حملات Sybil و دفاع در برابر آنها در اینترنت اشیاء

چکیده

اینترنت اشیاء (IoT) نوظهور در برابر حملات Sybil آسیب‌پذیر است در حالی که مهاجمان می‌توانند با هویت‌های جعلی یا سوءاستفاده از شناسه‌های ساختگی به بر روی اینترنت اشیاء تاثیر گذاشته و حتی هرزنامه منتشر کنند. در این مقاله، ما به بررسی حملات Sybil و روش‌های دفاع در برابر آنها در اینترنت اشیاء می‌پردازیم. به طور خاص، ما در ابتدا سه نوع حمله‌ی Sybil را با توجه به توانایی‌های مهاجم Sybil تعریف می‌کنیم: SA-1، SA-2 و SA-3. سپس برخی از روش‌های دفاع در برابر Sybil را به همراه مقایسه‌های جامع ارائه می‌دهیم که شامل تشخیص Sybil بر اساس گراف اجتماعی (SGSD)، تشخیص Sybil بر اساس طبقه‌بندی (BCSD)، و تشخیص Sybil متحرک می‌باشند. در نهایت، مسائل پژوهشی چالش‌برانگیز و مسیرهای آینده برای دفاع Sybil در اینترنت اشیاء را شرح می‌دهیم.

کلمات کلیدی: طبقه‌بندی رفتار؛ اینترنت اشیاء (IoT)؛ شبکه اجتماعی متحرک؛ شبکه اجتماعی؛ حمله‌ی Sybil.

I. مقدمه

اینترنت اشیاء (IoT)، که می‌تواند اینترنت معمولی را به یک شبکه‌ی همه‌جاحاضر گسترش دهد که اشیاء موجود در جهان فیزیکی را به هم متصل می‌کند، تکاملی را برای ارتقای تعامل بین افراد و اشیاء آغاز نموده است. با حسگرهای جاسازی شده در اشیاء، اینترنت اشیاء می‌تواند اطلاعاتی را از محیط، اشیاء و بدن ما (از طریق شبکه‌ی حسگر، روش شناسه‌ی فرکانس رادیویی (RFID)، وسایل پوشیدنی، و غیره) حس کرده و به دست آورد [۱]-[۳]. با ظهور روش‌های ارتباطی بی‌سیم، از قبیل ارتباطات بی‌سیم کوتاه بُرد و WiFi، اینترنت اشیاء می‌تواند کاربران را قادر سازد تا اطلاعات را با دیگران [۴] و [۵] در شبکه‌های اجتماعی و خودروهای متصل به اینترنت به اشتراک بگذارند [۶] و [۷]. علاوه بر این، اینترنت اشیاء با یکپارچه‌سازی قابلیت‌های حسی، ارتباطی، و محاسباتی [۸] و [۹] می‌تواند سرویس‌های هوشمند متنوعی [۱۰] را از قبیل تشکیل خانه‌ی هوشمند [۱۱]، شبکه‌ی توزیع برق هوشمند [۱۲]-[۱۴]، جامعه‌ی هوشمند [۱۵]، و شهر هوشمند [۱۶] و [۱۷] ارائه دهد که

در شکل ۱ نشان داده شده است. بنابراین با پیشرفت فناوری اینترنت اشیاء، این کاربردهای ارزش افـزوده بـرای تسهیل و کمک به تعامل افراد با اشیاء، افراد، و جهان شکوفا شده‌اند و روشی را که ما با یکـدیگر ارتبـاط برقـرار می‌کنیم را تغییر می‌دهد.

شکل ۱. نگاه کلی بر اینترنت اشیاء.

با این حال، اینترنت اشیاء نوظهور در برابر حملات Sybil آسـیب‌پـذیر هسـتند، حملاتـی کـه در آنهـا مهاجمان می‌توانند هویت‌ها را جعل نموده [۱۸]-[۲۰] یا با ایجاد هویت‌های جعلی، کارایی سیستم‌ها را به خطر بیاندازند. با حضور حملات Sybil، سیستم‌های اینترنت اشیاء ممکن است گزارش‌های اشـتباهی تولیـد کننـد، و کاربران ممکن است هرزنامه دریافت نموده و حریم خصوصی خود را از دست بدهند. از یـک گـزارش جدیـد در سال ۲۰۱۲ [۲۱]، تعداد قابل توجهی از حساب‌های کاربران به عنوان حساب‌های جعلی یا Sybil در شبکه‌هـای آنلاین اجتماعی[1] (OSNs) تایید شده‌اند، به طور کلی ۷۶ میلیون (۷٫۲٪) در Facebook، و ۲۰ میلیـون حسـاب

[1] Online Social Networks (OSNs)

جعلی هر هفته در Twitter ایجاد می‌شوند. این حساب‌های Sybil نه تنها هرزنامه و تبلیغات منتشر می‌کنند، بلکه همچنین بدافزار و وبسایت‌های فیشینگ نیز به دیگر کاربران انتشار می‌دهند تا اطلاعات حریم خصوصی دیگر کاربران را به سرقت ببرند. علاوه بر این، در یک سیستم ارتباطی خودرویی توزیع شده [۲۲] و سیستم‌های اجتماعی همراه [۲۳]، مهاجمان Sybil گزینه‌های مغرضانه‌ای را با حساب‌های "خوانا و واضح" تولید می‌کنند. بدون یک روش تشخیص کارآمد، نتایج جمعی نیز که در نهایت از روی این گزینه‌ها تولید می‌شوند، به سادگی توسط مهاجمان مورد دستکاری واقع می‌شود. از آنجایی که مهاجمان Sybil مانند کاربران عادی رفتار می‌کنند، پی بردن به اینکه یک حساب، Sybil است یا خیر بسیار دشوار می‌باشد، و این مسئله اهمیت زیادی به مبحث دفاع در برابر Sybil در اینترنت اشیاء می‌بخشد.

تلاش‌های اخیر تحقیقاتی [۲۴] و [۲۵] بر روی مطالعه‌ی حملات Sybil و نحوه‌ی تشخیص و دفاع در برابر آنها تمرکز داشته‌اند. SybilGuard [۲۴] یک روش تشخیص Sybil مبتنی بر گراف (شبکه) اجتماعی است، که گام تصادفی[1] را بررسی می‌کند تا کل گراف اجتماعی را به صورت مناطق درستکار و مناطق Sybil بخش‌بندی کند که مناطق Sybil شامل گره‌های Sybil در درون خود هستند. SybilGuard بر این فرض تکیه می‌کند که گره‌های Sybil می‌توانند تنها تعداد محدودی از اتصالات اجتماعی با گره‌های درستکار ایجاد کند. یک روش دیگر نیز با توجه به رفتارهای متفاوت کاربران عادی و Sybil، از قبیل جریان کلیک‌ها، در مرجع [۲۶] ارائه شده است که یک روش تشخیص Sybil مبتنی بر طبقه‌بندی رفتار[2] (BCSD) می‌باشد. با مشاهده‌ی جریان کلیک‌ها پی می‌بریم که مهاجمان Sybil الگوهای خاصی برای کلیک و تکرار عمدی آنها دارند. بدین ترتیب، این الگو برای تشخیص مهاجمان Sybil از طریق یادگیری ماشین بر روی جریان کلیک‌ها موثر است. علاوه بر این راه‌حل‌ها که برای مهاجمان Sybil آنلاین موجود است، دفاع در برابر Sybil نیز نقش مهمی در شبکه‌های متحرک ایفا می‌کند. در مرجع [۲۷]، تشخیص Sybil متحرک بر اساس لیست دوستان و مخالفان کاربران متحرک بررسی می‌شود. کاربران متحرک می‌توانند مهاجمان Sybil را با تطبیق پروفایل آنها تشخیص دهند وقتی که وارد سیستم می‌شوند. Liang و همکارانش [۲۳] به بررسی تاریخچه‌ی تماس‌ها و اعتماد کاربر متحرک محلی می‌پردازند تا وقتی که مهاجمان Sybil در حال آپلود کردن نظرات خود هستند، در برابر آنها مقاومت کنند. به ویژه، در یک شبکه‌ی متحرک، کاربران متحرک نمی‌توانند به طور موثری بدون دانش کافی، مهاجمان

[1] random walk
[2] Behavior Classification-based Sybil Detection (BCSD)

Sybil را تشخیص دهند. بنابراین، تلاش‌های تحقیقاتی زیادی برای توسعه‌ی روش‌های تشخیص Sybil متحرک و آنلاین و دفاع در برابر آنها در اینترنت اشیاء موردنیاز است.

در این مقاله، ما به بررسی حملات Sybil و روش‌های دفاع در برابر آنها در محیط اینترنت اشیاء می‌پردازیم. به طور خاص، ما در ابتدا سه نوع از حملات Sybil یعنی SA-1، SA-2 و SA-3 را تعریف می‌کنیم تا طیف وسیعی از حملات Sybil موجود را پوشش دهیم. حمله‌ی نوع SA-1 به صورتی در نظر گرفته می‌شود که در گراف اجتماعی تعداد محدودی از اتصالات با کاربران عادی دارد، در حالی که SA-2 به گونه‌ای در نظر گرفته می‌شود که اتصالات اجتماعی زیادی را با کاربران عادی ایجاد می‌کند. بنابراین، تشخیص SA-2 با استفاده از بخش‌بندی گراف اجتماعی بسیار دشوار است. SA-3 در شبکه‌های متحرک در نظر گرفته می‌شوند، یعنی جایی که اطلاعات گراف اجتماعی در دسترس نیست، و نمی‌تواند به سادگی تشخیص داده شود. ما سه نوع از روش‌های دفاع در برابر Sybil را نیز ارائه می‌دهیم: ۱) تشخیص Sybil بر اساس گراف اجتماعی[1] (SGSD)؛ ۲) دفاع در برابر Sybil بر اساس طبقه‌بندی رفتار[2] (BCSD)؛ و ۳) دفاع در برابر Sybil متحرک[3] (MSD). ما همچنین در مورد برخی از مسائل چالش‌برانگیز و راه‌حل‌های بالقوه‌ی آنها برای دفاع در برابر Sybil در اینترنت اشیاء بحث می‌کنیم.

این مقاله به صورت زیر سازماندهی شده است. ما در بخش II به معرفی کاربردها و دامنه‌های اینترنت اشیاء می‌پردازیم. بخش III به تعریف و تشریح حملات Sybil در دسته‌های مختلف می‌پردازد. ما سپس به ترتیب در بخش‌های IV تا VI به ارائه‌ی SGSD، BCSD، و MSD می‌پردازیم. در نهایت، در بخش VII نیز از مقاله نتیجه‌گیری می‌شود.

II. دامنه‌ها و کاربردهای اینترنت اشیاء

در این بخش، ما سه دامنه از اینترنت اشیاء را با توجه به کاربردهای مختلف اینترنت اشیاء به شرح زیر ارائه می‌دهیم.

[1] social graph based Sybil detection (SGSD)
[2] behavior classification based Sybil defense (BCSD)
[3] mobile Sybil defense (MSD)

A دامنه‌ی حسی

حس کردن محیط‌ها یکی از مهمترین قابلیت‌های ارزش افزوده در اینترنت اشیاء است که محیط‌هایی از جمله محیط زندگی [۲۸]، و بدن انسان [۲۹]-[۳۱] می‌باشند، تا بدین وسیله به کاربران اجازه‌ی تعامل با جهان فیزیکی داده شود [۳۲]. از این رو، حجم زیادی از حسگرهای نهفته در مناطق هدف مستقر می‌شوند تا به شرایط محیطی یا اطلاعات بیولوژیکی انسان نظارت نمایند [۳۳]. همانطور که در شکل ۲ نشان داده شده است، گره‌ی چاهک[1] (مانند، کاربران یا مرکز کنترل) با جمع‌آوری این داده‌های حس شده، می‌تواند به تحلیل و استخراج برخی از اطلاعات ذاتی یا پنهان بپردازد. به عنوان مثال، کنتورهای هوشمندی برای اندازه‌گیری مصرف لوازم خانگی یا توان مصرفی ساختمان یا منطقه‌ی مسکونی مورد استفاده قرار می‌گیرد، و در فواصل معین زمانی مقدار توان مصرفی توسط هر واحد را به مرکز کنترل ارسال می‌کند. با توجه به داده‌های اندازه‌گیری شده، مرکز کنترل می‌تواند توزیع توان را برای ذخیره‌ی مصرف غیرضروری انرژی زمانبندی کند. وسایل پوشیدنی [۳۴] و [۳۵] توسط افراد برای اندازه‌گیری پارامترهای بیولوژیکی از قبیل ضربان قلب، فشار خون، دمای بدن، اشباع اکسیژن، شاخص حجم خون، شاخص ضدآریتمی، کیفیت خواب در الگوی بی‌درنگ[2] مورد استفاده قرار می‌گیرند. یک گره‌ی چاهک یا کنترل‌کننده (به عنوان مثال، گوشی‌های هوشمند، مرکز کنترل) به جمع‌آوری تمام داده‌های حس شده پرداخته و آنها را برای کنترل به سیستم تشخیص و کاربران گزارش می‌دهد.

شکل ۲. دامنه‌های اینترنت اشیاء: دامنه‌ی حسی، دامنه‌ی اجتماعی، و دامنه‌ی متحرک

[1] Sink node
[2] real-time

B. دامنه‌ی اجتماعی

متفاوت از دامنه‌ی حسی که هدف آن نظارت محیطی است، دامنه‌ی اجتماعی کاربردهایی از اینترنت اشیاء را فراهم می‌کند تا به تعامل اجتماعی بین کاربران کمک نماید [۳۶]-[۳۸]. با در نظر گرفتن علایق مشابهی که در شکل ۲ نشان داده شده است، کاربران می‌توانند جامعه یا تجمع آنلاین مجازی برای تبادل اطلاعات و اشتراک‌گذاری منابع چندرسانه‌ای تشکیل دهند. به طور کلی، کاربران در دامنه‌ی اجتماعی به اینترنت دسترسی داشته و می‌توانند هم با سرورهای آنلاین و هم با دیگر کاربران به تعامل بپردازند. کاربران در دامنه‌ی اجتماعی می‌توانند محتوای موردنظر خود را جستجو کرده، اخبار جدید را دنبال نموده، و اطلاعات یا محتوا را با دیگر دوستان اجتماعی خود به اشتراک بگذارند.

C. دامنه‌ی متحرک

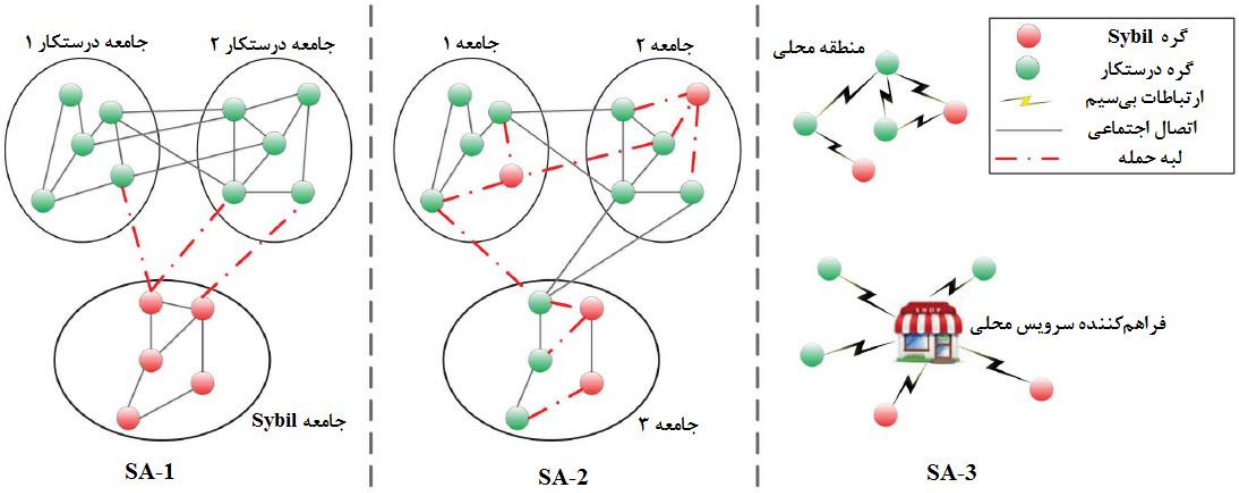
در دامنه‌ی متحرک، دسترسی به اینترنت کاربران ممکن است به علت محدودیت پوشش اینترنت و قابلیت تحرک آنها همیشگی نباشد. با این حال، کاربران می‌توانند از قابلیت تحرک خود برای تعامل با دیگرانی استفاده کنند که در مجاورت فیزیکی آنها قرار دارند و علایق خود را در قالب یک الگوی دستگاه-به-دستگاه با استفاده از ارتباطات بی‌سیم کوتاه بُرد، بلوتوث، WiFi و غیره به اشتراک بگذارند [۳۹] و [۴۰]. این ویژگی‌ها می‌توانند همچنین کاربردهای همه‌جاحاضری از اینترنت اشیاء از قبیل شبکه‌ی اجتماعی متحرک[1] (MSN) [۴۱]، شبکه‌ی ادهاک خودرویی[2] (VANET)، و شبکه‌ی تحمل‌پذیر تاخیر را ارائه دهند.

III. حملات SYBIL

حملات Sybil در اینترنت اشیاء برای دستکاری و به دست آوردن کنترل سیستم‌ها به صورت مخربی وجود دارند. در این بخش، ما سه نوع از حملات Sybil را تعریف می‌کنیم. در آغاز، مدل گراف اجتماعی را ارائه می‌دهیم. یک گراف اجتماعی بدون جهت را با نام G در نظر بگیرید که n گره‌ی درستکار H و در کل m یال دارد. گره‌های Sybil با نام S نشان داده می‌شوند. در گراف اجتماعی، ما از گره برای نمایش کاربر، هویت، یا

[1] Mobile Social Network (MSN)
[2] Vehicular Ad hoc Network (VANET)

حساب کاربری در شبکه‌ی واقعی استفاده می‌کنیم. یال بین هر زوج از گره‌ها توسط ارتباط‌های اجتماعی آنها وزن‌دهی می‌شود. همانطور که در شکل ۳ نشان داده شده است، یک یال مهاجم یعنی AG در واقع یالی است که یک گره‌ی درستکار و یک گره‌ی Sybil را به هم متصل می‌کند. توجه داشته باشید که در برخی از مقالات [۲۴] و [۲۵]، شبکه‌ی اجتماعی به گراف اجتماعی بدون جهت اشاره دارد.



شکل ۳. سه نوع از حملات Sybil: SA-1، SA-2، و SA-3.

A حملات Sybil SA-1

همانطور که در شکل ۳ نشان داده شده است، مهاجمان SA-1 معمولا اتصالاتی را در داخل جامعه‌ی Sybil ایجاد می‌کنند، به عنوان مثال گره‌های Sybil به صورت محکم به دیگر گره‌های Sybil متصل هستند. با این حال، توانایی SA-1 در ایجاد اتصالات اجتماعی با گره‌های درستکار، قوی نیست. به عبارت دیگر، تعداد اتصالات اجتماعی بین گره‌های Sybil و گره‌های درستکار، یعنی مانند آنچه در شکل ۳ دیده می‌شود، تعداد یال‌های حمله‌ی SA-1 محدود است.

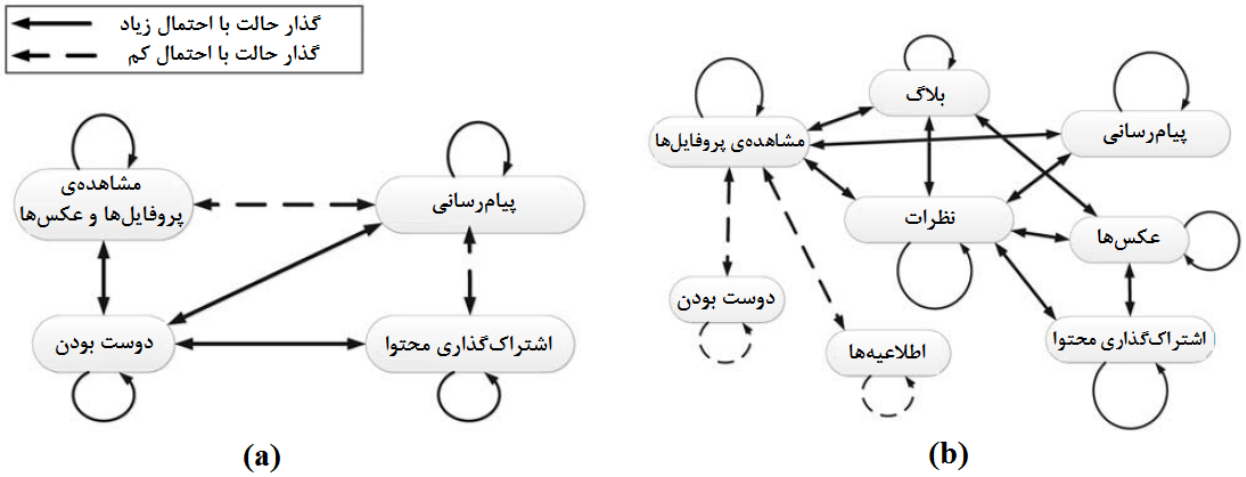
مهاجمان SA-1 معمولا در دامنه‌های حسی و اجتماعی وجود دارند، به عنوان مثال سیستم‌های OSN، سیستم‌های رأی‌گیری [۴۲]، یا سیستم‌های حسی متحرک [۴۳]. هدف اصلی این حمله، دستکاری گزینه‌های کلی یا محبوبیت است. به عنوان مثال، در یک سیستم رأی‌گیری آنلاین، SA-1 می‌تواند به طور قانونی حجم عظیمی از هویت‌های جعلی ایجاد کند تا مانند کاربران عادی عمل نموده و رأی‌هایی را برای گزینه‌های

مغرضانه‌ای ارسال نمایند. نتایج نهایی رأی‌گیری ممکن است توسط مهاجمان SA-1 دستکاری شده باشد، چرا که بخش قابل توجهی از آراء از جانب مهاجمان SA-1 صادر شده است. به طور مشابه، در سیستم حسی متحرک، SA-1 می‌تواند داده‌های حس شده‌ی نادرستی را به صورت جعلی ایجاد نموده و به طور غیرمستقیم تجمیع داده‌های جمع‌آوری شده را تغییر دهد. بنابراین، در برخی از موارد، تشخیص رفتارهای مهاجمان Sybil از رفتار کاربران عادی ممکن نیست.

B. حملات SA-2 Sybil

مهاجمان SA-2 معمولا در دامنه‌ی اجتماعی موجود است. برخلاف SA-1، حمله‌ی SA-2 نه تنها قادر به ایجاد اتصالات اجتماعی میان هویت‌های Sybil است، بلکه همچنین قادر به ایجاد اتصالات با کاربران عادی نیز می‌باشد. به عبارت دیگر، توانایی SA-2 برای تقلید ساختارهای اجتماعی کاربران عادی از دیدگاه گراف اجتماعی قوی است. بنابراین، تعداد یال‌های این حمله زیاد است.

هدف SA-2 به صورت انتشار هرزنامه، تبلیغات، و بدافزارها؛ سرقت و نقض حریم خصوصی کاربران؛ و دستکاری مخرب سیستم اعتباری است. برای مثال، در OSNها، SA-2 می‌تواند پروفایل‌ها و لیست دوستان را به عنوان یک کاربر عادی جعل کند، ولی از عمد به انتشار هرزنامه، تبلیغات، و بدافزار بپردازند. علاوه بر این، SA-2 می‌تواند مقدار زیادی از دیدگاه‌ها مثبت را در یک سیستم ارزیابی سرویس تولید کند تا در مورد مزایای سرویس مبالغه نماید، یا دیدگاه‌های منفی زیادی تولید کند تا به دست کم گرفته شدن سرویس‌ها منجر شود. بدیهی است که SA-2 بر روی برخی از رفتارهای خاص تمرکز نموده و آنها را با فرکانس بالایی تکرار می‌کند. در شکل ۴، رفتارهای SA-2 و کاربران عادی می‌توانند به عنوان یک زنجیره‌ی مارکوف مدل شوند.



شکل ۴. رفتارهای شبکه اجتماعی آنلاین و احتمالات گذار برای مهاجمان Sybil و کاربران عادی. (a) گذار حالات برای یک کاربر Sybil. (b) گذار حالات برای یک کاربر عادی.

C. حملات *SA-3 Sybil*

مهاجمان SA-3 Sybil در شبکه‌های متحرک (مانند دامنه‌ی متحرک) وجود دارند. هدف اصلی SA-3 مشابه حمله‌ی SA-2 است. با این حال، تاثیر SA-3 ممکن است در یک ناحیه‌ی محلی یا داخل یک دوره‌ی زمانی کوتاه باشد. با توجه به پویایی‌های شبکه‌های متحرک، کاربران متحرک نمی‌توانند اتصالات با دیگران را برای مدت زمان طولانی نگه دارند، یا اتصالات به صورت متناوب است. علاوه بر این، یک مقام مرکزی نمی‌تواند در شبکه‌های متحرک در تمام زمان‌ها وجود داشته باشد. بدین ترتیب، برخلاف آنچه در سیستم آنلاین وجود دارد، روابط اجتماعی، ساختار اجتماعی سراسری، توپولوژی، و الگوهای پیشینه‌ی رفتارها در شبکه‌های متحرک برای دفاع Sybil در برابر SA-3 به سادگی به دست نمی‌آید. قابلیت تحرک و فقدان اطلاعات سراسری به مشکلاتی در دفاع SA-3 در مقایسه با دفاع SA-1 و SA-2 منجر می‌شود. در جدول ۱، انواع حملات Sybil مختلف را مقایسه کرده‌ایم.

جدول ۱. حملات Sybil

دسته‌بندی حملات Sybil	ویژگی‌های گراف اجتماعی	هدف حمله	تفکیک رفتار	تحرک
SA-1	Sybilها در محدوده یا جامعه‌ی یکسانی وجود دارند، و تعداد یال‌های حمله محدود است	به صورت مخرب یا از روی عمد گزارش‌ها یا دیدگاه‌های مغرضانه‌ای را بارگذاری می‌کنند (مثبت یا منفی) تا انتخاب نهایی را دستکاری نموده و بر کل سیستم تسلط داشته باشند	مانند کاربران عادی عمل می‌کنند، و رفتارهای خاصی را بارها تکرار می‌نمایند.	×
SA-2	Sybilها ممکن است به شدت به کاربران عادی متصل باشند، و یال‌های حمله‌ی بیشتری را تولید کنند	انتشار هرزنامه و بدافزار جهت راه‌اندازی برخی دیگر از حملات، استتار به عنوان کاربران عادی، یا نقض حریم خصوصی دیگر کاربران	به عمد برخی از رفتارهای خاص را با فرکانس زیادی تکرار می‌کنند	×
SA-3	Sybilها ممکن است به شدت به کاربران عادی متصل باشند	دستکاری محبوبیت محلی، انتشار هرزنامه در محیط متحرک، یا نقض حریم خصوصی کاربران	رفتارهای خاصی را بارها تکرار می‌کنند	√

IV. تشخیص Sybil بر اساس گراف اجتماعی (SGSD)

ما در این بخش روش‌های SGSD را ارائه می‌دهیم. هدف SGSD این است که گره‌ی درستکار شناخته شده‌ی H را قادر سازد که توانایی برچسب زدن به هر گره‌ی S را به عنوان "Sybil" یا "درستکار" داشته باشد، یا با توجه به تشخیص جامعه آن را به عنوان SA-1 تشخیص دهد. در نتیجه، به طور اساسی دو نوع SGSD وجود دارد که به ترتیب، تشخیص Sybil بر اساس شبکه‌ی اجتماعی[1] (SNSD) و تشخیص بر اساس جامعه‌ی اجتماعی[2] (SCSD) هستند.

[1] Social Network-based Sybil Detection (SNSD)
[2] Social Community-based Detection (SCSD)

A. دفاع Sybil بر اساس شبکه‌ی اجتماعی

SNSD یک نوع دفاع در برابر Sybil بر اساس "شبکه‌ی اجتماعی" است، شبکه‌ی اجتماعی یک ساختار اجتماعی از روابط اجتماعی میان گره‌ها می‌باشد. نظریه جامعه‌شناسی [۴۵] یک ابزار مفید برای بررسی روابط اجتماعی میان کاربران است. در این بخش، اصطلاح "شبکه‌ی اجتماعی" در واقع گراف و ساختار اجتماعی کاربران را نشان می‌دهد، که می‌توانند روابط اجتماعی و اعتماد اجتماعی میان کاربران را منعکس نمایند [۴۶] و [۴۷]. با استفاده از ساختار شبکه‌ی اجتماعی، Yu و همکارانش در مرجع [۲۴] یک روش SNSD معروف به نام SybilGuard بر اساس گام تصادفی [۴۸] و [۴۹] ارائه کرده‌اند. پیش از توضیح SybilGuard با جزئیات دقیق، ما یک فرض را ارائه می‌کنیم.

فرض ۱: اگر چه گره‌های Sybil می‌توانند با دیگر گره‌های Sybil اتصال محکمی داشته باشند، ولی تعداد اتصالات اجتماعی میان گره‌های Sybil و گره‌های درستکار محدود می‌باشد.

SybilGuard بر فرض ۱ متکی است، و هر گره به صورت توزیع شده‌ای گره‌ی Sybil را تشخیص می‌دهد. به طور خاص، یک گره با درجه‌ی R به طور کلی R گام تصادفی تولید می‌کند که این مسیر از خود گره شروع شده و در امتداد یال خود با طول ثابت L ادامه دارد. اگر یک گام به یک گره‌ی درستکار شناخته شده برسد، آنگاه توسط این گره‌ی درستکار مورد تایید قرار می‌گیرد. به ویژه، اگر یکی از مسیرهای یک گره‌ی Sybil، S، به گره‌ی درستکار شناخته شده‌ی V برسد، آنگاه گره‌ی S ممکن است به عنوان یک گره‌ی تایید شده پذیرفته شود (به عنوان مثال، گامی از S به H معتبر نامیده می‌شود). سپس، با توجه به یک آستانه مانند T که $T \leq R$ است، S می‌تواند به عنوان یک گره‌ی درستکار پذیرفته شود، به شرطی که تعداد گام‌های مورد تایید قرار گرفته‌ی S بیشتر از T باشد. بر اساس فرض ۱، اگر T به درستی انتخاب شود، آنگاه تعداد محدودی از یال‌های حمله می‌توانند تعداد تاییدکننده‌هایی بیشتر از T ایجاد کنند. به عنوان مثال، اگر به طور کلی به تعداد X یال حمله وجود داشته باشد، آنگاه تعداد گروه‌های Sybil توسط X محدود می‌شوند. در مرجع [۵۰]، ثابت شده است که $T = \Theta(\sqrt{n}\log n)$ می‌تواند به طور قابل توجهی برای گره‌های درستکار بزرگ باشد، گره‌های درستکاری که گام تصادفی تشخیص از آنها عبور می‌کند. علاوه بر این، روش‌های امنیتی نیز برای تضمین احراز هویت گره‌ها و گام‌ها مورد استفاده قرار می‌گیرند. هر جفت از دو گره‌ای که به طور مستقیم متصل هستند (به

عنوان مثال، همسایگان یک-گامی) در مورد یک کلید مشترک بر روی یال توافق می‌کنند. کد احراز هویت پیام[1] (MAC) برای هر گره مورد استفاده قرار می‌گیرد تا گره‌ی دیگر را ارزیابی و تایید نماید. علاوه بر این، هر گام تصادفی تولید شده باید با یک توکن غیرقابل جعل (جدول شاهد) ثبت‌نام شود، توکنی که شامل تمام L گره‌ی موجود بر روی گام تصادفی است و بدین ترتیب مهاجمان نمی‌توانند اتصالات را انکار کرده و اطلاعات گام تصادفی را جعل نمایند.

صحت SybilGuard بر خاصیت ترکیب-سریع در گراف اجتماعی تکیه دارد. مدت زمان ترکیب t در یک گراف اجتماعی نشان می‌دهد که نقطه‌ی پایانی در یک الگوریتم تصادفی با چه سرعتی به توزیع ثابت دست می‌یابد. در اینجا، در یک گراف اجتماعی اگر نقطه‌ی پایانی توزیع، مستقل از نقطه‌ی شروع و به صورت $L \to \infty$ باشد، آنگاه توزیع ثابت است [۲۴]. اگر مدت زمان ترکیب برابر با $\Theta(\mathrm{t})$ باشد، آنگاه گراف به صورت ترکیب-سریع است. وقتی یک گام تصادفی با طول $L = \Theta(\sqrt{n}\log n)$ وجود داشته باشد، آنگاه به تعداد $\Theta(\sqrt{n})$ نمونه وجود دارند که مستقل از نقطه‌ی شروع هستند. احتمال اینکه یک گره‌ی Sybil توسط یک گره‌ی درستکار شناخته شده پذیرفته شود [به عنوان مثال، هم گره‌ی Sybil و هم گره‌ی درستکار، یال یکسانی (مانند، یال حمله) را در گام تصادفی انتخاب کنند] در روش Birthday Paradox (پارادوکس روز تولد) دنبال می‌شود [۵۱]. این احتمال برخورد برابر است با

$$\text{احتمال (برخورد)} = 1\text{-}(1 - \frac{1}{\sqrt{m}})^{\sqrt{m}} \qquad (۱)$$

بنابراین، SybilGuard احتمال زیادی برای تشخیص حمله‌ی نوع SA-1 با توجه به گام تصادفی دارد.

به منظور ارتقاء SybilGuard، Yu و همکارانش [۲۵] روش دفاع دیگری را به نام SybilLimit ارائه کرده‌اند که دفاع نزدیک به بهینه‌ای را تضمین می‌کند. در SybilLimit، هر گره به تولید گام‌های تصادفی $R = \Theta\sqrt{m}$ با طول $L = \Theta(\log n)$ می‌پردازد. با استفاده از الگوریتم گام تصادفی [۵۲]، گره‌های Sybil یا درستکار می‌توانند مشخص شوند، که از این نظر مشابه روش SybilGuard است. برخلاف SybilGuard، روش SybilLimit از تقاطع‌های بین یال‌ها به جای رئوس (گره‌ها) بهره می‌برد، و مسیردهی‌های کوتاه تصادفی با چندین گام تصادفی مستقل انجام می‌دهد. SybilLimit به تعداد $O(\log n)$ از گره‌های Sybil را در هر یال

[1] Message Authentication Code (MAC)

حمله می‌پذیرد، در حالی که در SybilGuard این تعداد برابر با $O(\sqrt{n}\log n)$ است [۲۵] و [۵۳]. هر دوی SybilGuard و SybilLimit بر اساس فرض ۱ هستند.

برای درک ویژگی‌های ساختارهای اجتماعی، Alvisi و همکارانش [۵۴] به بررسی ویژگی‌های ساختاری گراف‌های اجتماعی از جمله توزیع محبوبیت [۵۵]، ویژگی جهان کوچک [۴۵]، ضریب خوشه‌بندی [۵۶]، و هدایت [۵۷] پرداخته‌اند، و مشاهده کرده‌اند ویژگی "هدایت" که به مدت زمان ترکیب گام تصادفی مربوط است، در مقایسه با دیگر ویژگی‌ها در دفاع در برابر Sybil انعطاف‌پذیرتر است. توجه داشته باشید که توزیع محبوبیت میان گره‌ها از یک توزیع قاعده-توان یا لگاریتم-طبیعی پیروی می‌کند. ویژگی جهان کوچک نشان می‌دهد که فاصله‌ی بین هر دو گره تا چه حد کوچک است. ضریب خوشه‌بندی در واقع پارامتری است که نزدیکی گره‌ها را در یک شبکه‌ی اجتماعی منعکس می‌کند. هدایت $C(S)$ مدت زمان ترکیب را نشان می‌دهد، که در واقع حداقل طول یک گام تصادفی است. $C(S) = \frac{S_{out}}{S_{in}}$، که S_{out} نشان‌دهنده‌ی تعداد یال‌هایی است که بیرون S قرار دارند و S_{in} تعداد یال‌های داخل S است. اگر مقدار هدایت کم باشد، آنگاه مدت زمان ترکیب بالا خواهد بود. در مرجع [۵۴]، ثابت شده است که برای سه ویژگی اول، تعداد یال‌هایی که مهاجمان Sybil نیاز دارند تا یک حمله‌ی Sybil را راه‌اندازی کنند برابر با صفر یا یک است، در حالی که این تعداد برای ویژگی هدایت برابر با $\frac{C(S)m}{\log(C(S))}$ است. مهاجمان Sybil مجبور هستند که منابع بیشتری را برای رقابت با روش‌های تشخیص Sybil مبتنی بر هدایت مصرف کنند. بنابراین، تاثیر SybilLimit در مرجع [۲۵] مورد ارزیابی و تایید قرار گرفته است، که از ویژگی هدایت برای تشخیص گره‌های Sybil بهره می‌برد. علاوه بر این، یک مفهوم از حمله‌ی کامل برای تشریح یک حمله‌ی غیرقابل‌کشف معرفی شده است که برخی از گره‌های درستکار را در شبکه‌ی اجتماعی به داخل منطقه‌ی Sybil می‌کشد، بدون اینکه تاثیری بر کل شبکه اجتماعی داشته باشد. به عبارت دیگر، وقتی که یک گره‌ی Sybil به شبکه‌ی اجتماعی می‌پیوندد و اتصالات زیادی را با گره‌های درستکار ایجاد می‌کند، تشخیص چنین مهاجمی ساده نیست. یال حمله معیاری است که توانایی مهاجم را برای راه‌اندازی یک حمله‌ی کامل ارزیابی می‌کند. برای مقاومت حملات قوی Sybil، در مرجع [۵۴]، یک روش دفاعی SoK برای بررسی هدایت جهت توانمندسازی کاربران در ایجاد یک لیست سفید ارائه شده است که این لیست مجموعه‌ای از گره‌های رتبه‌بندی شده را به همراه مقدار اعتماد آنها نگه‌داری می‌کند. SoK در مقایسه با دیگر روش‌های SNSD از قبیل SybilGuard و SybilLimit، مقاومتر است.

به تازگی، تلاش‌های پژوهشی زیادی در زمینه‌ی SNSD صورت گرفته است. Cao و همکارانش [۵۸] روش SybilRank را برای کمک به سرورها یا اپراتورهای OSN متمرکز جهت تشخیص حملات Sybil ارائه کرده‌اند که از رتبه‌بندی گره‌ها با توجه به احتمال حسی از Sybil بودن این گره‌ها استفاده می‌کند. هدف SybilRank در واقع کاهش سربار محاسباتی و دستیابی به مقیاس‌پذیری در تشخیص Sybil در یک OSN با مقیاس بزرگ است. Danezis و Mittal [۵۹] به بررسی یک مدل احتمالی از گره‌های درستکار در شبکه‌ی اجتماعی پرداخته و یک رویکرد استنتاج بیزین را برای تقسیم کل گراف شبکه به دو منطقه‌ی درستکار و Sybil ارائه کرده‌اند. روش دیگری از دفاع در برابر Sybil [۶۰] از اصول امتیاز تضعیف [۶۱] برای SNSD استفاده می‌کند تا از مهاجمان مخرب Sybil با اضافه یا حذف یال‌ها در گراف اجتماعی جلوگیری کند، بدون اینکه از مهندسی اجتماعی، به ویژه برای حمله‌ی تبانی استفاده کند. برای ارتقاء بیشتر SybilLimit، Tran و همکارانش [۶۲] یک روش دفاع در برابر Sybil را به نام GateKeeper ارائه کرده‌اند، تا به بهینه‌سازی برای یال‌های حمله به صورت $O(1)$ دست یافته و تنها هویت‌های Sybil به صورت $O(1)$ را تضمین کنند. یک الگوریتم توزیع بلیط با چندین منبع نیز برای کمک به GateKeeper جهت کنترل پذیرش گره‌ها ارائه شده است.

یک گرایش جدید برای SNSD این است که میزان اعتماد برای ایجاد گراف اجتماعی و تشخیص حمله‌ی SA-1 بررسی شود. SybilFence [۶۳] از بازخوردهای منفی کاربران بر روی مهاجمان Sybil بهره گرفته و به یال‌ها در گراف اجتماعی، یک وزن اختصاص می‌دهد. برای مثال، اگر یک کاربر u_i نظرات و دیدگاه‌های منفی از دیگران دریافت کند، آنگاه وزن یال‌های u_i به نسبت کاهش خواهند یافت. در گراف‌های اجتماعی جهت‌دار، حمله‌ی SA-1 می‌توانند بهتر تشخیص داده شوند. SumUp، یک روش SNSD برای مسئله‌ی تجمیع آراء در یک سیستم امتیازدهی محتوای آنلاین است، همچنین به یک شبکه‌ی اعتباری [۴۶] و [۶۴] میان گره‌ها متکی است. SupUp در صورت رفتارهای نادرست پی در پی مهاجم، از تاریخچه‌ی رأی‌دهی کاربر به منظور محدود کردن قابلیت رأی‌دهی مهاجم استفاده می‌کند. در SumUp، یک گره‌ی مورد اعتماد به محاسبه‌ی مجموعه‌ای از مسیرهای حداکثر جریان بر روی گراف مورد اعتماد می‌پردازد و سپس آراء را جمع می‌کند. این روش اجازه می‌دهد تا آراء از کاربران مورد اعتماد به طور موثری جمع شوند، در حالی که رأی‌های کاربران غیرقابل اعتماد را محدود می‌کند. Canal [۶۵] نیز مشابه SumUp است. با یک روش پرداخت اعتباری در یک شبکه با مقیاس بزرگ، Canal ایجاد گراف اجتماعی را ارتقا داده و با SNSD موجود سازگار است.

Delaviz و همکارانش [۶۶] یک روش دفاع در برابر Sybil مبتنی بر اعتبار به نام SybilRes را ارائه کرده‌اند، که از یک گراف جهت‌دار وزن‌دار محلی درونی برای نشان دادن فعالیت‌های انتقال داده‌های کاربر استفاده می‌کند. هنگامی که یک کاربر u_i، داده‌های خود را آپلود می‌کند، آنگاه وزن یال بر روی مسیر از u_i تا دانلودکننده کاهش می‌یابد. برای حفظ وزن یال کاربران درستکار، دانلودکننده پس از دانلود کردن، به افزایش وزن یال‌های خود بر روی مسیرهایی می‌پردازد که از آپلودکننده‌ی u_i تا خودش امتداد یافته‌اند. سپس، کاربران Sybil می‌توانند با استفاده از SNSD پیچیده‌ای تشخیص داده شوند. Mohaisen و همکارانش [۶۷] همچنین به بررسی اعتماد جهت تشکیل گراف اجتماعی پرداخته‌اند. آنها مشاهده کرده‌اند که گره‌ها بیشتر از دیگر به خودشان اعتماد دارند، و اعتماد به دیگر گره‌ها به صورت واحد و یکنواختی برابر نیست. سپس، آنها از اعتماد تفاضلی در گراف اجتماعی استفاده کرده‌اند تا یال‌های ضعیف اعتماد را فیلتر کرده و اعتماد را توسط مسیرهای تصادفی مغرضانه و بایاس شده مدل کنند. بر خلاف SNSD پایه [۲۴] و [۲۵]، این روش‌های SNSD مبتنی بر اعتماد [۶۶] و [۶۷] بیشتر از اعتماد برای ایجاد یک گراف اجتماعی جهت‌دار استفاده می‌کند، به جای اینکه از گراف اجتماعی بدون جهت اصلی برای تشخیص Sybil گام تصادفی بهره گیرند. از آنجایی که این ارتقا بر یک فرض عملی متکی است که در آن، گره‌های درستکار اعتماد بالایی را به گره‌های ناشناخته (یا Sybil) ندارند، از این رو یال‌های حمله می‌توانند برای تضمین دقت SNSD فیلتر شوند. به طور خلاصه، اعتماد یا اعتبار می‌تواند ایجاد گراف اجتماعی را ارتقا داده و مهاجمان Sybil را جهت ایجاد اتصالات با کاربران عادی محدود کند و بدین ترتیب دقت تشخیص می‌تواند بهبود یابد.

B. تشخیص Sybil بر اساس جامعه‌ی اجتماعی

SCSD به بررسی تشخیص جامعه اجتماعی برای کمک به تشخیص Sybil می‌پردازد. امکان استفاده از الگوریتم‌های تشخیص جامعه اجتماعی برای تشخیص SA-1 در مرجع [۶۸] تایید شده است. در مرجع [۶۸]، Viswanath و همکارانش در ابتدا به تحلیل روش‌های SNSD پرداخته و آنها را به یک مسئله‌ی رتبه‌بندی خلاصه نموده‌اند. از آنجا که روش‌های SNSD معمولا گره‌های Sybil و گره‌های درستکار را به دو بخش یعنی منطقه‌ی Sybil و منطقه‌ی درستکار تقسیم می‌کنند، این تقسیم‌بندی به عنوان یک مسئله‌ی بخش‌بندی گراف در نظر گرفته خواهد شد. برای این روش‌های SNSD، هر گره‌ی ناشناخته مطابق اتصالات اجتماعی خود با

گره‌های مورد اعتماد شناخته شده رتبه‌بندی می‌شود. سپس، پارامترهای مختلفی (مانند آستانه‌ها) برای تقسیم گراف اجتماعی به دو بخش انتخاب می‌شوند. این پارامترها برای تعیین مرزهای هر بخش یا نقطه‌ی "قطع" مورد استفاده قرار می‌گیرند. رتبه‌بندی گره‌ها در راستای کاهش قدرت هدایت می‌باشد. به عبارت دیگر، گره‌هایی که محکم به گره‌های مورد اعتماد شناخته شده متصل شده‌اند (به عنوان مثال، هدایت کمتر) آنگاه امتیاز بیشتری در رتبه‌بندی دریافت خواهند نمود. علاوه بر این، الگوریتم‌های رتبه‌بندی به طور قابل توجهی در نتایج رتبه‌بندی و بخش‌بندی Sybil تاثیر می‌گذارند. در عین حال، مسئله‌ی دیگری که در اینجا مطرح می‌شود: اگر یک گره اتصال ضعیفی با گره‌های مورد اعتماد شناخته شده‌ی فعلی داشته باشد، آنگاه به احتمال زیاد به عنوان یک گره‌ی Sybil تشخیص داده خواهد و مهم نیست که چقدر به دیگر گره‌های مورد اعتماد شناخته شده به صورت محکم متصل باشد. به عبارت دیگر، وقتی که چندین جامعه‌ی اجتماعی در گراف وجود داشته باشد، آنگاه تشخیص گره‌های Sybil تنها از طریق بخش‌بندی شبکه اجتماعی، ناکارآمد و غیرموثر خواهد بود. بنابراین، استفاده از تشخیص جامعه برای تشخیص گره‌های Sybil به صورت یک وعده‌ی امیدوارکننده تبدیل شده و می‌تواند دقت تشخیص Sybil را ارتقا دهد.

SybilDefender [۶۹] یک روش معمولی SCSD است، که بر انجام تعداد محدودی از مسیرهای تصادفی برای شناسایی Sybil و تشخیص جامعه تکیه دارد. شناسایی Sybil مشابه دیگر روش‌های موجود SNSD، می‌تواند تشخیص دهد که آیا یک گره Sybil است یا خیر. پس از شناسایی Sybil، یک الگوریتم تشخیص جامعه نیز مورد استفاده قرار می‌گیرد تا دیگر گره‌های Sybil را شناسایی کند که در مجاورت و همسایگی گره‌ی Sybil تشخیص داده شده قرار دارند. علاوه بر یک ترکیب موثر و کارآمد از شناسایی Sybil و تشخیص جامعه که در روش SybilDefender ارائه شده است، SybilDefender همچنین به کاهش بیشتر سربار محاسباتی نیز کمک می‌کند. علاوه براین، با توجه به این امر که بخشی از روابط OSN میان کاربران، غیرقابل اعتماد است [۵۵]، SybilDefender همچنین شامل روشی برای محدود کردن تعداد یال‌های حمله است. این روش محدودکننده‌ی یال حمله در واقع کاربران را قادر می‌سازد تا به روابط خود با دوستان خود، رتبه‌هایی به عنوان "دوست" یا "غریبه" بدهند. از آنجایی که مهاجمان Sybil احتمالا از دید کاربران عادی به عنوان "غریبه" در نظر گرفته می‌شوند، به همین دلیل یال‌های حمله‌ی زیادی حذف شوند. توجه داشته باشید که SybilSheild بر فرض ۱ متکی است.

Cai و Jermaine [۷۰] از مدل جامعه‌ی پنهان و یادگیری ماشین برای تشخیص حملات Sybil استفاده می‌کنند، و جوامعی را که به صورت محکم به هم متصل شده‌اند را قادر می‌سازند تا بیشتر از جوامعی که به صورت ضعیف به هم متصل شده‌اند، به هم نزدیکتر شوند. حتی اگر برخی از جوامع خاص توسط مهاجمان Sybil در معرض خطر قرار بگیرد، باز هم همچنان جوامع حمله می‌توانند از طریق گذار حالات در مدل جامعه‌ی پنهان تشخیص داده شوند. با استفاده از ساختار شبکه اجتماعی با چندین جامعه، Shi و همکارانش [۷۱] روش SybilShield را ارائه کرده‌اند، که یک روش SCSD با کمک عامل است. SybilShield همچنین از روابط اعتماد میان کاربران برای تشکیل گراف اجتماعی استفاده می‌کند. با این حال، با توجه به این حقیقت که دو گره‌ی درستکار که به دو جامعه‌ی متفاوت اجتماعی تعلق دارند، ممکن است به صورت محکم به یکدیگر متصل نباشند، SybilShield به بررسی عوامل پرداخته و اطمینان حاصل می‌کند که گره‌های درستکار به صورت محکم به دیگر گره‌های درستکار متصل هستند. در مرجع [۷۱]، اولین گام تصادفی مانند SybilGuard در نظر گرفته شده است. سپس، برخی از عوامل از یک بررسی‌کننده انتخاب می‌شوند تا دور دوم گام تصادفی را اجرا کنند که عامل گام نامیده می‌شود، این عوامل تمام یال‌های بررسی‌کننده را می‌پیمایند تا گره‌های مظنون را شناسایی کنند. SybilShield بر فرض ۲ متکی است.

فرض ۲: گره‌های Sybil نمی‌توانند به صورت محکم با گره‌های درستکار در چندین جامعه‌ی درستکار متصل باشند، چرا که گره‌های درستکار به گره‌های Sybil اعتماد نخواهند داشت. گره‌های درستکار می‌توانند به صورت محکم به دیگران در جامعه‌ی درستکار اتصال داخلی داشته باشند.

با یک گراف دعوتنامه‌ی دوستی که با توجه به تعاملات دوستی کاربر ایجاد شده است (دعوت یا پذیرفتن دوستان)، VoteTrust [۷۲]، یک روش جدید SCSD است که از یک تخصیص رأی بر اساس اعتماد استفاده می‌کند، و رأی کلی را جمع‌آوری می‌نماید تا احتمال یک مهاجم Sybil را تخمین بزند. VoteTrust به ترکیب ساختار گراف اجتماعی و بازخورد کاربر (پذیرفتن یا رد درخواست دوستی) برای ایجاد یک گراف جهت‌دار می‌پردازد. این روش بر پایه‌ی یک فرض است که در آن کاربران Sybil نمی‌توانند بیشتر از تعداد معینی درخواست دوستی را از کاربران عادی دریافت کنند. تجمیع کلی آراء برای هر گره می‌تواند جهت تخمین رتبه‌ی سراسری این گره مورد استفاده قرار گیرد. با این روش دو طرفه (رأی‌گیری و بازخورد) (مانند آنچه در گراف جهت‌دار موجود است)، تشخیص Sybil در مقایسه با دیگر روش‌های موثرتر و کارآمدتر خواهد بود.

در جدول ۲، ما به مقایسه‌ی روش‌های SGSD با توجه به اصول مقدماتی، فرضیات، ویژگی‌های غیرمتمرکز و غیره پرداخته‌ایم. یک گرایش این است که به بررسی اعتماد برای کمک به تشخیص Sybil در حمله‌ی نوع SA-1 بپردازیم.

جدول ۲. مقایسه‌ی روش‌های تشخیص Sybil بر اساس گراف اجتماعی

روش دفاع در برابر Sybil	اصول مقدماتی	گراف اجتماعی	غیرمتمرکز	اعتماد
SybilGuard و SybilLimit	گام تصادفی	بدون جهت	√	×
SumUp	حداکثر جریان تطبیقی	بدون جهت	×	شبکه‌ی اعتباری
GateKeeper	گام تصادفی	بدون جهت	√	اعتماد
SybilDefender	تشخیص جامعه	جهت‌دار	×	اعتماد
SybilSheild	تشخیص جامعه	بدون جهت	√	اعتماد
VoteTrust	تشخیص جامعه	جهت‌دار	√	اعتماد نامتقارن

V. تشخیص Sybil بر اساس طبقه‌بندی رفتار

در این بخش، ما روش BCSD را ارائه می‌دهیم. با توجه به مطالعات اخیر [۲۶] و [۴۴]، کاربران Sybil در RenRen، که یک OSN محبوب در کشور چین است، می‌توانند اتصالاتی به تعداد نمایی با کاربران عادی (یا کاربران درستکار) ایجاد کنند. در مرجع [۷۳] نشان داده شده است که کاربران Sybil به ندرت به ایجاد اتصالات اجتماعی با دیگر کاربران Sybil در RenRen می‌پردازند. بنابرانی، به تنهایی با تکیه بر روش‌های SGSD نمی‌توان حملات Sybil را به طور موثر شناسایی نمود، چرا که ممکن است فرضیات ۱ و ۲ همیشه برقرار نباشند. بنابراین، برخی از روش‌های جدید تشخیص Sybil موردنیاز هستند و باید برخی از ویژگی‌های امیدوارکننده‌ای از حملات Sybil مورد بررسی قرار گرفته و استخراج شوند.

به تازگی، Wang و همکارانش [۴۴] به بررسی صفحات مرورگر و عادات کلیک کاربران OSN پرداخته و کاربران Sybil را از روی رفتارهای غیرعادی آنها در مقایسه با کاربران عادی تفکیک می‌کنند. با توجه به داده‌های به دست آمده از RenRen، فعالیت‌های اصلی کاربران OSN به صورت زیر انتخاب می‌شوند.

۱) *دوست بودن*: ارسال، پذیرفتن، یا رد درخواست‌های دوستی.

۲) عکس: آپلود کردن عکس‌ها، تگ کردن دوستان در تصاویر، مشاهده‌ی تصاویر، و نوشتن نظرات و دیدگاه‌ها برای تصاویر.

۳) *پروفایل*: مشاهده‌ی پروفایل دیگر کاربران.

۴) *اشتراک‌گذاری*: اشتراک‌گذاری محتواهای چندرسانه‌ای از جمله ویدئو، عکس، صوت، محتواها، و لینک‌های وبسایت‌ها.

۵) *پیام‌رسانی*: به‌روزرسانی وضعیت، نوشتارهای دیوار، ارسال یا دریافت پیام‌های متنی.

۶) *بلاگ*: نوشتن بلاگ‌ها، مشاهده‌ی بلاگ‌ها، و نگارش نظرات برای بلاگ‌ها.

با توجه به آمارها، فعالیت‌های اصلی کاربران Sybil به صورت دوست شدن (به ویژه، ارسال درخواست‌های دوستی)، مشاهده‌ی تصاویر و پروفایل دیگران، و اشتراک‌گذاری محتوا با دیگران است. در مقابل، کاربران عادی بخش بزرگی از مدت زمانی را که آنلاین هستند، به مشاهده‌ی پروفایل و انجام فعالیت‌های دیگر از قبیل مشاهده‌ی پروفایل‌ها، ارسال پیام‌ها، اشتراک‌گذاری محتوا با یک فرکانس مشابه صرف می‌کنند. هر دو مورد کاربران عادی و Sybil، اشتراک‌گذاری محتوا یا ارسال پیام‌ها را با فرکانس‌های مشابهی انجام می‌دهند. توجه داشته باشید که اشتراک‌گذاری محتوا یا ارسال پیام‌ها، رویکردهای رایجی برای Sybilها جهت انتشار هرزنامه در OSNها هستند. این مشاهدات نشان می‌دهد که روش‌های رایج تشخیص هرزنامه نمی‌توانند به سادگی از آستانه‌های عددی برای مقاومت در برابر هرزنامه استفاده کنند.

از شکل ۴، گذار حالات کلیک می‌تواند توسط زنجیره‌ی مارکوف با هر حالت به عنوان یک الگوی کلیک مدل شوند. کاربران عادی معمولا رفتارهای OSN متنوعی انجام می‌دهند، و گذار میان حالات واقعا پیچیده است. در مقابل، کاربران Sybil درگیر برخی از فعالیت‌های خاص با یک فرکانس بالا هستند. جهت تشخیص SA-2، ماشین بردار پشتیبان (SVM) [۷۴] و [۷۵] می‌تواند با توجه به ویژگی‌های نشست از قبیل متوسط کلیک هر شخص، متوسط طول هر نشست، متوسط مدت زمان بین هر دو کلیک متوالی، و متوسط تعداد نشست‌های هر روز، و ویژگی‌های کلیک استفاده شود. نتایج اولیه نشان می‌دهد که دقت تشخیص Sybil، بالا است. در مرجع [۴۴]، سه مدل (مدل توالی کلیک، مدل مبتنی بر زمان، مدل ترکیبی)، که می‌تواند الگوهای مشابه کلیک را خوشه‌بندی کند، و برای طبقه‌بندی رفتار استفاده شود. گراف شباهت توالی می‌تواند با توجه به معیارهای خاص شباهت ایجاد شود. از طریق خوشه‌بندی گراف، کاربران Sybil می‌توانند تشخیص داده شوند.

روش مبتنی بر SVM یک ابزار یادگیری نظارت شده است، که نیاز به مدت زمان یادگیری طولانی دارد. برای رسیدگی به این مسئله، یک روش یادگیری بدون نظارت ارائه شده است، که تنها بخش کوچکی از الگوهای کلیک کاربران عادی مورد نظر را به عنوان "دانه‌ها" در نظر می‌گیرد. آنها خوشه‌های عادی را که شامل یک دانه‌ی توالی هستند را رنگ می‌کنند؛ در غیر این صورت، خوشه‌های بدون رنگ را خوشه‌های Sybil در نظر می‌گیرد.

مهاجمان قوی Sybil به گراف اجتماعی نفوذ کرده و اتصالات اجتماعی زیادی را با کاربران عادی تولید می‌کنند، که مخالف فرض SGSD است. اگر مهاجمان Sybil به الگوهای کلیک یا عادات کاربران عادی آشنا باشند، به عنوان مثال، مهاجمان Sybil می‌توانند رفتار کاربران عادی را واقعا تقلید کنند، آنگاه BCSD را به طور موثری به خوبی تشخیص دهند. با این حال، واضح است که مهاجمان Sybil بخش بزرگی از زمان خود را برای تقلید رفتار کاربران عادی صرف می‌کنند که همین امر می‌تواند رفتارهای حمله را تا حدی محدود کند.

VI. دفاع Sybil متحرک[1] (MSD)

در این بخش، ما روش‌های دفاع Sybil در شبکه‌های متحرک را ارائه می‌دهیم. بدون استفاده از گراف اجتماعی سراسری برای تشخیص Sybil، دفاع Sybil متحرک (MSD) در نظر دارد تا هم SA-3 را تشخیص دهد و هم رفتارهای مهاجمان Sybil را محدود کند.

A تشخیص Sybil بر اساس ارتباط دوستی[2] (FRSD)

در یک شبکه‌ی متحرک، با توجه به تحرک و فقدان اطلاعات گراف اجتماعی سراسری، دفاع در برابر Sybil کاملا متفاوت و در مقایسه با شبکه‌های آنلاین، دشوار است. Quercia و Hailes [۲۷] یک روش MSD را ارائه کرده‌اند تا جوامع کاربران متحرک را مطابقت نموده و کاربرانی از جامعه‌ی Sybil را به عنوان مهاجمان Sybil برچسب‌گذاری کنند. در مرجع [۲۷]، یک فرضیه این است که هر کاربر متحرک دو لیست نگه‌داری می‌کند: لیست دوستان که شامل کاربران متحرک مورد اعتماد است، و لیست دشمنان که شامل کاربران غیر قابل اطمینان است. وقتی دو کاربر وارد شبکه می‌شوند، آنها با جوامع خود تطبیق داده می‌شوند. اگر یک کاربر در

[1] Mobile Sybil Defense (MSD)
[2] Friend Relationship-based Sybil Detection (FRSD)

جوامع مورد اعتماد قرار ندارد، آنگاه این کاربر به عنوان یک کاربر Sybil در نظر گرفته می‌شود. همچنین در مرجع [۷۸]، Chang و همکارانش یک روش دفاع در برابر Sybil را برای MSNها ارائه کرده‌اند، که این روش فرض می‌کند کاربران Sybil و کاربران عادی در جوامع مختلفی قرار دارند، و بر تطبیق جوامع برای تشخیص کاربران Sybil تکیه دارد. بنابراین، استفاده از روابط دوستی میان کاربران، یک راه‌حل موثر برای تشخیص مهاجمان Sybil است. با این حال، این نوع از روش‌های FR-MSD نیاز دارند که کاربران متحرک، اطلاعات پیشرفته‌ای از جوامع مورد اعتماد را نگه‌داری کنند.

B. تشخیص Sybil متحرک بر اساس رمزنگاری

رمزنگاری ابزار مفید دیگری برای دفاع در برابر Sybil به ویژه برای MSD است، و می‌تواند رفتارهای مخرب مهاجم Sybil را محدود کند. در این بخش، ما به ارائه‌ی برخی از روش‌های MSD مبتنی بر رمزنگاری (crypto-MSD) می‌پردازیم که بر اساس روش‌های رمزنگاری بوده و برای دفاع در برابر SA-3 می‌باشند.

VANET نوعی از اینترنت خودروها است، که به وسیله‌ی تحرک بسیار بالا مشخص می‌شوند. وقتی که حملات Sybil در VANET راه‌اندازی می‌شوند، آنگاه تحرک بسیار بالا در واقع یک چالش اضافی برای تشخیص SA-3 است که به طور فزاینده‌ای انتساب یک مکان را به یک مهاجم بسیار دشوار می‌سازد. برای رسیدگی به مسائل حمله‌ی Sybil در VANETها، Lin در مرجع [۲۲] یک روش LSR را برای مقاومت در برابر حملات Sybil ارائه می‌کند و آسیب‌پذیری‌های کمتر شناخته شده‌ی Sybil را کاهش داده و حریم خصوصی را حفظ می‌کند. کاربران محلی خودروها پیش از اینکه مهاجمان Sybil توسط یک مرجع مورد اعتماد (TA) بیرون انداخته شوند، خود کاربران قادر به تشخیص مهاجمان Sybil به صورت موثر و کارآمدی نیستند. برای این منظور، هر کاربر u_i باید هر رویدادی را که ارسال می‌کند، امضا نماید. با استفاده از امضای گروهی [۷۹]، اگر یک کاربر، رویداد یکسانی را برای چندین بار (به عنوان مثال، بیش از یک بار) امضا کند، آنگاه این امضاها ممکن است نامعتبر باشد. سپس، کاربر می‌تواند به سادگی به دیگر کاربران بپیوندد و به عنوان مهاجمان Sybil تشخیص داده شود. در مرجع [۲۲]، تاخیر گزارش Sybil مورد تحلیل قرار گرفته است، در حالی که گزارش‌های دو لایه‌ای و چند لایه‌ای برای ردیابی هویت واقعی مهاجمان Sybil معرفی شده و برای ابطال به سمت مرجع مورد اعتماد هدایت شود. از آنجایی که روش‌های نام مستعار به طور گسترده‌ای در شبکه‌های بی‌سیم و متحرک

استفاده می‌شوند، دو طرف از اسم مستعار وجود دارند: از یک طرف، نام مستعار می‌تواند برای حفاظت از هویت واقعی کاربران قانونی استفاده شود؛ از طرف دیگر، استفاده از هویت‌های مستعار ممکن است مانع تشخیص Sybil شود، چرا که ردیابی هویت‌های Sybil از نام‌های مستعار بسیار دشوار خواهد بود. به طور مشابه، در مراجع [۸۰] و [۸۱]، یک کاربر مخربی که تظاهر به هویت چندین خودروی دیگر می‌کند، می‌تواند به صورت توزیع شده‌ای از طریق استراق سمع توسط مجموعه‌ای از گره‌های ثابت شناسایی شود که این گره‌ها، جعبه‌های کنار جاده نامیده می‌شوند. تشخیص حملات Sybil به این صورت، نیازی ندارد که هیچ خودرویی هویت واقعی خود را افشا کند؛ از این رو، حریم خصوصی می‌تواند در تمام مواقع محافظت شود. Triki و همکارانش [۸۲] به بررسی برچسب‌های نهفته‌ی RFID بر روی خودروها پرداخته‌اند و طول عمر گواهینامه‌ها را از واحدهای کنار جاده‌ای (RSUها) کوتاهتر نموده‌اند تا به احراز هویت کاربران بپردازند. برخی از ناظران (مانند، RSUها یا خودروها) در امر نظارت رویدادهای حساس درگیر هستند تا تشخیص منفی کاذب را کاهش دهند. علاوه بر این، برای دستیابی به قابلیت غیرقابل پیوند بودن و حفاظت از حریم خصوصی، خودروها در هر بار که منطقه‌ی ارتباطی خود را به منطقه‌ی RSU دیگر تغییر می‌دهند، آنگاه هویت‌های خود را نیز تغییر می‌دهند.

C. تشخیص Sybil متحرک بر اساس ویژگی

برخی از ویژگی‌های خاص، از قبیل مشخصات کانال [۸۳] و [۸۴] و ویژگی‌های مربوط به تحرک، در شبکه‌های متحرک، می‌توانند برای طبقه‌بندی مهاجمان Sybil و کاربران عادی مورد بررسی قرار بگیرند. به عنوان مثال، در شبکه‌ی بی‌سیم معمولی، ویژگی‌های کانال به طور موثری برای تشخیص مهاجمان Sybil مورد مطالعه قرار گرفته‌اند [۸۵]. یک احراز هویت لایه‌ی فیزیکی ارتقا یافته استفاده شده است، در حالی که تنوع فضایی کانال‌های رادیویی در داخل ساختمان رایج است، و محیط‌های شهری نیز با پراکندگی زیاد مورد بهره‌برداری قرار گرفته است. ترکیب احراز هویت و ویژگی‌های کانال، مهاجمان Sybil را تشخیص می‌دهند. در عمل، با توجه به سربار روش‌های پیچیده‌ی تخمین کانال، روش پیشنهادی همچنین چه به صورت مستقل و چه به همراه دیگر روش‌های امنیتی لایه‌ی فیزیکی، مانند تشخیص حمله‌ی جعل[1] نیز امکانپذیر و عملی است. علاوه بر این، قدرت سیگنال دریافتی (RSS) نیز برای تشخیص مهاجمان Sybil در یک شبکه‌ی بی‌سیم ایستا، از قبیل شبکه‌های

[1] spoofing

حسگر بی‌سیم مورد استفاده قرار گرفته است [۸۶] و [۸۷]. اگر یک گره همیشه بسته‌هایی را با یک RSS مشابه دریافت کند، آنگاه فرستنده احتمالا یک مهاجم Sybil است. برخی از دیگر روش‌های MSD از ویژگی‌های شبکه‌ی متحرک برای دفاع در برابر حملات Sybil استفاده می‌کنند. Geutte و ducourthial [۸۸] مقدار گره‌های فریب خورده را تخمین می‌زنند تا میزان موفقیت حملات Sybil را اندازه‌گیری کنند. آنها همچنین به تخمین تاثیر تنظیم توان انتقال از فرستنده‌ها می‌پردازند، در حالی که تاثیر آنتن‌های دو طرفه را نسبت به آنتن‌های چند جهته برای گیرنده تحلیل می‌کنند. با بررسی تفاوت سیگنال انتقال، آنها می‌توانند تاثیر تفاوت فرضیات مختلف امنیتی را بر روی مهاجمان Sybil و تاثیر آنتن‌ها را بر روی دقت تشخیص Sybil اندازه‌گیری کنند. Yu و همکارانش [۸۹] نیز به تحلیل توزیع قدرت سیگنال بر روی خودروها پرداخته‌اند، و از یک روش آماری به طور مشارکتی برای تعیین مکان مبدأ خودروها استفاده می‌کنند. از آنجا که همسایگان به طور مشارکتی قدرت سیگنال یک خودروی خاص را اندازه‌گیری می‌کنند، دقت تخمین مکان می‌تواند به طور قابل توجهی بهبود یابد. Abbas و همکارانش [۹۰] یک روش کم حجم تشخیص Sybil بر اساس RSS در شبکه ادهاک متحرک ارائه کرده‌اند، بدون اینکه نیاز به یک مرجع متمرکز و سخت‌افزار اختصاصی (مانند، آنتن جهت‌دار یا سیستم موقعیت‌یابی جهانی (GPS)) داشته باشند. روش تشخیص کم حجم به تحرک گره متکی است، و آستانه را به مقدار تفاضل سرعت حرکت گره‌ها تنظیم می‌کند. اگر هر گره سریعتر از آستانه‌ی فعلی حرکت کند، آنگاه ممکن است این گره یک مهاجم Sybil باشد. به طور خلاصه، با بررسی رفتار کاربران عادی و مهاجمان Sybil مربوط به تحرک، شرایط کانال، مهاجمان SA-3 می‌توانند تفکیک شوند. استراتژی‌های تشخیص در شبکه‌های مختلف متنوع خواهند بود، چرا که ویژگی‌های سیستم‌ها به طور قابل توجهی تغییر می‌یابد.

در جدول ۳، روش‌های موجود دفاع در برابر Sybil را با توجه به برخی از اصول طراحی خلاصه نموده‌ایم. نسبت به مهاجمان Sybil در بخش III، روش‌های دفاع در برابر Sybil باید از ویژگی‌های متفاوتی برای طبقه‌بندی، تشخیص، و مقاومت در برابر حملات Sybil در سناریوها و شبکه‌های مختلف استفاده کنند.

جدول ۳. تشخیص Sybil: یک مقایسه

روش دفاع در برابر Sybil	نوع حمله‌ی Sybil	اصول مقدماتی	پایه / فرض	عدم تمرکز
SNSD	SA-1	بخش‌بندی گراف اجتماعی، گام تصادفی	فرض ۱	متمرکز
SCSD	SA-1	تشخیص جامعه	فرض ۲	متمرکز و غیرمتمرکز
BCSD	SA-2	طبقه‌بندی رفتار	تفاوت رفتاری	متمرکز و غیرمتمرکز
FR-MSD	SA-3	تشخیص جامعه، یا تطبیق پروفایل	ویژگی‌های جامعه‌ی مورد اعتماد	غیرمتمرکز
ویژگی-MSD	SA-3	تخمین کانال، طبقه‌بندی ویژگی	مشخصات کانال بی‌سیم، ویژگی‌های تحرک	غیرمتمرکز
crypto-MSD	SA-3	رمزنگاری	امنیت رمزنگاری	غیرمتمرکز

VII. چالش‌های تحقیقاتی

در این بخش، ما به ارائه‌ی برخی از چالش‌های تحقیقاتی و راه‌حل‌های بالقوه برای دفاع در برابر Sybil می‌پردازیم.

A. دفاع در برابر Sybil در MSNها

اگر چه برخی از روش‌های رایج دفاع در برابر Sybil می‌توانند در MSNها به کار گرفته شوند، ولی به علت فقدان گراف اجتماعی سراسری یا رفتارهای تاریخچه‌ای برای یادگیری روش‌های تشخیص، این روش‌های دفاعی نمی‌توانند به طور موثری حملات Sybil را تشخیص دهند. علاوه بر این، به علت تحرک پویای کاربران MSN، قابلیت ردیابی بر روی حملات Sybil تشخیص داده شده نیز ممکن است تضمین نشود. بر خلاف OSNها، همانطور که در جدول ۴ اشاره شده است، به علت تغییر پویای توپولوژی شبکه و ملاحظات حریم خصوصی، به دست آوردن ساختار اجتماعی در MSNها بسیار سخت است. روش‌های موجود MSD در مراجع [۲۲] و [۲۳] می‌توانند تا حدی مهاجمان Sybil و کاربران عادی را از هم تفکیک کنند، یا برخی از روش‌های رمزنگاری مانند

امضای گروهی را برای محدود کردن رفتار مهاجمان Sybil طراحی نمایند. یک راه‌حل ممکن این است که روابط اعتماد میان کاربران متحرک بررسی شده و یک ساختار اجتماعی محلی به شدت متصل ایجاد شود. علاوه بر این، اطلاعات تماس و مکان نیز باید در نظر گرفته شوند. از آنجایی که رفتارهای مهاجمان Sybil متحرک به اهداف حمله‌ی آنها مرتبط خواهد بود، به عنوان مثال، بازبینی‌ها یا هرزنامه‌های مخربی را به عمد تولید کنند ولی به طور غیرفعالانه‌ای در دیگر فعالیت‌های اجتماعی شرکت داشته باشند، تحرک مهاجمان Sybil متحرک از کاربران عادی متفاوت خواهد بود. علاوه بر این، اطلاعات تماس و مکان کاربران متحرک نیز می‌تواند در MSNها به دست آید. بنابراین، تلاش‌های تحقیقاتی زیادی باید بر روی تحلیل ویژگی‌های تماس و مکان کاربران متحرک صورت گیرد، که این اطلاعات برای دفاع در برابر Sybil در MSNها بسیار مفید خواهد بود.

جدول ۴. مقایسه‌ی روش‌های دفاع در برابر Sybil در MSNها و OSNها.

	MSNها	OSNها
تحرک	بله	خیر
گراف اجتماعی	خیر	بله
تبانی	بله	بله
آمار رفتار بلند مدت	خیر	بله
دفاع در برابر Sybil به صورت متمرکز	خیر	بله
توانایی تشخیص در کاربر	ضعیف	قوی

B. حریم خصوصی و دفاع در برابر Sybil

از آنجایی که اکثر دفاع‌های Sybil، به عنوان مثال BCSD و MSD، تمایل دارند که رفتارهای کاربران از قبیل جریان کلیک‌ها، تاریخچه‌ی مرور و بازدید از صفحات، و تماس‌ها را مورد مطالعه قرار دهند، از این رو بسیار مهم و حیاتی است که به نقض حریم خصوصی در حین دفاع در برابر Sybil به ویژه در یک محیط متحرک رسیدگی شود. برای مثال، هنگامی که اطلاعات تماس برای تشخیص SA-3 استفاده می‌شود، تاریخچه‌ی تماس کاربر ممکن است برای دیگران از جمله کاربران متحرک، مهاجمان Sybil یا LSPها آشکار شده و فاش شود. اگر چه این امر برای دفاع در برابر Sybil مفید است، ولی فاش شدن اطلاعات کاربران همچنان حریم خصوصی آنها را

نقض می‌کند. با رمزنگاری مناسب، به عنوان مثال رمزنگاری همریختی[1]، احتمال انجام کارهایی از قبیل مخفی کردن اطلاعات واقعی در متن رمز شده و همچنین انجام فعالیت‌های اضافی یا عملیات ضرب بر روی متن رمز شده نیز ممکن می‌شوند. با این حال، سربارهای محاسباتی و ارتباطی به طور چشمگیری افزایش می‌یابند، به ویژه در یک محیط متحرک که مصرف انرژی یک موضوع حیاتی و بسیار مهم برای کاربران متحرک است. روش دیگر این است که امکان جستجوی پروفایل و تنظیمات مشترک کاربر نیز وجود دارد، تا برای دفاع در برابر Sybil، آشکار شدن اطلاعات خصوصی را کاهش دهد. موضوع چالش‌برانگیز این است که چگونه دقت دفاع در برابر Sybil تضمین شود در حالی که از حریم خصوصی نیز محافظت می‌شود.

C. دفاع مشارکتی در برابر Sybil

با توجه به عدم دانش یا توانایی کافی کاربران، دفاع در برابر Sybil ممکن است در برخی از سناریوها بی‌تاثیر و ناکارآمد باشد. برای مثال، در یک شبکه‌ی متحرک، قابلیت کاربران متحرک به اندازه‌ی سمت سرور قدرتمند نیست، یا حتی در مقایسه با کاربران آنلاین نیز ضعیف می‌باشد. یک رویکرد امکانپذیر و امیدوارکننده این است که همکاری و مشارکتی میان سرورها و کاربران متحرک برای دفاع در برابر Sybil صورت گیرد. کاربران متحرک می‌توانند کاربران مشکوک به Sybil را در مراحل اولیه از طریق روش‌های رمزنگاری از قبیل احراز هویت یا تماس‌های کاربران، امضای رویدادها، و ساختار جامعه‌ی محلی تشخیص دهند. سپس کاربران متحرک این موارد مشکوک را به سرورها با تماس متناظر یا اطلاعات دیگر گزارش می‌دهند. سرورهای متمرکز به پردازش عملیات پیچیده از قبیل یادگیری رفتار کاربر، تشخیص گراف اجتماعی یا جامعه کمک خواهند نمود. سرورها می‌توانند از مزایای قابلیت محاسباتی و ذخیره‌سازی خود بهره گرفته و تشخیص Sybil انجام شده توسط کاربران متحرک را تایید نمایند. علاوه بر این، همکاری و مشارکت میان خود کاربران متحرک نیز می‌تواند دفاع در برابر Sybil را تسهیل کند. با همکاری و مشارکت می‌توان دانش بیشتری در مورد مهاجمان Sybil به دست آورد تا بهتر و بیشتر تشخیص داده شوند. بنابراین، دفاع مشارکتی در برابر Sybil باید یک گرایش و تمایل امیدوارکننده‌ای باشد.

[1] homomorphic encryption

VIII. نتیجه‌گیری

در این مقاله، یک بررسی از حملات Sybil و روش‌های دفاع در برابر آنها در اینترنت اشیاء را ارائه کـرده‌ایـم. بـه طور خاص، ما سه نوع از حملات Sybil را در اینترنت اشیاء توزیع شده تعریف کرده و برخی از روش‌هـای دفـاع Sybil را به همراه مقایسه ارائه نموده‌ایم. مشخصات تفکیک کننده از قبیل ساختارها و رفتارهای اجتمـاعی بـین مهاجمان Sybil و کاربران عادی می‌تواند به دفاع در برابر Sybil کمک نماید. علاوه بر ایـن، MSD مـی‌توانـد از ویژگی‌های شبکه‌ی تلفن همراه، مشخصات کانال بی‌سیم، و رمزنگاری برای مقاومـت در برابـر مهاجمـان Sybil استفاده کند. ما همچنین در مورد برخی از مسائل باز تحقیقاتی از قبیل دفـاع Sybil در MSNهـا، تـوازن بـین حریم خصوصی و یادگیری در دفاع Sybil، و دفاع مشـارکتی Sybil نیـز پیشـنهاداتی ارائـه کـرده‌ایـم. امیـداوار هستیم که این بررسی برای پژوهش‌ها و توسعه‌های آینده در اینترنت اشیاء مفید واقع شود.