

## Persian Abstract

### کنترل دسترسی در سیستم‌های فوق مقیاس وسیع با استفاده از یک میان‌افزار داده-محور

سعید شکرالهی<sup>۱</sup>، فریدون شمس<sup>۱</sup> و جواد اسماعیلی<sup>۱</sup>

<sup>۱</sup>دانشکده برق و کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران

مهمترین مشخصه سیستم‌های فوق مقیاس وسیع (ULS)، اندازه بسیار بزرگ این سیستم‌ها در همه ابعاد است. یک سیستم فوق مقیاس وسیع معمولاً به صورت سیستمی از سیستم‌ها (SoS) در نظر گرفته می‌شود که شامل گره‌های ناهمگن و دامنه‌های خودمختار است. هنگامی که اندازه سیستمی از سیستم‌ها رشد کرده و تعامل‌پذیری بین زیرسیستم‌های آن افزایش پیدا می‌کند، داشتن یک سیستم کنترل دسترسی مقیاس‌پذیر و پویا به عنوان یک نیاز اساسی در این سیستم‌ها مطرح می‌شود. مدل کنترل دسترسی خصوصیت-مبنا به عنوان گزینه‌ای مناسب برای رسیدن به چنین سیستم کنترل دسترسی محسوب می‌شود. استقرار و اعمال خط‌مشی‌های خصوصیت-مبنا در سیستم‌های فوق مقیاس نیازمند همکاری مقیاس‌پذیر و امن مؤلفه‌های کنترل دسترسی توزیع شده خواهد بود. نیاز به پیکربندی و بازپیکربندی پویای این مؤلفه‌ها، سیستم‌های کنترل دسترسی به‌کارگرفته شده در سیستم‌های فوق مقیاس وسیع را با پیچیدگی‌های مدیریت و نگهداشت روبرو خواهد کرد. برای غلبه بر این پیچیدگی‌ها، در این مقاله یک میان‌افزار کنترل دسترسی پیشنهاد می‌شود. میان‌افزار پیشنهادی، داده-محور بوده و شامل دو لایه است. لایه زیرین میان‌افزار شامل یک میان‌افزار سرویس توزیع داده (DDS) است که برای ارتباطات سست اتصال بین مؤلفه‌های کنترل دسترسی استفاده می‌شود. لایه بالایی میان‌افزار جهت پیکربندی و بازپیکربندی مؤلفه‌های کنترل دسترسی به‌کارگرفته می‌شود. از مدل OASIS در لایه بالایی میان‌افزار استفاده می‌شود تا سازوکاری فراهم شود که تنها مؤلفه‌های مجاز بتوانند اطلاعات پیکربندی و بازپیکربندی مربوط به خود را دریافت کنند. در انتها، یک مدل اجرایی از میان‌افزار کنترل دسترسی با استفاده از مدل شبکه‌های پتری رنگی ارائه شده است که می‌تواند در تحلیل رفتار میان‌افزار بکارگرفته شود.

واژه‌های کلیدی: سیستم‌های فوق مقیاس وسیع، کنترل دسترسی، میان‌افزار، میان‌افزار سرویس توزیع داده، مدل شبکه‌های پتری رنگی.

## Persian Abstract

### شکستن کامل Zorro با استفاده از حمله خطی و تفاضلی

شهرام رسولزاده<sup>۱</sup>، زهرا احمدیان<sup>۲</sup>، محمود سلماسی زاده<sup>۲</sup> و محمدرضا عارف<sup>۱</sup>

آزمایشگاه تئوری اطلاعات و مخابرات امن، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

<sup>۲</sup>پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

Zorro یک رمز قالبی سبک شبیه به AES می باشد که در کنفرانس CHES 2013 ارائه شد. این رمز قالبی، با وجودی که دارای حالت داخلی ۱۲۸ بیتی است، در هر دور فقط از ۴ جعبه جانشینی ۸ بیتی استفاده می کند. این ویژگی ضعیف غیرخطی Zorro به طور گسترده مورد نقد قرار گرفته است، تا جایی که هر یک از تحلیل های صورت گرفته تا به حال مستقیماً از این ویژگی بهره گرفته اند؛ که این تحلیل ها شامل حملات کلید ضعیف، دور کاهش یافته و حتی تمام دور می شود.

در این مقاله با استفاده از بعضی مشخصات یافته شده در تحلیل های قبلی، و برخی یافته های جدید، حملات تفاضلی و خطی جدیدی به Zorro ارائه می دهیم که هر دو حمله می توانند کلید مخفی را با پیچیدگی هایی عملی بازیابی کنند. این حملات بر اساس تمایزگرایی کارا و موثر پایه ریزی شده اند، طوری که فقط دو جعبه جانشینی در هر چهار دور فعالیت می کنند. پیچیدگی زمانی حمله تفاضلی و حمله خطی به ترتیب برابر ۲۵۵/۴۰ و ۲۴۵/۴۴ بوده و این در حالی است که این اعداد برای پیچیدگی داده حملات به ترتیب برابر ۲۵۵/۱۵ متن اصلی انتخاب شده و ۲۴۵/۴۴ متن اصلی معلوم می باشد. نتایج نشان می دهد که رمز قالبی Zorro امنیت کافی در برابر حملات تفاضلی و خطی را ندارد.

واژه های کلیدی: حمله خطی، حمله تفاضلی، رمز قالبی سبک، Zorro.

## Persian Abstract

### یک چارچوب مبتنی بر معماری متمرکز برای شبکه‌های اجتماعی با حفظ حریم خصوصی

فاطمه راجی<sup>۱</sup>، علی میری<sup>۲</sup>، و محمد داورپناه جزی<sup>۳</sup>

<sup>۱</sup>دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

<sup>۲</sup>دانشکده مهندسی کامپیوتر، دانشگاه رابرسون، تورنتو، کانادا

<sup>۳</sup>دانشکده مهندسی کامپیوتر و فناوری اطلاعات، موسسه آموزش عالی صنعتی فولاد، فولادشهر، اصفهان، ایران

در سال‌های اخیر، شبکه‌های اجتماعی آنلاین رشد قابل توجهی از نظر تعداد کاربران و محبوبیت داشته‌اند. در شبکه‌های اجتماعی، کاربران از طریق اشتراک اطلاعات مختلف با یکدیگر در ارتباط هستند. یکی از مهمترین مشکلات شبکه‌های اجتماعی فاش شدن اطلاعات خصوصی کاربران و در نتیجه نقض حریم خصوصی آن‌ها می‌باشد. تنظیمات حریم خصوصی گنجانده شده در این شبکه‌ها کنترل کاملی را به کاربران در جهت مدیریت و خصوصی‌سازی دسترسی به اطلاعات اشتراکی‌شان توسط دیگران نمی‌دهد. از طرفی کاربران قادر نیستند تنظیمات حریم خصوصی تعریف شده‌شان را با یکدیگر به اشتراک بگذارند. در این مقاله روشی در جهت طراحی یک شبکه اجتماعی با حفظ حریم خصوصی کاربران در معماری متمرکز پیشنهاد داده می‌شود. به طوری که کاربران می‌توانند محرمانگی و کنترل دسترسی کاملی روی داده‌های اشتراکی خود داشته باشند و در عین حال اتصالات و رابطه‌های اجتماعی خود با کاربران دیگر را به صورت گمنام حفظ نمایند. علاوه بر این کاربران می‌توانند تنظیمات حریم خصوصی متفاوتی برای داده‌های اشتراکی‌شان تعریف نموده و نیز از تنظیمات حریم خصوصی کاربران دیگر استفاده نمایند. نتایج بررسی مبسوط روش پیشنهادی نشان می‌دهند که نه تنها این روش می‌تواند (به خصوص در رابطه با کارهای گذشته) نیازمندی‌های اساسی حریم خصوصی در شبکه اجتماعی را فراهم نماید؛ بلکه در شرایط واقعی نیز به صورت کارا عمل می‌نماید.

**واژه‌های کلیدی:** شبکه‌های اجتماعی، حریم خصوصی، محرمانگی، کنترل دسترسی، اشتراک تنظیمات حریم خصوصی.

## Persian Abstract

# ارائه‌ی یک سیستم مدیریت کلید همگانی برای شبکه‌های حسگر بی‌سیم با مصرف پایین انرژی

حمزه قاسم‌زاده<sup>۱</sup>، علی پاینده<sup>۲</sup> و محمدرضا عارف<sup>۳</sup>

<sup>۱</sup>گروه الکترونیک، دانشگاه آزاد واحد دماوند، دماوند، ایران

<sup>۲</sup>دانشکده ICT، دانشگاه صنعتی مالک اشتر، تهران، ایران

<sup>۳</sup>آزمایشگاه تئوری اطلاعات و مخابرات امن، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

با توجه به محیط متخاصم و طبیعت کانال‌های بی‌سیم، امنیت به جزئی جدایی‌ناپذیر از شبکه‌های حسگر بی‌سیم تبدیل شده است. چنانکه می‌دانیم مدیریت کلید نقشی حیاتی در برقراری امنیت یک شبکه ایفا می‌کند. علی‌رغم این نکته، در عموم روش‌های پیشین مدیریت کلید در این شبکه‌ها، کاهش مصرف انرژی به بهای کاهش امنیت سیستم مدیریت کلید به دست آمده است. با توجه به اینکه این روش‌ها مقاومت‌پذیری کاملی ندارند، برای شبکه‌های با نیاز امنیتی بالا چندان مناسب نمی‌باشند. در این مقاله روشی نو بر پایه‌ی پیام‌های همه‌پخشی از ایستگاه پایه پیشنهاد شده است که امنیت سیستم‌های مدیریت کلید را در شبکه‌های حسگر بی‌سیم افزایش می‌دهد.

از طرف دیگر، در این شبکه‌ها گره‌هایی که منبع انرژی‌شان تمام شده است در محیط باقی می‌مانند. اطلاعات مربوط به کلید در این گره‌ها (همچون کلیدهای خصوصی) می‌توانند به نقطه‌ی آسیب‌پذیری در این شبکه‌ها تبدیل شوند. به‌عنوان مثال مهاجم می‌تواند با جمع‌آوری این گره‌ها و استخراج اطلاعات تولید کلید آن‌ها، گره‌های خود را برنامه‌ریزی نموده و بدین ترتیب حملات مؤثرتری را طرح‌ریزی نماید. در این مقاله نشان داده شده است که روش پیشنهادی توانایی حل این مسأله را نیز دارد. در نهایت چنانکه نتایج شبیه‌سازی نشان می‌دهد، مصرف انرژی روش پیشنهادی کمتر از یک سوم روش کلید همگانی بر پایه‌ی گواهی‌های دیجیتالی می‌باشد.

**واژه‌های کلیدی:** شبکه‌ی حسگر بی‌سیم، مدیریت کلید، رمزنگاری کلید همگانی، احراز اصالت پیام‌های همه‌پخشی.

## Persian Abstract

# بهبود امنیتی شبکه تر در برابر حمله‌های تحلیل ترافیک با استفاده از الگوریتم تصادفی سازی عادلانه

اصغر توکلی<sup>۱</sup> و رضا ابراهیمی آتانی<sup>۱</sup>

<sup>۱</sup>گروه مهندسی کامپیوتر، دانشکده فنی دانشگاه گیلان، رشت، ایران

تر یکی از محبوب‌ترین شبکه‌های فراهم‌کننده گمنامی و حفظ حریم خصوصی در سطح اینترنت است که با استفاده از بازپخش کننده‌های داوطلبانه از سرتاسر جهان کار می‌کند. کارکرد تر با تاخیر کم، آن را برای اموری هم چون گردش در وب مناسب می‌سازد. اگر چه این کارکرد باعث افزایش تعداد کاربران تر شده است، اما امکان انجام حملات تحلیل ترافیکی روی شبکه تر را ساده‌تر نموده است. در این مقاله، ابتدا طرز کار زمانبند مسیرها در شبکه تر تشریح و سپس تعدادی از حملات اخیر را بیان خواهیم نمود. سپس برخی از کارهای مرتبط در راستای مقابله و کم نمودن اثر حملات تحلیل ترافیکی بر روی شبکه‌های مختلط را ارائه خواهیم کرد. در ادامه زمانبند جدیدی را با نام تصادفی‌سازی عادلانه معرفی می‌نماییم و اثر آن را در مقابله با حملاتی که مبتنی بر ترافیک الگوی زمانی هستند، بررسی خواهیم کرد. نتایج به دست آمده نشان می‌دهند که زمانبند جدید می‌تواند به‌طور کلی تمامی حمله‌های مبتنی بر تحلیل و استخراج الگوی زمانی را سخت‌تر و حتی در مواردی ناممکن سازد.

**واژه‌های کلیدی:** شبکه تر، گمنامی، حملات تحلیل ترافیکی، زمانبند، تصادفی‌سازی، حریم خصوصی، شبکه‌های مختلط.

## Persian Abstract

# یک دیدگاه خوشه‌بندی مبتنی بر چگالی جهت تمایز روبات‌های وب از کاربران انسانی

مهدیه ذبیحی<sup>۱</sup>، مجید وفایی جهان<sup>۲</sup> و جواد حمیدزاده<sup>۳</sup>

<sup>۱</sup>دانشگاه بین‌المللی امام رضا (ع)، مشهد، ایران

<sup>۲</sup>گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد، مشهد، ایران

<sup>۳</sup>دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران

وابستگی دنیای امروز به اینترنت و ظهور کاربردهای مختلفی از آن، نیاز به حضور روبات‌های وب جهت پشتیبانی از این فناوری‌ها را افزایش داده است. صرف‌نظر از مزایای روبات‌ها، این نرم‌افزارها اشغال‌کننده پهنای باند شبکه بوده و کارایی سرورها را کاهش می‌دهند. علی‌رغم وجود تحقیقات گسترده در حوزه تشخیص روبات‌های وب، هنوز روشی سریع و کارا برای تمایز آن‌ها از حجم وسیعی از بازدیدکنندگان انسانی، وجود ندارد. علاوه بر این، روش مذکور باید ضمن عدم حساسیت به ترتیب نمونه‌های ورودی، قادر به تولید نتایجی دقیق و قطعی باشد. بنابراین در این مقاله، با به‌کارگیری یک الگوریتم مبتنی بر چگالی، DBSCAN، دو مجموعه عظیم و واقعی خوشه‌بندی می‌گردد. به‌علاوه، بر اساس الگوهای رفتاری بازدیدکنندگان، دو ویژگی جدید جهت توصیف کاربران انسانی و روبات‌ها پیشنهاد می‌شود. در ادامه، با انتخاب ۱۲ ویژگی مرسوم و به‌کارگیری آزمون تی، تعداد ابعاد مساله کاهش یافته و بر یکی از ضعف‌های الگوریتم DBSCAN غلبه می‌گردد. نتایج ارزیابی باناظر روش پیشنهادی نشان می‌دهد؛ این الگوریتم با داشتن معیار جاکاردا ۹۵٪، قادر به تولید دو خوشه نهایی با بی‌نظمی ۰/۰۲۴ و درجه خلوص ۰/۹۷ است. علاوه بر این، از نقطه نظر کیفیت و دقت تعیین خوشه‌ها، روش پیشنهادی عملکردی بهتر نسبت به سایر روش‌های مرز دانش دارد. در پایان، تفسیر خوشه‌های نهایی نشان می‌دهد برخی روبات‌های شناخته‌شده، از طریق تقلید رفتار انسانی، تمایل به مخفی‌سازی هویت خویش و ایجاد اشکال در روند شناسایی خود دارند.

**واژه‌های کلیدی:** خوشه‌بندی مبتنی بر چگالی، DBSCAN، روبات‌های وب، آزمون تی، الگوهای رفتاری بازدیدکنندگان وب.