلی به کاربرد بستگی دارند. در این مقاله امـن از ضـعیف تـرین ضوابط ادغام و انشعاب استفاده می کنیم. ضابطه ادغام به این مفهـوم ضـعیف تـرین اسـت کـه فقـط خصوصیات عضویت گروهی احتیاج دارد تا برای گروه جدید راضی باشد. ضابطه انشعاب به این مفهوم ضعیف ترین است که گروه انشعاب می کند اگر خصوصیت عضویت گروه نتوانـد بـدو انجـام دادن آن تضمین شود. هیچ شرط دیگری خارج از مشخصات عضویت اجبار به ماندن دارد.

۲–۳–۲ مدل سیستم

مدل سیستم ما فرض می کند که شکست های فشرده میزبان وجود نـدارد و هـیچ حـذف و شکسـت عملکردی با تراکم شبکه بوجود نیامده است. تنها شکست در مدل سیسـتم مـا توسـط بیـرون رفـتن میزبان ها از محدوده ارتباط یکدیگر است. این مدل، یک مـدل معتـدل آغـازین بـرای سیسـتم هـای متحرک ویژه به دو دلیل است. ابتدا، قطع شدت در اثر تحرک نسبت بـه شکسـت فشـرده میزبـان بـا مفروض بودن جریان سخت افزار و تکنولوژی نرم افزار بسیار مکررتر است. دوماً، یک شبکه متحرک در تئوری می تواند با پهنای باند کافی برای ارتباط لازم توسط کاربرد علاوه بر آن مجهز شود، بطوری که تراکم بتواند در مقایسه با انجام گرفتن تقسیم بندی به رویدادی نادر تبدیل شود.

مدل سیستم ما همچنین فرض می کند که خدمات ارتباط اصلی معتبر و بهنگام است [۲۹]، بـه ایـن مفهوم که یک پیام اطمینان یافته از آن تضمین می شود که در محدوده زمانی t_d تحویل داده شود،

اگر فرستنده و دریافت کننده طی این زمان بطور فیزیکی یکدیگر متصل باشند. منظور ما این است که میزبان ها یا در محدوده ارتباطی یکدیگر هستند یا بطور مجازی از طریق میزبان ها دیگری وصل شده اند. برای آسانی، فرض می کنیم که کلیه میزبان ها دارای شعاع ارتباطی یکسانی هستند و حلقه های ارتباطی دو سویه هستند. همچنین فرض می کنیم که کلیه میزبان ها در همه اوقات از مکان فیزیکی خود آگاهی دارند. فرض می کنیم هیچ اطلاعی از الگوهای تحریک میزبان هـای متحـرک نـداریم بـه استثنای این که حرکت در فضا متداوم است و دارای برخی محدودیت های V_{max}در سـرعت هسـتند. ما عملاً این مورد مفرط را برای کشف محدودیت های تحمیل شده روی مشکل عضویت با تحرک ویژه تصادفی انتخاب کردیم. کلاسیک حامی استراتژی راه حل ما در بخش بعدی توضیح داده شده اند.

استراتژی راه حل:

کلیه استراتژی ما در اجرای عضویت گروهی قوی تصور مسافت امن بین میزبـان هـا و گروههـا اسـت یعنی این ایده که اگر میزبان ها به اندازه "کافی نزدیک" باشند برای مدتی قطـع شـدن امکـان پـذیر نیست و اگر که آنها فقط نه اندازه "کافی دور" هستند زمان کافی برای تغییر پیکره بندی قبل از قطع شدن وجود دارد. به گفته دیگر ما یک نمودار اتصال منطقـی روی اتصـال فیزیکـی رسـم مـی کنـیم بطوری که لبه ای در نمودار منطقی ظاهر می شود اگر و فقط اگر دو میزبان نشان داده شده با تـارک های متناظر در محدوده مسافت امن هستند. عضـویت گروهـی تقسـیم بنـدی هـا در نمـودار اتصـال منطقی را منعکس می کنند بجای تقسیم بندی ها در نمودار اتصال فیزیکی، در باقیمانده این بخـش، مفهوم مسافت امن را توضیح می دهیم و کشف و پیکربندی پروتوکل ها را ارائه می دهیم.

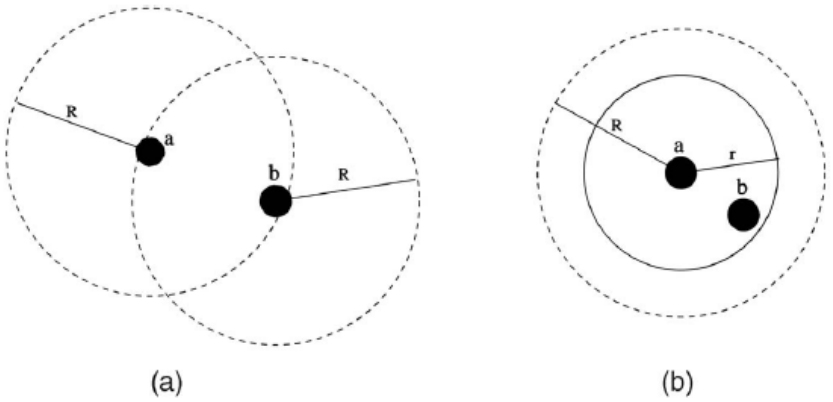
مفاهیم کلیدی: مسافت امن

با مفروض بودن دو میزبان متحرک مجهز با فرستنهای بی سیم سازگار بُرد برابر R_1، بیان مـی کنـیم که ساخت بین آنها یک مسافت امن است اگر از یک مقدار آغازین $r(\upsilon,t,t')$ تعریـف شـده بعنـوان حداکثر مسافت که در در آن می توان ضمانت کرد کار ارتباط که حداکثر t واحد زمانی طول می کشد تا بتواند محققاً کامل شود با فرض این که دو میزبان بطور تصادفی در سرعتی کـه از υ بیشـتر نمـی

شود حرکت می کنند و حد بالایی برای تغییر پیکربندی بسیار ریز تک t' است زیـادتر نشـود. بطـور واضح، مسافت امن نمی تواند با واژه های مطلق تعریف شود، امّا باید در زمینه داشتن تحرک قطعی و مشخصات کاربرد نسبی در نظر گرفته شود. برای مثال، در شکل 1a میزبان هـای a و b در محـدوده ارتباطی هستند (R) . یعنی آنها قادرند مستقیماً با یکدیگر صحبت کنند. آنها ممکن است بخواهند در یک گروه باشند و مشارکت در منابع و هماهنگی را بسرعت آغاز کنند. با این حال در این نقطه ممکن است نتوانند چنین کاری انجام دهند اگر مایلید تحویل دادن پیام در گروه را تضمین کنند. این بخاطر این است که a و b می توانند بسرعت پـس از اذعـان از عضـویت در یـک گـروه بسـرعت از محـدوده یکدیگر بیرون روند، با این نتیجه که پیام ها بین آنها نمی توانند با موفقیت تحویـل داده شـوند. ایـن مشکل از ماهیت متحرک میزبان ها و ماهیت همزمانی پیام عبور کننده ناشی شود، راه حل ما الزام a و b به موافقت در عضویت در یک گروه است هنگامیکه آنها فقط به اندازه "کـافی نزدیـک" هسـتند. (مثل شکل 1b). یعنی آنها به فاصله

$$r \le R - ۲\upsilon * (t + t') \qquad (۱)$$

هستند.



شکل ۲-۸ مثالی از مسافت امن

در این زمینه، t حد بالا برای دوره عکس العمل شـبکه اسـت (چـون الـزام ثبـات تحویـل پیـام قابـل اطمینان است) و t' زمان لازم برای عملکرد سطح گروهی لازم (ادغام یا انشـعاب) در حـال حاضـر در

حال پیشرفت برای کامل شدن است. عامل 2υ برای الگوی حرکت بدترین حالت است یعنی موقعیتی که a و b در جهت های مخالف با حداکثر سرعت حرکت می کنند. به آسانی می توان دید که با ایـن محدودیت، تحویل پیام قابل اطمینان بین اعضای گروه تضمین می شود چـون بـیش از $t+t'$ زمـان برای اعضای دو گروه طول می کشد تا بطور فیزیکی قطع شوند، اهمیت ندارد چطور حرکت می کنند. طی این مدت هر تحویل پیامی کامل می شود حتی اگر تغییر پیکربندی در حال انجام گرفتن است.

ما یک گروه را امن می خوانیم اگر هـر دو عضـوی از گـروه از طریـق یـک مسـیر کـه طـی آن کلیـه میزبان‌های متوالی (پی در پی) در مسافتی امن هستند متصل شده انـد، مـا تصـور مسـافت امـن را از جفت های میزبان به جفت های (امن) گروهها با بدست آوردن حداقل دو میزبان، یکی در هـر یـک از دو گروه، در یک مسافت امن گسترش می دهیم. در حالی که این تعریف بنظر می رسد فرض کند که مسافت امن مستقل از اندازه گروه است. این فرض بطور کلـی درسـت نیسـت چـون هـر دو سیسـتم تحویل پیام و دوباره پیکربندی واقعاً به تعداد جهش هایی که پیام ها باید در مسیر بپیماینـد بسـتگی دارد. چون محدودیت زمانی روی عبور پیام به اندازه گروه بستگی دارد، رهیافت ما فقط هنگـامی کـار می کند که اندازه گروه با محدودیت گروه محـدود شـده یـا بـا پروتوکـل دوبـاره پیکـره‌بنـدی مقیـد شده‌است.

مفهوم مسافت امن برای معین کردن زمانی که دو گروه می توانند ادغام شوند یا زمانی که یـک گـروه می تواند به منظور حفاظت از الزامات برای عضویت گروهی منشعب شود. برای معین کردن این که آیا دو گروه در محدوده مسافت امن هستند، باید محل کلیه میزبان ها را در منطقه بدانیم چون برای همه بسیار گرانقیمت است که از مکان دیگران در همه اوقات آگاه باشند، ما به هر یک از گروهها یک رهبر اختصاص داده ایم. همه میزبان ها بطور مداوم محل خود را به رهبر گزارش می دهند. و رهبـر نقشـه گروه را نگه می دارد. و دائماً امتحان می کند که اگر اعضای گروه در محـدوده مسـافت امـن یکـدیگر هستند و آیا میزبان های جدید در منطقه حضور دارند. نقشه یک گـروه محـل اعضـای گـروه را ثبـت می‌کند.

۲–۳–۳پروتوکل کشف گروه

همانطور که در مشخصات عضویت تعریف شد، به هر میزبان متحـرک یـک نشـانگر میزبـان آی ـ دی منحصر بفرد داده می شود و بعنوان یک گروه یگانه حاوی خود بعنوان تنها عضو آغاز می کند.

برای یک گروه تا با گروهی دیگر ادغام شود، باید ابتدا قادر باشد سایر گروههایی را کشف کند کـه در همسایگی او حضور دارند. پروتول کشف این عملکرد را انجام می دهد و بعنوان یک لایه پشتیبان برای پروتوکل حفاظت عضویت گروهی عمل می کند یعنی پروتوکل دوباره پیکربندی. در پروتوکـل کشـف ما، میزبان ها در هر گروه از مسافت ایمن بعنوان معیاری برای پی بردن به این که چه کسی به انـدازه کافی نزدیک است که یک نامزد ادغام شدن باشد و هر کشف ثبت را به رهبر خود گـزارش ی دهنـد. برای سادگی، میزبان دارای کوچک ترین نشانگر در یک گروه بعنوان رهبر گروه انتخاب می شود. برای راحتی، ما همچنین نشانگر میزبان رهبر گروه را برای بکار رفتن بعنوان اسم برای گروه خـود انتخـاب می کنیم. توجه کنید که جی ـ آی ـ دی مشابه نشانگر g بکار رفته در مشخصات عضویت نیسـت، در عوض، جی ـ آی ـ دی با عدد τ تعمیر توالی گروه ترکیب می شود تا نشانگر g گروه را به بار آورد.

راه کار کشف ما به هر میزبان برای فرستادن یک پیام سلام به طور دوره ای که حاوی اطلاعات مکـان آن و نشانگر گروه آن احتیاج دارد. هنگامیکه دو گروه نزدیک می شوند، چنـدین عضـو از یـک گـروه ممکن است پیام سلام را از اعضای سایر گروه دریافت کنند. هنگامیکه یـک میزبـان u پیـام سـلام را دریافت می کند، محل و نشانگر گروه فرستنده را امتحان می کند. اگر u فرستنده را پیدا کـرد، مـثلاً υ، که عضو گروهی دیگر واقع در مسافت امن باشد، u اطلاعات را به رهبر گروه می فرستد، به نوبـه، از آن برای ادغام عملکردهای مربوط استافده خواهد کرد. ضمن این که اعضای گروه در کشف درگیـر می شوند، احتمال دارد رهبر گروه نسخه های متعددی از تذکر در رابطه با ظهور یک میزبان دریافـت کند نسخه های ایمنی دور انداخته می شوند.

خبرهای متعددی وجود دارد که می شود برای کاهش هزینه کشف انجام داد. ابتدا، هر میزبان ممکـن است اطلاعات کشف را به محل دوره ای به رهبر گروه الحاق کند بجای آنکه آنرا جداگانه بفرستد. این اطلاعات کشف را برای رهبر به جلو می فرستد و تقریباً بـدون هزینـه اسـت چـون مکـان و اطلاعـات همسایه جدید فقط چند بایت نشان می دهد که براحتی در یک بسته تنهـا جـای مـی گیـرد. هزینـه مرتبط با این روش بر دوش کشیدن الزامی است برای هر میزبان تا حافظه کوتاه مدت (ζ) از همسایه های جدید نگه دارد. دوماً با استفاده از اطلاعات همسایگی در حال حاضر موجود در لایـه مَـک، یـک میزبان ممکن است خوشامدهایی برای همسایه بفرستد فقط هنگامیکـه لایـه مَـک همسـایه جدیـدی کشف کند این هزینه کشف را بطور مهمی کاهش می دهد در موردی که مکان شناسی شـبکه بطـور غیر مکرر تغییر می کند. نقطه ضعف این روش وابستگی آن به اجرای لایه مَک در حمایت کردن کاربر از طرف میزبان بخصوصی است. ما انتخاب می کنیم که در پیش نمونه خود این کار را انجام ندهیم.

پروتوکل کشف گروه در هر گروه را مجاز می کند فهرستی از گروهها نگـه دارد کـه بـه انـدازه کـافی نزدیک نیستند که برای ادغام در نظر گرفته شدند. در بخش بعـدی پروتوکـل ادغـام گـروه را عرضـه می‌کنیم.

پروتوکل پیکربندی دوباره:

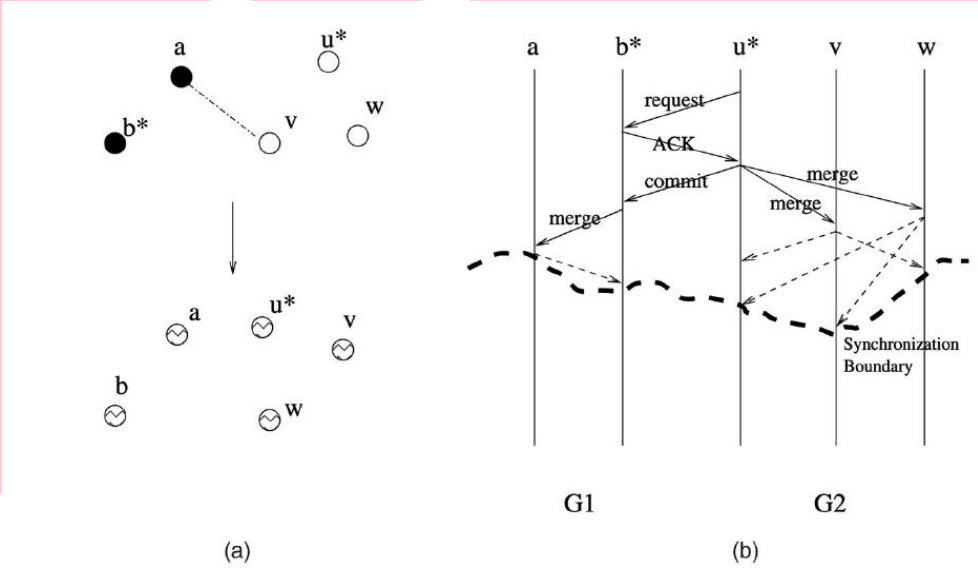
پروتوکل پیکربندی دوباره، لایه کلیدی در خدمات عضویت گروهی، است. در جستجوی ادغام گروهها در تماس است و از گروهها انشعاب کند که دیگر نمی توانند با هم بمانند. از اطلاعـاتی کـه در کشـف گروه جمع آوری شد، یک رهبر ممکن اسـت دریابـد کـه در گـروه بـالقوه یـا گروههـای بیشـتری در همسایگی وجود دارند که برای ادغام شدن مناسب هستند. اگر این طور است، مذاکرات ادغام شدن را با مجموعه (θ) از نامزدها (کاندیداها) آغاز می کند. به محض این که بخشی در رابطه با این کـه چـه کسی باید شرکت کند و چه کسی مسئول هماهنگ سازی ادغام شدن است، همه میزبان هـای تحـت تأثیر قرار گرفته تذکری رسمی درباره تغییر پیکربندی از هماهنگ کننده دریافت می کنند، علاوه بـر این بعد از این که یک میزبان تذکر تغییر گروه را دریافت کرد، برای جلوگیری از فرستاده شدن پیـام

ها در یک پیکربندی از پردازش شدن در پیکربندی دیگر، باید همزمان سازی جلوگیری را انجام دهد. بعلاوه شرکت کننده ها ملزم هستند پردازش پیام های دریافت شده را به تـأخیر اندازنـد تـا ایـن کـه همزمانی تکمیل شود. به تأخیر انداختن پیام ها می توانند با برچسب زدن هر پیام با پیکربندی تـوالی اعداد (τ) بدست آید. سراسیمه کردن میزبان های شرکت کننده را وادار می کند که پیام های اضافی بفرستند که رسیدن آنها تضمین می کند که پیام های دیگری از پیکره بنـدی قبلـی در راه نیسـتند. نتیجه تغییر پیکربندی بسیار کمی است. روش دیگری برای ایجاد مرز همزمـان سـازی بـا اسـتفاده از زمان تأخیر است. تقسیم بندی هم به همان طریق کار می کند امّا بدون هیچ مذاکره ای چون شـامل فقط دو گروه در هر زمان است. دوباره، ما از چندین مثال ساده برای نشـان دادن فراینـدهای تقسـیم بندی و ادغام استفاده کردیم.

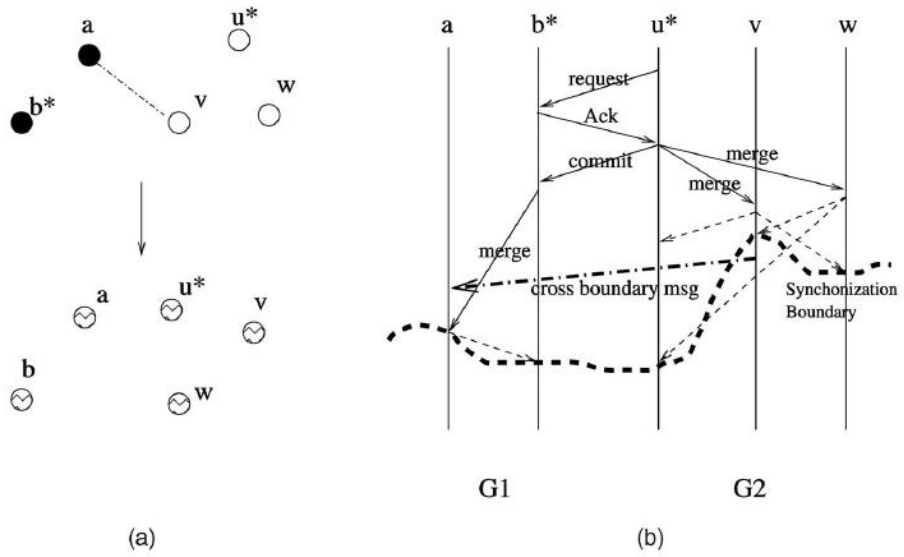
مثالی از ادغام کردن

شکل ۲ فرایند ادغام کردن بین دو گروه را نمایش می دهد، G۱و G۲ و G۱حاوی میزبانـان a و b است و b رهبر است. G۲ حاوی میزبانان u و υو w و u رهبر است. فرض کنید u پی برد کـه G۱ از طریق داده های کشف فرستاده شده در همسایگی او است و G۱ برای ادغام امن اسـت. بعـد، u بـا فرستادن یک درخواست ادغام به b رهبر G۱، ادغام را آغاز می کند. اگر مایل است در ادغام شـرکت کند، b یک اذعان همراه با فهرست عضویت گروهی خود و عدد توالی پیکربندی را پس می فرستد. در غیر این صورت یک پیام عدم موافقت می فرستد که u را وادار می کند ادغام با G۱ را متوقـف کنـد. اگر u به ACK بازگشت، مثل شکل ۲، یک عدد پیکربندی جدید با افزودن یک به بزرگترین جریـان پیکربندی از دو گروه ایجاد می کند. بعداً یک تعهد به ادغام برای b و دستور ادغام به اعضای خود می فرستد، تعهد به ادغام و دستور ادغام هر دو حاوی فهرست عضویت گروهـی جدیـد، عـدد پیکربنـدی جدید و شناساگر رهبر جدید هستند. متعاقب دریافت پیام تعهد به ادغـام، b یـک دسـتور ادغـام بـه اعضای خود می فرستد. یک میزبان به فاز درزگیـری خـود بعـد از دریافـت پیـام دسـتور ادغـام وارد می‌شود. یک پیام درزگیر به کلیه اعضای گروه اصلی خود می فرستد و از فرستادن هـر پیـام دیگـری

جلوگیری می کند تا همه پیام های مورد انتظار را از اعضای گروه خود در پیکربنـدی قـدیم دریافـت کند. بعد از دریافت کردن تمامی پیام های درزگیری، یک میزبان به پیکربندی جدید وارد می شـود و همه پیام هایی جدیدی که می فرستد عدد پیکربندی جدید را در سرساز خود خواهند داشـت. بطـور واضح، میزبان ها ممکن است وارد پیکربندی جدید از زمان های مختلف شوند. برای یک میزبان امکان دارد که هنوز در پیکربندی قدیم خود باشد و از میزبانی که وارد پیکربندی جدید خـود شـده پیـامی دریافت کند همانطور که در شکل ۳ نشان داده شده است. در چنین موردی، دریافـت کننـده بایـد از پردازش این پیام "آینده" را به عقب اندازد تا وقتی که پیکربندی جدید برقرار شود، بـدین ترتیـب بـا تظاهر به این که پیام "دریافت شد" در پیکربندی جدید. در غیر اینصورت از الزام ثباتی که پیام های باید در یک پیکربندی فرستاده شوند تخطی خواهد شد. اجرای این احتیاج دارد که یـک میزبـان هـر پیام دریافت شده را برای فرستادن پیام برای پیکربندی که پیام قبل از پردازش فرستاده شد آزمـایش کند.



شکل ۲-۹ فرآیند ادغام

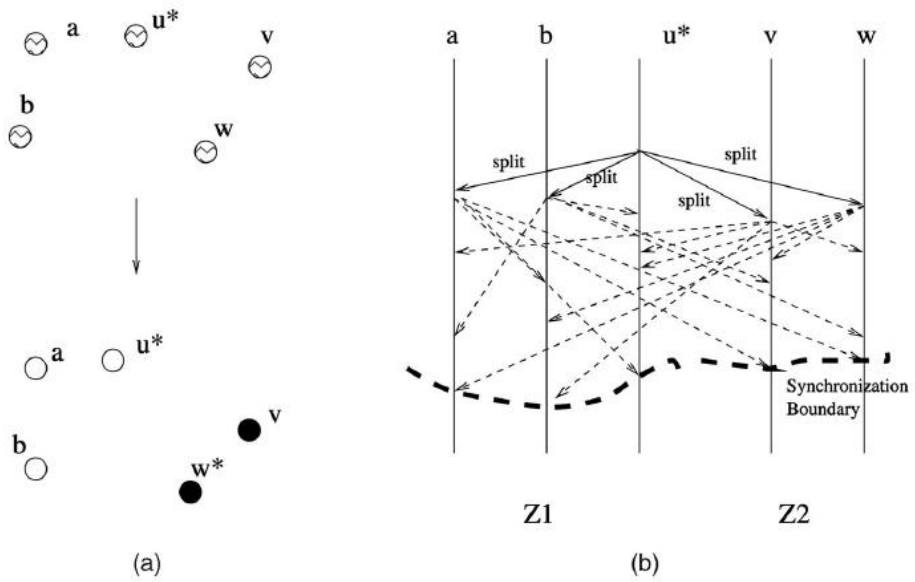


شکل ۲-۱۰ همزمان سازی و تعداد پیکربندی

برای u و b امکان دارد که ادغام را در زمان یکسان آغاز کنند. در این مورد یک راه کار شکننده کره تصمیم می گیرد که چه کسی ادغام را هماهنگ کند. ما از آی ـ دی بعنوان شکننده گره استفاده می کنیم. میزبان با کمترین آی ـ دی درخواست ادغام را هنگامیکه تصادم انجام می گیرد لغو می کند. هنگامیکه بیش از دو گروه شامل هستند پیچیدگی های اضافی ممکن است پدیدار شود. برای مثال: u ممکن است به فرآیند ادغام وارد شده باشد هنگامیکه درخواست ادغام b را دریافت می کند یا عکس دیگر رهبر نباشد چون با دیگر گروهها ادغام شده یا در اثر فرآیند تقسیم بندی. در کلیه چنین مواردی u با یک NACK پاسخ می دهد.

مثالی از تقسیم بندی:

شکل ۴ فرآیند تقسیم بندی را نشان می دهد. فرض کنید که دو زیر گروه از گروه G و Z۱ و Z۲ از یکدیگر دور می شوند، یا بطور مداوم بررسی کردن اعضای گروه خود، رهبر u قادر است مختص کند اگر گروه خود در فاصله پیکربندی امن است، مفروض بودن ضابطه ایمنی مبتنی بر مسافت. به محض این که رهبر u پنداشت که پیکربندی دیگر امن نیست، فوراً یک پیام دستور انشعاب به کلیه اعضای گروه خود صادر می کند. دستور انشعاب حاوی به قطعه اطلاعات است:



شکل ۲-۱۱ فرآیند تقسیم بندی

۱. رهبر جدیدی برای دریافت کننده

۲. فهرست عضویت گروهی جدید برای دریافت کننده

۳. عدد پیکربندی جدید که عدد پیکربندی به اضافه ۱ است.

u همیشه میزبان دارای کمترین از را در هر زیر گروه بعنوان رهبر برای زیر گروه جدید انتخاب می‌کند. به محض دریافت پیام دستور انشعاب، یک میزبان به فاز درزگیری پیام وارد می شود. شبیه فاز سوّم در فرآیند ادغام. هر میزبان سر می کند تا مطمئن شود که کلیه پیام های فرستاده شده به او توسط اعضای گروه و در پیکربندی قبلی دریافت شده‌اند، یا با دریافت کلیه پیام های درزگیری مورد انتظار یا با بکار بردن تأخیر وقفه ای. هر رهبر بتازگی تخصیص داده شده نقش رهبری خود را بعد از همزمان سازی از سر می‌گیرد.

رهبر گروه باید مکرراً به اندازه کافی پیکربندی گروه خود را بررسی کند تا هر موقعیت نا امن را به نحوه بهنگام کشف کند. مدخل برای مسافت امن به کثرت بررسی کردن بستگی ندارد، علاوه بر

عواملی که قبلاً بحث شد. مثال بالا فرآیندی که در آن یک گروه خود را به دو گروه دیگر تقسیم بندی می کند را نشان می دهد. بطور کلی، یک رهبر ممکن است الزامی بداند که گروه خود را به بیشتر از دو زیر گروه تقسیم کند تا خصوصیت مسافت امن را حفظ کند. فرآیند تقسیم بندی یکسان است. بعداً، توضیح می دهد چطور رهبر معین می کنید چه موقع پیکربندی گروه امن نیست و چطور آنرا به زیر گروههای امن تقسیم کند.

۲–۳–۴ معین کردن گروه های امن

برای معین کردن این که اگر پیکربندی گروه او امن است، رهبری نموداری از اتصال منطقی را نگه می دارد. در نمودار اتصال منطقی، دو گروه دارای یک لبه بوزن یک بین آنها دارد اگر مسافت فیزیکی بین آنها کمتر از یک تقسیم بندی مسافت امن (d_p) است و در غیر اینصورت بین آنها گروه ای وجود ندارد. هنگامیکه یک منطقه جدید گزارش می شود، گرافیک با دوباره محاسبه کردن همه لبه ها به گروه گزارش دهنده بهنگام می شود. این $O(N)$ مرحله در هر بهنگام سپری می کند، جائیکه N تعداد گره ها در گروه است. با مفروض بودن نمودار اتصال منطقی، الگوریتم تحقیق اوّل عمق دی ـ اف ـ اس می تواند توسط رهبر برای میعن کردن دسته های متصل در مراحل $O(N)$ بکار رود. بنابراین، پیچیدگی زمان کل برای نگه داشتن نمودار اتصال منطقی در رابطه با تعداد گره ها در گروه خطی است.

شکل ۵، وضعیت متغیرهایی را که یک کره احتیاج دارد برای اجرای پروتوکل نگه دارند و توابع پشتیبان این پروتوکل در شکل که نشان داده شده است. این جدول هر عمل انجام گرفته میزبان u، پیش شرط عمل، و اثر عمل، با مفروض بودن اقناع پیش شرط را فهرست می کند. در این سیستم دو نوع عمل وجود دارد. ستون اوّل شکل اعمالی را نشان می دهد را با تغییر در حالت محلی در میزبان u هدف قرار گرفته اند. ستون دوّم اعمالی را فهرست می کند که با رسیدن پیام ها در میزبان u هدف قرار گرفته اند. هر یک از اعمال در گروه بعدی دارای شکل GET MESSAGE هستند. برای هر یک از این ها یک SENO MESSAGE متناظر وجود دارد. برای مثال

GETNEIGHBORHELLO در میزبـــان u بـــا یـــک SENDNEIGHBORHELLO در میزبان دیگر، این تصویر نشان می دهد فقط یک پروتوکل در یک میزبان تک u در این سیســتم اجـرا شده است. هر میزبان در شبکه دارای لحظه عمل نشان داده خود است. اجرای ما از پروتوکل حفاظت عضویت گروهی در بخش بعدی بحث می شود.

متغیرهای حالت	
id	شناساگر گره
gid	شناساگر گروه
xy	مکان گره مداوماً توسط برخی راه کار بیرونی به روز می شود.
τ	تعداد توالی تبادل گروه
π	فهرست تعداد گروه
ξ	مجموعه رهبرهای بتازگی کشف شده
II	نقشه گروه حاوی مکان های کلیه اعضاء (خالی به استثنای رهبر)
Θ	مجموعه ارتباط های ادغام شونده، که همه آنها رهبرهای گروه دیگر هســتند (خـالی به استثنای رهبرها)
تایمر به روز کردن	تایمر برای به روز کردن مکان دوره ای
تایمر ورود	تایمر برای کشف همسایه دوره ای
توابع پشتیبانی	
به روز (gid,ξ)	gid را به فهرست رهبرهای بتازگی کشف شده اضافه کنید
به روز (ξ',Θ)	فهرست ارتباط به روز شده را با اعضای رهبرهای بتازگی کشف شده ادغام کنید
به روز (xy',v,II)	نقشه II گروه را با عضو گروه مکان جدید v'، xy' به روز کنید
ادغام امن (P,II',II)	بررسی کنید که ادغام II، II' امن است، طبـق خـط مشـیP کـه شـامل اطلاعـات مسافت امن و قالب های اعضای مرتبط
مجراهای قدیم واضح	مجراهای ارتباط همه گروه ها را واضح کنید
تقسیم بندی ها را ایجاد کنید (P,II)	برای II تقسیم بندی هایی ایجاد کنید، در معرض خط مشیP این تابع مجموعه ای از شکل سه گانه $(gid_{new}, \pi_{new}, II_{new})$ ایجاد می کنید.

جدول ۲-۱ متغییرهای حالت و توابع پشتیبان

۲-۱۴اجرا

پروتوکل کشف گروه و همسایه ما روی لایه مَک ساخته می شود، در حالیکه خدمات عضویت گروهـی تا یک اندازه روی یک لایه مسیریابی ویژه ساخته می شود. شکل ۷ معماری سیستم خدمات عضـویت گروهی را نشان می دهد. منطقه سایه روشن مؤلفه های کمک کننده ما را نشان می دهد.

شکل ۲-۱۲ معماری سیستم

اجرای خدمات تماماً در جاوا نوشته شده است. لایه کشف یک راه کار مبتنی بر راهنمایی با استفاده از یک شعاع که بطور دوره ای یک پیام سلام می فرستد را بکار می برد. یک شعاع دیگر به پیام در حال آمدن گوش می کند و این اطلاعات کشف شده را به لایه عضویت گروهی می فرستد. مؤلفه اصـلی در بسته عضویت گروهی (هدف عضو گروه) است که حاوی چندین شعاع است که ارتباط بین میزبان هـا و شبکه را کنترل می کند. هر نوع مختلف ارتباط با یک شعاع جاوای متفاوت اداره می شود. این شعاع ها از طریق هدف صاحب آنها (عضو گروه) هماهنگ می شـود. تـلاش هماهنـگ سـازی شـامل بجلـو فرستادن اطلاعات کشف برای رهبر گروه است، پاسخ دهنده به رهنمودهای ادغام و تقسیم بندی، و به روز کردن رهبر گروه با اطلاعات منطقه جاری. رهبرهای گروه مسئولیت اضافی گوش کردن به اعضای گروه آنها، ارتباط با سایر رهبران گروه مجاور و محاسبه کردن دوره ای ایمنی گروه را بعهده می‌گیرند.

بسته عضویت گروهی فرض را بر این قرار می دهد که مسیریابی ویژه روی هر تقسیم بندی میزبان در شبکه انجام شود. بنابراین بسیاری از پیام های بحث شده در بالا از طریق سایر میزبـان هـا در شـبکه مسیریابی می شوند. بدین طریق، رهبر گروه باید مستقیماً به هر عضو گروه وصل نشود.

هم کنشگر به پروتوکل عضویت گروهی روی گروههای (هدف رویداد) و (گوش دهنـده رویـدادها) در زبان جاوا ساخته می شود. یک کاربرد انجام گیرنده روی یک میزبان که از بسته عضویت گروهی برای مشارکت در شبکه استفاده می کند، بسادگی یک (هدف عضو گروه) بوجود مـی آورد. سـپس بعنـوان یک گوش کننده به (رویدادهای تغییر کرده گروه) ایجاد شده توسط (هدف عضو گـروه) ثبـت بشـود. هنگامیکه یک پیکربندی گروه جدید ناشی می شود، بسته عضویت گروهـی یـک (رویـدادهای تغییـر کرده گروه) بوجود آورده که به همه گوش کننده های ثبت منتقل می شـود. ایـن کـاربرد مـی توانـد اعمال بیشتری انجام دهد، بر مبنای اجرا کردن این گوش کننده ها.

هم کنشگر (عضو گروه) به کاربر اجازه می دهد پارامترهای لازم برای محاسبه مسافت امن را مشخص کند. برای مثال بوجود آورنده (عضو گروه) می تواند حداکثر سـرعت میزبـان و محـدوده ارتبـاط آنـرا مشخص کند. علاوه بر پارامترها برای مسافت امن، بوجود آورنده (عضو گروه) همچنین تکرار راهنمایی (سلام) و تکرار پیام های به روز گروه فرستاده شونده به رهبر را مشخص می کند.

در حالیکه اجرای الگوریتم تمرینی سر راست رو به جلو در شعاع های جاوا برنامه ریزی سـوکت بـود، برخی اختلاف ارزش توجه کردن سبب شد اجرای کردن با مثال های ارائه شده در بخش های پیشین متفاوت باشد. همانطور که ارائه شده، این پروتوکل فرض می کند که پیام های سـطح کـاربرد و پیـام های پروتوکل عضویت گروه در یک مجرا فرستاده شوند. همان طور که در بحث درباره‌ی ادغام و ریشه بندی نشان داده شده است، اطمینان می دهد که پیام ها در یک نظم FIFO دریافت می شوند و پیام های کاربرد فرستاده شده در پیکربندی گروه یکسان احتیاج به مقداری کار بیشتری دارند. مثال ارائـه شده در بخش قبلی از پیام های درزگیر به اعداد پیکربندی بـرای بدسـت آوردن ایـن اسـتفاده کـرد. بهرحال اجرا سعی می کند تا آنجا که امکـان دارد گـروه کشـف و حفاظـت از سـطح کـاربرد و اعـداد

پیکربندی و بنابراین، برگ های پیام درزگیری و اعداد پیکربندی ارائه شده به عنوان بخشی از پرتوکل مثال به کاربرد ویژه را جدا کند. این جدا شدن اجازه می دهد هر کاربرد راه کار خود را انتخاب را برای اطمینان حالت اتمی انتخاب کند. کاربردهای دارای الزامات یکنواختی ممکن است از بسته عضویت گروهی بدون هیچ ضمانت حالت اتمی استفاده کند.

در این طراحی موضوع دیگری که مورد توجه قرار گرفت جدا شدن تمیز بین بسته های عضویت گروهی و کاربرد بود. با ساختن روی مدل در حال حاضر بنیادی برای زبان جاوا، هم کنشگر ساده احتیاج دارد فقط برنامه ریز کاربرد مدل رویه جاوا را برای استفاده موفقیت آمیز این بسته درک کند. این هم کنشگر ترکیبی از یک نوع تک گوش کننده است و یک نوع تک رویداد سادگی مطلوب برای دک کردن را تأمین می کند. شکل ۸ هم کنشگر عمومی هدف (عضو گروه) را نشان می دهد. سازنده بافرها را برای محاسبه مسافت امن قبول می کند. با دستاویزی به هدف (عضو گروه) این برنامه ریز می تواند هدف (عضو گروه) را آغاز، متوقف و مکث کند و هدف (عضو گروه) را دوباره ادامه دهد. این روش ها رانش شعاع هایی را که هدف (عضو گروه) برای ارتباط پیدا کردن استفاده می کند تحت تأثیر قرار دهد. برنامه ریز همچنین می تواند یک (گوش کننده تغییر کرده گروه) را همچنین اضافه کند و بردارد. دو روش نهایی همانطور که توسط سایر بسته های لازم برای پروتوکل عضویت گروه برای عملکرد مناسب بکار می برند اغلب توسط برنامه ریز کاربرد مورد استفاده قرار نمی گیرند. روش اوّل اجازه می دهد یک بسته تولید کننده مکان (یعنی یک مانیتور GPS) مکان فیزیکی میزبان را به روز کند. روش دوّم اجازه می دهید (عضو گروه) به رویدادهای راهنما که توسط بسته راهنمایی کنند جدایی تولید می شود پاسخ دهد. این رهنمودها پیام های (سلام) چند شکلی هستند. شکل ۹ مثالی از کاربرد بسته عضویت گروهی را نشان می دهد.

```
public class GroupMember implements GroupBeaconListener {
      public GroupMember(InetAddress leaderAdd, Location loc,
                         int period, int range, int maxSpeed,
                         int updatePeriod, int networkDelay);
      public void start();
      public void stop();
      public void pause();
      public void resume();
      public synchronized void addGroupChangedListener(GroupChangedListener gcl);
      public synchronized void removeGroupChangedListener(GroupChangedListener gcl);
      public void setLocation(Location newLocation);
      public void newGroupBeacon(GroupBeaconEvent gbe);
}
```

شکل ۲-۱۳ هم کنشگر عمومی بسته عضویت گروهی

```
// The test class monitors the changes to a particular group member's group
// An instance of this class runs on each participating host
public class Test implements GroupChangedListener {
      // keep a handle to the group member object
      private GroupMember g;
      // integer count of the number of changes that have occurred
      private int changes = 0;
      public Test(GroupMember g) {
            this.g = g;
            // make this object a listener for events generated by the package
            g.addGroupChangedListener(this);
      }
      // this method is required by the GroupChangedListener interface
      // it is called when a new GroupChangedEvent occurs
      public void groupChanged(GroupChangedEvent gce) {
            // log the receipt of the change
            changes++;
            System.out.println(''Change:''  S + changes);
      }
      public static void main(String[] args) {
            // create a new GroupMember object for this host
            GroupMember g = new GroupMember(InetAddress.getLocalHost(),
                                    new Location(0,0), 1000, 3, 0, 100, 0);
            // create an instance of the Test class to monitor the GroupMember
            Test t = new Test(g);
            // start the GroupMember
            g.start();
      }
}
```

شکل ۲-۱٤ مثالی از کاربرد بسته عضویت گروهی

همانطور که در بخش های قبلی نشان داده شد این پروتوکل توسعه یافت چون میان افزار ، به توانایی سهیم شدن شفاف و با ثبات داده ها ما همه میزبان های متحرک در محیط های شبکه ویـژه احتیـاج دارد. میان افزار لایم همانطور که در اصل رها شد به یک عامل متحرک یا میزبان بـرای اعـلام کـردن صریح قصد آن برای درگیر شدن یا درگیر نشدن از یک گروه احتیـاج دارد. یکپـارچگی ایـن عضـویت گروهی با میان افزار لایـم فراینـدهای درگیـری و عـدم درگیـری در معالجـه شـفاف اطلاعـات لایـم هنگامیکه عوامل یا میزبان ها در شبکه حرکت می کنند را تشکیل شکل می دهـد. در نتیجـه حالـت آنها را در رابطه با الزامات ایمنی پروتوکل تغییر می دهد. در یک جنبش روشی، ما قـادر بـودیم یـک ویرایش آگاه از تحرک لایم را اجرا کنیم که بطور اتوماتیک بسته به مسافت نسبی الگوهای تحریـک و مسافت نسبی میزبان های شرکت کننده درگیر شود یا درگیر نشود.

چون بسته عضویت گروهی کاملاً مستقل از لایم یا هر کاربرد دیگـری اسـت کـه ممکـن اسـت از آن استفاده کند تغییرات در بسته لایم را تحت تأثیر قرار نمی دهد، تا زمانی که تغییـرات بـه بسـته هـم کنشگر آنرا تحت تأثیر قرار ندهد. این ویرایش های "قابل اتصال" بسته عضویت گروهی آینده را برای جایگزینی ویرایش جاری مجاز می کند. می شود اجرایی را تصور کرد که مسافت امن بر مبنای چیزی پیچیده تر از مکان فیزیکی است، از قبیل قدرت تک اثبات و غیره.

۲–۴–۱ تحلیل مسافت امن

خصوصیت کلیدی الگوریتم ما استفاده از اطلاعات مکان و مسافت امن در مـدیریت عضـویت گروهـی است. رهبر یک گروه مکرراً مکان های اعضا را برای اطمینان از این که فقـط آنهـا تضـمین شـده انـد متصل با گروه برای حداقل $t+t'$ واحد بیشتر از زمان باقی مانده در گروه باقی بمانند را بررسـی مـی کند جائیکه t زمان مشخص شده توسط لایه کاربرد و t' زمان محدود برای تغییرات پیکربندی اسـت. ترکیب t و t' مسافت امن برای یک عملکرد گروهی مشخص را معین می کند، که می تواند عملکـرد ادغام، عملکرد تقسیم بندی، یا هر عملکرد گروهی مشخص شده توسط کاربرد باشد اجازه دهید فرض

کنیم که t_d حداکثر تأخیر شبکه بین زمان کنترل یک پیامی که فرستاده و زمـان دریافـت شـده در گیرنده و پردازش شدن باشد. یعنی مجموع حداکثر تأخیر شبکه و حداکثر پردازش استعلام تأخیرهـا در فرستنده و گیرنده برای راحتی، ما به t_d به عنوان تأخیر شـبکه ارجـاع مـی کنـیم. در حالـت یـک انشعاب حداکثر زمان لازم برای یک گروه برای تقسیم بندی شدن بطور موفقیت آمیز دو برابـر تـأخیر شبکه است.

اگر رهبر بطور مداوم پیکربندی گروه را دیده بانی کند و کلیه مکان های اعضا به روز هستند پس قطع شدن اعلام نشده نتیجه شـده متحـرک مـی توانـد از پـیش گرفتـه شـود و بطـور موفقیـت آمیـز بـا $t' > ۲ * t_d$ لازم، آن رفتار شود. با اینحال اطلاعات رهبر درباره مکان های اعضا همیشه کمـی کهنـه است. اگر اعضا مکان های زمان خود را هر t_u واحد زمانی نمونـه بـرداری و گـزارش کننـد اطلاعـات مکانی که رهبر درباره یک عضو دارد می تواند با زمان $t + t'$ منسوخ شود. با در نظر گرفتن این، زمـان ذخیره شده T می تواند بیشتر از $t_u + t_d + ۲ * t_d = t_u + ۳t_d$ باشد. در هر حال مـا مـی تـوانیم از $d_r = R - ۲V_{max}(t_u + ۳t_d)$ بعنوان مسافت امن تقسیم بندی بسته به الزام بـرای ادغـام اسـتفاده کنیم. چون ما مجاز نیستیم بگذاریم یک فرآیند ادغام به محض این که آغاز شد متوقف شود، محاسبه مسافت امن برای تقسیم بندی همچنین احتیاج دارد برای زمان مرتبط با فرآیند ادغـام بحسـاب آیـد. زمینه ذیل را در نظر بگیرید: درست قبل از یک تعهد در فرآیند یک ادغام پیکربندی گروه با اسـتفاده از مسافت امن d_r امن است درست بعد از تعهد یک رهبر ممکن است کشف که گـروه او دیگـر امـن نیست و باید فوراً یک فرآیند تقسیم بندی انجام شود. بهرحال فرآیند ادغام پایـان نیافتـه اسـت. ایـن قابل قبول نیست، با بحساب آوردن این که دو فاز فرآیند ادغام، حداکثر به زمان اجـرای $۴t_d$ احتیـاج دارد چهار پیام و درست بعد از ادغام، پیکربندی باید امن باشد، کل زمان ذخیره شـده بـرای ادغـام و تقسیم بندی باید $t_u + ۳t_d + ۴t_d = t_u + ۷t_d$ باشد. به گفته دیگر، مسافت امن برای ادغـام تقسـیم بندی

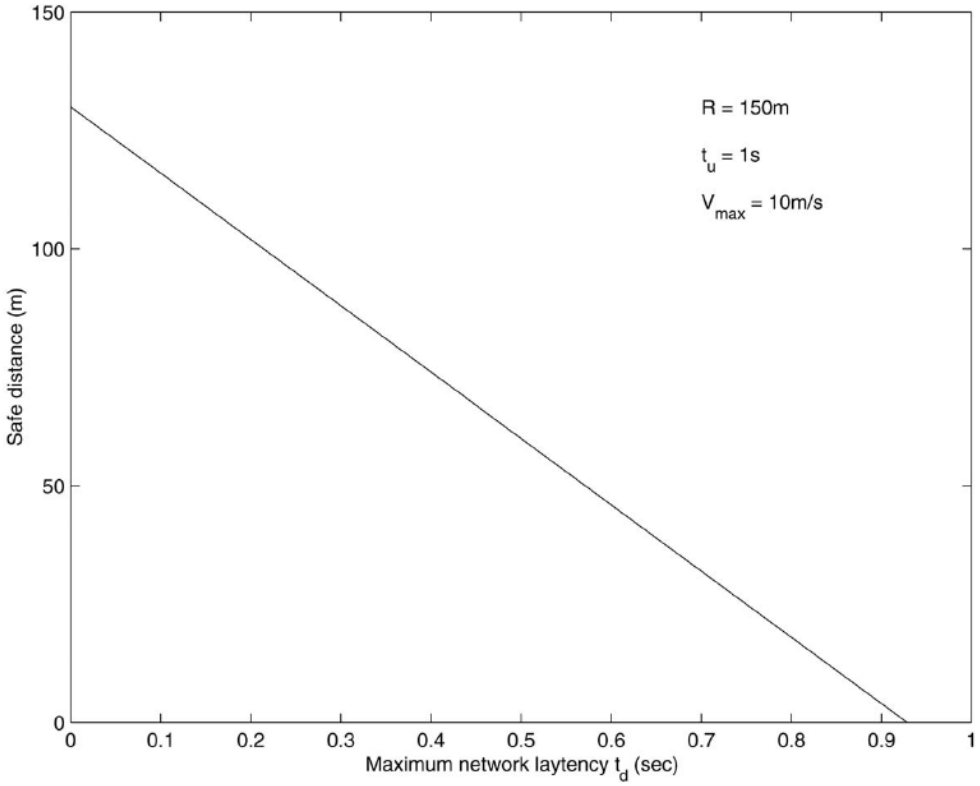
$$d_s = R - ۲V_{max}(t_u + ۷_{td}) \qquad (۲)$$

با استفاده از مسافت یکسان برای ادغام و تقسیم بندی مشکل "گره های رفت آمدگر" ارائه می شـود یعنی یک گره از مرز امن بیرون می رود و باز می گردد، ادغام و تقسیم بندی تکراراً انجام می گیرنـد. برای پرهیز از این می شود مسافت امن برای ادغام را با ایجاد "ناحیه ضربه گر" محکم تر کرد و بدین ترتیب احتمال رفت و آمدگری را کاهش داد.

الگوریتم، همچنین احتیاج دارد که V_{max} بیشتر از V_{adm} نباشد یعنی حداکثر سرعت قابل قبول بـرای سیستم شبکه بی سیم ویژه که از میزبان های متحرک استفاده می کنند. اکثر

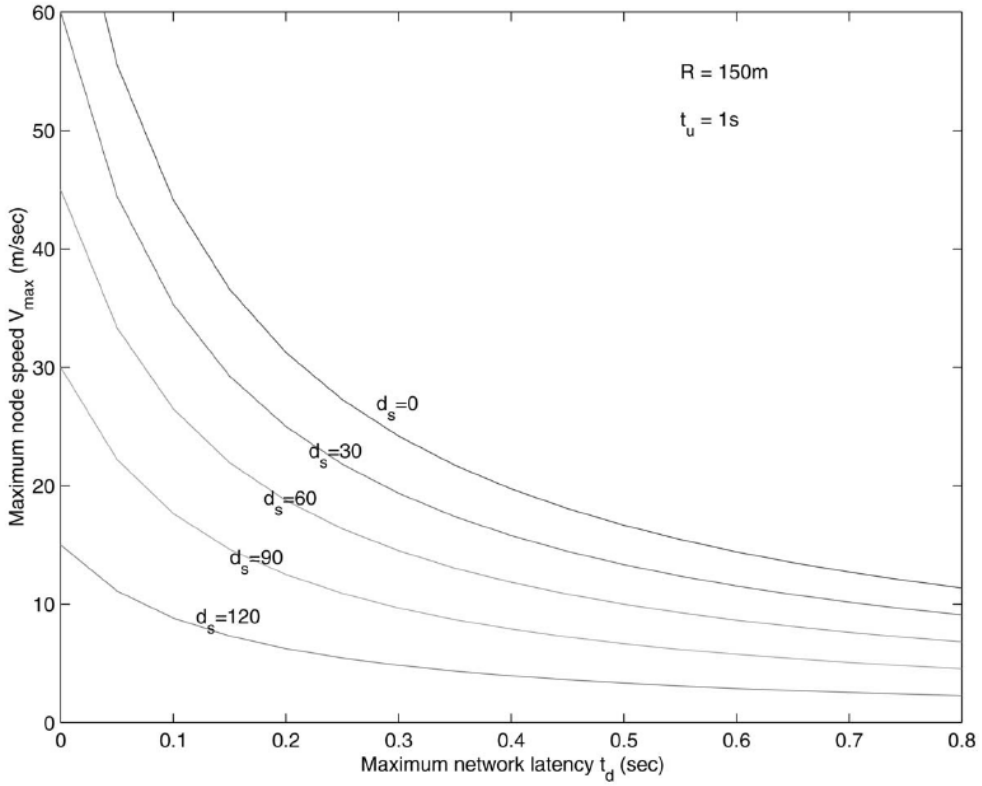
سیستم های شبکه بی سیم دارای حداکثر سرعت مجاز هسـتند [۹]، هنگامیکـه یـک گـره متحـرک خیلی سریع حرکت می کند، بسادگی برای شبکه نامرئی مـی شـود. بـرای GSM و PCS، V_{adm} در حدود ۵۰m/s است. برای DECT سیستم میکروسلولی V_{adm} در حدود ۱۱m/s اسـت. بـدون ایـن شرایط $V_{max} \le V_{adm}$، یک متغیر سرعت از $V \le V_{adm}$ به $V > V_{adm}$ یک قطع شدن اعلام نشده بوجـود می آورد. دیده بانی سرعت برای جلوگیری این نوع قطع شدن اعلام نشده از انجام گرفتن لازم خواهد بود.

شکل ۱۰، ارتباط بین مسافت امن را و حداکثر تأخیر مجاز شبکه t_d بـا مقـادیر معقـول $R = ۱۵۰m$، $V_{max} = ۱۰m/s$ و مکان گزارش دادن فرکانس ۱Hz(t=۱s) را نشان می دهد. می توان دید که، ضـمن این که محدودیت تأخیر افزایش می یابد، مسافت امن کاهش می یابد.



شکل ۲-۱۵ مسافت امن در مقایسه با تاخیر شبکه

شکل ۱۱ ارتباط بین مدخل مسافت امن، محدوده بالای سرعت، و محدوده تأخیر شبکه را نشان مـی دهد ناحیه بالای منحنی بالا مطابق d_s <۰ است. در این فاصله محدودیت، نمی توانیم هـیچ ضـمانت با ثباتی برای یک گروه شامل است یک عضو تأمین کنیم. از طرف دیگر، اگر محدودیت تـأخیر شـبکه سیستم متحرک و محدودیت حداکثر سرعت در ناحیه ای زیر منحنـی (d_s=۹۰m) قـرار گیـرد، مـی توانیم تأمین کنیم که گروه با استفاده از ۹۰m بعنوان حداکثر مسافت امن ضمانت با ثبات را ببینند.



شکل ۲-۱۶ ارتباط بین مسافت امن، حد سرعت و حد تاخیر

انتخاب کردن مسافت امن کلید پروتوکل است. انتخابی که به اندازه کافی محتاطانه نیست ممکن است حد درست بودن خدمات عضویت گروهی را به خطر بیاندازد. انتخابی که بیش از حد محتاطانـه اسـت ممکن است سبب این شود که گروه بیش از حد کوچک باشد یا کوچکتر از حـد لازم، بـرای سـودمند کردن خدمات عضویت گروهی تا آنجا که ممکن اسـت، بایـد بـین ایـن انتخـاب هـای متضـاد تـوازن حساسی ایجاد کرد.

۲-۴-۲ بحث

مشخصات عضویت گروه قابل تقسیم بندی ما از مشخصات سنتی قوی تر است به این صورت کـه نـه فقط به موجودیت طی تقسیم بندی احتیاج دارد بلکه همچنین طی تقسیم بندی به بـا ثبـاتی تأکیـد

کند. کار قبلی از عضویت گروهی طی تقسیم بندی یا بی ثباتی را قبول می کند، یا در دسترس بـودن طی تقسیم بندی را کاهش می دهد.

از طرف دیگر، خصوصیات قوی لازم توسط مشخصات عضویت گروهی قابلیت تقسیم ما، اجرا کردن در مدل های سیستم ناهمزمان سنتی را غیر ممکن می کند. کلیه راه حل ما به مشکل عضـویت گروهـی قابل تقسیم بندی ما تصور مسافت امن است و تصور مطابق از نمودار پیوند گروهی منطقی؛ با مفروض بودن اطلاعات درباره خصوصیات فیزیکی سیستم را پیش بینی کنیم. قادریم ثبـات قـوی لازم توسـط خدمات عضویت گروهی را بدست آوریم.

در حال حاضر الگوریتم ما فرض می کنید که همه گره های متحرک در سیستم دارای حداکثر سرعت شناخته شده هستند. سرعت نامحدود منبع احتمالی دیگر قطع شدن اعلام نشـده اسـت. بـرای اکثـر شبکه های بی سیم سرعت کم یک الزام است. در سیم های شامل گره های متحرک کـه مـی تواننـد سرعت خود را کنترل کنند، یعنی، ماشین ها، و هواپیماها، یک سرعت نسبی امن می تواند در تصمیم ادغام یا انشعاب بکار رود البته، در چنین موردی ما باید یک حداکثر سرعت برای گـره هـای متحـرک برای ممکن ساختن پیش بینی قطع شدن را فرض می کنیم.

خدمات عضویت ها می تواند هنگامیکه اطلاعات سرعت درباره و گره میزبان موجود است بهبود یابـد، برای مثال شکل ۱۲a و ۱۲b را در نظر بگیرید. در (a) میزبان های x و y از یکدیگر دور مـی شـوند، در حالیکه در b آنها در یک مسیر حرکت می کنند. بطور واضح، x و y احتمال کمی دارد کـه مـورد بعدی نسبت به مورد قبلی شوند. با ترجمه این به زبان امنیت امن، حداکثر مسـافت امـن بـین x و y بزرگتر از (b) نسبت به (a) است. در الگوریتم جاری، فرض می کنـیم کـه اطلاعـات سـرعت موجـود نیست. چون نمی توانیم (a) را از (b) متمایز شویم، باید بدترین حالت را در زمینه حرکت بـرای هـر جفت میزبان در نظر بگیریم، یعنی، آنها ممکن است از یکدیگر دور شوند با حداکثر سـرعت نسـبی در هر نقطه از زمان. هنگامیکه اطلاعات سرعت موجود است، مدخل مسافت امن بین میزبان های x و y (در شکل ۱۲) می توانند بطوری پویا طبق فرمول:

$$R-\left|\vec{\upsilon}_x-\vec{\upsilon}_y\right|.t-\left|\vec{a}_{max}.t^2\right| \qquad (۳)$$

تعمیر کنند.

جائیکه $\vec{a}_{max}$ حداکثر شتاب برای کلیه میزبان ها و t زمـان بـرای یـک گـروه عملکـرد قـبلاً در حـال پیشرفت برای خاتمه یافتن. ما می توانیم الگوریتم خود را برای استفاده اطلاعات سرعت به طریق ذیل مورد استفاده قرار دهیم: ۱) هر میزبان شامل اطلاعات سرعت خود در پیام های (سلام) و پیام های به روز کردن مکان و ۲) مسافدت امن با بکار بردن ۳) با $t=t_u+7t_d$ محاسبه مـی شـود. بـاقی الگـوریتم بصورت قبل می ماند.

هر چند در پروتوکل کل ما فقط مسافت فیزیکی امن برای پرهیز از قطع شدن اعلام نشده بکار گرفته می شود. سایر صفات فیزیکی می تواند برای معین کردن ایمنی می توانند بکار روند.

برای مثال اگر نقصان حلقه از طریق دیده بانی پهنای باند یا تغییر نیروی اتصـال بـین دو گـروه قابـل پیش بینی است. یک پروتوکل عضویت گروهی مشابه می تواند با بکـارگیری مفـاهیم مشـابه سـاخته شود. یعنی "پهنای باند" یا "سطح نیروی امن" و غیره.

فرض می کنیم که هر میزبان متحرک دارای از مکان خود آگاه است. این با موجود بودن سیستم های موقعیت یابی از قبل جی ـ پی ـ اس امکان پذیر است. با این حال، سیستم های موقعیت یاب همیشـه صحیح نیستند. برای سادگی، ما این را در تحلیل مسافت امن خود در نظر نگرفتیم. می توان همیشـه دقت داده ها و فرکانس نمونه یـک سیسـتم مکـانی را در مسـافت امـن معیـار قـرار داد و خـدمات را نیرومندتر کرد.

فرض می کنیم که مدل ارتباط بی سیم دارای شعاع ارتباطی شناخته شده ای است. این انتخاب اغلب بعنوان "مدل دیسک واحد" ذکر شده ([۱۳]، [۲۱])، بطور گسترده ای در مطالعـات تئوریـک دربـاره خصوصیات شبکه های ویژه بی سیم بکار می رود در حالیکه این مدل ارتبـاطی رادیـویی سـاده، یـک نقطه آغاز مناسب برای استدلال درباره خصوصیات شبکه بی سیم بخصـوص اسـت از قبیـل بزرگـراه، (خودروها) و بیابان (گروههای نبرد)، برای زمینه های درونی (جای سرپوشیده) معتبـر نیسـت. دلیـل

این است که ارتباط رادیویی دارای مشخصات بسیار غیر قابل پیش بینی در محـیط درونـی اسـت (در اثر انعکاس، جذب شدن، تداخل و غیره) و محدوده چند سویه ای جداسازی خوبی نیست. بطور منظم، خدمات عضویت گروهی مبتنی بر مسافت امن فقط در محیط های میدان صاف اجرا شدنی اسـت کـه محدودیت ارتباط بی سیم چند سویه تقریبی مناسب است.

صحت الگوریتم ما به فرضی که شبکه دارای یک محدودیت تأخیر است متکی است، در این لحظه، ما از هیچ پروتوکل مسیریابی ویژه که می تواند یک محدودیت تأخیر خوب عرضه کند آگاهی نداریم. بـا این حال، قابل تصور است که یک پروتوکل مسیریابی دارای محدودیت تأخیر خوب بـرای پیـام هـای کنترل گروه دارای اولویت با محدود کردن اندازه گروه و استفاده از اطلاعات مکان امکان پـذیر اسـت. یک رهیافت متناوب بالا بردن معیارهای ادغام با یک انـدازه گـروه حـداکثر یـا حتـی برخـی شـرایط پیکربندی فاصله ای گروه است. با انجام دادن این، ممکن است امکان داشته باشـد فـرض محـدودیت تأخیر را با احتمالات زیاد مواجه کرد.

انگیزه برای این که به اشتیاق ما برای تأمین ثبات در کاربردهایی که روی شبکه های ویـژه اجـرا مـی شوند متکی است، با این حال، نگه داشتن چشم اندازی یکپارچه از حالت کلی در یک شبکه گسـترده بطور کلی مشکل و اصولاً غیر ممکن با وجود قطع شدن هـای اعـلام نشـده اسـت. در سیسـتم هـای متحرک ویژه، قطع شدن اعلام نشده بوجود آمده در شهر تحرک مکرر بعنوان بخشی از عملکرد عادی شبکه انجام می گیرد. این باعث می شود توسعه سیستم های سازگار با کاستی علاوه بـر شـبکه هـای ویژه بسیار چالش برانگیز شوند هدف ما در کمک کردن به توسعه دهندگان نرم افزار در تـلاش هـای آنها برای طراحی و ساختن کاربردهای معتبر، منجر می شود خدمات عضـویت گروهـی قابـل تقسـیم بندی جدیدی با الزامات ثبات قوی را مشخص کنیم. ما همچنین یک استراتژی و یک الگوریتم بـرای اجرای خدمات، با مفرض بودن فرضیات سیستم مناسـب عرضـه کـرده ایـم. خصوصـیت جدیـد ایـن الگوریتم توانایی آن برای تولید تصور با کل از قطع شدن اعـلام شـده اسـت. بـا اسـتفاده از اطلاعـات تحرک و مکان در باره میزبان های متحرک در منطقه، خدمات عضویت قادر است بـرای لایـه کـاربرد

یک سرویس تحویل پیام معتبر به اعضای گروه در حضور قطعی اعلام نشده بوجود آمده در اثر تحرک با مفروض بودن فرضیات سیستم مناسب را تضمین کند. این رهیافت مسیری تازه در محاسبه کـردن گسترده سازگار با کاستی ارائه می دهد، همانی که معیار اطلاعات پروتوکل ها درباره تحرک و فاصـله می شود، این کار همچنین راه حلی عملی برای پوشش ایمنی تحرک بوجود آمده در اثر قطـع شـدن های اعلام نشده در سیستم های متحرک ویژه ارائه می کند.

فصل سوم

سیاست زیستگاه امن زندگی خصوصی

۳–۱سیاست زیستگاه امن زندگی خصوصی

شرکت الکوا در رابطه با اطلاعات شخصی که درباره آنها بدست مـی آورد، حقـوق زنـدگی خصوصـی (شخصی) همه افراد را قبول دارد و به آنها ارج می گذارد. بعنوان بخشی از پیـروی از قـوانین زنـدگی خصوصی اروپایی، الکوا در برنامه زیستگاه امن بین المللی مقرر شده توسـط ایـالات متحـده، اتحادیـه اروپا و سوئیس به منظور سامان دادن به انتقال اطلاعات شخصی از اروپـا بـه ایـالات متحـده شـرکت می‌کند.

پیشینه: این سیاست زندگی خصوصی با سیاست های جداگانه ارائه شده توسط الکوا برای سـه جـواز بیشین زیستگاه امن (برای فرآیند بررسی هـدایت تجـارت، بـرای محـیط سیسـتم AS/۴۰۰ و بـرای سیستم ای ـ بی ـ اس اوراکل) ادغام می شود و محدوده خود را برای شامل کردن یک جواز زیسـتگاه امن جدید توسط الکوا برای اطلاعات کارکنان شـامل در پایگـاه داده هـای HRMS اوراکـل، مخـزن (انبار) داده های کلی و انتقال داده های تک موردی (خلق الساعه) گسترش می دهد.

گستره: این خط مشی به کلیه اطلاعات دریافت شده توسط الکو از اروپا تحـت جـواز زیسـتگاه امـن ادغام شده اش اعمال می شود.

اطلاعات شخصی: اطلاعات شخصی هر اطلاعاتی درباره یک فرد شناسایی شـده یـا قابـل شناسـایی کردن، علیرغم واسطه یا شکلی که این اطلاعات ذخیره شده است می باشد.

اطلاعات حساس: اطلاعات حساس، اطلاعات شخصی است که به عنوان اقامـه کننـده ریسـک هـای ویژه به افراد در قوانین حفاظت داده های اروپایی تلق می شود، از قبیل اطلاعات درباره مبدأ نژادی یا قومی، عقاید سیاسی، اعتقادات مذهبی یا فلسـفی، عضـویت اتحادیـه کـارگری، زنـدگی بهداشـتی یـا جنسی. مقوله های دیگر داده های شخصی در برخی کشورهای اروپایی شامل اطلاعات درباره بیشینه جنایی، قضاوت های مدنی، تحریم های اداری، معیارهای ایمنی دولت، شماره های تعیین هویت ارائـه شده توسط دولت، داده های زیست سنجی، داده های توارثی، داده های موقعیت جغرافیایی، تاریخچه

های شخصیتی و اطلاعات در زمینه "لو دادن" (برنامه های گزارش دادن پیروی اخلاقـی) در معـرض حفاظت های ویژه قرار دارند.

کنترل کننده داده ها: یک کنترل کننده داده یک شخص یا ماهیت است کـه اهـداف و روش هـای پردازش اطلاعات شخصی را معین می کند. یک شرکت هنگامیکه تصمیم می گیرد چطور این داده ها باید بکار گرفته شوند و داده ها را طبق آن بکار می گیرد بعنوان یک کنترل کننده داده عمل می کند.

پردازنده داده ها: یک پردازنده داده ها شخص یا ماهیتی است که داده های شخصی را از جانب یک کنترل کننده داده ها پردازش می کند. یک شرکت هنگامیکه بعنوان نماینده شرکت دیگری عمل می کند و رهنمودهایش را بعنوان این که داده ها چطور باید اداره شده و پردازش شوند را دنبال می کند. بعنوان یک پردازنده داده ها عمل می کند.

۳–۲وظایف الکوا در اداره کردن داده های شخصی

برای برخی داده های تحت پوشش این خط و مشی، الکوا بعنوان یک کنترل کننده داده ها عمل مـی کند، و تصمیم هایی درباره اهداف و روش های پردازش کردن اطلاعات دریافت شده از اروپا و استفاده از این داده ها برای مقاصد بازرگانی، از قبیل مدیریت کارمندان و برنامه ریزی بازرگانی می گیرد. برای اطلاعات شخص دیگر، الکوا بعنوان یک پردازشگر داده ها عمل می کند و داده ها را در مرکز داده های شمال امریکا در شهر بینربورک ایالت پنسلوانیا فقط از جانب شعبه ها و وابسته های اروپایی نگـه مـی دارد.

ارتباط الکوا با اطلاعات شخصی دریافت شده از اروپا تحت جواز زیستگاه امن در جدول ذیـل خلاصـه می شود.

نوع اطلاعات شخصی	الکوا بعنوان کنترل کننده داده ها عمل می کند	الکوا بعنوان پردازشگر داده ها عمل می کند
فرآیند بررسی هدایت بازرگانی (بی ـ سی ـ اس). اطلاعـات ارائه شده توسط کارکنان از طریق هدایت بازرگانی سالانه و جـواز بررسی تضاد منافع و یا فرآیند آموزش	✓	
محیط سیستم های AS/۴۰۰. اطلاعات مربـوط بـه کارکنـان و مشتریان در کاربردهای بازمانده که از فرآیندهای تولید و بازرگانی حمایت می کند، شامل زمان و حضور یابی، قابلیت ردیابی تولید و رکوردهای آموزش		✓
سیستم هـای بازرگـانی شـرکت اوراکـل ای ـ بـی ـ اس. اطلاعات مربوط به مشتری ها، فروشنده ها و کارکنـان لازم بـرای پشتیبانی عملکردهای بازرگانی استاندارد، از قبیل خریداری، دفتر کل، حساب های پرداختی و دریافتی. این داده ها شامل اطلاعـات تماس بازرگانی، رکوردهای خرید و سـایر حسـاب هـای معاملـه و داده ها مربوط به صورتحسـاب، دریافـت هـا، خـدمات مشـتری و بازپرداخت به کارکنان برای سفر و هزینه ها		✓
پایگاه داده هـای اچ ـ آر ـ ام ـ اس اوراکـل. پایگـاه اچ ـ آر اصلی برای کارکنان الکوا در سراسر جهان		✓
انبار داده ها کلی. زیـر مجموعـه داده هـای اصـلی مربـوط بـه کارکنان لازم برای حمایت نظارت مدیریت، گزارش دادن و برنامـه ریزی	✓	
اتصال داده ها اچ ـ آر تک موردی. اطلاعاتی کـه سرپرسـتی و تأمین برخی مزایا را برای دور از وطن ها و کارکنانی که مسـتقیماً توسط مدیران در خارج از اروپا سرپرستی می شـود یـا در برنامـه های جهانی و تسهیلات گروه الکوا شرکت می کنـد حمایـت مـی کند.	✓	
سیستم ایمیل مایکروسافت اکس چـنج. سـرور و نـرم افـزار مربوط که توانایی های ایمیل برای کارکنان الکوا در سراسر جهان تأمین می کند.		✓

جدول ۳-۱

اصول خط و مشی اجرا شدنی

۳–۲–۱ الکوا به عنوان کنترل کننده داده ها

در رابطه با اطلاعات شخصی دریافت شده از اروپا جائیکه الکوا بعنوان کنترل کننده داده ها عمل مـی کند (یعنی، داده ها در فرآیند بی ـ سی ـ اس، انبار داده های کلی و اتصال داده هـای تـک مـوردی)، الکوا چنین اطلاعاتی را طبق هفت اصل زیستگاه امن زندگی خصوصی (توجه، گزینش، اتصـال رو بـه جلو، ایمنی، درستی داده ها، دستیابی و اجرا) اداره می کند. توضیح کامل این اصول، در زیـر خلاصـه شده

الکو افراد را درباره اهدافی که برای آن اطلاعات را درباره آنها جمع آوری و بکار می برد، چطور با الکوا برای هر استعلام یا شکایتی تماس گرفت، انواع اشخاص ثالثی که این اطلاعات را برای آنها فـاش مـی کند و انتخاب ها و روش هایی که الکوا به افراد برای محدود کردن استفاده و آشکارکردن این اطلاعات ارائه می دهد مطلع می کند. این توجه به زبانی صـریح و واضـح هنگامیکـه از افـراد بـرای اولـین بـار خواسته می شود اطلاعات شخصی را به الکوا عرضه کنند یا به الکوا اجازه دهند اطلاعـاتی از اشـخاص ثالث برای هدفی به غیر از آنچه که در اصل برای آن جمع شده بود ارائه می شود.

گزینش:

الکوا اطلاعات شخصی لازم را برای راندن تجارت خود جمع آوری کرده و اسـتفاده مـی کنـد. چنـین جمع آوری و بکاربری در معرض اصل توجه توضـیح داده شـده در بـالا قـرار دارد و در اکثـر شـرایط احتیاج به رضایت صریح فرد ندارد.

بهرحال، الکوا رضایت افراد را قبل از:

(1) آشکار کردن اطلاعات شخصی به شخص ثالث (بغیر از فاش کردن برای یک نماینـده یـا مقاطعـه کار پردازش کننده داده ها منحصراً از طرف الکوا، یا آشکارسازی از طرف قانون الزامی است)، یا

(2) استفاده از اطلاعات شخصی برای هدفی که با اهدافی که اصولاً برای آن جمع آوری شد یا متعاقباً توسط فرد مجاز بود مغایر است بدست می آورید.

جائیکه رضایت لازم است، به افراد راه کارهایی صریح و روشن که به آسـانی در دسـترس هسـتند و از عهده آنها بر می آیند تا گزینه را به کار گیرند عرضه می شـود. ایـن راه کارهـا معمـولاً ممکـن اسـت ترجیح داده نشود (الکوا ممکن است بدون مخالفت از طرف فرد در طرف زمان معقـولی کـار را دنبـال کند)، امّا اگر داده ها شامل اطلاعات حساس است (همانطور که در بالا تعریف شد)، الکوا بدون رضایت صریح از طرف فرد ادامه نخواهد داد.

انتقال به سوی جلو:

الکوا اطلاعات شخصی را فقط برای مقاطعه کاران ثالث یا نماینده هایی که این داده ها را از طرف الکوا پردازش می کنند. برآوردن الزامات گزارش به دولت، برآوردن سایر الزامات قانونی، تصریح یـا دفـاع از منافع، یا مطالبات قانونی، یا با رضایت فرد فاش می کنند.

قبل از فاش کردن برای یک شخص ثالث، الکوا ابتدا اصول گزینش و توجه را همانطور که در بالا ذکـر شد اعمال خواهد کرد. مگر این که آشکارسازی قانوناً الزامی باشد (از قبیـل گـزارش دادن مالیـات یـا جواب دادن به یک فراخوان قضایی) الکوا همچنین اطمینان پیدا می کند که شخص ثالث اجبـار دارد

(قانوناً، قرارداد، یا جواز زیستگاه امن خود) حداقل همان سطح از حفاظت زندگی خصوصی همان طور که با این خط و مشی الزامی است ارائه دهد.

جائیکه الکوا قراردادهایی با اشخاص ثالث برای پردازش اطلاعات شخصی از جانب خـودش مـی بنـدد خط مشی الکو این است که از نظر قـراردادی اشـخاص ثالـث را وادار کنـد محرمانـه بـودن و ایمنـی اطلاعات شخص را که دریافت می کنند را حفظ کنند و فقـط طبـق رهنمودهـایی کـه از الکـوا و یـا مشتری دریافت می کنند روی آن عمل کنند و این اطلاعات را اکیداً مطـابق ایـن خـط و مشـی اداره کنند.

ایمنی:

الکوا احتیاط های معقولی بکار می برد، شامل اداری، فنی، کارمندان و معیارهای فیزیکی تا از اطلاعات شخصی در مقابل اتلاف شدن، سوء استفاده و دسترسی غیرمجاز، فاش سازی، تغییر و نابودی حفاظت شود. خط و مشی های ایمنی الکوا، رویه های عملکرد و کنترل های فنی، هر جا که قابل اجـرا اسـت عموماً استانداردهای پذیرفته شده متداول، زیربنا، کاربردها و داده ها را رعایت می کنند.

الکوا جمع آوری اطلاعات شخصی خود را به آنچه که اهـداف قـانونی و تجـاری در نظـر گرفتـه شـده مربوط است محدود می کند. الکوا از داده ها به طریقی که مغایر با اهدافی اسـت کـه بـرای آن جمـع آوری شده اند یا متعاقباً از طرف فرد مجاز شده اند استفاده نمی کنند تا حدی که بـرای ایـن اهـداف الزامی است، الکوا قدم های معقولی برای اطمینان از این که اطلاعات شخصی برای کاربرد مورد انتظار معتبر، دقیق (صحیح) کامل و رایج است بر می دارد.

دسترسی:

الکوا به افراد فرصتی برای دسترسی اطلاعات شخصی درباره خودشـان بـرای صـحیح کـردن، اصـلاح کردن یا حذف کردن اطلاعاتی که ناصحیح، قدیمی یا نامربوط ارائه می دهد، به استثنای مـوقعی کـه بار مسئولیت یا هزینه تأمین کردن دسترسی با ریسک های زندگی خصوصی فرد نامتناسب باشـد، یـا هرگاه که حقوق اشخاصی به غیر از آن فرد تخطی می شود.

اجرا:

الکوا با صاحب منصبان حفاظت داده های اروپایی، وزارت بازرگانی ایالات متحـده، کمیسـیون اصـناف فدرال ایالات متحده، مؤسسه های ایالتی و ولایتی وابسته، و صاحب منصبان قضایی و اجرایـی قـانون در ارزیابی هر شکایت زندگی خصوصی یا تخطی های مشکوک از قوانین زندگی خصوصی یا تعهـدات زیستگاه امن بین المللی الکوا و همچنین در بر طرف کردن هر عمل ناموافق همیاری می کند.

کارکنان یا مقاطعه کاردانی که از شرایط ایـن خـط و مشـی تخطـی کننـد ممکـن اسـت در معـرض پیامدهای انضباطی تا و شامل پایان یابی شغل یا پایان یابی و عدم تمدید قرارداد، علاوه بر هـر معیـار قانونی که ممکن است توسط الکوا، مشتری ماشین، یا افراد تحت تأثیر قرار گرفتـه و نماینـدگان آنهـا قرار گیرند.

۳–۲–۲ الکو بعنوان پردازش کننده داده ها

در رابطه با اطلاعات شخصی دریافت شده از اروپا که در آنجا الکوا بعنوان یک پردازشگر داده ها (یعنی داده هـــا در AS/۴۰۰، EBS Oracle و HRMS Oracle و سیســـتم هـــای پســـت الکترونیکی Microsoft Exchange)، هر دسترسی با استفاده از چنین داده هایی توسط شعبه هـا و وابسته های اروپایی جمع آوری کننده این داده ها کنترل می شوند. کارمنـدان در مرکـز داده هـای امریکای شمالی الکوا به این داده ها دسترسی ندارند و کاربردی برای این داده ها ندارند، تنهـا وظیفـه آنها تأمین حمایت فنی محدود لازم برای راندن این سیستم ها روی سرورهای الکوا بـه نفـع کـاربران مجاز در اروپا است.

بر وفق پیش بینی های زیستگاه امن ۱۰- FAQ- ، الکو با هر یک از شعبه ها و وابسته های اروپـایی خود قراردادی بسته که داده ها را در یکی از سیستم های پشتیبانی شده کنترل کنند.

تحت شرایط این قرارداد، الکوا موظف است این داده ها را فقط مطابق رهنمودهایی از مؤسسه مستقل تجاری اروپایی صادر کننده پردازش کند و سطح مناسبی از ایمنی برای داده ها تأمین کند.

۱. محدودیت ها در پردازش

الکوا اکیداً بعنوان یک پردازش کننده "دراز ـ دست" داده ها در رابطه با داده های موجود در سیستم های مورد پشتیبانی ارجاع شده در بالا، با یگانه مسئولیت حفاظت و راندن سیستم ها عمل می کنـد. الکوا مجاز نیست به اطلاعات شخصی در این سیستم ها دسترسی داشته باشد و از آنها اسـتفاده کنـد. کارمندان مرکز داده های آمریکایی که سعی کنند تشریفات ایمنی را نادیـده بگیرنـد و بـه اطلاعـات شخصی دسترسی پیدا کنند در معرض اخراج شدن و پیگرد قانونی قرار می گیرند.

۲. ایمنی

الکوا اقدامات احتیاطی معقول، شامل معیارهای اداری، فنی، کارکنان و فیزیکی برای حفاظت اطلاعات شخصی در مقابل اتلاف، سوء استفاده، دزدی، و دسترسی غیر مجاز، فاش سـازی، تغییـر و نـابودی را انجام می دهد. خط و مشی ایمنی الکوا، رویه های عملکرد و کنترل های فنی هرگاه که اجـرا شـدنی است، عموماً به استانداردهای پذیرفته شده متداول برای ایمنی شبکه ها، زیربنـا، کاربردهـا و داده هـا جور هستند.

همانطور که در ۱۰ FAQ نشان داده شده، شعبه ها و وابسته های اروپایی الکوا، بعنوان کنترل کننده های داده ها، مسئول دنبال کردن سایر اصول زندگی خصوصی یا پیش بینی هـای قـانونی محلـی، از قبیل آنهایی که به توجه، گزینش، درستی داده ها، دسترسی و غیره مربوط هستند باقی می مانند.

اجابت: الکوا از یک برنامه خود ارزیابی سالانه برای رسیدگی به این که اثبات هایی کـه تحـت برنامـه زیستگاه امن انجام می دهد درست هستند و خط مشـی هـای زنـدگی خصوصـی آن در عمـل مجـاز هستند استفاده می کند. بعلاوه، الکوا با شعبه ها و وابسته های اروپایی خود و صاحب منصبان حفاظت داده های اروپایی برای برطرف کردن هر شکایتی که ممکن است در رابطه با اطلاعات شخصی منتقل شده تحت برنامه زیستگاه امن همکاری می کند.

محل ارتباط. ارتباط دارای سؤالات یا ملاحظات درباره اداره کـردن اطلاعـات شخصـی توسـط الکـوا بدنبال انتقال آن از اروپا می توانند با آلن لوین، متصدی خط و مشی زیستگاه امن در شهر بینربورک، ایالت پنسلوانیا.

سیستم های ادوبی به ثبت رسیده

۳–۳ موافقتنامه گواهینامه نرم افزار خوانشگر ادوبی

توضیح به کاربر: لطفاً این قرارداد را با دقت بخوانید. با بکار بردن تمامی یـا بخشـی از ایـن نـرم افـزار خوانشگر ادوبی ("نرم افزار") شما با کلیه‌ی شرایط و اهداف ایـن موافقتنامـه را مـی پذیریـد. شـامل، بخصوص محدودیت ها درباره‌ی: کاربرد مندرج در بخش ۲؛ انتقـال پـذیری در بخـش ۴، ضـمانت در بخش ۶، و مسئولیت در بخش ۷. شما موافقت می کنید که این موافقتنامه مثل هر موافقتنامه مذاکره شده کتبی امضاء شده توسط شما از نظر قانونی قابل اجرا است. این موافقتنامـه بـر علیـه شـما و هـر تمامیت قانونی که این نرم افزار را فراهم کرده و از جانب او بکار گرفته می شود از نظـر قـانونی قابـل اجرا است. اگر موافقت ندارید، از این نرم افزار اسـتفاده نکنیـد. اگـر ایـن نـرم افـزار را از رسـانه هـای محسوس (مثلاً سی ـ دی) بدون فرصتی برای مرور این گواهینامه فراهم کردیـد و ایـن موافقتنامـه را قبول ندارید، ممکن است پول خود بهر مقدار که در اصل پرداخت کردید را پس بگیرید اگر: (آ) از این نرم افزار استفاده نکنید و (بی) آنرا پس بدهید، با مدرک پرداخت، به محلی که از آنجا فـراهم شـد در ظرف سی (۳۰) روز از تاریخ خرید.

ادوبی تأمین کننده های آن مالک تمامی خصیصه فکری در نرم افزار است. ادوبی اجازه می دهد شـما این نرم افزار را فقط در هماهنگی با شرایط این موافقتنامه بکار گیرید. استفاده از برخی مطالب ثالـث شامل در نرم افزار ممکن است منوط به سایر شرایط و مناسبات باشند که بطور نمـادین در توافقنامـه گواهینامه جداگانه یا فایل (مرا بخوان) مستقر در نزدیکی چنین مطالبی یافته می شود.

۱. تعریف ها. "نرم افزار" یعنی (۱) کلیه‌ی محتویات فایل ها، دیسک (ها)، سی دی (ها) یا سایر رسانه هایی که با آن این موافقتنامه تدارک دیده شده، شامل امّا نه محدود به لذا ادوبی یا اطلاعـات یـا نـرم افزار رایانه ثلث؛ مطالب مکتوب توضیحی مربوط یا فایل ها ("تشکیل پرونده")! و فونت ها (یک دست حروف یک جور) و (۲) بهسازی ها، ویرایش های تعدیل شده، به روز شدن ها، اضافه ها، و نسخه هایی از نرم افزار، اگر هیچ، گواهی شده به شما از طرف ادوبی (مشترکاً "به روز شـدن هـا"). "کـاربرد" یـا "بکار بردن" یعنی دسترسی، نصب، دان لود، کپی، یا مزایای غیر از این از اسـتفاده کـاربرد پـذیری از نرم افزار مطابق با ارائه سند.

"تعداد مجاز" یعنی یک (۱) مگر این که بطور دیگری تحت یک گواهینامه معتبـر (یعنـی گواهینامـه مقدار زیاد) ارائه شده توسط ادوبی نشان داده شده اسـت. "رایانـه" یعنـی یـک دسـتگاه الکترونیکـی اطلاعات به شکل دیجیتال یا مشابه قبول می کند و بر مبنای یک توالی رهنمودها آنرا بکار مـی بـرد. "ادوبی" یعنی سیستم های ادوبی به ثبت رسیده، یک شرکت دارای شخصیت حقوقی از ایالـت دلاور (در امریکا) به آدرس پلاک ۳۴۵ خیابان پارک، شهر سن حوزه ایالت کالیفرنیا. ۹۵۱۱۰، اگر زیر بخش (a) 9 این توافقنامه بکار رود، در غیر این صورت یعنی سیستم های نرم افزار ادوبی ایرلند با مسئولیت محدود جمهوری ایرلند، یک شرکت سازمان یافتـه تحـت قـوانین ایرلنـد، شـعبه و دارنـده‌ی جـواز از سیستم های ادوبی به ثبت رسیده. ۲. گواهینامه نرم افزار. مادامیکـه شـما از شـرایط ایـن موافقتنامـه گواهینامه نرم افزار (این موافقتنامه) پیروی می کنید، ادوبی به شما یک گواهینامه غیر انحصاری برای استفاده از این نرم افزار برای مقاصد توصیف شده در مستندات اعطا می کند.

کاربرد عمومی. شما می توانید یک کپی از این نرم افزار را در رایانه دارای قطعات سازگار خود، حداکثر تا تعداد مجاز رایانه، نصب کنید.

کاربرد در سرور و توزیع

منوط به شرایط این موافقتنامه، شما می توانید یک کپی از این نـرم افـزار را در یـک سـرور فایـل در محدوده‌ی شبکه داخلی خود تنها برای هدف انحصاری کاربرد نرم افزار (از تعداد نامحدود رایانه هـای

مشتری در شبکه داخلی شما) از طریق سیستم فایل شبکه (ان ـ اف ـ اس) برای ویرایش های یونیکس نرم افزار سرویس های پایانه ویندوز نصب کنید. مگر این که صریحاً در ذیل اجازه داده شده، کاربرد شبکه یا سرور دیگری از این نرم افزار مجاز نیست. شامل امّا نه محدود به این نرم افزار مستقیماً یا از طریق دستورات، داده ها یا دستورها از یا به رایانه دیگر یا(برای شبکه داخلی، اینترنت یا خدمات میزبانی وب.

برای اطلاعات درباره چگونگی توزیع نرم افزار روی رسانه های محسوس یا از طریق یک شبکه داخلی لطفاً به بخش های با عنوان "چطور محیط خوانشگر ادوبی را توزیع کنیم."

کپی پشتیبان. شما می توانید یک کپی پشتیبان از این نرم افزار ایجاد کنید، مشروط بر این که کپی پشتیبان شما در هیچ رایانه ای نصب یا استفاده نمی شود. شما نمی توانید حق مالکیت را به کپی پشتیبان انتقال دهید مگر این که همه حقوق در نرم افزار را همانطور که ارائه شده انتقال دهید.

کاربرد در رایانه های قابل حمل یا خانگی. علاوه بر کپی تک مجاز تحت ، کاربر اصلی رایانه ای که این نرم افزار نصب شده می کند کپی ثانوی از این نرم افزار برای کاربرد انحصاری خود در رایانه قابل حمل یا رایانه مستقر در خانه او ایجاد کند، شروط بر این که این نرم افزار در رایانه قابل حمل یا خانگی در همان زمان بعنوان نرم افزار در رایانه اصلی بکار نمی رود.

عدم تغییر و تبدیل. شما می توانید نصب کننده برای این نرم افزار را سفارشی کنید یا گسترش دهید. (یعنی نصب فایل های کمک و نصب خودکار).

در غیر اینصورت شما نمی توانید این نرم افزار را تغییر دهید یا تبدیل کنید یا برای آن نصب کننده جدیدی ایجاد کنید. این نرم افزار توسط ادوبی برای مشاهده کردن، توزیع کردن یا بطور مشترک استفاده کردن فایل های پی ـ دی ـ اف گواهی شده است. شما مجاز نیستید این نرم افزار را ادغام کنید یا با هر نرم افزار دیگری، نصب خودکار یا بهسازی که از این نرم افزار در موقع تبدیل یا انتقال فایل های پی ـ دی ـ اف به سایر فرمت های فایل استفاده می کند یا به آن متکی است (یعنی یک فایل پی ـ دی ـ اف به فایل های تی ـ آی ـ اف ـ اف ، JPEG یا SVG) استفاده کنید. شما مجاز

نیستید این نرم افزار را با هر نرم افزار (1) نصب خودکار ایجـاد نشـده مطـابق موافقتنامـه گواهینامـه کلیدی ادغام ادوبی، (2) نرم افزار دیگری یا هم کنشگر برنامه ریزی شونده برای بهسازی با ایـن نـرم افزار به منظور ذخیره کردن داده ها بطور موضعی (در همان رایانه)، به اسـتثنای هنگامیکـه از طریـق استفاده از مشخصه (s) مدرک مجاز شده با استفاده از تکنولـوژی میسـر از ادوبـی فعـال شـده اسـت بوجود آوردن یک فایل که حاوی داده ها است ، ذخیره کردن تغییرات در یک فایل پـی ـ دی ـ اف، ادغام یا استفاده کنید.

دستیابی وب سایت ثالث. این نرم افزار شما را مجاز می کند که به وب سایت های ثالث دسترسی پیدا کنید ("سایت های ثالث"). دستیابی و استفاده شما از وب سایت ثالث، شـامل هـر کـالا، خـدمات یـا اطلاعات فایل دسترسی از چنین سایت هایی از طریق شرایط و مناسـبات یافتـه در هـر سـایت ثالـث کنترل می شود، اگر هیچ. سایت های ثالث در مالکیت ادوبی نیستند یا توسط ادوبی بکار انداخته نمی شوند. کاربرد شما از سایت های ثالث با ریسک خود شما است. ادوبی هیچ تضـمین، شـرایط، غرامـت، عرضه کردن یا مناسباتی صریح یا متضمن خواه با منزلـت، قـانون عرفـی، سـنت، کـاربرد یـا در غیـر اینصورت مثل هر مورد دیگری، شامل امّا نه محدود به حقوق ثالث عدم تخلف، عنـوان، ادغـام، دقـت، ایمنی، موجودیت، کیفیت رضایتبخش، قابلیت بازرگانی یا مناسب بودن برای هر هـدف بخصوصـی در رابطه با سایت های ثالث نمی کند.

۳–۳–۱مدارک گواهی شده

مدارک گواهی شده و خدمات سی ـ دی. این نرم افزار به شما اجازه می دهـد اسـناد گـواهی شـده را دارای اعتبار کنید. یک "مدرک گواهی شده" یا " سی دی" یک فایل پی ـ دی ـ اف است که بطریق دیجیتال با استفاده از (1) جواز و (2) یک کلید "خصوصی" کد گذاری که مشابه کلمه "عمومی" در جواز است امضاء شود. معتبر ساختن یک سی دی احتیاج به خدمات سی دی از تأمین کننده سرویس سی ـ دی احتیاج دارد که جواز را صادر کرد. "تأمین کننده جواز سی دی" یـک فروشـنده سـرویس

ثالث مستقل است "خدمات سی دی" خدماتی هستند که توسط تأمین کنندگان سـرویس سـی دی ارائه می شوند، شامل بدون محدودیت جوازهای عرضه شده توسط چنین ارائه دهنده سـی دی بـرای استفاده با مشخصه سی دی نرم افزار، (b) خدمات مرتبط با انتشار جوازها، و (c) سایر خدمات مرتبط با جوازها، شامل بدون محدودیت تأثیر خدمات.

تأمین کنندگان سرویس سی دی:

هر چند این نرم افزار خصوصیات ثانیه را تأمین می کند. ادوبی خدمات سـی دی لازم بـرای اسـتفاده این خصوصیات را عرضه نمی کند. خریداری، موجودیت و مسئولیت برای خدمات سی دی بین شما و تأمین کننده سرویس سی دی است. قبل از این که به هر سی دی متکی باشید. هر امضای دیجیتـال بکار برده شده در آنجا او یا هر خدمات سی دی مرتبط شما ابتدا باید با بیان ارائه کننده مربوط و این موافقتنامه را مرور کنید. "بیان ارائه کننده" یعنی مناسبات و شرایط که تحت آن هـر تـأمین کننـده سرویس سی دی خدمات سی دی ارائه می دهـد بـرای مثـال شـامل هـر موافقتنامـه امضـاء کننـده، موافقتنامه های گروه متکی، سیاست های جواز و بیانات عمل، و از این موافقتنامه. با معتبر کردن یک سی دی با استفاده از خدمات سی دی، شما اذعان و موافقت می کنید که جواز بکار رفته برای امضای دیجیتالی یک سی دی ممکن است در زمان بررسی لغو شود، معتبر کردن امضای دیجیتـالی در سـی دی هنگامیکه در واقع معتبر نیست، ایمنی یا درستی یک سی دی ممکن است در اثر یک عمل یا لغو شدن توسط امضاء کننده سی دی، تأمین کننده سـرویس سـی دی مربـوط، یـا هـر شـخص سـوّمی مصالحه شود و شما باید اظهاریه ارائه دهنده مربوط را بخوانید، درک کنید و به آن وابسته باشید.

تکذیب نامه ضمانت:

تأمین کنندگان سرویس سی دی، خدمات سی دی را فقط مطابق بـا اظهاریـه ارائـه دهنـده مربـوط عرضه می کنند. دسترسی به خدمات سی دی از طریـق اسـتفاده از ایـن نـرم افـزار فقـط بـر مبنـای "همانطور که هست" موجودیت پیدا می کند و هر ضمانت یا مصونت از هر نوع (به استثنای همانطور که توسط یک ارائه دهنده خدمات سی دی در اظهاریه ارائه دهنده آن عرضه شده). ادوبی و هر تأمین

کننده سرویس CD (به استثنای آنطور که صریحاً در اظهاریه ارائه دهنده عرضه شده) هیچ ضـمانت، مصونت، نمونه ها یا مناسبات بیان شده یا مستلزم، خواه با موقعیت، قانون عرفی، روان، کـاربرد یـا در غیر اینصورت بعنوان هر مورد دیگر شامل امّـا نـه محـدود بـه عـدم مصـونیت حقـوق ثالـث، عنـوان، یکپارچگی، دقت، ایمنی موجودیت، کیفیت رضایت بخش، قابلیت بازرگانی یا تناسب بـرای هـر هـدف بخصوص در رابطه با خدمات سی دی نمی کند.

مصونیت:

شما موافقت می کنید که ادوبی و هر تأمین کننده سرویس سی دی را (به استثنای آنکـه صـریحاً در اظهاریه ارائه دهنده عرضه شده) از هر و تمامیت مسئولیت ها، اتلاف ها، عملکردها، صدمات یا ادعاهـا (شامل همه مخارج معقول، هزینه ها و هزینه های وکیل ها) بوجود آمده از هر کاربرد مربوط، یا متکی به آن، هر سرویس سی دی، شامل، بدون محدودیت (1) اتکا به یک جواز خاتمه یافته یا لغو شده (2) بررسی نامناسب یک گواهی، (3) استفاده از یک جواز به غیر از آنچه توسط هر اظهاریه ارائـه دهنـده مربوط مجاز شده، این موافقت نامه یا قانون مربوط، (4) قصور از اجرای قضاوت معقول تحـت شـرایط در اتکا به خدمات سی دی، و (5) قصور در عملکرد هر الزاماتی همانطور که در اظهاریه ارائـه دهنـده مربوط است، صحیح و سالم حفظ کنید.

محدوده مسئولیت. تحت هیچ شرایطی ادوبی یا هیچ یک از تأمین کننـدگان سـرویس سـی دی (بـه استثنای آنچه صریحاً در اظهاریه ارائه دهنده بیان شده) در مورد شـما یـا هـر شـخص یـا موجودیـت دیگری برای هر اتلاف از کاربرد، درآمد یا سود، اتلاف یا صدمه داده ها، یا هر اتلاف اقتصادی یا تجاری برای هر نوع صدمات منتخبه مستقیم، غیر مستقیم، تصادفی، ویژه، کیفری، جزایی، هشدار دهنده، هر آنچه که به استفاده شما یا اتکا به خدمات سـی دی، حتـی اگـر مشـورت چنـین امکانـاتی از چنـین صدماتی یا اگر چنین صدماتی قابل پیش بینی هستند. مسئول خواهد بود. این محدودیت بایـد حتـی در مورد تخلف از موارد اصلی موافقتنامه اعمال خواهد شد.

بهره وران ثالث شما موافقت می کنید که هر ارائه دهنده سرویس سی دی را بکار می برید یک ذینفع ثالث در رابطه با بخش ۷. ۲ این موافقت نامه خواهد بود، که چنین تأمین کننـده سـرویس سـی دی حق خواهد داشت که این شرایط را به رسم خودش تحمیل کند اگر تأمین کننده سـرویس سـی دی ادوبی بود.

مالکیت خصلت هوشمندی:

حفاظت حق منبع و نشر. این نرم افـزار و کپـی هـای مجـاز آن کـه شـما تهیـه مـی کنیـد خصـلت هوشمندی و در مالکیت سیستم های ادوبی و فروشنده های آن است. ایـن نـرم افـزار تحـت حمایـت قانونی است شامل امّا نه محدود به قوانین حق منبع و نشر ایالات متحده و سایر کشورها و همچنـین تحت حمایت قوانین معاهده بین المللی است. به استثنای هنگامیکه صریحاً همه حقوقی کـه صـریحاً اعطا نشده اند به ادوبی و فروشنده های آن اختصاص دارند.

۳-۳-۲ محدودیت ها

ملاحظات:

شما نباید از این نرم افزار کپی بگیرید به استثنای آنطوری که در بخش ۲ نوشته شده. هر کپی از این نرم افزار که شما می گیرید باید شامل همان حق طبع و نشر و سایر ملاحظات دارای حقوق انحصاری باشد که روی این نرم افزار به چشم می خورد.

عدم پیرایش (اصلاح):

نباید این نرم افزار را اصلاح، اقتباس یا ترجمه کنید. نباید مهندسـی معکـوس، نـاهمگردانی، تـا هـم گذارد کنید یا در غیر اینصورت سعی در کشف کردن کد منبع نرم افزار داشته باشید بـه اسـتثنای تـا حدی که صریحاً به شما اجازه داده شده تحت قانون مربوط ناهمگردانی کنید. به منظور بدست آوردن کنش پذیری این نرم افزار با برنامه نرم افزاری دیگر انجام بین کار الزامی است، و شما ابتـدا از ادوبـی درخواست ارائه اطلاعات لازم برای چنین کـاربرد پـذیری کـرده ایـد و ادوبـی چنـین اطلاعـاتی را در

دسترس قرار نداد. ادوبـی حـق دارد شـرایط معتـدل تحمیـل کنـد و قبـل از ارائـه چنـین اطلاعـاتی درخواست اجرت (پول) معقول بکند. هر چنین اطلاعاتی عرضـه شـده توسـط ادوبـی و هـر اطلاعـات بدست آمده ای توسط شما برای انجام چنین ناهمگردانی مجازی نمی تواند فقط برای هـدف توصـیف شده در این باره بکار رود و نمی تواند برای شخص ثالثی افشاء شود و یا برای بوجود آورد نرم افـزاری که اساساً نشانگر این نرم افزار است بکار رود. درخواست ها برای اطلاعات باید به بخش حمایت مصرف کننده ادوبی فرستاده شود.

مشخصات سند:

این نرم افزار ممکن است شامل مشخصـات و کـارایی باشـد کـه از کـار افتـاده یـا "کمرنـگ شـده" ("مشخصات سند") به چشم بخورد. این مشخصات سند فقط هنگامی فعال می شود که سندهای پی ـ دی ـ اف بخصوصی را باز کنید که با استفاده از تکنولوژی قادر کننده متناظر موجود فقط از طریـق ادوبی بودجود آمده باشد ("کلیدها") شما موافقت می کنید که به مشخصات سند از کار افتـاده شـده دسترسی پیدا نکنید یا سعی نکنید دسترسی پیدا کنید، در غیر اینصورت اجازه هـایی را کـه کنتـرل فعال کردن چنین مشخصات سندی را دارند را در معرض خطر قرار می دهید. شما فقـط مـی توانیـد مشخصات سند را با سندهای پی ـ دی ـ اف استفاده کنید که با اسـتفاده از کلیـدهای بدسـت آمـده تحت گواهینامه معتبری از ادوبی بدست آمده است. کاربرد دیگری مجاز نیست.

اتصال. شما می توانید حقوق خود را در این نرم افزار را اجاره دهید، گواهینامه خود را جایگزین کنید، تخصیص یا اتصال دهید، یا اجازه دهید تمامیت یا بخشی از این نرم افزار به رایانه دیگری کپی شود به استثنای در این مورد صریحاً مجاز باشید. بهرحال، می توانید تمامی حقوق خود در مـورد اسـتفاده از این نرم افزار را به شخص دیگر یا نهاد قانونی دیگر انتقال دهید مشروط بر این که: (1) همچنین این توافق نامه و نرم افزار و همه نرم افزار یا سخت افزار دیگر که با نرم افزار بسته بنـدی شـده بـود یـا از بیش نصب شده بود، شامل همه کپی ها، نسخه های به روز شده و نسـخه هـای قبلـی، را بـه چنـین شخص یا نهادی انتقال دهید. (2) شما هیچ نسخه ای نگه ندارید، شامل پشـتیبان هـا، و کپـی هـای

ذخیره شده در رایانه و (3) دریافت کننده شرایط و مناسبات را بین موافقتنامه را مـی پـذیرد و همـه شرایطی دیگری را که قانون ها برای گواهینامه این نرم افزار خریداری کرد را با نپذیرفتن آنچه در بازار ذکر شد، شما نمی توانید کپی های آموزشی، از بیش بیرون داده شده یـا نـه بـرای فـروش را انتقـال دهید.

به روز سازی ها:

اگر این نرم افزار به روز شده یک ویرایش قبلی از این نرم افزار است، برای استفاده از ایـن نسـخه بـه روز شده می توانید از چنین ویرایش قبلی یک گواهینامه معتبر داشته باشید. همه به روز شده هـا بـر مبنای مبادله گواهینامه به شما عرضه می شوند. شما موافقت می کنید که با اسـتفاده از یـک نسـخه بروز شده داوطلبانه گواهینامه خود را برای استفاده از نسخه قبلی نرم افزار باطل کنیـد. بعنـوان یـک استثناء می توانید به استفاده از نسخه قبلی ادامه دهید تا به شما در انتقـال بـه نسـخه بـه روز شـده کمک کند مشروط بر این که: (1) نسخه های به روز شده و قبلی در یک رایانه نصب شده باشند (2) نسخه های قبلی یا کپی های به روز به همان رایانه یا بخش منتقل شده باشند و (3) شما اذعان مـی کنید که هر اجباری که ممکن است ادوبی برای پشتیبانی نسخه قبلی داشته باشید می توانید طبق در دسترس بودن نسخه به روز خاتمه یابد.

بدون ضمانت:

این نرم افزاربصورت "همانطور که هست" تحویل داده می شود و ادوبی در مورد استفاده یـا عملکـرد آن هیچ ضمانتی نمی کند. ادوبی و فروشندگان آن نمی توانند عملکرد یا نتایجی را که ممکن است با استفاده از این نرم افزار بدست آورید را ضمانت کند. به استثنای هر ضمانتی، شـرایط، نشـان دادن یـا مناسبت به حدی که بطور یکسان نمی تواند یا ممکن نیست با قانون مربـوط بـه حـوزه قضـایی شـما مربوط باشد انحصار داشته یا محدود باشد، ادوبی و فروشندگان آن هیچ ضمانتی از شرایط، ارائه دادن ها، یا مناسبات (صریح یا ضمنی، خواه با چگونگی، قانون عرفی، سنت، کاربرد با طور دیگـر) مثـل هـر مورد شامل بدون محدودیت بدون تخطی از حقوق شخص ثالث، قابلیت بازرگانی، یکپارچگی، کیفیـت رضایت بخش یا تناسب برای هر منظور بخصوص داشته باشند.

محدودیت مسئولیت:

تحت هیچ پیامدی ادوبی یا فروشندگان آن مسئول هیچ صدمه، ادعا یا هزینه ای به هر مقدار یا هیچ صدمه دارای عواقب، غیر مستقیم، تصادفی، یا هیچ اتلاف سود دهی یا اتلاف اندوخته ها حتی اگر یک نماینده ادوبی در مورد امکان چنین اتلاف، صدمات، ادعاها یا هزینه ها یا برای هر ادعـایی توسـط هـر شخص ثالثی مورد مشورت قرار گرفته باشد نخواهند بود. محدودیت های مذکور و استثناعات به حـد مجاز با قانون مربوط در حوزه قضایی شما اعمال می شود. مسئولیت بر افزوده ادوبی و فروشندگان آن تحت این موافقت نامه یا در رابطه با آن به مقدار پرداخت شده برای این نرم افزار محدود خواهـد بـود اگر چیزی پرداخت شده باشد. هیچ چیز محتوی این موافقتنامه مسئولیت ادوبی نسبت به شـما را در نتیجه مرگ یا آسیب شخصی منتج از قصور ادوبی یا عمل خلاف کلاهبرداران (فرسطری) محدود نمی کند. ادوبی به طرفداری از فروشندگان خود به منظور به عهده نگرفتن، جلوگیری و یا محـدود کـردن تعمدات، ضمانت ها و مسئولیت ارائه شده در این موافقتنامه اقدام می کند، امّا نه در مورد هیچ منظور و موردی دیگر. برای اطلاعـات بیشـتر، لطفـاً بـه اطلاعـات مخصـوص حـوزه قضـایی در انتهـای ایـن موافقتنامه مراجعه کنید. یا با بخش پشتیبانی مشتری ادوبی تماس بگیرید.

۳-۳-۳مقررات صادر کردن

شما موافقت می کنید که این نرم افزار به هیچ کشوری فرستاده، انتقال داده یا صادر نخواهد شد یا به هیچ طریقی مخالف یا لایحه اداره صادرات ایالات متحده با هـیچ قـانون صـادرات، محـدودیت هـا یـا مقررات بکار نخواهد رفت. (مشترکاً "قوانین صادرات"). بعلاوه، اگر این نرم افزار بعنوان اقـلام کنتـرل شده صادرات تحت قوانین صادرات مشخص شده وانمود می کنید و تضمین می کنید که یک شهروند نیستید، یا در غیر اینصورت مستقر در یک کشور تحریم شده (شامل و بدون محدودیت ایـران، عـراق، سوریه، سودان، لیبی، کوبا، کره شمالی و عربستان) و که در غیر اینصـورت تحـت قـوانین صـادرات از

دریافت این نرم افزار ممنوع نشده اید. تمام حقوق برای بکار بردن این نرم افزار به شرط آنکـه چنـین حقوقی از دست می روند اگر شما از پیروی از شرایط این توافقنامه قصور کنید اهدا می شوند.

قانون حاکم:

این موافقت نامه در مطابقت با قوانین اصولی معتبر ایجاد و اداره می شود: (1) در ایالت کالیفرنیا، اگر یک گواهینامه هنگامیکه در ایالت متحده، کانادا یا مکزیک هستید بدست می آیـد (2) در ژاپـن اگـر یک گواهینامه برای این نرم افزار بدست می آید هنگامیکه در ژاپن، چـین، کـره یـا سـایر کشـورهای آسیای جنوب شرقی هستید جائیکه هم زبان های رسمی به صورت چشم نگار نوشته شده اند (یعنـی هانزی، کانجی یا هنجا)، و یا سایر دستخط ها بر مبنای یا مشابه در ساختار به دستخط چشم نگـار از قبیل هانگول یا کانا یا (3) انگلستان، اگر یک گواهینامـه بـرای ایـن نـرم افـزار خریـداری مـی شـود هنگامیکه در سایر حوزه های قضایی توصیف نشده در بالا. دادگاههای بخش سـنتاکلارا، در کالیفرنیـا هنگامیکه قانون کالیفرنیا اعمال می شود، دادگاه ناحیه توکیو در ژاپن، هنگامیکه قانون ژاپنـی اعمـال می شود، و دادگاههای کاردان انگلستان، هنگامیکه قوانین انگلستان اعمال می شـود، هـر یـک حـوزه قضایی غیر انحصاری طی تمام حقارهای مربوط به این توافقنامه خواهند داشت. این توافق نامه با تضاد قوانین هر حوزه قضایی یا اجلاس سازمان ملل در قراردادهایی برای فروش کالاهای بـین المللـی، کـه کاربرد آن صریحاً جلوگیری شده حاکم نخواهد بود.

تبصره های عمومی:

اگر هر قسمت از این موافقتنامه فاقد ارزش قانونی و غیر قابل اجرا باشد، به اعتبار این موافقت نامه اثر نخواهد گذاشت. که مطابق با شرایط آن معتبر باقی خواهد ماند. این موافقت نامه حقوق قـانونی هـیچ شخصی را که بعنوان یک مصرف کننده است را است پیشداوری نخواهد کرد. این موافقت نامـه فقـط می تواند با اجازه امضاء شده یک صاحب منصب ادوبی اصلاح و پیرایش شود. به روز شده ها می توانند توسط ادوبی با شرایط اضافی یا مختلف گواهی شونده این تمام موافقـت نامـه بـین ادوبـی و شـما در

رابطه با این نرم افزار است و به هر ارائه بیشین بحث ها تقبل ها، محاورات یا تبلیغات مرتبط بـه ایـن نرم افزار ارجعیت دارد.

توضیح برای کاربران نهایی دولت ایالات متحده، این نرم افـزار و مسـتندات "اقـلام تجـاری" هسـتند بعنوان چنین حالتی در ۱۰۱. ۲ ۴۸C.F.R ، شامل "نرم افزار رایانه تجاری" و "مستندات نـرم افـزار رایانه تجاری" به این عنوان در ۲۱۲. ۱۲ ۴۸C.F.R یا ۷۲۰۲. ۲۲۷ ۴۸C.F.R همانطور که مرتبط هستند تعریف شده اند. سازگار با ۲۱۲. ۱۲ ۴۸C.F.R یا ۷۲۰۲. ۲۲۷ ۴۸C.F.R تا ۴-۷۲۰۲. ۲۲۷ همانطور که مرتبط هستند. گواهینامه نرم افزار رایانه تجاری و مستندات رایانه نرم افزار رایانه تجـاری به کاربران نهایی دولت ایالات متحده داده می شود. فقط بعنوان اقلام تجاری و (b) فقط با آن حقوق که به سایر کاربران نهایی در سایر کاربران نهایی پیرو این شرایط عرضه می شوند. حقوق چاپ نشـده منحصر تحت قوانین حق طبع و نشر ایالات متحده. سیستم های ادوبی به ثبت رسیده، برای کـاربران نهایی دولت ایالات متحده، ادوبی موافقت می کند از همه قوانین فرصـت برابـر مربـوط پیـروی کنـد، شامل، اگر مناسب باشد، تبصره های نظم اجرایی ۱۱۲۴۷، همانطور که در بخش ۲. ۴، لایه کمک بـه تجدید سازمان جنگ زده ها دوره ویتنام در سال ۱۹۷۴ و بخـش ۳. ۵ از لایحـه اعـاده سـال ۱۹۷۳، همانطور که تجدید نظر شد و مقـررات در سـی ـ اف ـ آر بخـش هـای ۱-۶۰ تـا ۶۰-۶۰، ۶۲۵-۶۰ و ۷۴۱-۶۰. سیاست جبران بی عدالتی ها نسبت به اقلیـت هـا و مقـررات محتـوی در جملـه قبلـی در مراجعه به این موافقت نامه تلفیق می شود.

توافق با گواهینامه. اگر یک بازرگانی یا سازمانی هستید. شما موافقت می کنید که طبق درخواسـت از ادوبی یا نماینده مجاز ادوبی، شما در سی (۳۰) روز با سند کامل و گواهی می کنید که هـر و تمـامی نرم افزار در زمان درخواست کاملاً با گواهینامه از ادوبی تطابق دارد.

استثناهای ویژه:

ضمانت محدود برای کاربران ساکن در آلمان یا اطریش. اگر این نرم افزار در آلمان یـا افـزایش کسـب کردید، و شما معمولاً در چنین کشوری ساکن هستید، پس بخش ۶ بـه شـما اعمـال نمـی شـود. در

عوض، ادوبی تضمین می کند که این نرم افزار کارایی مقرر در سند تأمین مـی کنـد ("کـارایی هـای توافق شده") برای ضمانت محدود بدنبال دریافت نرم افـزار هنگامیکـه در پیکربنـدی سـخت افـزاری توصیه شده بکار گرفته می شود. همانطور که در این بخش بکار رفت، "دوره ضمانت محـدود" یعنـی یک (۱) سال اگر یک کاربر تجاری هستید و دو (۲) سال اگر یک کاربر تجـاری نیسـتید. تغییـر غیـر اساسی از کارایی موافقت شده در نظر گرفته نخواهد شد و هیچ حقوق ضمانت برقرار نمـی کنـد. ایـن ضمانت محدود در نرم افزاری که به طور مجانی برای شما فراهم شده اعمال نمـی شـود، بـرای مثـال نسخه های به روز شده بیش از موعد پخش شده، تمرینی، نمونه محصول، نه برای فـروش (ان ـ اف ـ آر) یا نرم افزاری که توسط شما تغییر یافته، بطوری که تغییرات سبب نقص شـود. بـرای انجـام دادن ادعای ضمانت، طی دوره ضمانت محدود شما باید با هزینه خود، این نرم افزار و رسـید خریـد را پـس بفرستید. اگر کارایی های نرم افزار بطور اساسی از آنچه طبق آن موافقت شده تغییر کند. ادوبـی حـق دارد ـ از طریق عملکرد مجدد به اختیار خود. برای تعمیر یا جایگزینی این نرم افزار عمل کند. اگر این شکست خورد، شما مستحق به کاهشی در قیمت خرید یا لغـو کـردن موافقـت نامـه خریـد هسـتید. (ابطال). برای اطلاعات بیشتر در مورد ضمانت لطفاً با بخش پشتیبانی مصـرف کننـده ادوبـی ارتبـاط برقرار کنید.

۳–۴ محدودیت مسئولیت برای کاربران ساکن در آلمان و افزایش

اگر این نرم افزار را در آلمان یا افزایش کسب کردید، و معمولاً چنین کشوری اقامت دارید. مسـئولیت قانونی ادوبی برای صدمات بصورت ذیل محدود خواهد شد: (i) ادوبی فقط تـا مقـدار صـدمات سـؤال خواهد بود همانطور که نوعاً در زمان توافقنامه خرید پیش بینی شد نسـبت بـه صـدمات سـبب شـده توسط بی مبالاتی در اجبار قراردادی داده. و (ii) ادوبی برای صدمات سبب شده با بی مبالاتی جزیـی در اجبار قراردادی مسئول نخواهد بود.

محدودیت فوق الذکر مسئولیت به هیچ مسئولیت اجباری اعمال نخواهد شد بویژه تحت لایحه مسئولیت محصول آلمان، مسئولیت برای فرض ضمانت مشخص یا مسئولیت برای مقصر دانستن مسبب صدمات شخص.

شما الزام دارید همه معیارهای معتدل برای پرهیز و کاهش صدمات را در نظر بگیرید، بخصوص گرفتن کپی های پشتیبان از این نرم افزار برای داده های رایانه خود که در معرض تبصره های این موافقت نامه هستند.

شرایط اضافی محصول بیش از موعد پخش شده. اگر فرآورده ای که با این گواهینامه بدست آوردیده اید نرم افزار نمونه پیش تجاری یا بتارست ("نرم افزار بیش از موعد پخش شده") پس بخش بعدی اعمال می شود. به حدی که هر تبصره در این بخش با هیچ یک از شرایط یا روش ها در تضاد نیست این بخش باید به سایر شرایط و روش ها باید در رابطه با نرم افزار بیش از موعد پخش شده انتقال یابد، امّا فقط تا حدی که برای برطرف کردن تضاد لازم است. شما اذعان دارید که این نرم افزار ویرایش بیش از موعد است، نشانگر فرآورده نهایی از ادوبی نیست و ممکن است شامل ویروس ها، خطاها و سایر مشکلات باشد که ممکن است سبب از کار افتادن سیستم اتلاف داده ها شود. در نتیجه، نرم افزار بیش از موعد پخش شده به شما "همانطور که هست" عرضه می شود. و ادوبی منکر هر ضمانت یا مسئولیت اجباری نسبت به شما به هر طریق است. جائیکه مسئولیت برای نرم افزار بیش از موعد نمی تواند جلوگیری شود امّا می تواند محدود باشد، مسئولیت ادوبی. فروشنده های او به مجموع ۵۰ دلار امریکایی محدود خواهد بود، در کل.

شما اذعان دارید که ادوبی هیچ تعهدی به شما درباره این که نسخه بیش از موعد در آینده برای هر کس در دسترس خواهد بود، ندارد، ادوبی هیچ اجبار صریح یا متضمن نسبت به شما برای اعلام کردن یا معرفی نرم افزار بیش از موعد ندارد و ادوبی ممکن است فراورده ای شبیه یا هماهنگ (همسانه) یا نرم افزار بیش از مؤعد معرفی نکند. از اینرو، شما اذعان می کنید که هر تحقیق و توسعه ای که در رابطه با نرم افزار بیش از موعد انجام می دهید، کاملاً با ریسک خود آنرا انجام می دهید. طی شرایط

این موافقت نامه، در صورت درخواست ادوبی شما، بازتابی در رابطه با آزمایش و استفاده از نـرم افـزار بیش از موعد به ادوبی خواهید داد، شامل گزارش خطا یا ویروس. اگر نرم افزار بیش از موعد مقرر را با موافقت نامه ای کتبی بدست آورده اید از قبیل موافقت نامه چند بخشی ادوبـی بـرای فـرآورده هـای پخش نشده، استفاده شما از این نرم افزار تحت چنین موافقت نامه ای است. شما موافقت می کنید که و تضمین می کنید که این نرم افزار بیش از مؤعد پخش شده را اجازه نمی دهید یا گواهی نمی کنید و قرض نمی دهید. با دریافت ویرایش بعدی یا پخش شده توسط ادوبی از نسخه تجاری نرم افـزار، یـا بعنوان فرآورده منفرد یا بخشی از فرآورده ای بزرگتر، شما موافقت می کنید که همـه ویـرایش هـای قبلی را که از ادوبی دریافت کرده اید را نابود کنید. برعکس دوام نیافتی هیچ چیز در این تبصره، اگـر خارج از ایالات متحده امریکا هستید، شما موافقت می کنید کـه طـی سـی (۳۰) روز بعـد از تکمیـل کردن آزمایش نرم افزار همه ویرایش های بخش نشده را از بین خواهید برد هنگامیکه تاریخ زودتـر از تاریخ اولین ارسال تجاری است.

اگر هر سؤالی در مورد این موافقت نامه دارید یا مایلید از ادوبـی اطلاعـاتی درخواسـت کنیـد لطفـاً از آدرس و اطلاعات ارتباطی شامل با این فرآورده استفاده کنید که با دفتر کار ادوبی در خـدمت حـوزه قضایی شما ارتباط برقرار کنید. ادوبی و خوانشگر نام بازرگانی به ثبت رسیده سیستم هـای ادوبـی بـه ثبت رسیده در ایالات متحده و یا سایر کشورها است.

فصل چهارم

حفاظت در برابر حمله های تزریق از طریق ارزیابی

۴–۱ یکپارچه حساس حمله های متن

آسیب پذیری های تزریق تهدید بزرگی برای ایمنی سطح کاربرد مطرح می کند. برخـی از متـداول ترین انواع تزریق اس ـ کیو ـ ال، فایل آغازگر سراسری و آسیب پذیری های تزریـق برنامـه واسـطه است. روش های موجود برای حفاظت در برابر حمله های تزریق، یعنی، حمله هـایی از ایـن آسـیب پذیری ها بهره برداری می کنند به طور زیادی به توسعه دهندگان کاربرد متکی هسـتند و بنـابراین مستعد خطا هستند.

روشی برای کشف کردن و جلوگیری از حمله‌های تزریق. سی ـ اس ـ اس ـ ای با نشانی یابی ریشـه علت موفق شدن چنین حمله های کار می‌کند، یعنی تسلسل فاقـد عمومیـت ورودی توسـط کـاربر تأمین شده. استفاده از ترکـیبی از تخصـیص ابـر داده هـا بـه ورودی تـأمین شـده از طـرف کـاربر، عملکردهای حافظ ابر داده‌ها و ارزیابی یکپـارچه حساس به متن، یک برنامه عملی جدا از خط مشی ها ارائه می‌دهد.

سی ـ اس ـ اس ـ ای به فعل و انفعال توسعه دهنده کاربرد یا تعدیل های کد منبع کـاربرد احتیـاج ندارد. چون فقط تغییرات در برنامه عمل اصلی لازم هستند، بطور مثال بـار مسـئولیت اجـرا کـردن اقدام متقابل بر ضد حمله های تزریق از بسیاری توسعه دهندگان کاربرد را به تیم کوچکی از توسعه دهندگان برنامه ایمنی زیرک انتقال می دهد. روش ما در مقابل بیشارین انـواع حملـه هـای تزریـق موثر هستند، و ما نشان می دهیم به کمنر از سایر راه حل های تا بحال پیشنهاد شده کم تر مستعد خطا هستند.

ما برای پی ـ اچ ـ پی یک پیش نمونه اجرا کردن سی ـ اس ـ اس ـ ای ایجاد کرده ایم، طرحی کـه مخصوص مستعد این آسیب پذیری‌ها است. ما پیش‌نمونه خود را با پی ـ اچ ـ پی ـ بـی ـ بـی، یـک کاربرد تابلو اعلانات مشهور برای معتبر ساختن روش خد بکار بـردیم. سـی ـ اس ـ اس ـ ای کلیـه

حمله های تزریق اس ـ کیو ـ ال را P های باز تولید کرده و فقط سر جمع زمان عملکـرد معقـولی متحمل شویم را کشف و جلوگیری کرد.

در سال های اخیر افزایش یکنواختی در اهمیت آسیب پذیری های ایمنی سطح کـاربرد دیـده ایـم یعنی آسیب پذیری هایی که بجای سیستم عامل یا افزار میانی سیستم های رایانه به کاربردهـا اثـر می گذارند. از میان آسیب پذیری های سطح کاربرد، رتبه آسیب پذیری سطح ورودی برجسته ترین است. [H] و سزاوار توجه ویژه است.

آسیب پذیری های اعتبار ورودی کاستی های ناشی از فرضیات تلویحی انجام گرفته توسـط توسـعه دهندگان کابرد درباره کاربرد ورودی است. مخصوصاً، آسیب پذیری های اعتبار ورودی هنگامی کـه این فرضیات می توانند با استفاده از ورودی بصورت مضربی کارآمد شده که بـرای اثـر گذاشـتن بـه تغییر عمل کاربرد که برای حمله کننده سودمند است ناتوان شده است وجود دارد منوط بـه فـرض بی اعتبار، انواع مختلف آسیب پذیری‌های اعتبـار ورودی وجـود دارد. آسـیب پـذیری هـای اضـافی میانگیر از فرضیات بی‌اعتبار درباره حدود ورودی ناشی می شود.

حمله های اضافی کامل فرضیات بی‌اعتبار درباره حدود ورودی ناشی می شود. بطور مشـابه، آسـیب ذیری های تزریق از فرضیات بی اعتبار درباره حصور محتوی ترکیبی در ورودی کـاربرد ناشـی مـی شود. این کار روی این طبقه آخر آسیب پذیری ها و حمله هایی که آنها را بکار می گیرند تمرکز می کند. در این حمله ها، به اصطلاح حمله های تزریق، حمله کننده ورودی بطور مضـر کارآمـد شـده، حتصل محتوی ترکیبی را که معانی یک عبارت (نشانگر) در کاربرد را عوض مـی کنـد را ارائـه مـی دهد. این نتایج به کاربرد وابسته هستند اما نوعاً منجر به فاش شدن اطلاعات، بالا رفتن مصونیت یـا اجرای دستورهای اختیاری می‌شود.

ارزیابی یکپارچه حساس به متن را معرفی می کند (سی ـ اس ـ اس ـ ای)، که روش کشف دخالـت و جلوگیری در مقابل حمله های تزریق، این روش مزایای نسبت به روش های موجود ارائه می دهد: احتیاج به آگاهای کاربرد یا تغییر و تبدیل کد منبع کاربرد ندارند و بنابراین می تواند با کاربردهـای

بازمانده بکار رود. قویاً در مقابل بیشترین انواع حمله‌های تزریق موثر است، نه صـرفاً متـداول تـرین آنها. به توسعه دهنده کاربرد متکی نیست، که باعث می شود کمتر مسعد خطا باشـد. سـرانجام، بـه هیچ زبان برنامه نویسی وابسته نیست و می تواند در طرح های مختلفی اجرا شود.

سی ـ اس ـ اس ـ ای بطور موثری مسئولیت اقدام متقابل بر ضـد حملـه هـای تزریـق را از توسـعه دهندگان کاربرد به تیم کوچکی از توسعه دهندگان طرح زیرک ایمنی انتقال می‌دهـد. بـرای مثـال این به طریقی قابل مقایسه با برداشتن بار مسئولیت حدود آزمایش از توسعه دهندگان کاربرد برنامه عمل جاوا است که بدان وسیله کاربردها برای برنامه جاوا را واقعاً مصون از حمله های اضافی میانگیر کرد. سی ـ اس ـ اس ـ ای برای هر طرح که باید محافظت شود احتیاج به اجرای جداگانـه ای دارد. بهر حال، صحن این که تعداد طرح ها چند برابر کوچکتر از کاربردهای اجرا شده روی آنها است، این اجراها می توانند توسط حرفه ای های ایمنی اجرا شوند و محتمل آزمایش کاملی شوند.

ترکیب این مقاله دو بخشی است. ابتدال، چشم انداز یگانه ای از آسیب پذیری ها ارائه می دهد کـه استدلال درباره این طبقه از آسیب پذیری ها و پیش بینی انواع جدید آسیب پذیری های مربـوط را آسان می کند. دوم، و عمده برای این مقاله، با آدرس یابی سبب ریشه ای این مشـکل سـی ـ اس ـ اس ـ ای را به عنوان روشی برای مقابله بر ضد حمله های تزریق معرفی می کند.

ساختار بصورت ذیل است. بخش بعدی آسیب پذیری های تزریق و شرایطی را کـه باعـث قدرتمنـد شدن آنها می شوند را مورد بحث قرار می دهد. در مروری به تفصیل از سـی ـ اس ـ اس ـ ای ارائـه می دهیم. اجرای پیش نمونه سی ـ اس ـ اس ـ ای ما برای پـی ـ اچ ـ پـی مـی شـود. در بخـش ۶ نتایجی تجربی درباره ی موثر بودن و کارآیی اجرای خود عرضه می کنیم.

۴–۱–۱ آسیب پذیری های تزریق

ما این دسته از آسیب پذیری ها را با مثال ساده ای که برای اس ـ کیو ـ ال و تزریق برنامـه واسـطه آسیب پذیر است را معرفی می کنم. بعداً سبب ریشه ای با دلیل اصلی وجود داشتن که این آسـیب پذیری ها در کاربردها را مشخص می کنیم. سرانجام، چشم انـداز تشـکلی از انـواع مختلـف آسـیب پذیری های تزریق نشان می دهیم.

خصوصیات مهم آسیب پذیری های تزریق

آسیب پذیری های تزریق کاستی، در برنامه ریزی هستند که به حمله کننده اجازه می دهد معـانی یک عبارت در یک کاربرد را با ورودی شامل قسمت های مختلف تغییر دهد. در این بخش ما مثالی با تزریق اس ـ کیو ـ ال و آسیب پذیری های تزریق برنامه و واسطه برای بحث کردن درباره برخی از خصوصیات مهم این آسیب پذیری ها ارائه می دهیم.

کد زیر مثالی واقعی از بخشی از کاربرد یک پی ـ اچ ـ پی را نشان می دهد، که با روش آدرس پست الکترونیکی ($email) مسئول تصدیق کردن و یک کد ضمانت ($pincode) بر مبنی اعتبار آورها (ذخیره شده در پایگاه داده است. اگر یک مجموعه نتیجه غیر خالی برگشت کاربر با موفقیت تصدیق شده است.

این کد مستعد چندین حمله تزریق اس ـ کیو ـ ال اسـت. اگـر حملـه کننـده«ًdice@hostً» بـا «Lo=1» به عنوان آدرس پست الکترونیکی عرضه کند، این کاربرد یک انشعاب اجرا مـی‌کنـد، کـه نتیجه آن مستقل از کد ضمانت ارائه شده است. بخاطر حق اولویت گرداننده (عمل کننـده) چنـین، انشعابی معادل همان انشعاب دارای شرایط تک است «email=dice@host» که به حمله کننده اجازه می دهد منطق تصدیق کردن را نادیده بگیرید. حمله های مشابهی بـا اسـتفاده از متغیـر کـد ضمانت اجرا شدند که در یک زمینه عددی بکار می رود و بـه منطقـه هـای تـک در ورودی کـاربر احتیاج ندارد.

برای مثال با استفاده از یک آدرس پست الکترونیک معتبر (یعنیdice@host) و ۰ یا ۱ به عنـوان یک کد ضمانت، حمله کننده باید دوباره قادر باشد بدون اعتبارنامه مناسب تصـدیق کنـد بـا ادامـه مثال خود برای نشان دادن تزریق برنامه واسطه، کد نشان داده شده در زیر یک پسـت الکترونیکـی تاثیر به آدرس الکترونیکی تعیین شده زیر می‌فرستد.

در این مورد، هر یک چندین خصوصیت برنامه واسطه در زمینه آدرس پست الکترونیکی مـی توانـد برای اجرا کـردن فرمـان هـای اختیـاری روی سـر در بکـار رود. بـرای مثـال اگـر حملـه کننـده از dice@host به عنوان آدرس استفاده کند، سر در وب، علاوه بر فرستادن یک پسـت الکترونیکـی، سعی می کند همه فایل ها را از فهرست جاری بردارد.

د رتمام مثال های ما، ورودی بطور مضر کار آمده شده حامل محتوی ترکیبی است. محتوی هنگامی که شکل یا ساختار یک عبارت را تحت تاثیر قرار می دهد، ترکیبی در نظـر گرفتـه مـی شـود. ایـن تغییر ساختار نهایتاً منجر به تغییر معنایی عبارت می شود. خصوصیاتی که دارای کیفیت به عنـوان محتوی ترکیبی هستند به زمینه ای بستگی دارد که عبارت در آن بکار رفتـه اسـت (یعنـی فرمـان برنامه واسطه یا اس ـ کیو ـ ال)، به علاوه این زمینه همچنین به چگونگی کاربرد در عبارت بسـتگی دارد (یعنی ثابت یکپارچه در مقابل کـد ضـمانت عـددی در عبـارت اس ـ کیـو ـ ال در مثـال مـا). شناسایی کردن همه محتوی ترکیبی برای زمینه های مختلف بدین تریتب چالشی عظیم است.

برداشتن تک و فاصله ها از ورودی از حمله هایی که توضیح دادیم جلوگیری می کند، اما محققـاً از همه حمله ها دفاع نمی کند. سایر خصوصیات خطرناک شـامل تـوالی‌هـای تفسـیر (--، /*، ۰/*) و نقطه ویرگول (;) است، اما این فهرست هم جامعیت ندارد. [۸]

علاوه بر این، سـرورهای پایگـاه داده متـداولاً اسـتانداردهای ANJIاس-کیـو-ال را بـا خصوصـیات اختصاصی گسترش می دهد و بصور مفید خطاهای ترکیبی کوچک را تصحیح می کند. یعنی بجای تک (۱) استفاده از مضاعف (؟) را برای مرزیابی ثابت های یکپارچه مجاز می کنـد. ضـمن ایـن کـه

آزمایش های لازم مخصوص پایگاه داده ها است، یک کاربرد می تواند با تغییر محض پشتیبان پایگاه داده ها آسیب پذیر شود.

علت اصلی

آسیب پذیری های تزریق متداولاً به عنوان آسیب پذیری های اعتبار ورودی طبقه بندی می شـوند. بهر حال، که معتبر کردن ورودی کاربر برای جلوگیری از این حمله ها کلی و مستعد خطا هسـتند. سرو کار داشتن با این آسیب پذیری‌ها به عنوان آسیب پذیری ها ی اعتبـار محـض بنـابراین سـهل انگاری بیش از حد است.

در عوض، ما باید به علت اصلی آنها توجه کنیم، که می توانند بـالقوه راه حـل بـادوام تـر و مسـتقر خطای کمتر بار آورد. پیدا کردن این علت اصلی معادل آشکار سازی دلیل اصلی وجود داشتن یـک آسیب پذیری در یک سیستم ویژه است. در موردی که آسیب پذیری‌ها منجر به حمله های تزریـق می شوند. این به معنی معنی کردن این است که چرا ورودی کاربر بطور مخصوص کارآمد شده مـی تواند برای تغییر معنایی یک عبارت در درجه اول بکار رود.

خصوصیت معمولی آسیب پذیری های تزریق استفاده از ارائه های متنی عبارت های خروجی ساخته شده از ورودی تعیین شده از طرف کاربر است. ارائه های متنـی به شـکل متن قابل خواندن توسـط انسان هستند. عبارت های خروجی آنهایی هستند که توسط اجزای خـارجی بکار گرفته مـی شـوند (یعنی سـرور پایگاه داده ها، مضر برنامه واسطه).

ووردی کاربر نوعاً در بخش هایی از عبارت های خروجی بکار می رود، که مخالف ثابـت‌هـای تعـین شده از طرف توسعه دهنده که در بخش هایی کنترل هم بکار می رود. در صورت یک حمله تزریق، ورودی کاربر بطور ویژه کارآمد شده، به ترکیب اثر می گذارد، که منجـر بـه تعبیـر معنـایی عبـارت خروجی می شود. ما به این فرآیند بـه عنـوان مخلـوط کـردن کنتـرل و مجراهـای داده هـا ارجـاع خواهیم‌کرد.

آسیب پذیری های تزریق با استفاده از خود ارائه کردن متنی بوجود نمی آیند، بلکه به طریقـی کـه ارائه کردن هدایت شده است. نوعاً متغیرهای سرچشمه گرفته شـده از کـاربر بـا اسـتفاده از اعمـال یکپارچه (تمرکز یکپارچه، یا الحاق یکپارچه، همانطور که در مثال ما آمده) به صورت یک ارائه متنی مرتب شده اند. این فرآیند، درخواست کردن بصورت مستقیم اسـت امـا نهایتـاً تـک مـوردی اسـت: متغیرها اطلاعات نوع خود را از دست می دهند و مرتب کردن آنها، قطـع نظـر از عبـارت خروجـی انجام می شود. این مخلوط کردن داده‌ها و مجراهای کنترل در کاربرد را فراهم می کند که منجر به آسیب پذیری‌های تزریق می‌شود.

ما بنابراین، مرتب کردن ویژه ورودی کاربر را بـرای بوجـود آوردن ارائـه هـای متنـی عبـارت هـای خروجی به عنوان سبب اصلی حمله های تزریق در نظر می گیریم.

مرتب کردن ویژه ورودی کاربر (یا متغیرها بطور کلی) می تواند منجر بـه مخلـوط کـردن نـامطلوب مجراها شود، اما داروی برخی خصوصیات مطلوب هم هسـت. مهمتـرین آن درخواسـت بطـور غیـر مستقیم است و در نتیجه، توسط توسعه دهنده ی کاربرد براحتی نوشـته شـده و درک مـی شـوند. دوم، برای انواع متعددی از عبارت ها (یعنی Path *، فرمان برنامه واسطه) مرتب کردن ویژه ورودی کاربر مصرف کننده اعمال یکپارچه، تنها روش ایجاد کردن ارائه های متنی است.

با در نظر گرفتن این، دفاع در برابر حمله های تزریق باید توسعه دهنده کـاربرد را قـادر کنـد ارائـه متنی را به طریقی امن بکار ببرد. سی ـ اس ـ اس ـ ای این را از طریق یک جـدایی تحمیـل شـده برنامه از داده ها و کنترل مجراها بدست می آورد، و از این طریق علت اصـلی آسـیب پـذیری هـای تزریق را آدرس یابی می کند، در حالی که در همان زمان مزیت های ارائه متنی و مرتب کردن ویژه متغیرهای کاربر را حفظ می کند.

چشم اندازی یکنواخت از آسیب پذیری های تزریق:

برخی از انواع متداول آسیب پذیری های تزریق را عرضه کرد، اما تعداد دیگری وجـود دارد. در ایـن بخش، ما چشم اندازی یکنواخت از انواع مختلف ارائه می‌کنیم.

برای هر نوع از آسیب پذیری ها تا در یک کاربرد وجود داشته باشند، باید با دو پیش نیاز مواجه شد. اولی این است که کاربرد باید از یک عبارت ایجاد شده با استفاده از متغیرهـای مرتـب سـازی ویـژه استفاده کند. دومین آن است که عبارت خروجی به داده‌هـای ورودی تعیـین شـده از طـرف کـاربر بستگی دارد، بنابراین می تواند تحت تاثیر حمله کننده قرار گیرد. از این پس، ما از واژه بردار ورودی و بردار خروجی برای ارجاع به طبقه‌های منابع ورودی و عبارات خروجی استفاده می کنیم.

در جدول ۱ با برخی مثال های شناخته شده آسیب پـذیری هـای مطـابق بـا بردارهـای خروجـی و ورودی آنها طبقه بندی می کنیم و یک عدد CAN/ CAUC اگر موجود است را تأمین می کنیم. حفره ها در این اصول سیرهای احتمالی برای انواع آسیب پذیری‌های تزریق را نشان می دهد.

ردیف های این جدول به طبقه بندی زمخت بردارهای ورودی را نمـایش مـی دهـد: ورودی شـبکه، ورودی مستقیم و ورودی ذخیره شده. ورودی شبکه شامل کلیه ورودی تأمین شده توسط کاربرهای از راه دور است و ترکیبی است از ورودی لایه اتصال (یعنی داده‌های POST و تعبیه کننده هـا در اچ ـ تی ـ تی ـ پی و ورودی سطح کاربرد (یعنـی درخواسـت SOAP). ورودی مسـتقیم، از طـرف دیگر، ورودی است که از طریق یک هم کنشگر محلی عبور می کند، یعنی از طریق یک هم کنشگر خط فرمان یا متغیرهای محیط، سرانجام، ورودی ذخیره شده، ورودیی است کـه مسـتقیماً از کـاربر ناشی نمی شود، بلکه شامل یک مرحله ذخیره واسطه است، یعنـی در یـک فیـل XML یـت یـک پایگاه داده ها. توجه کنید که برای برخی کاربردها تفاوت بین ورودی شبکه و ورودی اخیـر ممکـن است صریح نباشد (یعنی کاربردهای سی ـ جی ـ آی به داده هـای اچ ـ تـی ـ تـی ـ پـی از طریـق متغیرهای محیط دسترسی پیدا می‌کند). با این حال ما بین ایـن انـواع چـون اغلـب بیشـتر از هـم کنشگرهای برنامه ریزی مختلف استفاده می کنند تفاوت را تشخیص می دهیم.

جدول۱. مثال هایی از آسیب پذیری های مختلف با اعداد CAV/ CAN آنها، متداول‌تـرین انـواع آسیب پذیری به صورت غلیظ نوشته شده اند.

ستون های این جدول بردارهای خرجی یا انواع کلمه بندی هایی که باید توسط اجزای بیرونی بکـار گرفته شوند را نمایش می دهد. ما بین مقوله های ذیل تفاوت قائـل می‌شویم. اجرا کردن، استعلام، تعیین محل، تحویل دادن، ذخیره کردن. مقوله «اجرا کردن» عبارات شـامل محتـوی فایـل اجـرا را تحت پوشش قرار می دهد، از قبـیل فرمان های برنامه واسطه یـا فایـل آغـازگر. مقولـه «اسـتعلام» شامل عباراتی است که در انتخاب کردن و اداره کردن داده ها از یک مخـزن، یعنـیXPoth اس ـ کیو ـ ال یا عباراتی معمولی بکار می روند. مقوله «تعیین محل» به قبـی مـرتبط اسـت، امـا حـاوی عبارت هایی است که به تعیـین محل مخـزن‌ها کمک می کنـد یعنـی مسـیرها و یـو ـ آر ـ ال هـا. عبارت ها در مقوله های «تحویل دادن» حاوی اطلاعات درباره تجسم کردن داده ها است، یعنـی اچ ـ تی ـ ام ـ ال، SV6 و پی نوشت ها. سرانجام، مقوله «ذخیره» شامل عبارت هـایی بـرای ذخـــیره کردن داده ها در یک انبار است.

این مقوله آخر چون حفره های این ستون آسیب پذیری های تزریق را نمایش نمی دهند ویژه است، اما در عوض آماده شدن برای تزریق های مرتبه بالاتر است.

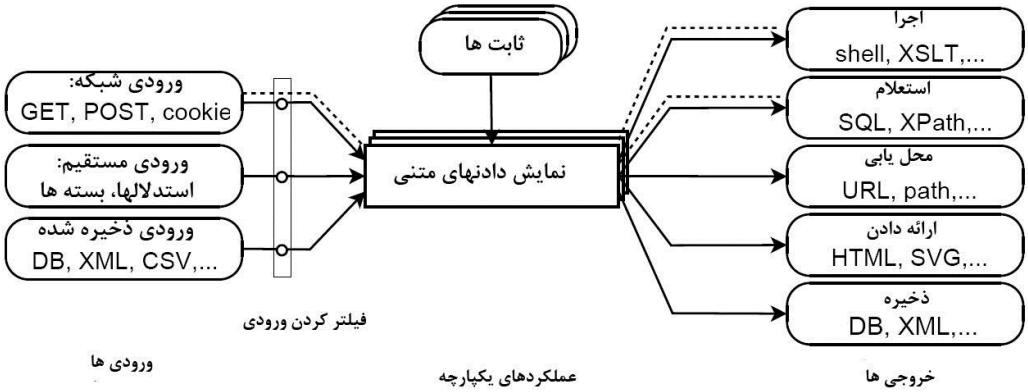
چنین تزریق مرتبه بالاتری به عنوان تزریق هایی که در آنها ورودی تحمیل شده به تزریق ابتـدا در یک مخزن پایا ذخیره می شود. تزریق واقعی هنگامی انجام می گیرد که این داده های ذخیره شـده مورد دسترسی قرار گرفته و بکار برده می شوند. مثال های بخوبی شناخته شده تزریق هـای درجـه دوم، تزریق های اس ـ کیو ـ ال و XSS هستند، جایی که داده های ذخیره شده، در بوجود آوردن حستارهای اس ـ کیو ـ ال و خروجی اچ ـ تی ـ ام ـ ال بکار رفته به عنوان بخشی از ترکیب اچ ـ تی ـ ام ـ ال و اس ـ کیو ـ ال تعبیر می شوند.

حمله های بالاتر از مرتبه دوم کمتر متداول هستند، اما بالقوه خطرناک تر هستند، همانطور که داده های بادوام تر معمولاً قابـل تبدل تر در نظر گرفته می شوند. توجـه کنید که تعریف تـزریق مرتبـه بالاتر گستـرده تر از آن است تزریـق اولامن است (۱۳) که به ماهیت تاخیر پذیر آن تاکید می کند. در رهیافت ما، به خصوصـیات اصلی آن تمرکز می‌کنیم، یعنی مخزن پایای داده های صـدمه زننـده

علی رغم این که خواه اثـر آن فوری است یا نه (مثل برخی حمـله های XSS)، (مثل حملـه هـای نشـان داده شـده توسط اولامن).

این جدول چشم انداز یکنواختی از همه انواع آسیب پذیری های تزریق ارائه می دهد. ما می تـوانیم از آن برای طبقه بندی آسیب پذیری های موجود استفاده کنیم، اما به آسیب پذیری هـایی کـه مـا انتظار داریم در آینه هم اتفاق افتد هم نظری می اندازد. برای مثال، هر چند ما هنـوز هـیچ آسـیب پذیری های تزریق XPoth را ندیده ایم، احتمال دارد که ما در ضمن این که تکنولوژی های اصلی گسترده تر بکار می روند پیدایش آنها را خواهیم دید. همچنین نشان مـی دهـد کـه برخـی آسـیب پذیری ها که نوعاً به عنوان آسیب پذیری های تزریق در نظر گرفته نمی شوند یعنی پیمایش مسیر. در حقیقت بسیار مرتبط هستند و می‌توانند با اسـتفاده از روش هـای یکسـان ماننـد سـایر آسـیب پذیری های تزریق جلوگیری شوند.

شکل ۱ جریان داده ها در یک کاربرد از دید این مقاله را نشان می دهد. این داده ها از ورودی های متعدد و ثابت از طریق یک رشته اعمال یکپارچه برای تشکیل عبـارات خروجـی جریـان پیـدا مـی کنند. خطوط تیره مثالی از این بخش را نمایش می دهند که یک ورودی تک مـی توانـد منجـر بـه خروجی های مختلف بسته به مسیر در نمودار جریان شود. مشکل در ایمن کردن چنـین کـاربردی در این حقیقت نهفته است که همه مسیرهای ممکن بین ورودی ها و خروجی ها باید بحساب آیند.



شکل ٤-۱ استفاده از نمایش دادن متنی در یک کاربرد، خطهای تیره مثالهایی را نمایش می دهند، جائیکه به یـک ورودی تک می تواند خروجی های زیادی بدهد

به عنوان یک مثال، کاربردهای وب نوعاً دارای بردارهای ورودی مختلف متعدد هستند: پارامترهـای ULR, QOST, GET، تعبیه کننده ها، اطلاعات تصدیق و سایر عنوان های اچ ـ تی ـ تی ـ پـی برای هر درخواست احتمالی. به علاوه، ورودی می توانند از پایگاه داده ها، فایل‌های XML یا سـایر منابع بیرونی ناشی شود. در همان زمان، یک کاربرد وب نمونه می توانـد دارای بردارهـای خروجـی متعدد باشد:

خروجی اچ ـ تی ـ ام ـ ال برای هر صفحه که می تواند احتمالاً توصیه شود، یک پایگـاه داده هـا بـا فایل XML پست الکترونیکی و غیره

تعداد ترکیبات زیاد باعث افزایش آزمایش های مستعد خطا بودن اعتبار ورودی لازم مـی‌شـود ایـن فقط در مورد کاربردهای وب صحت ندارد، بلکه در عوض برنامه هایی که با اداره کردن ورودی کاربر سر و کار دارند هم تحت تاثیر قرار می گیرند. بهر حال، بـه دلیـل هـای گونـاگون، کاربردهـای وب بخصوص بیشتر صدمه پذیر هستند. آنها نوعاً متن هستند و اغلب از اجزای به سسـتی جفـت شـده ساخته شده اند و در یک محیط متخاطم وجود دارند که در آنجا بسیاری از ورودی کاربرد غیر قابل اعتماد دریافت می کنند. به علاوه، اغلب فقدان ابزار توسعه مناسب وجود دارد و جنبه هـای ایمنـی تمرکز اصلی توسعه دهندگان کاربرد نیست.

آنچه جدول ۱ و شکل ۱ نمی توانند نشان دهند اثر آسیب پذیری تزریق مشخصـی اسـت کـه مـی تواند روی ایمنی یک کاربرد داشته باشد. برای مثال، تزریق اس ـ کیو ـ ال منجر به احتمال تصدیق شدن بدون اعتبار مناسب شود. در موارد دیگر، یک تزریق منجر به خطاهـای زمـان رانـدن بصـورت محرمانه یا مشکلات یکپارچگی (درستی). بدیت ترتیب اثر واقعی بسیار به موقعیت بستگی دارد.

۴–۱–۲ کار مرتبط

رواج جمله ها بکار برنده آسیب پذیری های اضافی میانگیر تلاش تحقیق قابل ملاحظـه ای را بـرای جلوگیری و کشف این آسیب پذیری ها را بر می انگیزد. توجه کم قابل ملاحظه‌ای به شکل مرتبط با آسیب پذیری های تزریق شده است (۳) که در عوض به عمدتاً توسط کاروران بررسی شده است [۱، ۲، ۸، ۱۲، ۱۳]. ما بین دو مقوله زمخت راه حل های موجود تفاوت قائل هستیم: "مرتب سازی ویژه امن" و "مرتب سازی API ها" در این بخش آنها مورد بحث قرار می دهیم و مزیـت هـا و کاسـتی های آنها را مورد بحث قرار می‌دهیم.

مرتب سازی ویژه امن این مقوله اول شامل راه حل های تسهیل مرتب سازی ویژه امن است. مقرارت معتبر کردن ورودی در این مقوله قرار می گیرد، و بخاطر سـادگی مفهـومی آن مهمتـرین رهیافـت عمومی باقی می ماند. این شامل آزمایش دستی کلیه ورودی تـأمین شـده انـد طـرف کـاربر بـرای محتوی ترکیبی است که سپس رد شده یا رها می شود. حمایت ابزار، نوعاً به شـکل یـک آ ـ پـی ـ آی، به فیلترهای ار پیش تعریف شده با بردارهای خروجـی قطعـی محـدود اسـت. اسـتفاده از ایـن فیلترها تحت مسئولیت توسعه دهنده کاربرد باقی می‌ماند.

تایید ورودی دستی مستعد خطا است چون بطور زیادی به توسعه دهنده کاربرد متکی است. اجرای آن بطور صحیح بدلیل پیامدهای ذیل بسیار مشکل از آب در می آید. ابتدا، کاربردهـا معمـولاً دارای تعداد زیادی ورودی هستند و کد اداره کردن تماماً پراکنده شده است. بدسـت آوردن کلیـدی ایـن ورودی ها بنابراین می تواند کار نا ایمد کننده ای باشد. به علاوه، این آزمایش ها به طور الـزام آوری به زمینه بستگی دارد و می توانند برای بردارهای خروجی مخصوص، بسیار پیچیـده باشند.سـرانجام باید مراقبت به عمل آید که آزمایش ها در محل درستی انجام می گیرند، چون آزمایش های انجـام گرفته قبل از انجام متغیر در مرحله رمزگذاری باشد منجر به آسیب پـذیری رمزگـذاری مـی شـود.

اینها هنگامی که اعتبار می تواند با استفاده از رمزگذاری ویژه آشکار شود، یعنـی بـا تمامیـت مـادر رمزگذاری XML یا یو ـ آر ـ ال وجود دارد.

تایید ورودی بصورت اتوماتیک، رهیافت دوم است که هـدف آن کمتـر مسـتعد خطـا کـردن تاییـد ورودی با بدون اتکا به توسعه دهنده کاربرد است. بهترین مثال شناخته شده «Magic Quo1es» در پی ـ اچ ـ پی است [۱۴]، که با تأیید کردن کلیه داده های ورودی در زمان دریافت کار می کند. پیامد دوم که برای تایید ورودی دستی بوجود آوردیم هم به این رهیافـت اعمـال مـی شـود، چـون زمینه کاربرد هنگامی که تایید انجام می گیرد شناخته نیست. در نتیجه، مشخص نیست چه زمینـه ای باید ترکیبی در نظر گرفته شود. در عوض، بردارهای خروجی متداول، تقبل می شوند و طبق آن تایید انجام می گیرد. این می تواند منجر به آسیب پذیری هایی شود هنگامی که فرض غلـط از آب درآید.

متغیر صدمه دیده در پرل [۲۰] رهیافت سوم است، با نشانی یابی پیامـد اول تاییـد ورودی دسـتی یعنی ورودی های زیادی در سراسر کد پراکنده شده اند، این، ملوث کردن تمامیت ورودی با کاربرد و اعلام خطر هنگامی که عبارت های دربسته بدون تحمل تایید دستی بکار رفته ان کـار مـی کنـد. توسعه دهنده کاربرد هنوز سوال انجام دادن آزمایش های واقعی است، اما راه کار ملوث کردن آن را کمتر محتمل می کند که آزمایش های لازم در نظر گرفته شده اند. ملوث کردن متغیرهـای ورودی الهام گرفته شده توسط پرل، همچنین به سایر زبان ها برای جلوگیری لبریـز شـدن بـافر (میـانگیر) اعمال می شود. لارسون و استن اعمال یکپارچه ای در برنامـه هـای زبـان C بـرای پـی بـردن بـه خطاهای نرم افزار سبب شده با محدودیت نامناسب ورودی کاربر تجهیـز کردنـد شـنکار و دیگـر از تحلیل ملوث شدن ایستا (متعادل) برای کشف فرمت (آرایش) آسیب پذیری هـای یکپارچـه در فـاز همگردانی (کامپایل کردن) استفاده کردن.

آخرین رهیافت در این مقوله توسط اس ـ کیـو ـ ال reud ارائـه شـده اسـت کـه بـا جـدا کـردن فرمان‌های رمزگذاری شده در کد برنامه از داده های ارائه شده از طرف کاربر از تزریق اس-کیـو-ال

جلوگیری می کند. اس ـ کیـو ـ ال reud بـر مبنـای ایـن فـرض اسـت کـه بخـش هـای ترکیبـی دستورهای اس ـ کیو ـ ال تنها می توانند به عنوان ثابت ها در کد برنامه ظاهر شوند و نباید توسـط ورودی کاربر تأمین شود. اس ـ کیو ـ ال reud کد منبع کاربردها را پیش پردازش می کند و کلیـه دستورهای ویرایش های رمزگذاری شده را اس ـ کیو ـ ال را جایگزین می کند.

دستورهای اصلاح شده سپس توسط یک نماینده اس ـ کیو ـ ال جدا می شوند و فقط اجازه می‌هـد رهنمودهای رمزگذاری شده به پایگاه داده ها عبور کنند. کاستی های اصلی این رهیافت آن هستند که به مقدمه چینی پیچیده ای احتیاج دارد و ویژه اس ـ کیو ـ ال است.

تسلسل آ ـ پی ـ آی ها مقوله دوم شامل راه حل هایی است که می توانند به عنوان تسلسل آ ـ پـی ـ آی ها مشخص شوند (هم کنشگرهای برنامه ریزی کاربرد). این آ ـ پی ـ آی ها به توسـعه دهنـده کاربرد در مرتب کردن متغیرها کمک می کند و بدین ترتیب نمایش دادن ایمنی بوجـود مـی آورد، آنها یا اصلاً از نمایش دادن متنی واضح استفاده نمی کنند، و نمایش دادن در عوض با استفاده از آ ـ پی ـ آی برنامه بوجود می آید یا از الگوهای تسلسل ویژه استفاده می کنند، که در آن نمایش دادن متنی توسط توسعه دهنده کاربرد بوجود می آید فقط متغیرها با استفاده از آ ـ پی ـ آی بـه ترتیـب مرتب می شوند.

مثالی از نوع قبلی (مدل سمی سند) است، که پشتیبان برنامه ای برای سندهای X/M بوجود مـی آورد که بوسیله آن علاوه بر سایر مزایا از حمله های تزریق اس ـ کیو ـ ال جلوگیری می شـود، کـه برای زبان های برنامه ریزی مختلف متعـددی وجـود دارد: Prepared Statement در جـاوا، (۰) ADOds در Salcommal, Pythan, پی ـ اچ ـ پی در ویزوال بیسیک و (۴) دی ـ بی ـ آی در پول. مزیت کلیدی این رهیافت این است که مرتب کردن بطور خودکار توسط برنامه اداره می شود. هر چند این روش کمتر مستعد خطا است، مشکلاتی باقی می ماند. ابتدا، پشتیبانی ابزار محدود بـه چند بردار خروجی مکرراً بکار رفته است. برای مثال برای عبـارت هـای اس ـ کیـو ـ ال، توضـیحات آماده ای وجود دارند و همینطور برای DOM و XML، اما از هیـچ حمایت ابزاری بـرای Xpoth

یا عبارات معـمولی آگاه نیسـتم. دوم، توسعه دهنده کاربرد هنوز مسئول فعالیت و تصحیح، استفاده از این راه کار است. و سوم، تعداد زیادی از کاربردهای بازمانده وجود دارد که ار ایـن کـاربردپـذیری استفاده نمی کنند یا برنامه هایی را می دانند که این حمایت ابزاری را ارائه نمی کنند.

همچنین در این مقوله رهیافت انتخاب شده توسط Xem [a] است که کاملاً XML و اس ـ کیو ـ ال را با زبان های سازگار با شی یکپارچه می کند. از قبل C^{++}. Xem ترکیـب زبـان را بـا افـزودن انواع جدید و عبارات گسترش می دهد، که از تسلسل ویژه جلـوگیری مـی کنـد و بـدین ترتیـب از آسیب پذیری های تزریق جلوگیری می کند. کاستی این روش آن است که نمی تواند به سادگی به کاربردهای موجود اعمال شود.

۴–۲ ارزیابی یکپارچه حساس به متن

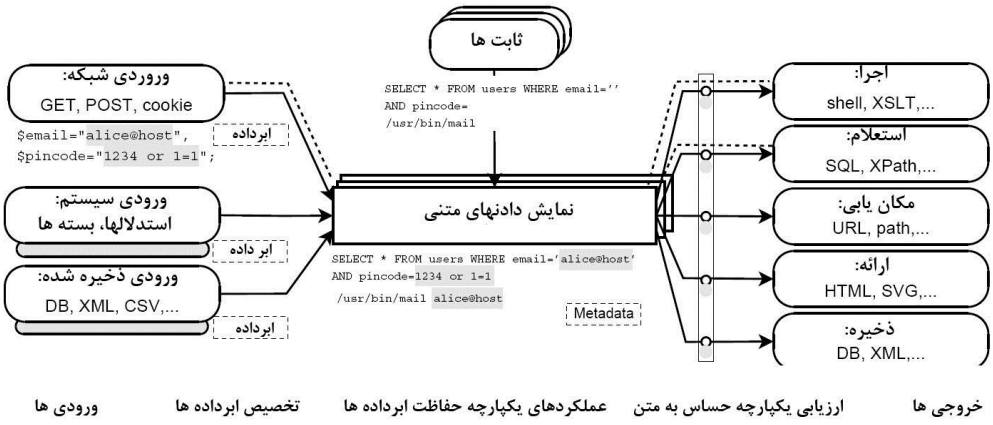
در این بخش توضیح مفصلی از سی ـ اس ـ اس ـ ای ارائه می کنیم و نشـان مـی دهـیم چطـور بـا مدل‌های موجود برای دفاع در مقابل محل های تزریق مقایسه می شود.

سی ـ اس ـ اس ـ ای با تحمیل کردن جدایی محض به سـبب اصـلی آسـیب پـذیری هـای تزریـق نظارت می کند. در حالی که هنوز استفاده عرفی از تسلسل ویژه بـرای بوجـود آوردن عبـارت هـای خروجی را مجاز می شمارد. یک برنامه تدارک دیده شده توسط سی ـ اس ـ اس ـ ای اطمینان مـی دهد این عبارت ها در مقابل حمله های تزریق با اعمال خودکار آزمایش ها در بخش هایی از عبارت ها که توسط کاربر ارائه شده مقاوم است.

سی ـ اس ـ اس ـ ای این را با تجهیز کردن برنامه بطوری که قادر است: (۱) بین بخش های تأمین شده توسط توسعه دهنده و کاربر عبارت های خروجی و معنی کردن آزمـایش هـای مناسـب بـرای انجام شدن روی بخش های تأمین شده از طرف کاربر تفاوت گذارده بدست می‌آورد.

شرط اول از طریق یک سیستم پیگیری که ابر داده ها را به همه بخـش هـای یکپارچـه در کـاربرد اضافه می کند مسیر بخش های اصلی را نگه دارد بدست می آید. فرض اصلی این اسـت کـه بخـش

های یکپارچه سرچشمه گرفته از توسعه دهنده معتبر هستند، در حالی که آنهایی که از ورودی کاربر تأمین می شوند، معتبر نیستند. تخصیص ابر داده ها بدون اثر متقابل توسعه دهنده کاربرد تا تعدیل کد منبع کاربرد انجام می شود، و در عوض از طریق دخالت بردارهای ورودی ایمنی شبکه، فایل، برنامه سی ـ اس ـ اس ـ ای بدست می آورد.



شکل ٤-۲ استفاده از CSSE برای حفاظت ابرداده ها از ارائه شدن های یکپارچه و مجاز دانستن برای ارزیابی یکپارچه بعدی.

سی ـ اس ـ اس ـ ای اعمال یکپارچه را برای حفاظت و به روز کردن ابر داده های تخصیص داده شده به کارگزاران آنها بیشتر تجهیز می کند. در نتیجه، ابر داده ها به ما اجازه می دهند بین بخش های از طرف توسعه دهنده تأمین شده (معتبر) و از طرف کاربر تأمین شده (نامعتبر) عبارت های خروجی در هر مرحله از تولید آنها تفاوت قائل شدیم. شکل ۲ جریان داده های کاربرد آسیب پذیر اجرا شده در یک برنامه قادر شده سی ـ اس ـ اس ـ ای را نشان می دهد.

شرط دوم با به عقب انداختن آزمایش های لازم به آخرین مرحله. یعنی تا لحظه ای که کاربرد خودستار عملکرد آ ـ پی ـ آی برای عبور دادن عبارت خروجی به اجزای اداره کننده است (بردار خروجی) سی ـ اس ـ اس ـ ای کلیه درخواست های آ ـ پی ـ آی مربوط به بردارهای خروجی را جدا می کند و نوعی بردار خروجی (یعنی برنامه واسطه Myاس ـ کیو ـ ال) از عملکرد واقعی بنام

(mys/ p- queny21) را می راند. این به سی ـ اس ـ اس ـ ای اجازه می دهد، برای بردار خروجی ویژه آزمایش ها مناسب اعمال کند.

در این نقطه، سی ـ اس ـ اس ـ ای متن کامل را می راند. بخش اول متن توسط ابر داده هـا تـأمین شده است، که بخش هایی از عبارت خروجی را که احتیاج به آزمایش شدن دارد را توضیح می‌دهد. بخش دوم متن با آزمایش کردن درخواست جدا شده به عملکرد آ ـ پی ـ آی تـأمین مـی‌شـود کـه تعیین می کند کدام آزمایش ها اجرا خواهند شد. سی ـ اس ـ اس ـ ای سپس از این اطـلاعات متن برای آزمایش بخش های نا امن برای محتوی ترکیبی استفاده می کند. بسته به حالت سـی ـ اس ـ اس ـ ای بکار رفته، می تواند از محتوی ترکیبی رها شود یا از اجرای خطرنـاک محتـوی جلـوگیری کند (هر دو جلوگر دخالت؟) یا یک هشدار بوجود آورند (کشف مزاحمت).

جدید بودن روش ما در توانایی آن برای گردآوری خودکار کلیه قطعات لازم اطلاعات است که به آن اجازه می دهد آزمایش های لازم برای کشف کردن و جلوگیری از آسیب پذیری های تزریق را انجام دهد. یک اجرای سی ـ اس ـ اس ـ ای مختص برنامه است، اما برای کلیه کاربردهای اجـرا شـده در این برنامه موثر است. تحلیل یا تعدیل کاربرد لازم نیست، به استثنای ندارد خیلی نادر که ورودی از طرف کاربر تأمین شده صریحاً قابل اطمینان است. این مفصل تر در بـاقی مانـده ایـن بخـش بحـث خواهد شد.

سی ـ اس ـ اس ـ ای بطور مطلوب با روش های موجود توصیف شده در بخش ۳ مقایسه می شـود. چون آزمایش های آن از طرف برنامه تحمیل می شوند هنگامی که عبارت مثـلاً رمزگـذاری شـده است، دارای هیچ یک از کاستی هایی که روش های مرتب سازی ویژه ایمن را مستعد خطا می کند نیست. همچنین نسبت به مرتب سازی آ ـ پی ـ آی ها دارای مزایای متعددی اسـت، همـانطور کـه برای گستره گوناگونی از بردارهای خروجی انجام شدنی است و به اعمال توسعه دهنده احتیاج ندارد و می تواند در کاربردهای باقـی مانده هم بکار رود.

اجرای سی ـ اس ـ اس ـ ای را تشکیل می دهد. نمایش دادن ابـر داده هـا، تخصـیص ابـر داده هـا، اعمال یکپارچه حافظه ابر داده ها و ارزیابی یکپارچه حساس به متن. سه شکل اول سیستم ردیـابی ابر داده ها، با در نظر گرفتن این که بخش آخر سؤال معنی کردن و اجرای آزمـایش هـای مناسـب است. اینجا، به جنبه های معماری تمرکز می کنیم، اجرا در بخش ۵ بحث خواهد شد.

نمایش دادن ابـر داده هـا: در سـی ـ اس ـــ اس ـ ای واژه «ابـر داده هـا» بـه اطلاعـاتی دربـاره ی سرچشمه (تأمین شده از طرف کاربر یا تأمین شده از طرف توسعه دهنده) کلیـه بخـش هـایی کـه متغیرهای یکپارچه را تشکیل می دهد ارجاع می کند. تصوراً، این ابر داده ها به متغیرهای یکپارچـه متصل هستند، ضمن اینکه با آنها از طریق کاربرد عبور می کند.

بهر حال، اجرای واقعی ابر داده ها شدیداً به برنامه وابسته است. بـرای مثـال، ابـر داده مـی‌توانـد در مخزن گسترده برنامه یا واقعاً به عنوان بخشی از داده واقعی ذخیره شود.

همچنین خود ابر داده ها می توانند به طرق مختلف نشان داده شـوند، یعنـی بـا اسـتـفاده از یـک bitmop یا فهرستی از نقـاط تعیین حدود مختلف بخش های یک عبارت. سرانجام فقدان ابـر داده ها برای یک متغـیر می تواند تلویحاً اطلاعاتی از مبدأ خودش حمل کند.

ابر داده سی ـ اس ـ اس ـ ای مشابه ملوث کردن متغیر در پرل است، همانطور که مبـدأ متغیرهـای یکپارچه را مشخص می کند و همچنین خواه آنها قابل اطمینان هستن یا نه، بهرحال، برای روش ها یک نمایش ابر داده غنی تر لازم است. در حالی که ملوث کردن متغیر در پرل فقط توضیح می دهد اگر بخشی از متغیر یکپارچه سرچشمه گرفته از کاربر وجود دارد، ابر داده سی ـ اس ـ اس ـ ای بعداً کلیه بخش های منفرد را که یک متغیر یکپارچه را تشکیل می دهـد را توضـیح مـی دهـد. (بخـش مرکزی بخش های سایه دار در شکل ۲).

همچنین امکان دارد ابر داده ه سی ـ اس ـ اس ـ ای برای مسیریابی یک «پیشـینیه» داده اسـتفاده کرد که با دنبال کردن زنجیره اعمال انجام شده روی بخش های آن (یعنی فیلتر کردن، منطقه های رها شده) برای اطمینان از اینکه روش معتبر اعمال شده مناسب بردار خروجی است (یعنی آزمایش

برای مشخصات پایگاه داده نامناسب هنگامی که متغیر به عنوان بخشی از فرمان برنامه واسطه بکـار می رود). بهر حال در باقی مانده مقاله ما قلمرو ابر داده را برای توضیح مبدأ محدود می کنیم، چون این برای هدف ما کافی است.

تخصیص ابر داده: یک برنامه توانمند شده سـی ـ اس ـ اس ـ ای بطـور خودکـار ابـر داده هـا را بـه کلیه‌ی متغیرهای یکپارچه تخصیص می دهد. برای ورودی از طرف کاربر تأمین شده ایـن از طریـق تجهیز بردارهای ورودی برنامه بدست می آید. هنگامی که کاربرد از کاربر ورودی دریافت می کنـد، یعنی به شکل یک پارامتر اچ ـ تی ـ تی ـ پی، برنامه تجهیز شده ای ـ پی ـ تی اطمینان خواهد داد که متغیرهای دریافت شده با ابر داده های مناسب ارائه شده اند، که آنها را نامتغیر می کند. از طرف دیگر، ثابت های یکپارچه ایستا موجود در کد برنامه بطور خودکار امـن در نظـر گرفتـه مـی شـوند، احتیاجی برای توسعه دهنده کاربرد برای تعدیل آنها یا به هر طریق نشان دهد چطـور بکـار خواهـد رفت وجود ندارد (یعنی به عنوان یک اس ـ کیو ـ ال یا فرمان برنامه واسطه، کد اچ ـ تی ـ ام ـ ال).

برای یک برنامه توانمند شده سی ـ اس ـ اس ـ ای حفاظت کاربردهـای وب، تجهیـز کـردن بـردار ورودی اچ ـ تی ـ تی ـ پی مهمترین است چون این مسیر معمولی برای ورودی از طرف کاربر تأمین شده است. سایر بردارهای ورودی شامل پارامترهای کاربرد (یعنی پارامترهای محیط یا زمان رانـش) و داده خوانده شده از یک ذخیره مادام است (یعنی پایگاه داده ها و فایل های XML).

اگر کاربرد از انبار بادوام به عنوان بردار ورودی و بردار خروجی استفاده کند، تزریق‌های مرتبه بالاتر انجام می گیرند. برای جلوگیری از این عمل سی ـ اس ـ اس ـ ای همچنین احتیاج دارد که ابر داده ها بادوام شوند بطوری که بتوانند بعداً ذخیره شوند، اگر اجرای سی ـ اس ـ اس ـ ای از این عملکرد پذیری حمایت نکند، ممکن است قادر نباشد از کلیه حمله های تزریق مرتبه بالاتر جلوگیری کنـد. در یک چنین زمینه ای سی ـ اس ـ اس ـ ای می تواند کلیـه انبـار بـادوام را بـه عنـوان نااطمینـان علامت گذاری کند، که از حمله های مرتبه بالاتر جلوگیری مـی کنـد امـا ممکـن اسـت منجـر بـه صفحات دروغین شوند.

سی ـ اس ـ اس ـ ای همچنین می تواند یک هم کنشگر برنامه ریزی برای دسترسی مستقیم به ابر داده‌ها تأمین کند. این اجازه می دهد توسعه دهنده کاربرد موارد ویژه را از قبیل هنگامی که داده ها خوانده شده از یک منبع ناامن بالقوه صریحاً معتبر است، یا هنگامی که داده‌های نـامعتبر در زمینـه غیر نوعی بکار می روند.

عملکردهای یکپارچه حافظ داده ها: عبارت های خروجی نوعاً از ثابت های کـاربرد و ورودی تـأمین شده از طرف کاربر با استفاده از یک رشته کاربردهای یکپارچه، یعنی تسلسـل (رده بنـدی)، ردیـف های فرعی، تعدیل مورد، یا تطبیق سریع متعارفی.

ما می خواهیم مطمئن شویم که ابر داده های تخصیص داده شـده بـه متغیرهـای یکپارچـه از ایـن رشته عملکردها زنده بماند. شبیه به تجهیز بردارهای ورودی برای تخصیص دادن به ابر داده ها، سی ـ اس ـ اس ـ ای هم عملکردهـای یکپارچـه تـأمین شـده توسـط برنامـه را تجهیـز مـی‌کنـد. ایـن کارکردهای یکپارچه تجهیز شده، ابر داده های آگاه هستند و ابر داده های کارگزارهـای خـود را بـه روز می کنند.

پیچیدگی تجهیز کردن به عملکردهای یکپارچه ویژه بستگی دارد. در بسـیاری مـوارد، ایـن جزیـی خواهد بود، یعنی کارکردی که مورد یک ردیف را تغییر می دهد مبدأ بخـش هـای ردیـف را تغییـر نمی دهد و بدین ترتیب فقط کپی کردن ابر داده لازم است. در موارد دیگر، ممکـن اسـت اسـتدلال بیشتری لازم باشد، یعنی تسلسل یکپارچه این دو ردیف شامل ترکیب شدن ابر داده دو ردیف است. تعداد عملکردهای یکپارچه در یک برنامه نوعـاً نسبتاً بزرگ است، و برای اینکـه سـی ـ اس ـ اس ـ ای کامل شود، کل مجموعه به تجهیز شدن احتیاج دارد.

ابر داده ها در سی ـ اس ـ اس ـ ای از یک جداسازی ردیفی استفاده می کند که مخالف نشان دادن داخلی سطح پایین ردیف ها است (یعنی بیت یا آرایـه هـای علامـت. در مـوارد نـادر کـه کاربردهـا مستقیماً نمایش داخلی داده ها را اداره می کنند، سی ـ اس ـ اس ـ ای ممکن است قادر نباشد ابر داده ها به روز شده را تضمین کند. این می تواند بالقوه منجر به نتایج مثبت یا منفی کاذب شود.

در بالا سیستم مسیریابی ابر داده سی ـ اس ـ اس ـ ای را تشکیل می دهد. هنگامی که ایـن بخـش ها اجرا شدند، امکان دارد بین بخش های از طرف کاربر و توسعه دهنده تـأمین شـده عبـارت هـای خروجی در هر مرحله از تولید آنها تفاوت گذاشت این شرط اول قبلاً ذکر شده را قانع می کند.

ارزیابی یکپارچه حساس به متن بخش نهایی سی ـ اس ـ اس ـ ای است و مسـئول معـین کـردن و اجرا کردن آزمایش هایی است که در عبارت های خروجی، جدایی مجـرای محـض را تضـمین مـی کند. این دوباره با تجهیز کردن برنامه بدست می آید، در این مورد بردارهای خروجی، ایـن تضـمین می کند که هنگامیکه کاربرد از بردار خروجی می خواهد تا یک عبارت خروجی را "اجرا" کند. سی ـ اس ـ اس ـ ای قادر است جلو اجرا را بگیرد.

در این نقطه، متن کامل شناخته شده است. ابر داده عبارت خروجی مبدأ داده را توضیح می دهـد و بدین ترتیب بخش هایی از عبارت را که احتیاج به آزمایش دارند را معـین مـی کنـد. ایـن عملکـرد خواسته شده توسط کاربرد بخش دوّم متن را تأمین می کند: بردار خروجی که عبـارت مخـتص آن است، و بدنبال این، آزمایش های لازم بـرای مثـال، هنگامیکـه یـک کـاربرد mysql-query( ) را درخواست می کند، تجهیزات سی ـ اس ـ اس ـ ای این بردار خروجی این درخواست را مـی گیـرد. ضمن این که سی ـ اس ـ اس ـ ای عملکرد خواسته شده را تجهیز می کند، همچنین آگاه است که این عملکرد مسئول بردار خروجی MySQL است و بدین ترتیب می تواند آزمایش های لازم روی بخش های نامعتبر عبارت خروجی را معین کند.

برای برخی بردارهـای خروجـی، سـی ـ اس ـ اس ـ ای بایـد تحلیـل ترکیبـی محـدودی از عبـارت خروجی انجام دهد. این با مثال بخش ۱. ۲ نشان داده شده است. در یک استعلام SQL تک ثابـت ردیف و ثابت عددی دارای تفسیرهای مختلف هستند و بـدین ترتیـب بـه آزمـایش هـای مختلفـی

احتیاج دارند. مثال دیگری HTML است، جائیکه برای عناصر، نشان ها، و بخش های داده ـ نشانه همین مورد صادق است. پیچیدگی تحلیل ترکیبی لازم به بردار خروجی بستگی دارد.

هنگامیکه سی ـ اس ـ اس ـ ای قطعات متغیر سرچشمه گرفته از کاربر را کشف می کند که حامل محتوی ترکیبی در یک متن مفروض است قادر است از جمله تزریق جلوگیری کند یا اعلام خطر کند. معیارهای واقعی مورد قبول برای جلوگیری از حمله به اجرا شدن و بردار خروجی ویژه بستگی دارد. نوعاً، سی ـ اس ـ اس ـ ای از محتوی تخصصی کنند. می گریزد یا درخواست را مسدود می کند.

اجرا کردن

سی ـ اس ـ اس ـ ای روشی عموماً اجرا شدنی است، و مقید به هیچ برنامه بخصوصی نیست. بهرحال، چندین دلیل وجود دارد که چرا ما پی ـ اچ ـ پی را بعنوان برنامه هدف برای انجام دادن پیش نمونه خود انتخاب کردیم. ابتدا، کاربردهای پی ـ اچ ـ پی مخصوصاً مستعدد آسیب پذیری های تزریق هستند که بخاطر فقدان ویژگی محض و آ ـ پی ـ آی های مناسب برای مرتب کردن داده ها است. دوّم، کاربردهای وب پی ـ اچ ـ پی منبع باز متعددی موجود هستند، که به ما اجازه می دهد به راحتی روش خود را معتبر و اجرا کنیم. سرانجام خود برنامه منبع آزاد است که به ما اجازه می دهد تعمیرات توصیف شده در این بخش را انجام دهیم. سی ـ اس ـ اس ـ ای می تواند در لایه های مختلف مقدار زیادی نرم افزار اجرا شود. بخصوص، سی ـ اس ـ اس ـ ای می تواند در خود کاربرد یا در اجرا کردن کاربرد انجام شود. قبلی به تعدیلاتی در کاربرد احتیاج دارد، که برای نگه داشتن یکی از مهمترین مزیت های سی ـ اس ـ اس ـ ای احتیاج دارد که اتوماتیک شود، یعنی که به توسعه دهنده کاربرد متکی نیست. این می تواند با استفاده از یک پیش پردازشگر کد که فراخون های عملکردها و اعمال مربوط را مجهز می کند بدست آید. یک راه حل ساده و انعطاف پذیر از برنامه ریزی موقعیت سازگار استفاده می کند الگوی آ ـ اُ ـ پی برای در آمیختن کاربرد پذیری لازم در کد کاربرد در زمان همگردانی یا زمان اجرا است. چون اجراهای آ ـ اُ ـ پی برای پی ـ اچ ـ پی با

این حال از مشخصه های لازم پشتیبانی نمی کند (قطع کردن اعمال یکپارچـه، نـه صـرفاً فراخـوان های عملکرد)، در پیش نمونه ها، با استفاده از رهیافـت دوّم سـی ـ اس ـ اس ـ ای را اجـرا کـردیم. یعنی با تعدیل برنامه پی ـ اچ ـ پی.

تعدیل های برنامه پی ـ اچ ـ پی شامل بازدارنده پی ـ اچ ـ پی، و کتابخانه های زمان اجرا، مسـتلزم اجرای چهار بخش سی ـ اس ـ اس ـ ای ارائه ابر داده، تخصیص ابر داده، اعمال یکپارچه حـافظ ابـر داده و ارزیابی یکپارچه حساس به متن است. اجرا کردن این ها در برنامه موجود کاری جزیی نیست و در مورد پی ـ اچ ـ پی، شامل تغییرات متعدد به کد C بطور نامتراکم هستند شده است (به ضمیه A برای فهرست مفصل از فایل های تعدیل شده و بخش کوچکی از کدها نگاه کنید).

هدف از اجرای پیش نمونه سی ـ اس ـ اس ـ ای ها سه لایی است. ابتدا، ابـزاری بـرای نشـان دادن روش ها و پیدا کردن آگاهی در مورد پیچیدگی درگیر در اجرا کـردن آن بـرای برنامـه ای موجـود است. دوّم، این به ما اجازه می دهد مؤثر بودن آنرا در یک کاربرد واقعی آزمایش کنیم و نشان دهیم. سرانجام، به ما برآوردی از اثر عملکرد بوجود آمده توسط سی ـ اس ـ اس ـ ای ارائـه مـی دهـد. بـه عنوان هدف پیش نمونه ها اثبات مفهوم است، ما چهار بخش از سی ـ اس ـ اس ـ ای توصیف شده. پیش نمونه توصیف شده در اینجا بر مبنای ویرایش ۵/۰/۲ برنامه پی ـ اچ ـ پی. ما آنرا طوری تعدیل کردیم که سی ـ اس ـ اس ـ ای می تواند بطور انتخابی در رابطه با کاربرد بخصوصـی کـه در حـال اجرا شدن است خاموش و روشن شود. قلمرو اجرای ما جلوگیری از تزریق هـای اس ـ کیـو ـ ال در کاربردهای وب است. بنابراین، برای بردارهای ورودی، ما به آنهایی که به اچ ـ تی ـ تی ـ پی مرتبط هستند تمرکز کردیم یعنی GET، POST ، ابداع کننده ها و سایر پارامترهای اچ ـ تی ـ تی ـ پی و برای بردارهای خروجی به MySQL تمرکز کردیم. پیش نمونه ها چهار بخش سی ـ اس ـ اس ـ ای را بصورت ذیل اجرا می کند.

نشان دادن ابر داده: سی ـ اس ـ اس ـ ای احتیاج دارد کـه هـر رشـته متغیـر سرچشـمه گرفتـه از ورودی کاربر دارای ابر داده مربوط به آن باشد. در پیش نمونه هـا از یـک مخـزن ابـر داده مرکـزی

استفاده می کنیم. که بعنوان یک جدول آمیزش نشان داده شده توسط نشانگر zval یـک سـاختار حافظه پویا نشان دهنده یک متغیر در پی ـ اچ ـ پی اجرا می شود.

خود ابر داده بعنوان یک بیت مپ (bitmap) بطول یک رشته نشان داده می شود که شاخص مبدأ هر علامت است. در حال حاضر، ما فقط از یک بیت اطلاعات برای هر علامت استفاده می کنـیم، تـا نشان دهیم خواه داده های بخصوصی از طرف کاربر تأمین شده اند. همانطور که در بخـش ۴ بحـث شد. بیت های باقیمانده می توانند برای مسیریابی سرچشمه های احتمالی مختلف داده ها بکار روند (یعنی ورودی کاربر، داده های خوانده شده از پایگاه داده، ورودی کاربر رهـا شـده و داده هـای رهـا شده خوانده شده از پایگاه داده ها)

رشته متغیرهایی که فقط شامل بخش هایی هستند که از طرف کاربر تأمین نشده اند با فقـدان ابـر داده مشخص می شوند. این عملکرد زمان رانش و کارآیی حافظه را بهبود می بخشد. بهرحال، بایـد توجه کرد که کارآیی حافظه یکی از اهداف طراحی پیش نمونه ها نبوده بـا اسـتفاده از نشـان دادن کارآیی حافظه بیشتر، کارآیی حافظه پیش نمونه ها می تواند بطور قابل توجهی بهبود یابد.

تخصیص ابر داده:

هنگامیکه درخواست اچ ـ تی ـ تی ـ پی توسط موتور پی ـ اچ ـ پی دریافت شد، کلیه ورودی کاربر به محل متغیر پی ـ اچ ـ پی وارد می شوند. ما عملکردهای مناسب را برای مـرتبط کـردن ابـر داده مناسب با هر یک از متغیرها طی فاز وارد شدن تجهیز می کنم، بدین طریـق از جملـه هـای درجـه دوّم جلوگیری می کنیم. (جدول ۱)

تخصص دادن ابر داده ها به متغیرهای وارد شده از محیط و درخواست هـای اچ ـ تـی ـ تـی ـ پـی (GET ، POST ، ابداع کننده ها و اطلاعات سندیت) به تعدیل های فقـط یـک عملکـرد احتیـاج دارد، یعنی آنکه مسئول ثبت کردن متغیرهای بیرونی بعنوان متغیرهای پی ـ اچ ـ پی -register-variable-ex) سایر بردارهای ورودی (یعنی ورودی پایگاه اطلاعاتی) بـه تعـدیل هـایی در مـدول های بیرونی مناسب احتیاج دارد، یعنی ext/mysql در مورد MySQL.

رشته عملکردهای حافظ ابرداده : به محض این که ابر داده به یک رشته متغیر تخصیص داده شـده، باید طی طول عمر این متغیر حفاظت و به روز شود. برای از عهده برآمدن این الزام، ما مجموعـه ای از عملکردهای مهم را برای حفاظت کردن از ابر داده تجهیز می کنیم. این مجموعه شـامل متـداول ترین رشته عملیات بکار رفته در تولید عبارت و شامل تسلسل و الحاق و عملکردی است کـه از ابـر علامت ها در داده ها رها شده و برای انجام دادن ارزیابی مفصل ما مشخص کردیم که در یک اجرای کامل، ۶۲ عملکرد (از میان ۳۴۶۸ عملکرد در پی ـ اچ ـ پی) احتیاج به تجهیز شـدن دارنـد. توجـه کنید که در اکثر موارد تجهیزات شامل کپی کردن کلیه یا بخشی از ابر داده مرتبط با رشته ورودی است.

در کاربردهای عملکردهای یکپارچه چه بسیار متداول هسـتند، و بـدین ترتیـب بایـد بـرای حـداقل کردن اثر عملکرد سی ـ اس ـ اس ـ ای روی این نوع عملکردها باید مراقبت ویژه بعمل آید. در یک کاربرد نمونه اکثر اعمال یکپارچه روی عواملی که شامل ابر داده نیسـتند، یعنـی متغیرهـایی کـه از طرف کاربر تأمین نشده اند انجام خواهند شد. ما این را با اجرا کردن اعمال یکپارچه حافظ ابـر داده به طریقی که سر جمع در بند ابر داده قابل صرف نظر کـردن اسـت اداره کـرده ایـم (یـک جـدول آمیزش برای جستجوی و عامل برای آزمایش این که آیا ابر داده وجود دارد).

ارزیابی یکپارچه حساس به متن: در پـیش نمونـه، مـا روی MySQL تمرکـز کـردیم، یـک بـردار خروجی بسیار متداول برای کاربردهای وب. این به مجهز کردن کلیه عملکردهـای مسـئول اجـرای استعلام MySQL لازم است. هنگامیکه این عملکردها خوانده می شوند. آنها از ابر داده موجـود و آگاهی درباره بردار خروجی برای انجام دادن آزمایش های لازم روی عبارت های اجرا شده اسـتفاده می کنند.

هنگامیکه عملکردی که استعلام MySQL را به پایگاه داده ها می فرستد احضار می شود، توسـط سی ـ اس ـ اس ـ ای گرفته می شود. قبل از اجرا شدن، سـی ـ اس ـ اس ـ ای آزمـایش مـی کنـد خواه هیچ ابر داده ای مرتبط با عبارت اس ـ کیو ـ ال وجود دارد . در مورد MySQL، ما بـه یـک

تحلیل ترکیبی محدود از این عبارت احتیاج داریم که بین ثابت های یکپارچه (یعنی e.g., select * from table where user='$username') و ثابت های عددی (یعنی e.g. SELECT * from table where id=$id) تفاوت می گذارد. روش ها همه علامت های نا امن را بر مـی دارد (منطقه های تک رها نشده در مورد اوّل و کلیـه علامـت هـای غیـر عـددی در مـورد دوّم) قبـل از فرستادن استعلام به سرور پایگاه داده.

نتایج آزمایش

این بخش روی آزمایش بویژه بودن و عملکرد سی ـ اس ـ اس ـ ای روی کاربرد پی ـ اچ ـ پی واقعی تمرکز می کند. مهم است توجه کرد که پیش نمونه ها بدون تحلیل کردن کـد منبـع ایـن کـاربرد طراحی شد. در عوض، ما معین کردیم که مجموعه عملکردهای یکپارچه و بردارهای ورودی خروجی مرتبط با پیش نمونه ها بر مبنای آگاهی از کاربردهای وب بطور کلی است. این مقداری اعتبار عرضه می کند که روش ما معتبر است و نتایج مشابهی با سایر کاربردها بدست خواهد آورد.

برای آزمایش های ما کاربرد تایلو تبلیغات phpBB معمول را ترجیح می دهیم، که بر مبنـای سـه دلیل ذیل است. ابتدا، phpBB بعلاوه گسترده بکار می رود و بدین ترتیب نتایج به جامعه مصـرف کننده بزرگی مربوط است. دوّم، دارای درجه بزرگی از پیچیدگی است و بدین ترتیب تأیید ما نشـان می دهد که پیش نمونه بطور مؤثری روی نمونه های غیر جزیی کار می کند سرانجام phpBB در ویرایش های قبلی برای آسیب پذیری های تزریق شناخته شده است [۱۶]. در آزمایش هـای مـا از ویرایش ۰. ۰. ۲ (بتاریخ ۴ آوریل ۲۰۰۲) استفاده کردیم، که در آن چندین آسـیب پـذیری تزریـق شناسایی شده است.

۴–۳ جلوگیری از حمله های تزریق

در زمان نوشتن اس ـ کیو ـ ال ۱۲ آسیب پذیری های تزیرق مربوط به phpBB v2.0.x در پایگاه داده بوتراگ وجود داشت. ما قادر بودیم با موفقیت هفت حمله بکار برنده این آسیب پذیری ها را باز تولید کنیم. (Bugtraq IDs: 6634, 9122, 9314, 9942, 9896, 9883, 10722) . پـنج تای دیگر یا مختص ویرایش های بعد از 2.0.0 بودند یا قادر نبودیم آنها را باز تولید کنیم.

در آزمایش های ما بکارگیری های این آسیب پذیری ها را بـا سـی ـ اس ـ اس ـ ای از کـار افتـاده اعمال کردیم و مطمئن شدیم که موفق شدند. متعاقباً، ما سی ـ اس ـ اس ـ ای را بکـار انـداختیم و حمله ها را تکرار کردیم. پیش نمونه اصلی از شش حمله از میـان هفـت حملـه را جلـوگیری کـرد، بدون این که بطور معکوس قابلیـت اسـتفاده phpBB را تحـت تـأثیر قـرار دهـد. از حملـه هفـتم (Bugtraq ID 6634)، هم بعد از این که یک عملکرد یکپارچه اضافی را تجهیز کردیم، جلوگیری شد، implode با phpBB بکار رفت.

امتحان کردن کُد منبع آشکار کرد که با اعمـال آزمـایش هـای ترکیبـی بـرای اچ ـ تـی ـ ام ـ ال و ارزیابی فایل آغازگر، پیش نمونه ما همچنین از XSS شناخته شده و آسـیب پـذیری هـای تزریـق فایل آغازگر در phpBB جلوگیری می کند. ما تزریق های فایـل آغـازگر را بیشـتر در ضـمیمه B بحث می کنیم، جائیکه نشان می دهیم سی ـ اس ـ اس ـ ای از یک آسیب پذیری بکار گرفته شده توسط کرم ("سانتی" Santy) جدید جلوگیری می کند.

برای نشان دادن این که سی ـ اس ـ اس ـ ای چطور کار می کند، ما نشان خواهیم داد که چطور از یکی از هفت آسیب پذیری ها جلوگیری می کند ـ آسـیب پـذیری بـا Bugtraq ID 9112. ایـن آسیب پذیری ها توسط کد ذیل در Search.php بوجود می آید:

متغیر search-id $ دارای همه منطقه های رها شده است، یا توسط متغیر پـی ـ اچ ـ پـی (اگـر انتخاب "MagicQuotes" توانمند شده است) یا بطور اتوماتیک توسط فایل آغازگر و بنابراین این

منطقه ها در اینجا مشکلی نیستند. مشکل این است کـه متغیـر در مـتن عـددی بکـار رفتـه اسـت جائیکه علامت های زیادی هر علامت عددی هستند. شرایط در مقایسه در خـط ۴ هنگامیکـه یـک پیشوند عددی غیر صفر در متغیر وجود دارد، درست ارزیابی می شـود، نـه هنگامیکـه متغیـر فقـط شامل یک مقدار عددی است (آنچه احتمالاً منظور توسـعه دهنـده بـوده). در نتیجـه ایـن مقایسـه نامعتبر، این کد به حمله های تزریق آسیب پذیر است. برای مثال: با تأمین مقدار ذیل بعنـوان یـک متغیر search-id $ "۱ یا ۱=۱"، استعلام ذیل در پایگاه داده را اجرا می کند.

هنگامیکه سی ـ اس ـ اس ـ ای توانمند شد. ابر داده مرتبط با متغیـر $aql قطعـه "۱ یـا ۱=۱" را علامت می گذارد همانطور که از کاربر سرچشمه گرفته است. قبی از این کـه اسـتعلام واقعـی اجـرا شود (خط ۷) سی ـ اس ـ اس ـ ای محتوی استعلام اس ـ کیو ـ ال بالا را تجزیه می کنـد و معـین می کند که داده سرچشمه گرفته از کاربر (با خاکستری علامت گذاری شده) در متن عـددی ظـاهر می شود. بنابراین، بخشی از داده سرچشمه گرفته از کاربر را که مجاز نیست در این متن انجام گیرد را کشف کرده و برمی دارد (با سیاه علامت گذاری شده). نتیجه یکسان است اگر این متغیر در یـک عدد یا استفاده از تابع intval ($search-id) طبقه بندی می کند، امّا کـل فرآینـد کـاملاً بـرای توسعه دهنده کاربرد آشکار است.

۴–۳–۱ تصریح و تکذیب کاذب

دو نوع خطای مربوط به روش های کشف دخالت و جلوگیری وجود دارد، که عموماً بعنـوان تصـریح کاذب و تکذیب کاذب ارجاع می شود. در این زمینه، تصریح کاذب رویدادهایی هسـتند کـه اعمـال مشروعی هستند که بعنوان مخرب در نظر گرفته می شوند و بنابراین مسدود مـی شـوند. بـرعکس، تکذیب کاذب رویدادهایی هستند که اعمال مخرب کشف نشده هستند.

ما نشان داده ایم که سی ـ اس ـ اس ـ ای یک روش مؤثر برای دفاع در مقابل حملـه هـای تزریـق است، بهرحال، در برخی موقعیت ها تصریح کاذب یا تکذیب کاذب می توانند ظـاهر شـوند. مـا سـه زمینه ذیل را شناسایی کردیم:

اجراهای ناکامل: یک اجرای سی ـ اس ـ اس ـ ای کامـل احتیـاج دارد کـه کلیـه بردارهـای ورودی مربوط، عملکردهای یکپارچه و بردارهای ورودی تجهیز شوند. برای مثال، هنگامیکـه یـک عملکـرد یکپارچه ای که مجهز نشده روی داده کمی نامعتبر بکار گرفته شود، ابـر داده مـرتبط بـا ایـن داده ممکن است از دست رفته یا منسوخ شود. در مورد اوّل، این ممکن اسـت منجـر بـه تکـذیب کـاذب شود. در مورد دوّم، این ممکن است منجر به تکذیب کاذب یا تفریح کاذب شود.

حفاظت در مقابل تزریق های درجه بالاتر به توجه ویژه احتیاج دارد. برای این که سی ـ اس ـ اس ـ ای به درستی این طبقه از آسیب پذیرهای تزریق را آدرس یابی کند، ابر داده مرتبط بـا داده بـادوام هم با بادوام شود. اگر این کار بست پذیری اجرا نشد. همینطور که مورد پیش نمونه مـا اسـت، ایـن ممکن است منجر به تصریح کاذب یا تکذیب کاذب شود که بسته به خط و مشـی از پـیش تعیـین شده ورودی بیرون کشیده شده از انبار بادوام دارد.

اجراهای ناصحیح: زمینهٔ دوّم که در آن تصریح کاذب یا تکذیب کاذب ممکن است اتفاق افتد، اجرای ناصحیح یکی از بخش هایی است که سی ـ اس ـ اس ـ ای را تشکیل مـی دهـد. تجهیـز بردارهـای خروجی پیچیده ترین بخش است، چون این به تحلیل ترکیبی محـدودی از عبـارت هـای خروجـی احتیاج دارد و بنابراین بیشتر مستعد خطاهای اجرا شدن است. این ممکن اسـت منجـر بـه تصـریح کاذب یا تکذیب کاذب شود.

برای مثال در اجرای اس ـ کیو ـ ال ما، فرض کردیم که یک بخش عرضه شده از طرف کاربر ممکن است در یک رشته یا ثابت عددی اتفاق افتد. این با MySQL بخوبی کار می کند. امّـا پایگـاه داده های دیگر ممکن است به آزمایش های پیچیده تری یا تحلیل ترکیبی احتیـاج داشـته باشـد. مثـال دیگر به حمله های XSS مرتبط است. در حالیکه جلوگیری از کلیه برچسب های اچ ـ تی ـ ام ـ ال

از یک متن بسیار ساده است، جلوگیری از برچسب های اچ ـ تی ـ ام ـ ال فقط نا امـن احتیـاج بـه تحلیل پیچیده تر سند دارد (یعنی حتی یک برچسب <b> بـالقوه امـن مـی توانـد یـک صـفت a onMouseover بدنبال یک فایل آغاز گردد Bugtraq ID: 6248 داشته باشد).

ارزش دارد تأکید که سی ـ اس ـ اس ـ ای احتیاج دارد فقط یک بار برای هـر برنامـه اجـرا شـود، و بنابراین می تواند توسط متخصص ها توسعه یافته و در معرض آزمایش قرار گیرند.

فرضیات نامعتبر:

زمینه سوّم به فرض های انجام شده در سی ـ اس ـ اس ـ ای مربوط است. در موفقیت های نادر که این فرضیات در نظر گرفته نمی شوند، این ممکن است منجر به تصریح کاذب تا تکذیب کاذب شود. یک فرض مهم که در آن سی ـ اس ـ اس ـ ای ساخته شد آن است کـه داده هـای تـأمین شـده از طرف کاربر حامل محتوی ترکیبی نباشد. در برخی موارد بخصوص ما به داده هـای از طـرف کـاربر تأمین شده اطمینان نداریم و بدین ترتیب محتوی ترکیبی در این داده ها را مجاز می کنیم. در یک برنامه سی ـ اس ـ اس ـ ای توانمند شده این منجر به تصریح کـاذب مـی شـود، بهرحـال، دو روش برای کم کردن این مشکل وجود دارد: سی ـ اس ـ اس ـ ای می تواند بطور انتخابی بسته به کـاربرد توانمند شود و داده های محققی می توانند بعنوان قابل اطمینان با اسـتفاده از آ ـ پـی ـ آی تـأمین شده صریحاً علامت گذاری شوند.

فرض دوّم به نشان دادن یکپارچه اداره کردن مستقیم نمایش دادن سطح پائین کار می کند، یعنـی یک آرایه علامت، سی ـ اس ـ اس ـ ای ممکن است قادر نباشد ابر داده ها را بطور مناسـبی بـه روز کند. در یک چنین موقعیتی، برای جلوگیری از تصریح کاذب یا تکذیب کاذب، ابر داده بایـد توسـط توسعه دهنده کاربرد با استفاده از یک آ ـ پی ـ آی تأمین شده بطور دستی به روز شود.

۴–۳–۲اندازه گیری های زمان رانش

ما همچنین اثر سی ـ اس ـ اس ـ ای روی عملکرد پی ـ اچ ـ پی را تحلیل کردیم. ما پـنج آزمـایش انجام دادیم که در آن زمان اجرا را اندازه گرفتیم.

T1-cgi: صفحه وب phpBB2/viewforum.php? f=1 را که شامل محتوی یک کنکاش است درخواست می کند. این عمل شامل چندین خواندن و نوشتن پایگاه داده (شامل تولید و ذخیـره آی ـ دی یک جلسه جدید). پی ـ اچ ـ پی بعنوان یک کاربرد سی ـ جی ـ آی عمل می کرد.

T1-mod: آزمایشی شـبیه T1-cgi، بـه اسـتثنای ایـن کـه پـی ـ اچ ـ پـی بعنـوان یـک مـدول Apaches2 عمل می کرد.

T2-cgi: صفحه وب phpBB2/profile.php?mode=editprofile&sid=, شامل محتـوی یک کنکاش با آی ـ دی جلسه معتبر را درخواست می کند. این آزمـایش شـامل چنـدین خوانـدن پایگاه داده و قالب بندی خروجی پیچیده با عملکردهای یکپارچه زیادی بود (تولید کننده یک شکل پیچیده با داده های عرضه شده از طرف کاربر). پی ـ اچ ـ پی بعنوان یک کـاربرد سـی ـ جـی ـ آی عمل می کرد.

T2-mod: آزمایشی شـبیه T2-cgi، بـه اسـتثنای ایـن کـه پـی ـ اچ ـ پـی بعنـوان یـک مـدول Apache2 عمل می کرد.

T3-CLI: این آزمـایش، آزمـایش پـی ـ اچ ـ پـی اسـتاندارد بـود (برنامـه آغـازگر -script run) tests.پی ـ اچ ـ پی (شامل کد منبع پی ـ اچ ـ پی این آزمایش، آزمایش های طراحی شده توسط توسعه دهنده برنامه پی ـ اچ ـ پی را برای آزمایش صحیح بودن پی ـ اچ ـ پی[3] انجام می دهد. توجه کنید که این آزمایش ها شامل یک سرور وب. نیست و معمولاً متشـکر I/O نیسـتند، بنـابراین اثـر مورد انتظار سی ـ اس ـ اس ـ ای باید با T1 و T2 کمتر باشد.

نتایج بدست آمده در جدول ۲ نشان داده شده اند. آزمـایش هـای T1-cgi، T1-mod، T2-cgi، T2-mod اجرا شدند که ۶۰۰ مرتبه از آن ۱۰۰ مرتبه اوّل برای جلوگیری از ذخیره شدن مصنوعی دور انداخته شدند. زمان بندی ها توسط سرور Apache محاسبه شدند. بخاطر زمان رانش طولانی، آخرین آزمایش فقط ۲۰ مرتبه اجرا شـد. ایـن جـدول همچنـین ۹۵٪ فواصـل اطمینـان بـرای هـر مجموعه آزمایش نشان می دهد. همه اندازه گیری ها روی یک دستگاه دارای پردازشگر پنتیـوم M در ۱/۷GHz ، ۱GM ، رام RAM با لینکوس (Linux) انجام گرفتند. ما پـی ـ اچ ـ پـی را در سه پیکربندی ذیل انجام دادیم:

نام آزمایش	T1 (phpbb2 get)		T2 (phpbb2 get)		T3 (PHP tests)
نوع	CGI	mod_apache	CGI	mod_apache	CLI
پچ نشده	61.67 ± 0.23 ms	61.12 ± 0.28 ms	58.59 ± 0.07 ms	57.87 ± 0.07 ms	21.19 ± 0.06 s
CSSE از کار افتاده	62.22 ± 0.24 ms	62.85 ± 0.29 ms	58.85 ± 0.06 ms	59.41 ± 0.08 ms	21.28 ± 0.05 s
CSSE فعال شده	66.42 ± 0.29 ms	71.54 ± 0.37 ms	61.29 ± 0.07 ms	66.63 ± 0.09 ms	21.67 ± 0.07 s

جدول ٤–۱ ارزیابی سرجمع زمان : زمان اجرا برای آزمایشهای مختلف، خطاهای نشان داده شـده فاصـله هـای اطمینان ۹۵٪ هستند با اندازه نمونه ۵۰۰

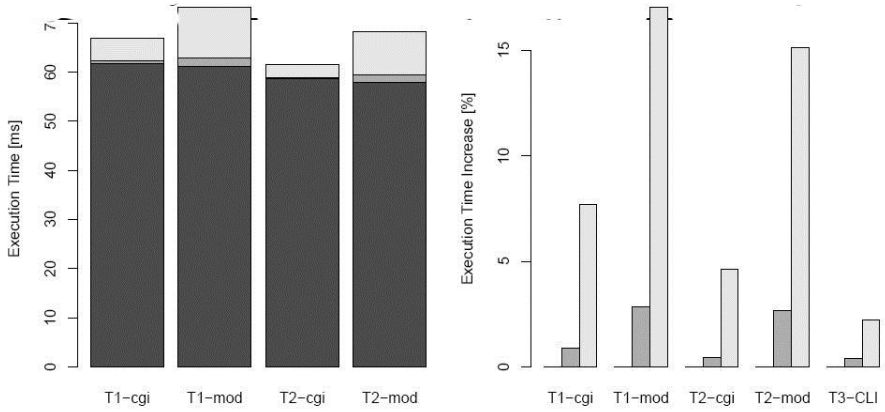
پرگاله نشده: کد منبع پی ـ اچ ـ پی معمولی، همگردانی با انتخاب های استاندارد.

سی ـ اس ـ اس ـ ای ناتوان شده: پی ـ اچ ـ پی برای شامل شدن پی ـ اچ ـ پی پرگاله شد، بهرحال سی ـ اس ـ اس ـ ای توسط انتخاب پیکربندی زمان رانش ناتوان شـد. سـر جمـع آزمـایش کـردن حالت یک برچسب پیکربندی کلی پی ـ اچ ـ پی است که در هر یک از روش های تعدیل شده است.

سی ـ اس ـ اس ـ ای توانمند شده: پی ـ اچ ـ پی برای شامل شدن سی ـ اس ـ اس ـ ای پرگاله شد و سی ـ اس ـ اس ـ ای توانمند شد. توجه کنید که این آزمایش هـا خروجـی مشـابه در همـه سـه پیکربندی تولید کردند و تفاوت فقط در زمان اجرا بود.

سر جمع زمان رانش

ما مشاهده کردیم که سر جمع زمان رانش کل از ۸٪ زمان رانش بیشتر نشـود اگـر پـی ـ اچ ـ پـی بعنوان یک کاربرد سی ـ جی ـ آی عمل کند و یا تعجب بالاتر است، مثلاً ۱۷٪، اگر پی ـ اچ ـ پی در مدول Apaches عمل کند. این در شکل ۳ نشان داده شده است، جائیکه نوارها (میلـه هـا) سـیاه رنگ زمان اجرای یک پی ـ اچ ـ پی پرگاله نشده را نشان می دهد، نوارهای خاکستری سر جمع را با سی ـ اس ـ اس ـ ای ناتوان شده را نشان می دهد. و نوارهای خاکستری کمرنگ سـر جمـع سـی ـ اس ـ اس ـ ای را نشان می دهد. همانطور که انتظار می رود، سر جمع عملکـرد بـرای عملکردهـای I/O (خروجی / ورودی) غیر تنشگر (آخرین آزمایش با صفر پـی ـ اچ ـ پـی تـک ایسـتا) فقـط در حدود۲٪ کل زمان اجرا است.



شکل ٤-۳ ارزیابی سرجمع زمان: زمان پردازش و افزایش نسبی برای آزمایش های مختلف. میلـه هـای سـیاه زمان رانش کل را نشان می دهند، میله های خاکستری سرجمع زمان رانش با CSSE از کار افتاده را نشـان مـی دهند، میلهای خاکستری کمرنگ سرجمع CSSE فعال شده را

مهم است تأکید کرد که این اعداد در زمینه مجموعه اهداف برای پیش نمونه ما در بخـش ۵ تعبیـر شوند. چون این پیش نمونه به عملکردهای یکپارچه دارای بیشترین مصـرف محـدود اسـت، انـدازه

گیری های ما اثر عملکرد واقعی را ناچیز خواهد شمرد. بهرحال، این تخمین کم خیلی کوچک است همانطور که فراخوان های عملکردهای یکپارچه تجهیز شده برای مزیت تعـداد کـل فراخـوان هـای عملکرد یکپارچه بحساب می آید. بعلاوه، پیش نمونه ها برای عملکـرد بهینـه نشـده و بـرای مثـال، استفاده کردن از ارائه ابر داده ثانوی بعنوان مقادیر Zurich روی عملکرد اثر مثبتی خواهد داشت.

بر خلاف انتظارات ما، سر جمع سی ـ اس ـ اس ـ ای بیشتر از ۲/۵ برابر بود هنگامیکه پی ـ اچ ـ پی در یک مدول عمل می کرد، در عوض یک کاربرد سی ـ دی ـ آی، حتی با یک نمایه آزمایش سـاده برای معین کردن این که آیا سی ـ اس ـ اس ـ ای توانمند شده است. این بـه احتمـال زیـاد در اثـر برخی امور دنباله دار است که منجر به بار کردن کل پیکربندی داده های زمان رانش در هر عملکرد یکپارچه است که احتمـالاً مـی توانـد بـا طراحـی دقیـق پـیش نمونـه پرهیـز شـود (بـه فراخـوان TSRMLS-FETCH در ضمیمه A نگاه کنید).

مشاهده جالب دیگر این است که عمل کردن پی ـ اچ ـ پی بعنـوان یـک مـدول Apache2 هـیچ افزایش عملکرد مهمی در مقایسه با کاربرد سی ـ جی ـ آی بـه بـار نمـی آورد. مـا ایـن را بـه طـرز قرارگیری آزمایش خود ما منتسب می کنیم که در آن مفسر پی ـ اچ ـ پی قـبلاً در حافظـه پنهـان شده بود و فقط در یک کار تنها عمل می کرد. طی عملکرد عادی، مـدول هـای Apache2 بطـور قابل توجهی سریع تر از سی ـ جی ـ آی هستند.

در خاتمه، سر جمع عملکرد رویهمرفته به کاربرد وابسته است (به کاربرد بستگی دارد). آزمایش‌های ما توصیه می کنند که حد آن از ۲٪ برای کاربردهـای دارای عملکردهـای I/O (ورودی / خروجـی) کم تا در حدود ۱۰٪ برای کاربردهای وب نمونه با پی ـ اچ ـ پی عمل کننده با یک سرور وب است.

در اجرای جاری ردیف های شامل حداقل یک بخش نامعتبر دو برابر حافظه بیشتر نسبت به مکمـل های عادی خود مصرف می کنند. برای ارزیابی کارایی حافظه سی ـ اس ـ اس ـ ای ما اعتبار مقـدار زیادی از رانش پی ـ اچ ـ پی، سی ـ اس ـ اس ـ ای توانمند شـده بـا آزمـایش هـای T۱ و T۲ بـا استفاده از والگرانیم را تحلیل کریم [۱۱]. در هر دو مورد اثر سی ـ اس ـ اس ـ ای در حدود ۲٪ بود

(۴۰kB افزایش برای کل حدود ۲MB مقدار تخصیص داده شد). این قابل درک است چـون فقـط مقدار کمی از حافظه تخصیص یافته توسط پی ـ اچ ـ پی برای ذخیره کردن متغیرهـای پـی ـ اچ ـ پی بکار می رود و فقط برخی از آنها شامل ردیف های دارای داده های کاربر هستند.

بطور بدیهی، این نتایج به کاربرد وابستگی دارند، امّا برای کاربردهای وب نمونه بایـد مشـابه باشـند. همانطور که قبلاً متذکر شدیم، روش های گوناگون بهینه سازی می توانند برای کاهش این ذخیـره کردن حافظه اضافی اعمال شوند. امّا این ماورای قلمرو پیش نمونه ما بود. نتایج ما نشانه مـی دهـد که حتی با این اجرای ناکافی اثر حافظه جزیی است.

آسیب پذیری های تزریق مشکل مهمی در ایمنی سطح کاربرد به وجود می آورند. در ایـن کـار مـا مسبب اصلی این آسیب پذیری ها را مشخص کردیم ـ ترتیب ویژه ورودی تأمین شده توسط کاربرد بعلاوه، ما چشم انداز یکنواختی از آسیب پذیری های تزریق عرضه کردیم، که استدلال دربـاره ایـن طبقه آسیب پذیری ها را تسهیل می کند و پیش بینی انواع جدید آسـیب پـذیری هـای مـرتبط را بحساب می آورد.

بر مبنای درک بهبود یافته ها، ارزیابی یکپارچه حساس بـه مـتن سـی ـ اس ـ اس ـ ای بـا روشـی جدید برای حفاظت در مقابل حملات تزریق را توسعه دادیم. سی ـ اس ـ اس ـ ای با اعمـال کـردن صریح جدا کردن مجرا، سبب اصلی آسیب پذیری ها را نشان می دهـد، در حالیکـه بـا ایـن وجـود استفاده عرفی از ترتیب ویژه را مجاز می کند. سی ـ اس ـ اس ـ ای برای توسعه دهنده کاربرد واضح است، چون آزمایش های لازم در سطح برنامه اعمال می شوند: نه تعدیل و نه تحلیل کاربردهـا لازم است. در نتیجه، نسبت به دو مقوله را حل های مربوط برتر است: ترتیب ویژه ایمن و ترتیب آ ـ دی ـ آی ها.

سی ـ اس ـ اس ـ ای با علامت گذاری اتوماتیک کلیه داده های سرچشمه گرفته از طرف کاربر با ابر داده های در حدود بعداً آن کار می کند و ضمانت می کند که این ابر داده حفظ شده و به روز شده، هنگامیکه عملکردها روی داده ها انجام می شوند. این ابر داده یک برنامه توانمند شده توسط سی ـ

اس ـ اس ـ ای را قادر می کند بطور اتوماتیک آزمایش های لازم در هـر مرحلـه خیلـی دیـر انجـام دهد، مثلاً هنگامیکه عبارت های خروجی آماده فرستاده شدن به مؤلفه اداره کننده اسـت. چـون در این نقطه متن کامل عبارت های خروجی شناخته شده اند، سی ـ اس ـ اس ـ ای قادر است مستقلاً آزمایش های مناسب روی داده هایی را قبلاً نا امن علامت گذاری شده بودند را معین و اجرا کند.

ما برای برنامه پی ـ اچ ـ پی اجرای پـیش نمونـه سـی ـ اس ـ اس ـ ای راتوسـعه دادیـم، و آنـرا بـا phpBB، کاربردی واقعی بزرگ، ارزیابی کردیم. پیش نمونه ما از کلیه حمله های تزریق اس ـ کیو ـ ال شناخته شده، با اثر عملکرد در حدود ۱۰٪ جلوگیری کرد.

بعنوان کاری مداوم، ما عملکردهای یکپارچه باقی مانده و بردارهـای خروجـی را بـرای جلـوگیری از حمله های تزریق پیشرفته تر شامل حمله های XSS تجهیز کـردیم و سـی ـ اس ـ اس ـ ای را بـا سایر کاربردها ارزیابی کردیم. ما همچنین اجرای سـطح کـاربرد سـی ـ اس ـ اس ـ ای بـرای یـک برنامه که نمونه برنامه ریزی ساز با دیدگاه را حمایت می کند توسعه دادیم.

۴–۴تعدیلات مفصل کد منبع پی ـ اچ ـ پی

برای کُد منبع مفسر V.5.0 PHP بحث شده در بخش ۵ را رائه می دهیم. فهرست فایل های پی ـ اچ ـ پی تعدیل شده و تعدیل های نمونه نشان داده شده اند.

چطور سی ـ اس ـ اس ـ ای از کرم سانتی (santy) جلوگیری می کند

شیوع اخیر (۲۲ دسامبر سـال ۲۰۰۴) کـرم سـانتی بکـار گیرنـده آسـیب پـذیری Bugtraq ID 10701 در phpBB باعث شد ما توجه نزدیک تری به این آسیب پذیری داشته باشیم، این یکی از پنج آسیب پذیری باقی مانده بود که در phpBB v2.0.0 که بکار بردیم حضـور نداشـت. مـا پـی بردیم که مجرم یک کد آن لاین در فایل viewtopic.php افزوده شده بـه phpBB در ویـرایش های غیر از آنکه در پیش نمونه خود بکار بردیم.

این بخصوص جالب است چون این آسیب پذیری تزریق نوع ویژه ای از تزریق فایل اصلی دیده شده در جدول ۱ است. تزریق واقعی در تابع preg-replace از یک عبارت معمولی با تعدیل کننده "e" استفاده می کند انجام می گیرد. و این تعدیل کننده باعث مـی شـود پـی ـ اچ ـ پـی یـک عبـارت ساخته شده پویا شامل متغیر سرچشمه گرفته از کاربر $highlight-match بعنوان کد پی ـ اچ ـ پی زیر خط کشیده شده در خط ۹ را ارزیابی کند.

این تزریق انجام می گیرد چون تابع urldecode، منطقه تک رمز گذاری شده توسط یـو ـ آر ـ ال را که متعاقباً در ثابت یکپارچه در عبارت ارزیابی شده توسط پی ـ اچ ـ پی را رمزگشایی مـی کنـد. این آسیب پذیری می توانست توسط سی ـ اس ـ اس ـ ای جلوگیری شود اگر عملکردهای یکپارچه و کلیه بردارهای خروجی برای ارزیابی کد پویا تجهیز شده بودند. تحلیل ترکیبی حساس به متن در سی ـ اس ـ اس ـ ای راه حلی جامع بردار تزریق فایل گرداننده ارائه می دهد. قبـل از اجـرا، سـی ـ اس ـ اس ـ ای ارزیابی می کند که آیا کد ارزیابی شده شامل ورودی سرچشمه گرفته از طرف کاربر در یک متن امن است. در مورد این آسیب پذیری، این متن یک ثابت یکپارچه تک منطقه ای بود با یک منطقه تک بعنوان ابر علامت، امّا سایر متن ها برای ارزیابی کد هم امکـان دارنـد (یعنـی ثابـت عددی، ثابت یکپارچه دو منطقه ای). بردارهای خروجی تجهیز شـده مناسـب از ایـن گـروه آسـیب پذیری های تزریق فایل آغازگر جلوگیری می کند.

منـابـع و مـراجع :

http://www.adobe.Com/products/acrobat/distribute.html
http://www.adobe.com/support/main.html
http://partners,adobe.com
http://www.adobe.com/security/partners cds.html
http://www.adobe.com/security/partners cds.html
Reader _WWWEULA - en_US-20040915_1630
www.export.gov/safehabor
www.export.gov/safeharbor/eg main 018247. asp