

□ دفاع از رساله دکتری

□ سمینار عمومی (Colloquium)

■ دفاع از پایان نامه کارشناسی ارشد

□ سمینار تخصصی (Seminar)

□ سمینار تخصصی و مشورتی (Informal Seminar)

عنوان: ارائه راهکاری برای حفظ حریم خصوصی در شبکه‌های محتوا محور

سخنران: فاطمه گودرزی

چکیده:

شبکه‌ی داده نام‌گذاری شده، یکی از پنج پروژه‌ی سرمایه‌گذاری شده توسط بنیاد ملی علوم ایالات متحده‌ی آمریکا، برای برنامه‌ی آینده-اش در حوزه‌ی معماری اینترنت و بهبود ضعف‌های معماری فعلی است. NDN فرضیه‌ی سیر تکاملی جیکسون مبنی بر تحول معماری شبکه، از میزبان محور به داده محور را بررسی می‌کند. این جایجایی ساده در مفهوم، الزامات ویژه‌ای برای چگونگی طراحی، توسعه و استفاده در کاربردها دارد.

قابلیت ذخیره‌سازی داده‌های مورد نظر در مکان‌های دلخواه شبکه یکی از مهم‌ترین ویژگی‌های شبکه‌های محتوامحور است. این ویژگی از سویی موجب کاهش ازدحام، پهنای باند مصرفی و کاهش تأخیر دریافت محتوا می‌شود و از سوی دیگر موجب بروز چالش‌هایی در حوزه‌ی حریم خصوصی در این شبکه‌ها شده است. یکی از این چالش‌ها امکان استفاده از اطلاعات زمانی و شناسایی برخوردهای حافظه‌ی نهان و پی-بردن همسایگان یک مسیریاب به محتواهایی است که درخواست دسترسی به آن‌ها داده شده است. روش‌های متعددی برای حل این چالش ارائه شده است که البته مصالحه‌ای میان حفظ حریم خصوصی کاربران و قابلیت ذخیره‌سازی محتوا و در واقع کارایی ایجاد می‌کند. به طور خاص در این پایان‌نامه بر روی این نوع حمله با عنوان حمله‌ی زمانی متمرکز می‌شویم که در آن اختلاف زمانی بین دریافت پاسخ محتوای ذخیره شده و ذخیره نشده به عنوان یک اثر کانال جانبی برای استنتاج اینکه آیا یک کاربر مجاور قبلاً همان محتوا را درخواست داده یا نه، استفاده می‌شود.

اکثر روش‌های ارائه شده برای کاهش حمله‌ی زمانی، در زمان انتقال محتوا تأخیر مصنوعی ایجاد می‌کنند. علی‌رغم تأثیر این رویکرد در به اشتباه انداختن مهاجم، یکی از مهم‌ترین مزیت‌های شبکه‌های محتوامحور یعنی ارتباطات با تأخیر پایین بر مبنای نهان‌سازی تحت تأثیر قرار می‌گیرد. تأثیر منفی دیگری که این رویکرد بر شبکه دارد، تنزل QOE کاربران به ویژه برای محتوای عام است. طبق آنچه گفته شد نیاز است از زاویه‌ی دیگری با این مسئله برخورد کرده و برای آن راه حل ارائه شود. رویکردی که در این پژوهش به آن پرداخته شده طراحی مکانیزمی با عنوان PCC برای نهان‌سازی مشترک است که نه تنها مجموعه‌ی گمنامی را افزایش می‌دهد بلکه از طریق کاهش افزونگی محتوا، ضریب برخورد حافظه‌ی نهان گره‌های همکار را نیز افزایش می‌دهد.

کلمات کلیدی: شبکه محتوا محور، ذخیره‌سازی، حریم خصوصی، حمله زمانی.

زمان برگزاری: ۹۶/۰۲/۱۲

مکان برگزاری: دانشکده مهندسی و علوم کامپیوتر