سخنرانی‌های هفته پژوهش دانشکده مهندسی کامپیوتر

دوشنبه ۱۴۰۲/۱۰/۱۱

Click or Scan

ساعت	سخنران	عنوان و چکیده
۱۰ الی ۱۰:۳۰	دکتر مهدی دولتی	**عنوان: همکاری در سطح داده برای کاهش تاخیر هدایت ترافیک شبکه** **چکیده:** شبکه های نرم افزار محور این امکان را فراهم کرده‌اند که ترافیک شبکه را با ریزدانگی و انعطاف بیشتر نسبت به شبکه‌های سنتی مدیریت نمود. این ویژگی‌ها حاصل مسیریابی شخصی‌سازی‌شده برای جریان‌های ترافیکی به وسیله لایه کنترل متمرکز شبکه هستند. شخصی‌سازی مسیرها نیازمند درج قوانین مشخص در حافظه سوییچهای شبکه است. با افزایش حجم ترافیک شبکه و تنوع کاربردهای مبتنی بر شبکه تعداد مسیرهای متفاوت و در نتیجه آن تعداد قوانین مورد نیاز بیشتر می‌شود. ظرفیت حافظه بسیاری از سوئیچهای موجود پاسخگوی این نیاز نیست و سوئیچهایی که حافظه کافی در اختیار دارند گران قیمت و پرمصرف هستند. استفاده از این راه حل اخیر نه تنها منجر به افزایش هزینه‌ها می‌گردد بلکه بسیار بیشتر در معرض هدر رفت منابع می‌باشد، چرا که معمولاً توزیع ترافیک در شبکه نابرابر است. با پیشرفت نرم‌افزاری‌سازی شبکه این امکان فراهم شده است که بتوان فعالیت‌های خاص‌منظوره را در سوئیچهای شبکه قرار داد. از این طریق می‌توان این امکان را فراهم آورد تا سوئیچهای شبکه قوانین هدایت را برای سوئیچ دیگری ذخیره کنند و در زمان نیاز آن را فراهم کنند. تأخیرهای اندک در سطح داده باعث می‌شود که این راه حل مبتنی بر همکاری در عمل از نظر کارایی قابل پذیرش باشد و به‌صورت شایانی به بهبود مدیریت ترافیک در شبکه کمک کند بدون آن‌که هزینه‌های اضافی را به شبکه تحمیل نماید.
۱۰:۳۰ الی ۱۱	دکتر امیر نجفی	**عنوان: یادگیری سادک‌ها در ابعاد بالا با استفاده از نمونه‌های نویزی** **چکیده:** در این ارائه، درباره آخرین نتایج نظری مرتبط با یادگیری سادک‌های بعد بالا از روی نمونه‌های نویزی بحث خواهد شد. این مسئله کاربردهای فراوانی در حوزه‌هایی همچون سنجش از راه دور، شناسایی تنوع سلولی در تومورهای سرطانی، و همچنین یادگیری مدل‌های مخلوط آماری دارد. به بیان ریاضی‌تر، فرض کنید که تعداد n نمونه تصادفی مستقل و یکنواخت از داخل یک سادک نامعلوم در فضای K-بعدی در اختیار داشته باشیم. همچنین فرض کنید نمونه‌های مذکور توسط یک نویز جمع‌شونده با قدرت (واریانسی) نامعلوم تخریب شده باشند. ما در مقاله اخیر خود نشان دادیم که یک تخمین‌گر سازگار برای بدست آوردن تقریبی این سادک وجود دارد. همچنین اثبات کردیم که تخمین‌گر مذکور قادر است سادک اصلی را با احتمال زیاد و خطای به دلخواه کوچکی تخمین بزند، مادامی که تعداد نمونه‌ها n به صورت مربعی با K، و به صورت نمایی با عبارت «K/SNR^2» افزایش یافته باشد. در اینجا مقصود از SNR نسبت سیگنال به نویز برای نمونه‌های تخریب شده است. نتیجه فوق که جوابی برای حل یکی از مسائل باز این حوزه به شمار می‌رود، در واقع نشان می‌دهد مادامی که SNR نمونه‌ها به صورت توان ۲/۱ از بعد فضا افزایش یابد، پیچیدگی نمونه‌ای یادگیری سادک‌ها در رژیم نویزی فرق چندانی با حالت ایده‌آل بدون نویز ندارد. روش‌ها و ابزارهای استفاده شده در این تحقیق و سیر اثبات‌ها، ترکیبی از روش موسوم به «فشرده‌سازی نمونه‌ای»، ابزارهایی ریاضیاتی مرتبط با هندسه و آمار در ابعاد بالا، و همچنین آنالیز فوریه هستند. به طور خاص، رویکرد نوین مبتنی بر تحلیل فوریه که در این کار معرفی شده است می‌تواند برای حل دسته وسیع‌تری از مسائل مشابه مورد استفاده پژوهشگران قرار بگیرد.

۱۱ الی ۱۱:۳۰	دکتر محمدحسین رهبان	**عنوان: انواع تعمیم‌پذیری در آشکارسازی داده‌های خارج توزیع** **چکیده:** تشخیص داده‌های خارج توزیع یکی از مولفه‌های مهم ایمنی و قابلیت اطمینان در بکارگیری مدل‌های هوشمند است. روش‌های توسعه داده شده در این حوزه، در چند سال اخیر رشد قابل توجهی داشته‌اند. با این حال، تعمیم‌پذیری این روش‌ها در شرایط مختلف تغییر توزیع، مانند حملات خصمانه، یا تغییرات در روشنایی یا کنتراست تصویر، یا تغییر در سوگیری قیاسی مانند نوع، جنس، و تنوع ناهنجاری‌های مورد نظر، دچار افت کیفیت می‌شوند. در این سخنرانی، راه‌کارهایی برای افزایش تعمیم‌پذیری آشکارسازی داده‌های خارج از توزیع در تصاویر در مدل‌های ژرف ارائه کرده، و با روش‌های پیشین روی دادگان استاندارد تصویری مانند کنترل کیفیت و بازشناسی اشیاء مقایسه می‌کنیم. به صورت خاص، یکی از عناصر اصلی راهکارهای پیشنهادی استفاده از داده ساختگی خارج از توزیع و بعضا یادگیری تضادی است. در انتها جهت‌های پیش رو و کارهای آتی مورد بحث و بررسی قرار می‌گیرند.
۱۱:۳۰ الی ۱۲	دکتر احسان‌الدین عسگری	**عنوان: معرفی پژوهش‌های آزمایشگاه پردازش هوشمند متن و زبان و علوم انسانی محاسباتی** **چکیده:** در این ارائه به معرفی اجمالی برخی عرصه‌های پژوهشی و دستاوردهای اخیر آزمایشگاه پردازش هوشمند متن و زبان و علوم انسانی محاسباتی در حوزه‌های ۱) داده کاوی قرآن و حدیث ۲) زبانهای ایرانی و ۳) تولید تصویر از متن خواهیم پرداخت.
۱۴ الی ۱۴:۳۰	دکترمحسن انصاری	**عنوان: چالش‌های طراحی سامانه‌های رایافیزیکی** **چکیده:** در اکثر سامانه‌های پیشرفته، اجزای محاسباتی به موجودیت‌های فیزیکی مرتبط هستند که در سال‌های اخیر تحت عنوان «سامانه‌های رایافیزیکی» شناخته می‌شوند. نمونه‌هایی از این سامانه‌ها در وسایل نقلیه خودکار، ربات‌های جراحی، شبکه‌های هوشمند و تولیدات مشترک انسان و ربات وجود دارد. توصیف، مدل‌سازی، طراحی، تحلیل و کنترل سامانه‌های رایافیزیکی امری پیچیده و زمانبر است. از این رو در این ارایه به مدل سازی، توصیف و چالش های طراحی این سامانه ها خواهیم پرداخت. از طرفی اخیرا روش های یادگیری ماشین برای مدیریت نیازمندی های اساسی اینگونه از سامانه ها استفاده می شوند که ممکن است راه حل مناسبی برای مدیریت نیازمندی های آن ها باشند. همچنین معماری های متفاوتی از جمله محاسبات لبه/مه/ابر ممکن است به کمک سامانه های رایافیزیکی آمده و در امر محاسبات ما را کمک کنند. در این ارایه قرار است راه حل های ذکر شده برای حل مسایل سامانه های رایافیزیکی شرح داده شوند.
۱۴:۳۰ الی ۱۵	دکتر امیرمهدی صادق زاده	**عنوان: مروری بر امنیت مدل‌های بزرگ زبانی در برابر کاربران متخاصم** **چکیده:** مدل‌های زبانی بزرگ(LLM) ، مانندChatGPT ، درک و تولید متون زبان طبیعی را متحول کرده‌اند. آنها دارای درک عمیقی از متون، قابلیت های تولید متن شبیه به انسان، آگاهی زمینه ای، و مهارت های حل مسئله قوی هستند که آنها را در حوزه های مختلف (مانند موتورهای جستجو، پشتیبانی مشتری، ترجمه) ارزشمند می کند. با توجه به گستردگی کاربرد مدل‌ها زبانی بزرگ در حوزه‌های مختلف، این مدل‌ها مورد توجه پژوهشگران حوزه امنیت اطلاعات قرار گرفته‌اند. مدل‌های زبانی بزرگ اکنون به گونه‌ای تنظیم شده‌اند که با اهداف سازندگان خود، یعنی «مفید و بی‌ضرر» هماهنگ شوند. این مدل‌ها باید به سؤالات کاربر پاسخ مفیدی بدهند، اما از پاسخ دادن به درخواست‌هایی که ممکن است باعث آسیب شوند، خودداری کنند. با این حال، کاربران متخاصم می‌توانند ورودی‌هایی بسازند که باعث شوند تا مدل‌های زبانی بزرگ عملکردی دور از انتظار طراحان آن‌ها داشته باشد. در این ارائه به مرور امنیت مدل‌های بزگ زبانی در برابر کاربران متخاصم می‌پردازیم و بررسی می‌کنیم که به چه میزان این مدل‌ها در راستای اهداف طراحان آن‌ها هستند.

۱۵ الی ۱۵:۳۰	دکتر امیرحسین جهانگیر	**عنوان: الزامات و چالش‌های آزمون و ارزیابی نرم‌افزارهای تحت وب** **چکیده:** با توجه به انواع و اقسام حملات سایبری به سامانه‌های تحت وب از یک سو و لزوم مراقبت و محافظت از منابع اطلاعاتی و برنامه‌های هر سازمان و شخص از سوی دیگر، شناسایی آسیب‌پذیری‌ها و نقاط ضعف امنیتی نرم‌افزارها به معنای عام و برنامه‌های تحت وب به طور خاص اهمیت زیادی در کسب و کارهای اینترنتی پیدا کرده است به طوری‌که غفلت از موضوع امنیت می‌تواند خسارت‌های سنگین به افراد حقیقی و حقوقی وارد کند. ارزیابی امنیتی نرم‌افزار نوعاً بر اساس یک مدل تهدید و حملات محتمل بدان و همین‌طور، یک چارچوب و نمایه حفاظتی (Protection profile) مشخص انجام می‌شود. به عنوان نمونه، موسسه (Open Web Application Security Project: OWASP) هر چند وقت یک‌بار، ده آسیب‌پذیری مهم و خطرناک برنامه‌های تحت وب را رتبه‌بندی و منتشر می‌کند. همین طور، روش‌های تست و راهنماهای گوناگونی نیز در اختیار می‌گذارد. بنابراین چه توسعه‌دهندگان (Developers) نرم‌افزار و چه مشتریان و استفاده‌کنندگان آن می‌توانند بر روی الگوی طراحی و ارزیابی امنیتی نرم‌افزار توافق کنند. ما در این سمینار، به ارائه الزامات، چالش‌ها، مسائل فنی و اجرایی آزمون و ارزیابی امنیتی نرم‌افزار و روش‌های مورد استفاده در آزمایشگاه آزمون و ارزیابی تجهیزات شبکه و امنیت و نمایه‌های حفاظتی مورد استفاده می‌پردازیم. همین‌طور ایده‌هایی برای تسهیل و بهبود فرایند این آزمون‌ها پیشنهاد می‌دهیم که می‌تواند هم برای توسعه‌دهندگان نرم‌افزار و هم بهره‌برداران نهایی مفید و تا حد زیادی اطمینان‌بخش باشد.