یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

امنیت و حریم خصوصی در شبکه‌های اجتماعی آنلاین

زینب تابع بردبار[۱]، زینب نیک نژاد[۲]،کبری باقری[۳]

[۱] گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه ای، تهران، ایران، Zeynabtabebordbar.77@gmail.com
[۲] گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه ای، تهران، ایران، Zeynab.niknezhad76972@gmail.com
[۳] گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه ای، تهران، ایران، bagheri128@gmail.com

چکیده

امروزه شبکه‌های اجتماعی آنلاین حضور دائمی در زندگی شخصی و حرفه‌ای افراد زیادی دارند و تاثیر زیادی بر روی فعالیت‌های آفلاین دارند. این شبکه‌ها بر پایه پایه اعتماد بنا شده اند و کاربران با علایق مشترک به صورت آنلاین با همدیگر ارتباط برقرار می‌کنند. شبکه‌های اجتماعی و برنامه‌های کاربردی مرتبط اطلاعات شخصی زیادی را استخراج می‌کنند. تعجب آور نیست که خطرات جدی حریم خصوصی و امنیتی را تهدید می‌کند و دو نوع تهدید را می‌توان در نظر گرفت. سوءاستفاده از اعتماد در روابط اجتماعی و جمع‌آوری اطلاعات شخصی کاربر برای استفاده نادرست. این مقاله یک نمای کلی از مسائل مربوط به حریم خصوصی و امنیتی شبکه‌های اجتماعی آنلاین ارائه می دهد. در این مقاله حملات به حریم خصوصی و امنیتی در شبکه‌های اجتماعی آنلاین و راه حل‌های موجود برای کاهش حملات بررسی می گردد و چالش‌هایی که برای غلبه بر این موارد وجود دارد نیز ذکر می‌گردد.

واژه‌های کلیدی

شبکه‌های اجتماعی آنلاین، حریم خصوصی، امنیت، پایگاه داده، حملات Sybil.

۱. مقدمه

شبکه‌های اجتماعی آنلاین به یک پدیده فرهنگی در میان میلیون‌ها کاربر اینترنت تبدیل شده است. تا سال ۲۰۱۷، فیس بوک ماهانه بیش از یک میلیارد کاربر فعال داشت و سومین سایت پر بازدید در اینترنت به شمار می‌رفت [1]. توییتر، یک پلت فرم میکروبلاگینگ اجتماعی است که ادعا می‌کند ماهانه بیش از ۳۱۳ میلیون کاربر فعال دارد که به بیش از ۴۰ زبان توییت ارسال می‌کنند [2]. امروزه بیشتر از گذشته شبکه‌های اجتماعی آنلاین با زندگی واقعی پیوند خورده‌اند: به عنوان مثال شرکت‌ها در حال استخراج روش‌های ماینینگ در فیس بوک و توییتر برای ایجاد محتوای ویروسی برای اشتراک‌گذاری و لایک هستند، کارفرمایان در حال بررسی پروفایل‌های فیس بوک، لینکدین و توییتر رقبای شغلی خود هستند [3]، سازمان‌های مجری قانون در حال جمع‌آوری شواهد از شبکه‌های اجتماعی آنلاین برای حل جرایم هستند[4]، فعالیت‌هایی در بسترهای اجتماعی آنلاین به منظور تغییر رژیم‌های سیاسی انجام می‌شود [5] و نتایج انتخابات نیز می‌تواند به واسطه شبکه های اجتماعی آنلاین تغییر کند [6].

از آنجایی که کاربران در شبکه‌های اجتماعی آنلاین معمولاً با دوستان، خانواده و آشنایان ارتباط برقرار می‌کنند، تصور رایج این است که شبکه‌های اجتماعی آنلاین یک محیط امن تر، خصوصی تر و قابل اعتماد تر را فراهم می‌کنند [۷]. اما در واقعیت، شبکه‌های اجتماعی آنلاین حفاظت از حریم خصوصی را افزایش داده‌اند، زیرا حجم عظیمی از داده‌های شخصی کاربر در این شبکه‌ها در دسترس هستند. مهمترین دلیل این امر این است که شبکه‌های اجتماعی آنلاین اطلاعاتی را از چندین حوزه اجتماعی در معرض دید قرار می‌دهند: به عنوان مثال، اطلاعات شخصی در فیس بوک و فعالیت‌های حرفه‌ای در لینکدین که در مجموع، منجر به ایجاد پروفایل‌های دقیق می‌شود [۸].

افشای ناخواسته اطلاعات توسط شبکه‌های اجتماعی آنلاین و مبهم بودن جنبه‌های حرفه‌ای و شخصی زندگی کاربر امکان وقوع حوادث با عواقب جبران ناپذیر را فراهم می کند. رسانه‌ها برخی از این موارد را پوشش دادند، مانند معلمی که به دلیل انتشار عکس اسلحه از کار تعلیق شد [9] یا کارمندی که به دلیل اظهار نظر در مورد حقوق خود در مقایسه با حقوق رئیسش اخراج شد [10] علاوه بر این، شبکه‌های اجتماعی عمدا یا ناخواسته به نقض حریم خصوصی کاربر کمک می‌کنند [11]. علاوه بر این، افشای اطلاعات شخصی نیاز به ابزارهای پیچیده حفظ حریم خصوصی را به خود جلب کرده است زیرا اطلاعات کاربر جمع آوری و فروخته می‌شود. علاوه بر این، اعتماد در شبکه‌های اجتماعی آنلاین مکانیسمی موثر برای انتشار هرزنامه، بدافزار و حملات فیشینگ می‌باشد. نهادهای مخرب در حال راه اندازی طیف گسترده‌ای از حملات با ایجاد پروفایل های جعلی، استفاده از اعتبار حساب سرقت شده، استقرار خودکار روبات‌های اجتماعی [12] هستند که در بازار زیرزمینی فروخته می شود [13].

۲. شبکه‌های اجتماعی آنلاین

شبکه اجتماعی اکوسیستمی است که از تعدادی نهاد تشکیل شده است. این نهادها شامل کاربران، ارائه‌دهنده خدمات در شبکه‌های اجتماعی آنلاین، برنامه‌های کاربردی شخص ثالث و تبلیغ‌کنندگان هستند. با این حال، ذینفعان اصلی این اکوسیستم کاربران (که خدمات مختلف شبکه‌های اجتماعی را دریافت می کنند) و ارائه‌دهندگان (که خدمات شبکه

اجتماعی را ارائه می‌دهند) هستند. مشکلات حریم خصوصی و امنیت عواقب زیادی برای کاربران و ارائه دهندگان خدمات شبکه‌های اجتماعی آنلاین به همراه دارد. برای کاربران، پیامدهای بالقوه به اشتراک گذاری نامناسب اطلاعات شخصی، پخش و بهره برداری از اطلاعات شخصی با استفاده از استخراج فعال یعنی لینک اطلاعات می‌باشد [14]. تهدیدات حریم خصوصی و امنیتی به عملکرد مناسب سرویس های شبکه‌های اجتماعی و اعتبار ارائه دهندگان سرویس آسیب می زند.

در این مقاله مشکلات حریم خصوصی و امنیتی در شبکه‌های اجتماعی آنلاین بررسی شده است. دو ذینفع اصلی شبکه‌های اجتماعی آنلاین، کاربران شبکه‌های اجتماعی آنلاین و خود شبکه‌های اجتماعی آنلاین هستند. کاربران اطلاعات شخصی زیادی را در شبکه‌های اجتماعی آنلاین ، از جمله ویژگی‌های فیزیکی، روانی، فرهنگی و اولویت‌هایشان به نمایش می‌گذارند. ۹۰/۸ درصد از پروفایل های فیس بوک عکس دار، ۸۷/۸ درصد از پروفایل‌ها دارای تاریخ تولد و ۳۹/۹درصد دارای شماره تلفن هستند و ۵۰/۸ از پروفایل‌ها محل سکونت شان را ذکر کرده اند و همچنین اکثر کاربران دیدگاه‌های سیاسی، اولویت-های دوستیابی، وضعیت رابطه فعلی و علایق مختلف (از جمله موسیقی، کتاب و فیلم) خود را بیان کرده‌اند [15].

با توجه به تنوع و اختصاصی بودن اطلاعات شخصی به اشتراک گذاشته شده در شبکه‌های اجتماعی آنلاین، کاربران خود را در معرض حملات سایبری و فیزیکی مختلفی قرار می‌دهند. به عنوان مثال، تعقیب یک خطر رایج به دلیل اطلاعات مکان محافظت نشده برای کاربران به شمار می‌رود [16]. ۸۷ درصد از جمعیت ایالات متحده را می‌توان منحصرا بر اساس جنسیت، کد پستی و تاریخ تولد شناسایی کرد [17]. علاوه بر این، تاریخ تولد، زادگاه و محل سکونت کاربر برای تخمین شماره تامین اجتماعی کاربر کافی است و در نتیجه کاربر را در معرض سرقت هویت قرار می دهد [15]. افشای ناخواسته اطلاعات شخصی خطراتی از جمله فیشینگ اجتماعی [18] و مهندسی خودکار اجتماعی [19] را به ارمغان می آورد.

در اکوسیستم یک شبکه اجتماعی آنلاین، کاربران با سایر کاربران تعامل دارند (بسیاری از آن‌ها غریبه هستند)، از برنامه‌های اجتماعی شخص ثالث استفاده می‌کنند و روی تبلیغات کلیک می کنند. نشت اطلاعات کاربران ممکن است اتفاق بیفتد. از سوی دیگر، سرویس‌های شبکه اجتماعی آنلاین، اطلاعات و تمام فعالیت های کاربران در شبکه را مدیریت می‌کنند و مسئول عملکرد صحیح این سروریس‌ها و حفظ سودآوری مدل کسب و کار می‌باشند. در نتیجه کاربران می توانند از خدمات بدون اینکه قربانی اقدامات مخرب شوند استفاده کنند. با این حال، حملاتی مانند Sybil، DDoS، هرزنامه و بدافزار در شبکه‌های اجتماعی آنلاین ممکن است به شهرت آن‌ها آسیب بزند و در سرویس اختلال ایجاد کند.

بنابراین مسائل مربوط به حریم خصوصی و امنیت شبکه‌های اجتماعی آنلاین به دسته های زیر طبقه بندی می‌شود:

۱. نشت و لینک اطلاعات و محتوای کاربر این مسائل به تهدیدات افشای اطلاعات مربوط می‌شوند. نهادهایی که با اطلاعات و نشت و لینک محتوا درگیر هستند شناسایی شده است که در ادامه توضیح داده خواهد شد.

(الف) نشت به سایر کاربران: کاربران ممکن است خود را در خطر زمان ارتباط با سایر کاربران غریبه یا حتی آشنا قرار دهند. برخی از این کاربران ممکن است انسان نباشند (به عنوان مثال، روبات‌های اجتماعی [20])، یا افرادی با اهداف شیطانی هستند [21]. بنابراین محافظت از کاربران و اطلاعات آنها در برابر سایر کاربران یک چالش است.

(ب) نشت از طریق برنامه‌های اجتماعی: کاربران به منظور افزایش عملکرد خود ممکن است با از برنامه‌های اجتماعی مختلف شخص ثالث استفاده کنند. برای تسهیل تعامل بین کاربران شبکه‌های اجتماعی آنلاین و برنامه‌های کاربردی خارجی، شبکه‌های اجتماعی آنلاین به توسعه دهندگان برنامه رابطی ارائه می دهند که از طریق آن به اطلاعات کاربر دسترسی داشته باشند. متأسفانه، شبکه‌های اجتماعی آنلاین با افشای اطلاعات، کاربران را در معرض خطر اطلاعات بیشتر از نیاز این برنامه ها قرار می دهند. برنامه های مخرب می توانند اطلاعات خصوصی کاربران را جمع آوری و برای اهداف نامطلوب استفاده کنند [22].

ج) نشت از طریق شبکه‌های اجتماعی آنلاین: تعامل کاربران با همدیگر و برنامه‌های اجتماعی توسط سرویس‌های شبکه‌های اجتماعی آنلاین تسهیل می‌گردد که معمولا در ازای کنترل کامل بر اطلاعات منتشر شده کاربر در شبکه‌های اجتماعی آنلاین انجام می‌شود در حالی که این مبادله به صراحت در اسناد شرایط خدمات ذکر شده است که کاربر باید با آن موافقت کند. در واقعیت، تعداد کمی از کاربران میزان این تبادل را درک می‌کنند [23] و اکثر کاربران در صورت داشتن انتخاب واقعی، انتخابی ندارند. در نتیجه، بهره برداری شبکه‌های اجتماعی آنلاین از اطلاعات شخصی کاربر نقض اعتماد است و راه حل‌های بسیاری برای پنهان کردن اطلاعات شخصی از سرویس در نظر گرفته شده است.

۲. حملات به شبکه‌های اجتماعی آنلاین: هدف این حملات تهدید کردن کسب و کار ارائه‌دهنده سرویس شبکه‌های اجتماعی آنلاین می‌باشد. شبکه‌های اجتماعی آنلاین هدف حمله انکار سرویس توزیع شده شده‌اند که به عنوان پلتفرم برای انتشار بدافزار و هرزنامه‌های اجتماعی استفاده می‌شوند. این حملات با روش های زیادی صورت می گیرد. به عنوان مثال، مهاجمان می توانند تعدادی هویت Sybil ایجاد کرده و از آنها برای محتوای کمپین هرزنامه یا انتشار بدافزار استفاده کنند. مهاجمان همچنین می‌توانند به طور غیرقانونی کنترل حساب‌های ایجاد شده توسط سایر کاربران را در دست بگیرند و از حساب‌های در معرض خطر برای سازماندهی و برنامه ریزی حملات استفاده کنند. توجه داشته باشید که کاربران پلتفرم‌ها نیز تحت تأثیر حملات شبکه‌های اجتماعی آنلاین قرار می‌گیرند و از نمودار اجتماعی شبکه اجتماعی آنلاین سوء استفاده می‌کند و با انتشار سریع کاربران بیشتری را قربانی می‌کنند. بنابراین، اولویت ارائه دهنده سرویس باید شناسایی نشت و توقف حملات باشد. در ادامه به طور مختصر درباره Sybis ها، حساب‌های در معرض خطر که برای حملات از هرزنامه‌های اجتماعی، بدافزارها، حملات DDoS استفاده می‌کنند بحث خواهد شد.

حملات Sybil: حملات Sybil توسط کاربران با هویت‌های مختلف انجام می‌شود که خروجی سرویس را دستکاری می‌کند [24]. حملات Sybil مختص شبکه‌های اجتماعی آنلاین نمی‌باشد و بر تعیین نتیجه رای گیری الکترونیکی [25]، افزایش ساختگی محبوبیت برخی رسانه‌ها [26] و دستکاری نتایج جستجوی اجتماعی [27] موثر است. با این حال، شبکه‌های اجتماعی آنلاین نیز در برابر حملات Sybil آسیب پذیر شده اند: با کنترل بسیاری از حساب‌ها، کاربران Sybil به طور نامشروع در حال افزایش نفوذ و قدرت در شبکه‌های اجتماعی آنلاین هستند [28].

حملات از طریق حساب‌های در معرض خطر: حساب‌های در معرض خطر ، حساب‌های کاربری قانونی هستند که صاحبان آنها به صورت عادلانه از آنها استفاده می کند، اما توسط مهاجمان تهدید می شود [29]. برخلاف حساب‌های Sybil، این حساب‌ها قبلاً ارتباطات اجتماعی برقرار کرده‌اند و سابقه استفاده عادی از شبکه‌های اجتماعی را دارند. اما ناگهان توسط مهاجمان هک می شوند و بعدا مورد اهداف سوء مهاجمان قرار می گیرند.

هرزنامه اجتماعی و بدافزار: هرزنامه اجتماعی محتوا یا پروفایل‌هایی هستند که کاربران «مشروع» یک شبکه اجتماعی آنلاین مایل نیستند آنها را دریافت کنند [30]. هرزنامه با تضعیف اشتراک‌گذاری منابع، کمک به حملات فیشینگ، پیام‌های تجاری ناخواسته، تعامل بین کاربران و وب سایت‌های تبلیغاتی را مختل می‌کند. هرزنامه‌های اجتماعی به سرعت از طریق شبکه‌های اجتماعی آنلاین پخش می شوند و به دلیل اعتماد سازی در میان دوستان آنلاین، به کاربر انگیزه خواندن پیام‌ها و کلیک بر روی لینک های به اشتراک گذاشته شده توسط دوستان کاربر می‌دهند.

بدافزارها برنامه‌هایی هستند که دسترسی را ایجاد می‌کنند، عملکرد رایانه را مختل می کنند، اطلاعات حساس را جمع آوری می کنند و به رایانه بدون شناخت مالک آن آسیب می زنند. شبکه‌های اجتماعی آنلاین معمولا با استفاده مکرر از هرزنامه‌های اجتماعی، مورد سوء استفاده انتشار بدافزار قرار می گیرند [31].

حملات انکار سرویس توزیع شده : حملاتی هستند که سرویس درخواست‌های به ظاهر غیر توهین آمیز زیادی ارسال می‌کند که موجب بارگذاری بیش از حد سرویس می‌گردد و دسترسی به آن را ممنوع می‌کند [32]. مانند بسیاری از سرویس های محبوب، شبکه‌های اجتماعی آنلاین نیز در معرض چنین حملات هماهنگ و توزیع شده قرار می گیرند.

۳. محافظت از داده‌های کاربر در شبکه‌های اجتماعی آنلاین

رویکرد "آگاهی و رضایت" برای حفظ حریم خصوصی آنلاین در تمام سرویس های آنلاین از جمله شبکه‌های اجتماعی آنلاین وجود دارد. این رویکرد کاربر را از شیوه‌های حفظ حریم خصوصی سرویس مطلع می‌کند و به کاربر این امکان را می دهد که آیا از سرویس استفاده کند یا نه. محدودیت‌های این رویکرد شناخته شده است. اول، درک خط مشی‌های حفظ حریم خصوصی مبهم است و عملاً خواندن آن غیرممکن و وقت گیر است، حتی اگر کاربر مایل باشد برای خواندن آنها وقت بگذارد. به عنوان مثال، در می سال ۲۰۱۷، ۳۰۴۸ کلمه خط مشی های حفظ حریم خصوصی اینستاگرام و ۳۸۰۶ کلمه در مورد خط مشی های حفظ حریم خصوصی توییتر یافت شد. دوم، چنین خط مشی‌هایی طی زمان تغییر می‌کنند. بنابراین، از کاربر انتظار می رود آنها را مکررا" بخواند تا آگاهانه رضایت داشته باشد. و سوم، تا زمانی که این خط مشی‌های حفظ حریم خصوصی ناقص هستند [33]، اغلب نمی‌توانند همه طرفین شبکه های اجتماعی آنلاین را در نظر بگیرند. در نتیجه، معمولا افراد شرایط سرویس را نمی‌خوانند و هنگامی که شرایط را می‌خوانند آنها را درک نمی‌کنند [23]. دومین عامل بازدارنده جدی برای کاربرانی که از حریم خصوصی آنلاین خود محافظت می‌کنند انتخابی است که به کاربران پیشنهاد می‌شود. این انتخاب ممکن است آزاد به نظر برسد، در واقع هزینه عدم استفاده از سرویس آنلاین (اعم از ایمیل، مرورگر، خرید و غیره) خیلی بالا است.

۳. ۱. حفاظت با پنهان کردن اطلاعات

این ویژگی توسط مطالعه اکوئیستی و گراس پیشنهاد شد. در حالی که ۶۰٪ از کاربران به دوستان خود اعتماد دارند و به طور کامل اطلاعات خصوصی و شخصی خود را در اختیار هم می‌گذارند و فقط ۱۸ درصد از کاربران به فیس بوک اعتماد دارند. روش کلی پنهان کردن اطلاعات از شبکه‌های اجتماعی آنلاین بر اساس این مشاهدات است که شبکه‌های اجتماعی آنلاین از داده‌های جعلی استفاده کنند. اگر عملیاتی که شبکه‌های اجتماعی آنلاین با استفاده از داده‌های جعلی انجام می‌دهند با داده‌های اصلی صورت گیرد، کاربران همچنان می توانند از شبکه های اجتماعی آنلاین بدون ارائه اطلاعات واقعی استفاده کنند. داده‌های جعلی می تواند به صورت متن رمز شده (رمزگذاری شده) یا جایگزینی داده‌های اصلی با داده‌های از پیش نقشه‌برداری شده از یک فرهنگ لغت باشد. داده‌های رمزگذاری شده را می‌توان در یک دستگاه قابل اعتماد کاربر (از جمله سرورهای شخص ثالث یا رایانه یک دوست) ذخیره کرد. کنترل های دسترسی به کاربران مجاز (به عنوان مثال، دوستان) برای دریافت داده‌های اصلی اجازه می دهد. دو روش حفاظت با پنهان کردن اطلاعات در ادامه ارائه می‌شود [34].

Persona داده‌های کاربر را با ترکیب رمزگذاری مبتنی بر ویژگی (ABE) و رمزنگاری کلید عمومی از شبکه‌های اجتماعی آنلاین پنهان می‌کند. در عملکردهای اصلی شبکه‌های اجتماعی آنلاین مانند پروفایل‌ها، دیوارها، یادداشت‌ها و غیره در Persona به عنوان برنامه کاربردی پیاده سازی می‌شوند. Persona از برنامه "Storage" برای ذخیره اطلاعات شخصی کاربران و به اشتراک گذاری آن‌ها با دیگران از طریق یک API استفاده می‌کند [35] .

NOYB تلاش کاربر را برای پنهان کردن اطلاعات هویت واقعی در شبکه های اجتماعی آنلاین تحریف می کند که فقط به کاربران قابل اعتماد (به عنوان مثال، دوستان) برای دسترسی به اطلاعات بازیابی شده و صحیح اجازه می‌دهد. برای پیاده

سازی این ایده، NOYB اطلاعات کاربر را به اتم تقسیم می‌کند. به جای رمزگذاری اطلاعات، در NOY اتم کاربر با اتم کاربر دیگری که به طور شبه تصادفی انتخاب شده جایگزین می گردد. همه اتم‌ها با کلاس یکسان برای همه کاربران در یک فرهنگ لغت ذخیره می‌شود. NOYB از پروفایل اتم کاربر رمزگذاری شده برای جایگزینی اتم از این فرهنگ لغت استفاده می‌کند. فقط یک دوست مجاز کلید رمزگذاری را می داند و می تواند رمزگذاری را معکوس کند. زیرکی NOYB این است که اتم‌های قانونی اطلاعات را در متن ساده ذخیره می‌کند، بنابراین باعث ایجاد سوء ظن در مورد شبکه های اجتماعی آنلاین نمی گردد. با این حال چالش مقیاس پذیری فرهنگ لغت م باشد: فرهنگ لغت عمومی هستند و حاوی اتم‌های هر دو کاربران و غیرکاربرانNOYB هستند [36] .

۳. ۲. حفاظت از طریق عدم تمرکز

یک راه حل برای مبهم کردن اطلاعات در شبکه‌های اجتماعی آنلاین، انتقال به سرویس دیگری است که به طور اختصاصی برای محافظت از حریم خصوصی کاربر طراحی شده است. تحقیقات در این زمینه فضای طراحی معماری‌های غیرمتمرکز (همتا به همتا) برای مدیریت اطلاعات کاربر را مورد بررسی قرار داده است، بنابراین از سرویس متمرکز اجتناب می‌شود. روش پوشش معمول بر اساس جداول هش توزیع شده رایج‌ترین راه حلی است که استفاده می‌شود و پوشش‌های بدون ساختار ترجیح داده می‌شود. علاوه بر این، داده‌ها رمزگذاری شده است و فقط کاربران مجاز به متن آن دسترسی دارند. در ادامه دو راه حل ذکر شده است.

Prometheus یک سیستم مدیریت داده اجتماعی همتا به همتا برای برنامه‌های آگاهی اجتماعی است. عملکردهای سنتی شبکه‌های اجتماعی (مانند ایجاد پروفایل، مدیریت، مخاطبین، پیام‌رسانی و غیره)، اطلاعات اجتماعی کاربران را از منابع مختلف مدیریت می‌کند و API ها را برای برنامه‌های اجتماعی در معرض نمایش می‌گذارد. داده‌های اجتماعی کاربران رمزگذاری شده و در گروهی از همتایان مورد اعتماد منتخب کاربران به منظور دسترسی بالای سرویس به آن ذخیره می‌شود. معماری Prometheus بر اساس یک پوشش مبتنی بر DHT، و از گذشته برای رونویسی داده‌های اجتماعی کاربر داشته است [37, 38] .

LotusNet چارچوبی برای اجرای P2P مبتنی بر Likir DHT در شبکه‌های اجتماعی آنلاین است [39] و هویت کاربر را به گره‌های همپوشان و منابع منتشر شده به منظور استحکام شبکه همپوشانی متصل می‌کند و بازیابی منابع مبتنی بر هویت را ایمن می کند. اطلاعات کاربران رمزگذاری می‌شود و در Likir DHT ذخیره می شود. مسئولیت کنترل دسترسی به گره های شاخص همپوشانی تخصیص داده می شود. مشکل کاربران گرانده‌ای امضا شده به سایر کاربران برای دسترسی به داده‌های آنها است. DHT داده های ذخیره شده را تنها در صورتی به درخواست کننده می‌دهد که بتواند گراند مناسب امضا شده توسط مالک را ارائه دهد [40]

۴.کاهش حملات خزنده‌ها

شبکه‌های اجتماعی آنلاین با اجازه دادن به کاربران به منظور مشاهده پروفایل‌های دیگران تجربه مشاهده سایت های اجتماعی را افزایش می‌دهند. به این ترتیب کاربر با کاربران دیگر ملاقات می‌کند و فرصتی برای شناخت غریبه‌ها پیدا می‌کند و در نهایت با برخی از آنها دوست می‌شود و متأسفانه، مهاجمان در شبکه‌های اجتماعی آنلاین وجود دارند که از این قابلیت سوء استفاده می‌کنند. داده‌های اجتماعی کاربران همیشه برای بازاریابان ارزشمند است. جمع‌کننده‌های حرفه‌ای داده، پایگاه‌های داده خود را با استفاده از پروفایل‌ها و لینک‌های اجتماعی و فروش، پایگاه‌های داده شرکت‌های بیمه، آژانس های بررسی پیشینه و آژانس های رتبه بندی اعتباری می‌سازند[41]. گاهی اوقات خزیدن نقض شرایط سرویس است.

فیس بوک اعلام می‌کند اینکه کسی نباید «...محتوا یا اطلاعات کاربران را به تنهایی با استفاده از ابزارهای خودکار بدون اجازه قبلی [42] جمع آوری کند.

یکی از راه حل های این مشکل حذف پروفایل عمومی افراد است. اما حذف پروفایل عمومی برخلاف مدل کسب و کار شبکه‌های اجتماعی آنلاین است. خدماتی مانند جستجو و تبلیغات هدفمند کاربران جدیدی را به ارمغان می‌آورد و در نهایت شبکه‌های اجتماعی آنلاین درآمد کسب می‌کنند اما محتوای قابل دسترسی آزاد برای عملیات آن‌ها ضروری است. علاوه بر این، حذف پروفایل عمومی تجربه کاربر را تضعیف می‌کند، زیرا اتصال، ارتباط و اشتراک گذاری با افراد ناشناس در شبکه را آسان می‌کند.

اپراتورهای شبکه‌های اجتماعی آنلاین مانند فیس بوک و توییتر تلاش می‌کنند از خزیدن در مقیاس بزرگ با محدود کردن تعداد پروفایل‌های کاربر دفاع کنند که آدرس IP کاربر را می‌توانند از پنجره زمانی [43] مشاهده کنند. با این حال، ردیابی کاربران با شناسه‌های سطح پایین شبکه (مانند آدرس IP، شماره پورت TCP یا شناسه جلسه SSL) این راه حل را دچار مشکل می‌کند [44]. مهاجمان متجاوز ممکن است بردار بزرگی از شناسه‌ها را با ایجاد تعداد زیادی از حساب‌های کاربری جعلی، دسترسی به حساب‌های در معرض خطر، مجازی‌سازی در فضای ابری، استفاده از باتنت و ارسال درخواست‌ها به پروکسی‌ها جمع آوری کنند. تا به حال، محققان از تکنیک رمزگذاری مبتنی بر اهرم [44] و رفتار مشاهده‌ای خزنده [45] برای مبارزه با مشکل استفاده می‌کردند.

تکنیک های ضد خزیدن شبکه اجتماعی آنلاین از این واقعیت رنج می‌برند که مشتریان وب می توانند با استفاده از یک URL مشترک در دسترس به یک صفحه خاص به همه مشتریان دسترسی پیدا کنند [44] که توسط یک خزنده توزیع شده مورد سوء استفاده قرار می‌گیرد. به عنوان مثال، یک رشته خزنده می‌تواند یک صفحه را برای لینک‌ها با استفاده از یک کلید جلسه، دانلود و تجزیه کند و می‌تواند آن لینک‌ها را به خزنده دیگری برای دانلود و تجزیه با استفاده از کلیدهای جلسه مختلف تحویل دهد. اگر برخی از خزنده‌ها به دلیل فعالیت‌های مخرب از شبکه‌های اجتماعی آنلاین محروم می‌شوند، لینک هایی که آنها تجزیه کرده اند هنوز معتبر هستند و شروع جدیدی از همان لینک ها امکان پذیر است. SpikeStrip بر این مشکل با ایجاد "نماهای" منحصر به فرد در هر جلسه از وب سایت محافظت شده غلبه می‌کند که هر مشتری به اجبار کلیدهای جلسه خود را می‌بندد. SpikeStrip یک سرور وب افزودنی است که از تکنیک رمزگذاری لینک‌ها استفاده می‌کند و به مدیران شبکه‌های اجتماعی آنلاین در تعدیل دسترسی به داده‌ها اجازه می‌دهد و بر خزیدن در مقیاس بزرگ با هویت ایمن و محدود کردن نرخ جلسات فردی غلبه می‌کند. هنگامی که یک خزنده از یک صفحه بازدید می کند، یک کلید جلسه جدید دریافت می ند و یک کپی از صفحه‌ای که همه لینک‌های آن رمزگذاری شده است. SpikeStrip کلید جلسه هر کاربر را به آن لینک ها اضافه می‌کند و سپس نتیجه آن را با استفاده از یک کلید متقارن مخفی جانبی سرور رمزگذاری می‌کند [44].

۵. کاهش حملات Sybil

حمله Sybil یک مشکل اصلی در سیستم‌های توزیع شده است. اصطلاح Sybil اولین بار توسط Douceur از کتابی به همین نام در سال ۱۹۷۳ معرفی شد. در حمله Sybil ، مهاجم هویت‌های متعددی را ایجاد می‌کند و بر عملکرد سیستم تأثیر می‌گذارد. شبکه‌های اجتماعی از جمله Digg، YouTube و فیس بوک و بیت تورنت در برابر حملات Sybil آسیب پذیر شده‌اند[24] .

به عنوان مثال، فیس بوک پیش‌بینی می‌کند که تا ۸۳ میلیون نفر از کاربران ممکن است نامشروع باشند [46]. محققان دریافتند که کاربران Sybil با محتوای مخرب بر عملکرد صحیح سیستم [27, 47] و افزایش نفوذ و قدرت غیرقانونی [28, 48] تأثیر می‌گذارند.

فعالیت‌های مخرب کاربران Sybil تهدیدی جدی برای کاربران شبکه‌های اجتماعی آنلاین به شمار می‌روند که به این سرویس اعتماد دارند و به صورت آنلاین به فعل و انفعالات آن وابسته هستند. Sybil ها برای ارائه‌دهندگان شبکه‌های اجتماعی آنلاین نیز هزینه دارد. ارائه دهندگان شبکه‌های اجتماعی آنلاین منابع قابل توجهی را صرف زمان شناسایی، تأیید، و خاموش کردن هویت های Sybil می‌کنند مثلا Tuenti، بزرگترین شبکه های اجتماعی آنلاین در اسپانیا، ۱۴ کارمند تمام وقت برای تأیید دستی هویت های Sybil گزارش شده توسط کاربر را اختصاص داده است [49].

Ostra از اعتماد موجود بین کاربران استفاده می کند و ارتباط ناخواسته را خنثی می‌کند و همه ارتباطات ناخواسته کاربر Sybil را محدود می‌کند ک با تخصیص مقادیر اعتباری به لینک های مورد اعتماد ایجاد شده است. اگر کاربر پیامی را به کاربر دیگری ارسال کند، Ostra مسیری با اعتبار کافی از فرستنده به گیرنده می یابد. اگر مسیری در دسترس باشد، اعتبار در امتداد تمام لینک های موجود در مسیر تخصیص داده می شود و اگر گیرنده پیام‌ها را ناخواسته بداند برگردانده می شود. با این حال، اگر چنین مسیری وجود نداشته باشد، Ostra ارتباط را مسدود می کند، اما اعتبار پرداخت می‌شود. که به این ترتیب، Ostra تضمین می کند که کاربر با هویت‌های متعدد نمی تواند تعداد زیادی ارتباطات ناخواسته را ارسال کند، مگر اینکه روابط اعتماد اضافی داشته باشد[50] .

Bazaar برای تقویت شهرت کاربران در نظر گرفته شده است. *Bazaar* آنلاین مانند eBay. با حساب کاربری آزادانه منجر به ایجاد چندین حساب توسط کاربران Sybil می ردد و باعث اتلاف وقت و ضررهای مالی قابل توجه به کاربرانی می‌گردد که از آن‌ها کلاهبرداری شده است.

برای کاهش کاربران Sybil، *Bazaar* شبکه تراکنش را با لینک کردن ایجاد می کند که تراکنش موفقی داشته باشند. وزن لینک مقداری است که با موفقیت منتقل شده است. قبل از تراکنش، با استفاده از تکنیک مبتنی بر حداکثر جریان ، *Bazaar* اعتبار کاربرانی را که این کار را انجام می دهند محاسبه می کند و با ارزش تراکنش جدید مقایسه می‌کند. اگر این جریان موجود را پیدا کند، ارزش تراکنش بین کاربران را به عنوان اعتبار حذف می کند و در نهایت اگر تراکنش تقلبی باشد، دوباره به آن اضافه می کند. با این حال اگر جریان کافی یافت نشود، تراکنش جدید رد می شود[51] .

Canal مکمل شبکه‌های اعتباری Ostra و Bazaar مبتنی بر طرح‌های مقاومت Sybil می‌باشد که از تکنیک‌های مبتنی بر مسیریابی شاخص در محاسبه پرداخت‌های اعتباری یک شبکه بزرگ استفاده می‌کند [52]. یکی از مشکلات عمده Ostra و Bazaar نیاز به محاسبه حداکثر جریان بر روی یک نمودار می‌باشد. با این حال، اندازه بزرگ شبکه‌های امروزی (فیس بوک بیش از میلیارد گره در نمودار اجتماعی دارد) منجر به پیچیدگی محاسباتی قابل توجهی برای محاسبه حداکثر جریان بین دو گره در شبکه می شود. به این ترتیب Canal یک پل ارتباطی برای استقرار شبکه‌های اجتماعی در دنیای واقعی می‌باشد. Canal به طور موثر یک مسیر حداکثر جریان تقریبی را با استفاده از الگوریتم مبتنی بر مسیریابی شاخص موجود محاسبه می‌کند [53, 54].

TrueTop یک سیستم انعطاف‌پذیر sybil در توییتر است که تأثیر کاربران توییتر را با توجه به حضور Sybil ها اندازه‌گیری می‌کند و بر اساس دو مشاهده است: (۱) کاربران غیر Sybil ممکن است افراد غریبه را دنبال کنند، اما آن‌ها در بازتوییت کردن، پاسخ دادن و منشن کردن به سایر کاربران دقت و انتخاب بیشتری دارند. (۲) کاربران تأثیرگذار در مقایسه با سایر کاربران، بازتوییت‌ها، پاسخ‌ها و منش‌های بیشتری دریافت می کنند. TrueTop ابتدا یک نمودار تعامل با استفاده از کاربران و بازتوییت‌ها، پاسخ‌ها و منشن‌های آنها می‌سازد. سپس توزیع اعتبار تکراری را در نمودار تعامل انجام می‌دهد و در نهایت کاربران با نفوذ بالا را انتخاب می‌کند [55] .

۶. نتیجه گیری

میلیون ها کاربر اینترنت از شبکه‌های اجتماعی آنلاین برای ارتباط و همکاری استفاده می کنند. بسیاری از شرکت‌ها به شبکه‌های اجتماعی آنلاین برای تبلیغ محصولات و تأثیرگذاری بر بازار متکی هستند. تصور زندگی بدون استفاده از ابزار های شبکه‌های اجتماعی آنلاین سخت می‌باشد. حریم خصوصی و مسائل امنیتی شبکه‌های اجتماعی آنلاین قابل تفکیک از هم نمی‌باشد. در برخی زمینه ها، حریم خصوصی و اهداف امنیتی یکسان هستند، اما زمینه‌های دیگری نیز وجود دارد که ممکن است متعامد باشند و همچنین زمینه‌هایی وجود دارد که در تضاد با همدیگر هستند. برای به عنوان مثال، در یک شبکه اجتماعی آنلاین، زمانی که کاربر از طریق سرویس پیام رسانی با سایر کاربران ارتباط برقرار می‌کند، حریم خصوصی می‌خواهد. کاربر انتظار دارد غیر گیرندگان پیام کسی قادر به خواندن آن نباشند. سرویس‌های اجتماعی آنلاین با ارائه یک کانال ارتباطی ایمن این امر را تضمین خواهند کرد. شبکه‌های اجتماعی آنلاین احراز هویت حساب کاربری را معمولا با ارسال یک لینک فعال سازی به عنوان یک پیام به آدرس ایمیل کاربر انجام می‌دهند. این یک مشکل حریم خصوصی نیست، شبکه‌های اجتماعی آنلاین فقط تأیید می کنند که کاربران مخرب از ایمیل کاربر قانونی برای ثبت نام استفاده نمی کنند. شبکه‌های اجتماعی آنلاین و برنامه های اجتماعی ثابت هستند در حالی که حملات امنیتی و حریم خصوصی جدیدی شکل خواهند گرفت. پیشرفت‌های فنی در این زمینه در صورت عدم پشتیبانی با اقدامات قانونی برای محافظت از کاربر در برابر سایر کاربران و ارائه‌دهندگان خدمات می‌تواند تأثیر کمی داشته باشند.

منابع

[1] Zephoria, The Top 20 Valuable Facebook Statistics, Zephoria, 2017, URL: https: //zephoria.com/top-15-valuable-facebook-statistics/.
[2] Twitter, Twitter Usage/Company Facts, Twitter2017, URL: https://about. twitter.com/company.
[3] Protalinski, E., 2012. 56% of employers check applicants' Facebook, LinkedIn, Twitter, URL: http://www.zdnet.com/article/ 56-of-employers-check-applicants-facebook-linkedin-twitter/.
[4] Kelly, H., 2012. Police embrace social media as crime-fighting tool, URL: http: //www.cnn.com/2012/08/30/tech/social media/fighting-crime-social-media.
[5] Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I., 2011. The arab spring the revolutions were tweeted: Information flows during the 2011 tunisian and egyptian revolutions, Int. J. Commun. 5 (31).
[6] Jha, P., 2013. Facebook users could swing the results in 160 Lok Sabha constituencies, URL: http://www.thehindu.com/news/national/, facebook-users-could-swing-the-results-in-160-lok-sabha constituencies/ article4607060.ece.
[7] Cutillo, L., Molva, R., Strufe, T., 2009. Safebook: a privacy-preserving online social network leveraging on real-life trust, IEEE Commun. Mag, 47 (12), 94–101.
[8] Nissenbaum, H., 2011. A contextual approach to privacy online, Daedalus,140 (4), 32–48.
[9] W.B. photo, Dam, 2009, School UR L: teacher suspended for Facebook gun. http://www.foxnews.com/story/2009/02/05/, schoolteacher-suspended-for-facebook-gun-photo/.
[10] Mail, D., 2011. Bank worker fired for Facebook post comparing her 7-an-hour wage to Lloyds boss's 4000-an-hour salary, URL: http://dailym.ai/fjRTlC.
[11] Narayanan, A., Shi, E., B.I. 2011. Rubinstein, Link prediction by de-anonymization: how we won the Kaggle social network challenge, in: Proceedings of the 2011 International Joint Conference on Neural Networks (IJCNN), IEEE,1825–1834.
[12] Staff, E., 2010. Verisign: 1.5 m Facebook accounts for sale in web forum, , URL: http://www.pcmag.com/article2/0,2817,2363004,00.asp.
[13] Wagner, C., Mitter, S., Körner, C., Strohmaier, M. 2012. When social bots attack: modeling susceptibility of users in online social networks, in: Proceedings of the 2012 International Conference on World wide web (WWW), 12.

[14] Krishnamurthy, B., 2013. Privacy and online social networks: can colorless green ideas sleep furiously? IEEE Secur. Priv. 11 (3), 14–20.
[15] Gross, R., Acquisti, A., 2005. Information revelation and privacy in online social networks, in: Proceedings of the ACM Workshop on Privacy in the Electronic Society, ACM, 71–80.
[16] Hansen, T., 2015. Social media gives stalkers unprecedented access to victims, URL: http://www.mcphersonsentinel.com/article/20150112/NEWS/150119927.
[17] Sweeney, L., 2000. Uniqueness of Simple Demographics in the US population, Carnegie Mellon University, Laboratory for International Data Privacy.
[18] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F., 2007. Social phishing, Commun, ACM, 50 (10). 94–10
[19] Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., 2009. All your contacts are belong to us: automated identity theft attacks on social networks, in: Proceedings of the Eighteenth International Conference on World Wide Web, ACM, 551–560.
[20] Hwang, T., Pearce, I., Nanis, M., 2012. Socialbots: voices from the fronts, Interactions, 19 (2), 38–45, doi:10.1145/2090150.2090161.
[21] Stringhini, G., Wang, G., Egele, M., Kruegel, C., Vigna, G., Zheng, H., Zhao, B.Y., 2013.Follow the green: growth and dynamics in twitter follower markets, in: Proceedings of the 2013 Conference on Internet Measurement Conference, IMC '13, ACM, New York, NY, USA, , 163–176, doi:10.1145/2504730.2504731.
[22] Felt, A., Evans, D., 2008. Privacy protection for social networking APIs, in: Proceedings of the 2008 Web 2.0 Security and Privacy.
[23] Fiesler, C., Bruckman, A., 2014. Copyright terms in online creative communities, in: Proceedings of the Annual Conference Extended Abstracts on Human Factors in Computing Systems, CHI'14, ACM, 2551–2556.
[24] Douceur, J., 2002.The Sybil attack, in: Proceedings of the Peer-to-Peer Systems, Springer Berlin, Heidelberg, 251–260.
[25] Riley, D., 2007.Stat gaming services come to YouTube, URL: http://www.bbc. co.uk/news/technology-18813237.
[26] Ratkiewicz, J., Conover, M., Meiss, M., Gonçalves, B., Flammini, A., Menczer, F., 2011. Detecting and tracking political abuse in social media, in: Proceedings of the 2011 International Conference on Weblogs and Social Media, ICWSM.
[27] Jurek, M., 2011. Google explores URL: +1 button to influence search results, http://www.tekgoblin.com/2011/08/29/ google-explores-1-button-to-influence-search-results/.
[28] Yu, H., Kaminsky, M., Gibbons, P.B., Flaxman, A., 2006.Sybilguard: defending against Sybil attacks via social networks, in: Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM, 267–278.
[29] Egele, M., Stringhini, G., Kruegel, C., Vigna, G., 2013. Compa: detecting compromised social network accounts, in: Proceedings of the 2013 Symposium on Network and Distributed System Security (NDSS).
[30] Heymann, P., Koutrika, G., Garcia-Molina, H., Fighting spam on social web sites: a survey of approaches and future challenges, IEEE Internet Comput, 11 (6),36–45.
[31] Facebook, Facebook's Continued Fight Against Koobface, Facebook, 2012, URL: http://on.fb.me/y5ibe1.

[32] Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P., Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security), Prentice Hall PTR, Upper Saddle River, NJ, USA.
[33]. Commissioner, P., 2009.Facebook needs to improve privacy practices, investigation finds, URL: https://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.asp.
[34] Acquisti, R., 2006. Gross, Imagined communities: awareness, information sharing, and privacy on the Facebook, in: Privacy Enhancing Technologies, Springer, 36–58.
[35] Baden, R., Bender, A., Spring, N., Bhattacharjee, B., Starin, D., 2009. Persona: an online social network with user-defined privacy, in: Proceedings of the ACM SIGCOMM Conference on Data Communication, ACM, 135–146.
[36] Guha, S., Tang, K., Francis, P., 2008. NOYB: privacy in online social networks, in: Proceedings of the First Workshop on Online Social Networks, ACM, 49–54.
[37] Kourtellis, N., Finnis, J., Anderson, P., Blackburn, J., Borcea, C., Iamnitchi, A., 2010. Prometheus: user-controlled P2P social data management for socially-aware applications, in: Proceedings of the Eleventh International Middleware Conference.
[38] Kourtellis, N., Blackburn, J., Borcea, C., Iamnitchi, A., 2015. Enabling social applications via decentralized social data management, ACM Trans. Internet Technol. (TOIT), 15 (1), 1–26. Special Issue on Foundations of Social Computing.
[39] Aiello, L., Milanesio, M., Ruffo, G., Schifanella, R., 2008. Tempering Kademlia with a robust identity based system, in: Proceedings of the Eighth International Conference on Peer-to-Peer Computing, 30–39
[40] Aiello, L.M., Ruffo, G., 2012. Lotusnet: tunable privacy for distributed online social network services, Comput. Commun, 35 (1), 75–88.
[41] Bonneau, J, Anderson, .J., Danezis, G., 2009. Prying data out of a social network, in: Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining, 249–254.
[42] Facebook, Statement of Rights and Responsibilities, Facebook. 2015, URL: https: //www.facebook.com/legal/terms.
[43] tein, T., Chen, E., Mangla, K., 2011. Facebook immune system, in: Proceedings of the Fourth Workshop on Social Network Systems, ACM, 8:1–8:8.
[44] Wilson, C., Sala, A., Bonneau, J., Zablit, R., Zhao, B.Y., 2010. Don't tread on me: moderating access to OSN data with SpikeStrip, in: Proceedings of the Third Workshop on Online Social Networks, USENIX Association, 2010.
[45] Mondal, M., Viswanath, B., Clement, A., Druschel, P., Gummadi, K.P., Mislove, A., Post, A., 2012. Defending against large-scale crawls in online social networks, in: Proceedings of the Eighth ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT'12), ACM, Nice, France.
[46] BBC, Facebook has More Than 83 Million Illegitimate Accounts, BBC2012, URL: http://www.bbc.co.uk/news/technology-19093078.
[47] Grier, C., Thomas, K., Paxson, V., Zhang, M., 2010. @spam: the underground on 140 characters or less, in: Proceedings of the Seventeenth ACM Conference on Computer and Communications Security, ACM, 27–37.
[48] Nazir, A., Raza, S., Chuah, C.-N., Schipper, B., 2010. Ghostbusting Facebook: detecting and characterizing phantom profiles in online social gaming applications, in: Proceedings of the Third Conference on Online Social Networks, USENIX Association.

[49] Cao, Q., Sirivianos, M., Yang, X., Pregueiro, T., 2012. Aiding the detection of fake accounts in large scale social online services, in: Proceedings of the Ninth USENIX Conference on Networked Systems Design and Implementation, USENIX Association.
[50] Mislove, A., Post, P., Druschel, K.P., 2008. Gummadi, Ostra: leveraging trust to thwart unwanted communication, in: Proceedings of the Fifth USENIX Symposium on Networked Systems Design and Implementation, USENIX Association, 15–30.
[51] Post, A., Shah, V., Mislove, A., 2011. Bazaar: strengthening user reputations in online marketplaces, in: Proceedings of the Eighth USENIX Conference on Networked Systems Design and Implementation, USENIX Association.
[52] Viswanath, B., Mondal, M., Gummadi, K.P., Mislove, A., Post, A., 2012. Canal: scaling social network-based Sybil tolerance schemes, in: Proceedings of the Seventh ACM European Conference on Computer Systems, ACM, 309–322.
[53] Tsuchiya, P.F., 1988.The landmark hierarchy: a new hierarchy for routing in very large networks, Comput. Commun. Rev. 18 (4), 35–42.
[54] Gubichev, A., Bedathur, S., Seufert, S., Weikum, G., 2010.Fast and accurate estimation of shortest paths in large graphs, in: Proceedings of the Nineteenth ACM International Conference on Information and Knowledge Management, ACM, 499–508.
[55] Zhang, J., Zhang, R., Sun, J., Zhang, C Y., 2016. Zhang, TrueTop: a Sybil-resilient system for user influence measurement on Twitter, IEEE/ACM Trans. Netw. 24 (5), 2834–2846