به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

اعمال خط مشی‌های امنیتی روی ترافیک حجیم شبکه

Security Policy Enforcement on Heavy Network Traffic

امیرمهدی صادق‌زاده

زمان: شنبه ۱۰ بهمن ماه ۱۳۹۴ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن خوارزمی (۴۰۴)

یکی از نیازهای اساسی برای اعمال خط‌مشی‌های امنیتی روی ترافیک حجیم شبکه، دسته‌بندی ترافیک حجیم شبکه است. برای دسته‌بندی ترافیک شبکه سه روش اصلی موجود است: دسته‌بندی مبتنی بر درگاه، دسته‌بندی مبتنی بر نظارت عمیق بسته‌ها و دسته‌بندی مبتنی بر ویژگی‌های آماری ترافیک. تمرکز اصلی این ارائه بر دسته‌بندهای مبتنی بر ویژگی‌های آماری ترافیک با استفاده از الگوریتم‌های یادگیری ماشین است. برای مواجهه با ترافیک حجیم شبکه و افزایش مقیاس‌پذیری دسته‌بندهای مبتنی بر ویژگی‌های آماری ترافیک از الگوریتم‌های دسته‌بندی جویبار داده استفاده می‌کنیم. یکی از چالش‌هایی که در دسته‌بندی ترافیک شبکه با آن مواجه می‌شویم، پدیده تغییر مفهوم است که به بررسی این پدیده می‌پردازیم. در انتها با ارائه یک چارچوب ترکیبی از دسته‌بندهای مبتنی بر ویژگی‌های آماری ترافیک و دسته‌بندهای مبتنی بر نظارت عمیق بسته‌ها سعی خواهیم نمود تا مشکلات دسته‌بندی ترافیک حجیم شبکه ازجمله مقیاس‌پذیری و پدیده تغییر مفهوم را حل کنیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.