تاریخ دریافت مقاله: ۹۸/۱۰/۲۵
تاریخ پذیرش مقاله: ۹۹/۰۴/۱۷

تأمین گمنامی مکان مشارکت‌کنندگان در شبکهٔ اینترنت اشیاء با توانایی تحمل تأخیر برای کاربردهای سنجش جمعی

امیرمهدی سازدار
دانشجوی دکتری مخابرات، دانشکدهٔ مهندسی برق، دانشگاه شهید بهشتی، تهران
پست الکترونیکی: a_sazdar@sbu.ac.ir

سید علی قرشی*
دانشیار دانشکدهٔ مهندسی برق، دانشگاه شهید بهشتی، تهران
پست الکترونیکی: a_ghorashi@sbu.ac.ir

احمد خونساری
دانشیار دانشکدهٔ مهندسی برق و کامپیوتر، دانشگاه تهران، تهران
پست الکترونیکی: a_khonsari@ut.ac.ir

چکیده:

میزان استفاده و محبوبیت فناوری اینترنت اشیاء[1] در کاربردهای سنجش جمعی[2] رو به افزایش است و در دسترس بودن همیشگی گره‌ها، حفظ حریم خصوصی کاربران و همچنین تأمین امنیت اطلاعات مبادله شده در آن از اهمیت بالایی برخوردار است. در این مقاله ساختاری جدید برای حفظ گمنامی در شبکهٔ اینترنت اشیاء با توانایی تحمل تأخیر برای کاربردهای سنجش جمعی، معرفی می‌شود. به‌منظور حصول اطمینان از در دسترس بودن همیشگی اطلاعات، از سازوکار شبکه‌های با تحمل تأخیر بالا و همچنین به‌منظور تأمین گمنامی و حفظ حریم خصوصی کاربران، از ترکیب روش‌های تسهیم راز و روش‌های گمنامی استفاده شده است. روش پیشنهادی، توانایی استفاده از زیرساخت‌های موجود در محیط را داشته و در کنار تحمل تأخیر، گمنامی گره‌ها را به‌طور کامل حفظ می‌کند. همچنین در این روش علاوه بر امکان مدیریت و استفادهٔ کارآمد از پهنای باند ارتباطی، سربارِ محاسباتی گره‌ها نیز در مقایسه با روش‌های موجود، کمتر است. بررسی نتایج حاصل از شبیه‌سازی‌ها و پیاده‌سازی‌های آزمایشگاهی نشان می‌دهد میانگین زمان اجرای بخش‌های مختلف روش پیشنهادی در شبیه‌سازی‌ها حدود ۶۰ درصد و در نتایج آزمایشگاهی حدود ۵۵ درصد کم‌تر از روش‌های مشابه است. به‌علاوه، میانگین زمان ارسال بسته‌ها در مقایسه با روش‌های مشابه در شبیه‌سازی‌ها حدود ۸ درصد و در نتایج آزمایشگاهی حدود ۵ درصد بهبود یافته است. این ارتقای عملکرد در کنار حفظ گمنامی کاربران، ناشی از تغییر نوع روش رمزنگاری و فرایند دست‌به‌دست شدن بسته‌ها در روش پیشنهادی است.

واژه‌های کلیدی: حریم خصوصی، اینترنت اشیاء، سنجش جمعی، گمنامی، شبکه‌های باتحمل تأخیر.

* نویسندهٔ مسئول

1-Internet of Things (IoT)
2-Crowdsensing

۱- مقدمه

امروزه اینترنت اشـیاء یکی از فناوری‌های محبوب و مورد توجه جوامع علمی و صنعتی اسـت. از این فناوری در جنبه‌هـای مختلف عملیات سـنجش جمعی مانند پایش وضعیت سـلامت افراد جامعه، شهرهای هوشمند، صنایع تولیدی و نظایر آن اسـتفاده‌های فراوانی می‌شود [۱]. در این فناوری گاهی ارتباط مستقیم دستگاه‌ها با اینترنت مختل می‌شود. این مشکل، انگیزهٔ ایجاد بستری امن، قابل‌اطمینان و غیرقابل شـنود برای مخابرهٔ داده‌ها از مبدأ تا مقصد را ایجـاد می‌کند. از طرف دیگر، نقض حریم شـخصی افراد، اهمیت استفاده از روش‌های گمنامی در شبکه‌های ارتباطی را پررنگ می‌سـازد [۲]. محدودیـت منابع و تحرّک‌پذیری بالای فناوری اینترنت اشـیاء، امکان همکاری دستگاه‌های مختلـف در این فنـاوری را با چالش روبرو کرده اسـت. یکی از راه‌کارهـای کاهش اثرات این چالش، اسـتفاده از شبکه‌های باتحمل تأخیر[3] (DTN) یا شبکه‌های گسست‌پذیر[4] اسـت. این شـبکه‌ها، توانایی رسـاندن پیام با فرض قطع شـدن‌های مکرر را حفـظ می‌کنند [۳]. در این شـبکه‌ها، می‌تـوان با ذخیـرهٔ داده‌ها در گره‌های شـبکه و مخابرهٔ آن‌هـا در زمان وجود لینک (اتصال بـه مقصد)، داده‌ها را منتقل کرد. شبکه‌های DTN اجازه می‌دهند تا داده‌ها ذخیره و در زمان مناسـب منتقل شوند. با این روش می‌توان کل مجموعهٔ داده را در ساعات غیر اوج ترافیک منتقل نمود و ظرفیت بسیار بالایی با هزینهٔ پایین ایجاد کرد. در این نوع از ارتباطـات، علاوه بر حصول اطمینان از دریافت پیام‌ها، می‌توان با رمزگـذاری نقطه‌به‌نقطه، امنیت محتوای پیام را تأمین کرد. اما در این شبکه‌ها نیز بجز محتوای پیام، مخفی نمودن هویت و موقعیت فرستنده و گیرنده از درجهٔ اهمیت بالایی برخوردار است. در این شبکه‌ها معمولاً از ارتباطات دستگاه به دستگاه[5] (D2D) و رویکردهای گروهی استفاده می‌شود [۳].

در این مقاله با استفاده از مزایای موجود در فعالیت‌های گروهی مشـارکتی و روش‌های گمنامی، ساختاری جدید برای حفظ گمنامی در شبکهٔ اینترنت اشیاء با توانایی تحمل تأخیر برای کاربردهای سـنجش جمعی، معرفی می‌شود. در بخش بعد ضمن مرور پژوهش‌های انجام‌شـده در این حوزه، روش‌های گمنامی در شبکه‌های ارتباطی D2D شرح داده می‌شـود. در بخش سوم روش پیشنهادی برای حفظ گمنامیِ مشارکت‌کنندگان در سنجش جمعی بیان شده است. بخش چهارم به توضیح شبیه‌سـازی‌ها و پیاده‌سازیهای آزمایشگاهی و تحلیل نتایج آن اختصاص داده شده است. بخـش پنجم به ارزیابی نتایج حاصل و مقایسـه با برخی روش‌های موجود پرداخته شده و در انتها نتیجه‌گیری شده است.

۲- کارهای پیشین

به‌منظور تأمین امنیت اینترنت اشیاء باید موارد امنیتی از قبیل محرمانگی، یکپارچگی، احراز هویت، انکارناپذیری، در دسترس بودن و حفظ حریم خصوصی را رعایت نمود [۱]. البتـه در کاربردهـای مختلف اینترنت اشـیاء، میزان اهمیت خدمات فوق متفاوت است. برای مثال در فرایندهای مالی، صحت و احراز هویت افراد، در سفارش‌های اینترنتی، انکارناپذیری و همچنین در پایش وضعیت سـلامت افراد، احترام بـه حریم خصوصی بیمـار دارای اهمیت ویژه‌ای است [۱]. از طرف دیگر وسایل هوشمند اکثراً کوچک بوده و از نظر منابع انرژی، پردازشـی و حافظه محدودیت‌هایی دارند. به همین دلیل اسـتفاده از الگوریتم‌های محاسباتی پیچیده و پرهزینه در آن‌ها معقول نیست. از آنجا که روش پیشـنهادی این مقاله از روش‌های مشارکتی و گروهی با کمـک ارتباطات D2D برای حفظ حریـم خصوصی مکانِ مشـارکت‌کنندگان در سنجش‌جمعی اسـتفاده می‌کند، در ادامـهٔ این بخش، ابتـدا برخی از روش‌هـای مطرح برای حفظ حریم خصوصی در سـنجش جمعی معرفی و مزایا و معایب هرکدام به اختصار بررسی می‌شود. سپس ضمن معرفی روش‌های مشارکتی برای حفظ حریم خصوصی،

3- Delay-Tolerant Networks (DTN)
4- Disruption-Tolerant Network
5- Device to Device

انواع روش‌های ارتباطی D2D و تهدیدات امنیتی آن‌ها بیان می‌شود.

۲-۱ حریم خصوصی در سنجش جمعی

یکی از مهم‌تریـــن روش‌های حفـــظ حریم خصوصی کاربران، اســـتفاده از شبه‌شناســـه[6] اســـت. شبه‌شناســـه به‌عنوان واســـطی بین داده‌هـــا و ویژگی‌هایی مانند تاریخ تولد، جنســـیت، کدپســـتی و نظایر آن قرار می‌گیرد. تغییر ایـــن ویژگی‌هـــا منجر به تغییر شبه‌شناســـه می‌شـــود. با سازوکارهایی که برای تغییر این ویژگی‌ها انجام می‌شود، می‌توان شبه‌شناســـه‌ها را تغییر داد تا قابلیت شناسایی و ردیابی کاربران وجود نداشـــته باشد. این سازوکارها در حریم خصوصی مکان به دو دســـتهٔ کلی ابهام[7] و گمنامی[8] تقســـیم می‌شـــوند [۲]. در ابهام، وضوح مکانـــی کاربران کاهـــش می‌یابد تا محل دقیق حضور آن‌ها قابل‌تشـــخیص نباشد. در برخی موارد نیز مجموعه‌ای از مکان‌های جعلی برای کاربر به‌منظور حفـــظ حریم خصوصی وی تولید و ارسال می‌شود [٤]. الگوریتم‌های پوشش مکان و یا مسیر[9] از نمونه‌های ابهام هســـتند. ایدهٔ اصلـــی این روش‌ها محو کردن مکان کاربر در یک پوشـــش مکانی است که به‌نوعی به معنی وسعت بخشـــیدن به محل کاربران یا به‌اصطلاح کاهش وضوح مکان حضور آن‌ها است. گاهی نیز منطقه به قسمت‌های مکانی تقسیم‌بندی می‌شود و برای هر قسمت، محلـــی خاص (مثلاً مرکز آن) به‌عنوان نقطهٔ موردعلاقه در نظر گرفته می‌شود و پس از شناسایی مکان کاربران، نقطهٔ مورد علاقهٔ آن قسمت ارسال می‌شود. این روش که آن را نقطهٔ موردعلاقه[10] (PoI) می‌نامنـــد، علاوه بر ابهام مکانی، نوعی گمنامی نیز برای کاربران حاضر در آن منطقه ایجاد می‌کند [۲]. در برخی از روش‌ها ابهام با تغییر ویژگی‌ها و تبدیل ابعادِ مکانِ حضور کاربران ایجاد می‌شود. به عنوان نمونه می‌توان به اســـتفاده از منحنی هیلبرت[11] برای تغییر این ابعاد اشاره نمود. در این تبدیل، مختصات (x,y) حضور کاربر به نقطه‌ای روی منحنی هلبرت تبدیل می‌شود [٥].

در حالـــت کلـــی به‌منظور ایجـــاد گمنامی در شـــبکه، راه‌حل‌هـــای مختلفی در مقالات مختلف پیشنهادشـــده که دو راه‌حل «سیاســـت‌گذاری» و «طراحی» از پرکاربردترین آن‌ها هستند. گمنامی به‌واســـطهٔ سیاست‌گذاری، عموماً با یک خدمت‌دهندهٔ گمنامی یا به‌اصطلاح «گمنام‌کننده» انجام می‌شـــود. کاربر باید هنگام شـــروع اســـتفاده از خدمات سازمان‌ها، سیاست‌های گمنامی آنان را بپذیرد. اما سازمان در هرلحظه مختار به تغییر سیاست‌گذاری‌های خود بوده و کســـی حق شـــکایت ندارد. اما گمنامی به‌واسطهٔ طراحی معمولاً به‌عنـــوان خدمت به کاربران ارائه می‌شـــود. برای مثال می‌توان اســـتفاده از خدمت‌دهندهٔ پراکسی را نام برد. مختل شـــدن تک نقطه‌ای و دانستن تمامی اطلاعات توسط خدمت‌دهندهٔ پراکســـی (گمنام‌کننده‌ها) از جمله معایب این روش‌ها است [٦]. پنهان کردن کاربر میان k-1 کاربر دیگر که به k-گمنامی مشهور است، ایدهٔ اصلی گمنامی می‌باشد. این روش، تضمینی برای پنهان شدن کاربر میان k-1 کاربر متمایزِ دیگر است [۲]. در این روش، احتمال شناسایی مکان دقیق کاربر برابر بـــا $\frac{1}{K}$ خواهد بود. در برخی روش‌ها نیز همهٔ ارسال و دریافت‌ها برای ممانعت از شنود توسط افراد غیرمجـــاز و مهاجمان، رمزی می‌شـــود. در این حالت دو خدمت‌دهنده وجود دارند که یکی برای شناســـایی افراد و دیگری برای تشـــخیص کاربردها و داده‌ها به‌کار می‌روند. در ایـــن روش، اطلاعات با کمک کلیدهـــای عمومیِ این دو خدمت‌دهنده دو بار رمزی می‌شود. با این کار خدمت‌دهندهٔ اول که گمنام‌کننده است، تنها می‌تواند تشخیص دهد که چه کسی اقدام به ارسال اطلاعات کرده است. خدمت‌دهندهٔ دوم نیز فقط محتوای پیام‌ها را متوجه می‌شـــود و از این‌که چه کسی آن را ارسال کرده، آگاهی ندارد. بنابراین ارتباط بین کاربران، محل حضور و یا داده‌های حس‌شده توسط آن‌ها با این روش رمزگذاری دوگانه[12]، پنهان می‌ماند [۲].

6- Quasi Identifier
7- Obfuscating
8- Anonymity
9- Path Cloaking Algorithms
10-Point of Interest
11- Hilber Curve
12-Double Encryption

استفاده از ایده‌های مطرح در طرح‌های تسهیم راز[13] نیز روش دیگری برای حفظ حریم خصوصی مکان کاربران است. در این طرح‌ها ابتدا راز که همان مکان کاربر است، به n سهم متمایز تسهیم می‌شود و به هر کاربر یک سهم اختصاص می‌یابد. برای بازیابی راز، می‌توان با وجود $t(t<n)$ سهم از کل سهم‌های تولیدشده، آن را بازیابی نمود و امکان بازیابی راز با کمتر از t سهم وجود ندارد. چنین طرح‌هایی را طرح‌های تسهیم راز آستانه (t,n) می‌نامند [۷]. در این روش ابتدا از روی مکان کاربر، سهم‌ها تولید می‌شوند. سپس در هر بار ارسال اطلاعات و یا درخواست‌های مبتنی بر مکان، سهمی از سهم‌های تولیدشده برای خدمت‌دهنده ارسال می‌شود [۲]. ترکیب هرکدام از روش‌های فوق با یکدیگر نیز می‌تواند به‌عنوان روشی برای افزایش سطح حریم خصوصی مکان کاربران استفاده شود. به‌عنوان نمونه در [۸] با ترکیب PoI و رمزگذاری دوگانه، روشی برای حفظ حریم خصوصی پیشنهاد شده است. در این روش، زمانی که تعداد افراد حاضر در قسمت موردنظر زیاد باشد، از روش PoI و در مناطق کم‌جمعیت و قسمت‌های تُنُک از رمزنگاری دومرتبه‌ای برای افزایش سطح امنیت و حریم خصوصی کاربران استفاده می‌شود.

در اکثر روش‌های ذکر شدهٔ بالا بجز روش رمزگذاری دوگانه، خدمت‌دهنده به اطلاعات مکانی و هویتی کاربران دسترسی دارد و در هیچ‌کدام از این روش‌ها قابلیت پنهان ماندن از دید خدمت‌دهنده وجود ندارد. به همین دلیل و برای حفظ امنیت و حریم خصوصی کاربران در برابر خدمت‌دهندهٔ کنجکاو، روش‌های مشارکتی و گروهی طراحی شده‌اند. لازم به ذکر است که کاربران و اعضای کنجکاو تنها تمایل به دانستن محتوای اطلاعات تبادل شده دارند اما کاربران بدخواه برای دست‌کاری، تغییر و یا تولید بسته‌های جعلی و انتشار آن‌ها تلاش می‌کنند.

روش‌های مشارکتی و توزیع‌شده از جمله روش‌هایی هستند که حریم خصوصی کاربران را از دید خدمت‌دهنده حفظ می‌کنند. در بسیاری موارد برای حفظ امنیت سامانه‌های توزیع‌شده و گروهی از روش‌های مشارکتی یا امنیت مشارکتی[14] استفاده می‌شود. از مصادیق امنیت مشارکتی می‌توان به تشخیص نفوذ و آسیب‌پذیری، مقاومت در مقابل شبکهٔ بات[15] و پالایش هرزنامه‌ها اشاره نمود [۹]. برخی از این روش‌های مشارکتی برای کنترل نظارت‌های شهری (ترافیکی/زیست‌محیطی) [۱۰]، مصرف انرژی [۱۱]، تشخیص ناهنجاری [۱۲]، حفظ حریم خصوصی در خدمات مبتنی بر مکان (LBS) [۱۳، ۱۴]، شبکه‌های اقتضایی خودرویی[16] [۱۵] و بهبود امنیت سناریوهای خودرویی [۱۶] به‌کار می‌روند. اما همهٔ این روش‌ها نمی‌توانند به‌طور مستقیم در فرایندهای سنجش جمعی به‌کار گرفته شوند و کاربرد مخصوص به خود را دارند. روش‌های مشارکتیِ گروهی و توزیع‌شده روش‌هایی هستند که حریم خصوصی کاربران را از دید خدمت‌دهنده حفظ می‌کنند. در برخی روش‌های k-گمنامی نیز از امضای گروهی استفاده می‌شود. در این روش‌ها هر کاربر بین گروهی از کاربران قرار می‌گیرد و زمان ارسال اطلاعات خود، آن‌ها را با امضای گروه تأیید می‌کند. با این روش، کاربر بین k عضو گروه پنهان شده و به همراه حفظ گمنامی کاربران، یکپارچگی داده‌ها نیز حفظ می‌گردد [۲].

از جمله روش‌های مشارکتی دیگر برای حفظ حریم خصوصی کاربران در سنجش جمعی می‌توان به روش k–گمنامی مبتنی بر ویژگی[17] (ABAKA) برای حفظ حریم خصوصیِ هویتی[18] کاربران در خدمات مبتنی بر مکان با در نظر گرفتن ویژگی‌های پروفایلی آنان اشاره نمود [۱۷]. در ABAKA گمنامی با روش‌های رمزگذاری مبتنی بر ویژگی و نواحی پوششی با همکاری مشارکت‌کنندگان و ارسال چندپرشی[19] دستگاه به دستگاه انجام شده است. این روش، از رمزگذاری مبتنی بر ویژگی استفاده کرده و

13-Secret Sharing Schemes

14- Collaborative Security
15- Bot Networks
16- Vehicular Ad-hoc Networks (VANET)
17- Attribute-Based k-Anonymous (ABAKA)
18- Identity Privacy
19- Multi-Hop Forwarding

جدول ۱: تهدیدات و روش‌های مقابله با آن‌ها در ارتباطات دستگاه به دستگاه[۱۹]

چالش	تهدید	راه‌کار مقابله
امنیت	جعل، نقاب گذاری	مدیریت کلید
	جعل، نقاب گذاری، فرد در میانه	احراز هویت
	حملهٔ بدافزار (نشت اطلاعات)	محرمانگی، جامعیت
	منع خدمت	دسترس‌پذیری، اعتمادپذیری
	شنود، جعل IP، نشست‌ربایی	مسیریابی امن، امنیت انتقال
حریم خصوصی	حملهٔ بدافزار (نشت اطلاعات)	کنترل دسترسی
	حملهٔ استنتاج، جعل مکان	ابهام
	حملهٔ استنتاج (نشت مفهوم اطلاعات)	گمنامی، آشفتگی
	شنود، نشست‌ربایی، فرد در میانه	رمزنگاری
کارایی	جعل پهنای باند	آشفتگی
	عدم مشارکت	سازوکارهای تشویقی
	دست‌کاری اعتماد	روش‌های تولید رسید

با همکاری سایر کاربران یک پوشش مکانی برای گمنامی مولد داده‌ها ایجاد می‌نماید [۱۷]. نویسندگان در [۱۸] نیز روش مشارکتی دیگری را مطرح کرده‌اند. آن‌ها با استفاده از روش‌های مبتنی بر ابرِ گمنامی[۲۰] و تسهیم پیام اصلی، مکان مولد داده‌ها[۲۱] (SPAC) در شبکه‌های حسگر بی‌سیم[۲۲] (WSN) را حفظ کرده‌اند. در طرح پیشنهادی [۱۸] با تولید سهم‌های کوچک‌تر از پیام اصلی، مصرف انرژیِ پردازش و انتقال، کاهش‌یافته است. در این طرح، گره مبدأ برای حفظ حریم خصوصی مکان خود بر اساس سهم‌ها، یک ابرِ ناشناس با شکل نامنظم در اطراف خود ایجاد می‌کند. این ابر شامل مجموعه‌ای از گره‌های فعال با اقدامات رادیویی مشابه که ازنظر آماری قابل‌تمایز نیستند، می‌باشد. اندازهٔ ابر با توجه به مقدار از پیش تعیین‌شده‌ای از تعداد پرش‌های هر سهم مشخص شده است. در مرز ابرها نیز گره‌های منبع جعلی از طریق الگوریتم‌های مسیریابی مناسب، به‌طور مستقل سهم‌ها را به گره مبدأ می‌فرستند. در انتها، پیام اصلی را می‌توان با دریافت حداقل t سهم بازیابی نمود. این طرح باعث افزایش محرمانگی داده‌های شبکه می‌شود و همچنین فرایند انتقال داده در برابر خرابی گره‌ها، تحمل بالایی دارد [۱۸].

در اکثر روش‌های مشارکتی از روش‌های ارتباطی D2D استفاده شده است. این ارتباطات توسط فناوری‌های مختلفی مانند اِن‌اِف‌سی (NFC)، زیگ‌بی (ZigBee)، بلوتوث (Bluetooth) و وای‌فای (WiFi) انجام می‌شود [۱۹]. تهدیدات امنیتی، حریم خصوصی، کارایی و روش‌های مقابله با این تهدیدات در ارتباطات D2D در جدول (۱) جمع‌آوری شده است.

در روش پیشنهادی این مقاله با استفاده از روش‌های مشارکتی و همکاری گروهی، مدلی از k-گمنامی برای حفظ حریم خصوصی مکان مشارکت‌کنندگان در سنجش جمعی معرفی شده است. در این روش با کمک روش‌های تسهیم راز، توانایی تحمل تأخیر و خرابی گره‌ها برای شبکه‌های سنجش جمعی بیشتر شده و علاوه بر افزایش سرعت انتقالِ بسته‌های سنجیده‌شده، عملکرد سریعتری را در مقایسه با روش‌های مشابه دارد.

۳- روش پیشنهادی

در روش پیشنهادی با استفاده از روش‌های مشارکتی و ارتباطات D2D و همچنین به‌کارگیری روش‌های تسهیم راز، حریم خصوصیِ مکان کاربران حفظ می‌شود. در این روش با ایجاد گروه‌های مختلف و کمک سرگروه‌های هر گروه، بسته‌های تولیدشده برای خدمت‌دهنده ارسال می‌شود. هر چه تعداد اعضای گروه بیشتر باشد، عملاً گمنامی کاربران بیشتر حفظ می‌شود. هر کاربر پس از عضویت در سامانه، اقدام به سنجش اطلاعات موردنظر برنامه می‌نماید و سپس با استفاده از کلید عمومی خدمت‌دهنده آن‌ها را رمزی و امضاء می‌کند. بستهٔ امضاءشده برای سرگروه فرستاده می‌شود. سرگروه اقدام به انجام طرح تسهیم راز

20- Anonymity Cloud
21- Source location privacy Protection based on Anonymity Cloud (SPAC)
22- Wireless Sensor Network

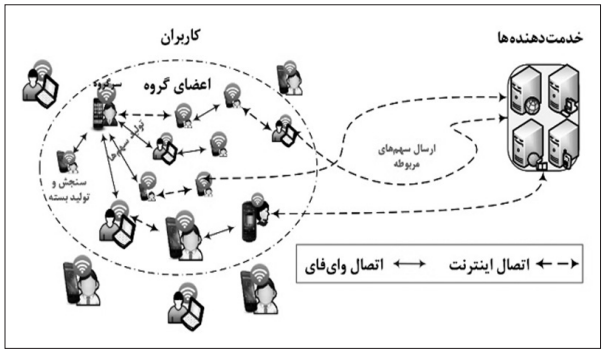
و تولید سهم‌ها از روی بستهٔ ارسالی نموده و سهم‌ها را برای خدمت‌دهنده و یا سایر اعضای گروه ارسال می‌کند. خدمت‌دهنده پس از دریافت سهم‌ها، بسته را بازیابی نموده و محتویات آن را استخراج می‌کند. ساختار کلی روش پیشنهادی در شکل (۱) و جزئیات بخش‌های مختلف روش پیشنهادی در ادامهٔ این بخش ارائه می‌شود.

روش پیشنهادی از زیرساخت کلید عمومی برای انجام رمزگذاری و امضای بسته‌ها استفاده می‌کند. ارتباط بین دستگاه‌های یک گروه با خدمت‌دهنده از طریق اینترنت و ارتباط بین گروهی علاوه بر اینترنت، ممکن است از طریق پروتکل ارتباطی وای‌فای مستقیم نیز انجام شود. در طرح پیشنهادی، حریم خصوصی کاربران با استفاده از روش‌های k-گمنامی با امکان مقابله با تهدید خدمت‌دهندهٔ کنجکاو حفظ می‌شود. در طرح پیشنهادی فرض می‌شود هر بستهٔ سنجیده شده توسط کلید عمومیِ خدمت‌دهنده، رمزی و با کلید خصوصیِ مولّد آن امضاء می‌شود. سپس مشابه آنچه در شکل (۱) مشاهده می‌شود، تولیدکنندهٔ داده می‌تواند بین اعضای گروه گمنام شود و خدمت‌دهنده توانایی شناسایی او را تنها با احتمالی برابر با نسبت معکوس تعداد اعضای گروه، دارد.

در روش پیشنهادی سرگروه و خدمت‌دهنده برای جلوگیری از اقدامات خرابکارانه هر کدام دو فهرست خاکستری و سیاه دارند. اگر مشارکت‌کنندگان و یا هر یک از اعضای گروه قصد انجام اعمال خرابکارانه داشته باشند، مشخصات آن‌ها با توجه به نوع و شدت تهدید در این فهرست‌ها ثبت می‌شود. به عنوان مثال اگر یک مشارکت‌کننده بسته‌های تکراری یا جعلی بفرستد، در فهرست خاکستری ثبت می‌شود و به ازای چند بار تکرار وارد فهرست سیاه شده و عضویت او لغو می‌شود.

۳-۱ مدل سامانه

فرض کنید مجموعهٔ کاربران $U = \{u1, u2, ..., um\}$ در یک محدودهٔ جغرافیایی حضور دارند. هرکدام از آن‌ها می‌توانند عضوی (سرگروه یا عادی) از طرح پیشنهادی



شکل ۱: ساختار کلی طرح پیشنهادی برای حفظ گمنامی مشارکت‌کنندگان در سنجش جمعی.

باشند. فرض بر این است که ارتباط اعضای گروه با یکدیگر و خدمت‌دهنده، با توجه به شرایط و اولویت‌های آن‌ها می‌تواند به دو صورت اتصال D2D و یا ارتباط اینترنتی باشد تا نحوهٔ امتیازگیری گروه‌ها و یا اجرای سناریوهای مقابله با تهدیدات (بخش ۳-۳) امکان‌پذیر باشد. کاربران پس از انجام سنجش اطلاعات خواسته شده، از طریق وای‌فای یا اینترنت با سرگروه یا هم‌گروهی‌های خود ارتباط برقرار می‌کنند. اگر کاربری نتواند بسته‌ای را که از هم‌گروهی خود گرفته شناسایی و یا امضای سرگروه را تأیید نماید، برای جلوگیری از تهدید حملات منع خدمت، بلافاصله این بسته را به همراه مشخصات و شناسهٔ فرستندهٔ آن، برای سرگروه ارسال می‌کند (بخش ۳-۳). در روش پیشنهادی بدون از دست دادن کلیت موضوع، فرض‌های زیر وجود دارد:

الف) کلید عمومی خدمت‌دهنده به‌صورت نرم‌افزاری در برنامهٔ کاربردی سنجش جمعی وجود دارد و با نصب نرم‌افزار، هرکدام از دستگاه‌ها به آن دسترسی دارند. فرض بر این است که خدمت‌دهنده صادق اما کنجکاو است و هیچ‌یک از کاربران تمایلی به افشای هویت و مکان خود ندارند، لذا در بین سایر کاربران پنهان می‌شوند.

ب) فرایند تولید کلید به این صورت است که هر دستگاهِ کاربر (به عنوان مشارکت‌کننده) هنگام عضویت قادر به تولید کلید عمومی و خصوصی خود است و خدمت‌دهنده توان بازیابی کلید خصوصی کاربر را با استفاده از داده‌های موجود و کلید عمومی او ندارد [۲۰].

پ) فرایند تسهیم راز در طرح پیشنهادی، طرح تسهیم رازِ بیتی است و هر بیت به سهم‌های بیتی تبدیل می‌شود و منظور از روی‌هم قرار دادن سهم‌های بیتی همان OR کردن آن‌ها است.

ت) ارتباط اعضای گروه با یکدیگر از طریق اینترنت و یا وای‌فای برقرار می‌شود، که می‌تواند با توجه به خواست کاربران یا توانایی‌ها و امکانات آن‌ها متفاوت باشد.

ث) فرض می‌شود سرگروه‌ها اطلاعات اعضای خود را در اختیار هیچ‌کس قرار نمی‌دهند و فقط تعداد افراد گروه برای سایرین مشخص است.

ج) با توجه به این‌که هر سهم می‌تواند بعد از دست‌به‌دست شدن‌های متعدد و یا حتی فراهم شدن شرایط و دسترسی به اینترنت توسط هر یک از اعضای گروه برای خدمت‌دهنده ارسال شود، طرح از قابلیت شبکه‌های DTN نیز استفاده می‌کند. با رسیدن حداقل k سهم از مجموع n سهم، امکان استخراج اطلاعات توسط خدمت‌دهنده وجود دارد.

چ) هر کاربر در صورت دریافت سهم‌ها، هرکدام از آن‌ها را فقط یک‌بار ارسال می‌کند. همچنین در صورت دریافت بستهٔ تکراری از سایر مسیرها آن را دور می‌ریزد و از ارسال دوبارهٔ آن صرف‌نظر می‌کند.

۳-۲ مدل تهدیدات

در طرح پیشنهادی دو نوع مهاجمِ فعال و غیرفعال در نظر گرفته و فرض شده که همهٔ آن‌ها دانش اولیه‌ای در مورد کاربران دارند [۲۱]. این دانش اولیه شامل سوابق مشارکت کاربران در جمع‌آوری اطلاعات و سنجش جمعی است. مهاجم فعال یک شنودگر خارجی است که می‌داند بدون عضویت در طرح پیشنهادی، توانایی تولید بسته‌های سنجش جمعی را ندارد. چنین مهاجمی علاقه‌مند به دست‌کاری داده‌ها، شناسایی هویت کاربران و یا کاهش سطح حریم خصوصی آن‌ها است. برای کاهش سطح حریم خصوصی کاربران، آن‌ها علاقه‌مند به کاهش تعداد اعضای حاضر در گروه هستند تا بتوانند احتمال k-گمنامی را کاهش دهند. مهاجمان غیرفعال که به دو دستهٔ صادق اما کنجکاو و بدخواه تقسیم می‌شوند. مهاجم صادق اما کنجکاو تنها تمایل به دانستن محتوای اطلاعات تبادل شده دارد اما مهاجم بدخواه تمایل به دست‌کاری، تغییر بستهٔ ارسالی و سهم‌های مبادله شده و یا تولید سهم‌های جعلی و انتشار آن‌ها دارد. مهاجم غیرفعال می‌تواند یکی از موجودیت‌های زیر باشد و فعالیت‌های بیان شده را انجام دهد:

۱- خدمت‌دهندهٔ غیرقابل‌اعتماد که قصد جمع‌آوری اطلاعات هویتی و مکانی مشارکت‌کنندگان را بر اساس داده‌های حس‌شده دارد.

۲- سرگروه کنجکاو یا بدخواه که قصد تولید بسته‌های جعلی یا شناسایی علاقه‌مندی‌های کاربران را دارد.

۳- یک مهاجم یا شنودگر خارجی که روی ارتباطات وای‌فای شنود کرده و قصد شناسایی هویت یا مکان مولد بسته را دارد.

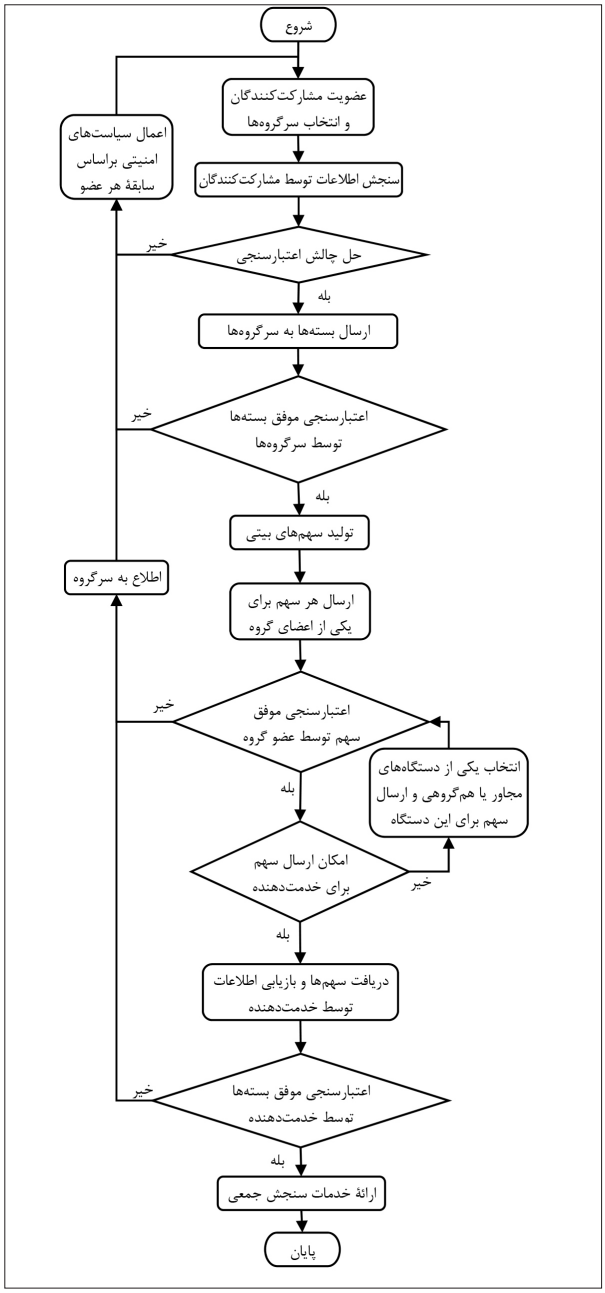
٤- کاربران شبکه و اعضای گروه‌ها که به‌طور کامل قابل‌اعتماد نیستند و به اصطلاح نیمه-مطمئن هستند. طرح پیشنهادی، این کاربران را به دو دستهٔ صادق اما کنجکاو و بدخواه تقسیم‌بندی می‌کند.

۳-۳- مراحل روش پیشنهادی

در این بخش ابتدا برای واضح‌تر شدن روش پیشنهادی، روندنمای کلی آن در شکل (۲) نشان داده شده است و سپس جزئیات و بخش‌های مختلف روش پیشنهادی مطرح گردیده است. نمادهای استفاده شده در روش پیشنهادی و تعاریف مربوط به آن‌ها در جدول (۲) آمده است.

۳-۳-۱ فرایند عضویت دستگاه‌ها و ایجاد گروه

در این فرایند، خدمت‌دهنده برای کاربران گواهی‌نامه‌های D2D تولید و منتشر می‌کند. برای این منظور، خدمت‌دهنده تمام پارامترهای $\{F_q, G_q, P, P_{pub}, h\}$ مطرح شده در جدول (۲) را مقداردهی اولیه می‌نماید. برای عضویت در فرایند سنجش جمعی، دستگاه‌های هوشمند باید برنامهٔ مربوط را نصب نمایند و در سامانه عضو شوند. به‌طورکلی فرض



شکل۲: روندنمای کلی روش پیشنهادی.

کنید دستگاهِ کاربر u قصد عضویت در خدمت‌دهندهٔ SP را دارد. در ایـــن فرایند، کاربر u ابتدا زوج کلید محلی جزئی[۲۳] (x_u, P_u) که در آن x_u یک عدد تصادفی و $P_u = x_u P$ است را انتخاب می‌کند. ســـپس خدمت‌دهنده با اســـتفاده از P_u و یک عدد تصادفیِ r_u اقدام به تولید $R_u = r_u P$ و ســـپس محاســـبهٔ $d_u = r_u + x_{sp}.h(u \| R_u \| P_u)$ نمـــوده و زوج کلید جزئی احراز هویت شـــدهٔ (d_u, R_u) را اســـتخراج می‌نماید.

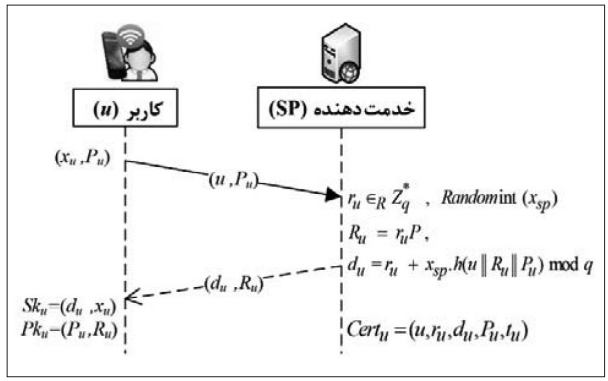
23- Local Partial Key Pair

جدول ۲: نمادهای استفاده شده در توضیح طرح پیشنهادی

ردیف	نماد	تعریف
۱	u و SP، U، C، G	خدمت‌دهنده، مجموعهٔ کاربران، هم‌گروهی، سرگروه و کاربر
۲	(sk_u, pk_u)	زوج کلید عمومی و خصوصی کاربر u.
۳	$Sign_u(m)$	امضای پیام m با کلید خصوصی کاربر u.
۴	$Enc_u(m)$	رمزنگاری پیام m با کلید عمومی کاربر u.
۵	$\|\|$	اتصال دو رشته.
۶	E	خم بیضوی روی میدان متناهی Fq، که به‌عنوان یک گروه دوری جمعی Gp با مولد میدان p و مرتبه گروه q در نظر گرفته می‌شود.
۷	xu	یک عدد تصادفی صحیح و مثبت کوچک‌تر از q، $x \in_R Z_q^*$ به‌عنوان کلید خصوصی اصلی که توسط هر عضو u نگهداری می‌شود.
۸	Ppub	نقطه‌ای روی خم E (P_{pub}=xP) کلید عمومی اصلی و حاصل‌ضرب نقطه‌ای روی E
۹	h	تابع درهم‌ساز $h: \{0,1\}^* \to Z^*$

درنهایـــت (sk_u, pk_u) به‌عنـــوان گواهی کاربـــر u در نظر گرفته می‌شود، که در آن $sk_u = (d_u, x_u)$ و $pk_u = (P_u, R_u)$ به ترتیب زوج کلید خصوصی و عمومی کاربر u هســـتند. خدمت‌دهنـــده نیز پنج‌تایی (u, r_u, d_u, P_u, t_u) کـــه در آن t_u زمان تولید گواهی‌نامه اســـت را ذخیـــره می‌نماید. مراحل انجام این عضویت در شکل (۲) نشان داده‌شده است.

پـــس از تولید زوج کلید، کاربران حدود شـــعاع مکانی خود به‌عنوان پوشش مکانی و یک نقطهٔ مکانی موردعلاقه (که لزوماً مکان حضور این کاربر نیســـت) را به‌عنوان PoI برای خدمت‌دهنده ارسال می‌کنند. خدمت‌دهنده با مشاهدهٔ PoI و شعاع پوشش مکانی، فهرستی از اطلاعات گروه‌های موجود در آن ناحیهٔ PoI تا شعاع اعلام‌شده را برای کاربر ارســـال می‌کند. کاربر پس از دریافت این فهرست می‌تواند بـــا توجه به امتیاز هر گـــروه و یا بنا به هر اولویت دیگری (مثـــلاً تعداد اعضای گروه) عضو یک یا چند گروه شـــود. پس‌از این مرحله کاربر می‌تواند برای ارســـال بســـته‌های ســـنجش جمعی خود از این گروه‌ها اســـتفاده کند و خود



شکل ۲: مراحل عضویت دستگاه‌ها [۲۰].

را میـــان اعضای آن‌ها پنهـــان نماید. به‌عـــلاوه هر کاربر می‌توانـــد برای خود گروه ایجاد نمایـــد و با دادن اطلاع به خدمت‌دهنده، سرگروه آن شود. این سرگروه تا زمانی که می‌تواند فعالیت خود را ادامه دهد، به‌عنوان سرگروه باقی می‌ماند. درصورتی‌که به هر دلیلی این ســـرگروه از گروه کنار رود یا تمایلی به ادامه نداشـــته باشـــد، سایر کاربران با روش مطرح‌شـــده در الگوریتم اجمـــاع[۲۴] RAFT اقدام به انتخاب سرگروه جدید می‌نمایند [۲۲]. در روش پیشنهادی، سرگروه در فواصل زمانی ۲۵۰ تا ۳۰۰ میلی‌ثانیه حضور خود را برای دســـتگاه‌های مجـــاور اعلام می‌نماید. یکی از دلایل اســـتفاده از این الگوریتم اجماع، ســـرعت و سادگی پیاده‌ســـازی آن اســـت. در ضمن در این روشِ اجماع تنها با وجود دوســـوم اعضای صادق، می‌توان به عملکرد آن اطمینان داشت و برای مختل نمودن فرایند انتخاب سرگروه نیاز به بیش از یک‌ســـوم عضو بدخواه است [۲۳] که البته این سطح آستانه بسته به کاربرد می‌تواند تغییر کند.

۳-۳-۲ تولید و ارسال سهم‌ها

مشارکت‌کننده برای ارسال بسته‌های خود باید پس از انجام فرایند سنجش، درخواستی را برای سرگروه ارسال نماید. ســـرگروه به‌صورت کاملاً تصادفی مدت زمانی را صبر کرده و سپس مشابه آنچه در [۲٤] آمده است، از این مشـــارکت‌کننده می‌خواهد تا چالشی را پاسخ دهد. پس از حل چالش توسط مشارکت‌کننده، سرگروه آمادگی پذیرش بســـته از مشـــارکت‌کننده را دارد. مشـــارکت‌کننده مشابه رابطهٔ (۱)، ابتدا اطلاعات ســـنجیده شده را با کلید عمومیِ خدمت‌دهنده (SP) رمزی می‌کند و پس از افزودن شناســـهٔ کاربری خود و مُهرِ زمانی، همهٔ اطلاعات را با کلید عمومی سرگروه (G) رمزی کرده و پیام را آماده می‌کند. سپس آن پیام را امضاء کرده و برای سرگروه ارسال می‌کند.

$$Msg = ID \| Timestamp \| Enc_{SP}(SensedData)$$
$$Packet = Msg \| Sign_u(Msg) \quad (۱)$$

در ایـــن رابطـــه SensedData اطلاعات ســـنجیده شـــده، Timestamp مُهر زمانی و ID، شناسهٔ کاربری که اطلاعات را سنجیده است، می‌باشد. سرگروه پس از بررسی صحت امضـــاء، ابتدا شناســـهٔ مولد داده را از روی بســـته حذف می‌کند. سپس در یک جدول مشخص، مقادیر Timestamp و ID را ذخیـــره می‌کند. در ادامه ســـرگروه با اســـتفاده از روش‌های تســـهیم رازِ بیتی (بخش ۳-٤-۳) اقدام به تولید سهم‌ها از $Enc_{SP}(SensedData)$ کرده و مشخصات کلی آن مانند شناســـهٔ گروه، تعداد کل ســـهم‌ها و تعداد سهم‌های آستانه برای بازیابی آن را مشابه رابطهٔ (۲) تولید و امضاء می‌نماید.

$$Msg = Share \| GroupID \| t \| n$$
$$Packet = Msg \| Sign_G(Msg) \quad (۲)$$

در رابطهٔ (۲) Share ســـهم تولیدشـــده، GroupID شناسهٔ گروه و n و t پارامترهای تسهیم راز هستند. در این مرحله ســـرگروه می‌تواند به‌دلخـــواه در صورت دسترســـی به اینترنت اقدام به ارسال تمامی و یا تعدادی از سهم‌ها آن‌ها نماید و یا می‌تواند آن‌ها را برای اعضای گروه بفرســـتد تا اعضای گروه در صورت دسترسی به اینترنت، آن سهم‌ها را ارسال نمایند. البته این اعضاء می‌توانند سهم‌های دریافتی را نگه‌داشـــته و در صورت برقراری اتصال اینترنت برای خدمت‌دهنده بفرســـتند و یا در صورت وجود هم‌گروهی، از طریق وای‌فای برای دســـتگاه‌های مجاورِ خود ارســـال نمایند تا آن‌ها ســـهم را به خدمت‌دهنده برسانند. هر عضو گـــروه در صورت دریافت ســـهم از هم‌گروهی خود، ابتدا صحت امضای آن را کنترل می‌کند و در صورت مغایرت، مشخصات فرســـتنده را در اختیار سرگروه قرار می‌دهد.

24- RAFT Consensus Algorithm

گام‌های مختلف ارسال بسته‌ها در الگوریتم (۱) آمده است.

الگوریتم ۱- الگوریتم ارسال بسته‌ها در روش پیشنهادی

ورودی: بستهٔ رمزنگاری‌شدهٔ $Enc_u(m)$ و مقادیر n و t $(t \le k)$
خروجی: ارسال سهم‌های تولیدشده
محل اجرا: مشارکت‌کننده (گره مولد)، سرگروه و اعضای گروه

۱- مشارکت‌کننده اطلاعات مورد نظر سنجیده می‌شود.
۲- درخواستی برای ارسال بسته به یکی از سرگروه‌ها ارسال می‌شود.
۳- سرگروه بعد از گذشت مدّت زمانی تصادفی، چالشی را آغاز و پارامترهای آن را برای مشارکت‌کننده ارسال می‌کند.
۴- مشارکت‌کننده چالش را حل کرده، سپس بسته‌ای را مطابق رابطهٔ (۱) تولید و برای سرگروه ارسال می‌کند.
۵- در صورت صحیح بودن پاسخ چالش، سرگروه بسته را می‌پذیرد. در غیر این صورت به مشارکت‌کننده اطلاع داده و الگوریتم به گام ۴ می‌رود.
۶- اگر صحت بستهٔ دریافتی با کنترل امضای فرستنده توسط سرگروه تأیید شد، الگوریتم به گام بعدی می‌رود. در غیر این صورت فرستنده را در فهرست خاکستری قرار داده و به گام ۱۰ بروید.
۷-سرگروه شناسهٔ مشارکت‌کننده را از بسته حذف و با توجه به مقادیر n و t سهم‌ها را تولید می‌کند.
۸-سرگروه به‌صورت اختیاری (یا هر اولویت دیگری) می‌تواند آن سهم را به‌طور مستقیم برای خدمت‌دهنده و یا برای هر یک از اعضای گروه بفرستد.
۹-تا زمانی که سهمی در گروه وجود دارد، نگه‌دارندهٔ آن سهم می‌تواند یکی از دو حالت زیر انتخاب کند:
۹-۱ در صورت وجود شرایط انتقال، سهم برای خدمت‌دهنده ارسال شود و یا تا زمان تحقق شرایط، نگه‌داشته شود.
۹-۲ با استفاده از ارتباط وای‌فای، سهم را برای یکی از دستگاه‌های مجاور ارسال کند.
۱۰- پایان.

۳-۳-۳- تسهیم بسته و تولید سهم‌ها

اساس روش تسهیم رازِ بیتی ارائه‌شده بر این قاعده استوار است که راز با روی‌هم قرار دادن t سهم از میان n سهم، بازسازی می‌شود. با کنار گذاشتن این t سهم، تعداد n-t سهم باقی می‌ماند. بنابراین اگر در بیتی از راز، مقدار یک وجود دارد، باید در موقعیت متناظر همان بیت برای (n-t)+1 سهم مقدارِ یک و برای سایر سهم‌ها مقدارِ صفر درج شود. یعنی حتی اگر n-t سهم نیز از بین برود، در سهم‌های باقیمانده حداقل یک سهم وجود دارد که مقدار بیت موردنظر را در خود حفظ کرده باشد. با استفاده از مولد اعداد تصادفی برای مشخص نمودن این $(n-t)+1$ سهم، می‌توان سهم‌های کاملاً تصادفی تولید نمود. روش تسهیم راز بیتیِ استفاده‌شده در روش پیشنهادی در الگوریتم (۲) نشان داده‌شده است. در این طرح، بازسازی پیام‌ها نیز تنها با OR نمودن بیت‌های متناظر در سهم‌ها به‌سادگی امکان‌پذیر است.

الگوریتم ۲- طرح تسهیم راز بیتی برای تولید سهم‌ها

ورودی: بستهٔ رمزنگاری‌شدهٔ $Enc_u(m)$ و مقادیر n و t $(t \le k)$
خروجی: سهم‌های تولیدشده
محل اجرا: سرگروه

۱- حاصل مقدار r=(n-t)+1 و طول بستهٔ رمزنگاری‌شده Len=size(Encu(m))-۲ را محاسبه کنید.
آرایهٔ دوبعدی Share[n][Len] را با مقدار اولیهٔ صفر برای نگهداری سهم‌ها تشکیل دهید.
۳- به ازای هر بیت b از پیام Encu(m) مراحل زیر را انجام دهید:
۳-۱ اگر بیت b برابر یک است:
الف) آرایهٔ r عضوی rand را به‌صورت تصادفی با مقادیر یک تا r کامل کنید.
ب) برای k=1 تا r مقدار Share[rand[k]][b]=1 قرار دهید.
۴- سهم‌های تولیدشده را به خروجی بفرستید.
۵-پایان.

۳-۳-٤ دریافت و بازیابی بسته‌ها

بعد از دریافت حداقل t سهم از n سهم تولیدشده توسط خدمت‌دهنده، راز (همان بستهٔ سنجش جمعی) بازیابی می‌شود. سپس توسط خدمت‌دهنده رمزگشایی می‌شود تا محتوای آن مشخص گردد. پس از تأیید محتوای پیام، خدمت‌دهنده امتیاز گروه ارسال‌کننده را افزایش می‌دهد. اما درصورتی‌که بسته جعلی باشد یا محتوای پیام با داده‌های مشابهِ سنجیده شده همخوانی نداشته باشد، به سرگروه اطلاع داده می‌شود. سرگروه که می‌داند این بسته را از کدام عضو گروه دریافت کرده، او را در فهرست خاکستری قرار می‌دهد و در صورت تکرار این خطا وارد فهرست سیاه سرگروه شده و دیگر بسته‌ای از او دریافت نخواهد شد. نتیجهٔ این اقدام به اطلاع خدمت‌دهنده می‌رسد. اگر سرگروه نتواند مولد بسته را شناسایی و معرفی نماید عضویت خود او توسط خدمت‌دهنده لغو می‌شود. برای لغو عضویت اعضاء، خدمت‌دهنده مقدار t_u ذخیره‌شده در زمان فرایند تولید گواهی آن‌ها را برابر منفی یک قرار می‌دهد و گواهینامهٔ مشارکت‌کننده از اعتبار خارج می‌شود. با توجه به این‌که فهرست‌های سیاه در اختیار خدمت‌دهنده نیز قرار دارد، اگر یک شناسهٔ کاربری در چند فهرست سیاه باشد، عضویت او توسط خدمت‌دهنده لغو می‌شود.

خدمت‌دهنده برای اثبات نادرستی بسته، دلیل و محتوای صحیح را به همراه محتوای بستهٔ اصلی برای سرگروه

ارسال می‌کند. سرگروه با کنترل دلیل و محتوای صحیح، اطلاعات محتوای بسته را دوباره با کلید عمومی خدمت‌دهنده رمزی می‌کند و با بستهٔ ارسال‌شده توسط مولد آن مطابقت می‌دهد. اگر اطلاعات مشابه بود، تخلف مشارکت‌کنندهٔ تولیدکنندهٔ بسته اثبات می‌شود. همچنین در صورت دریافت سهم‌های تکراری و زیاد بودن نرخ آن (مثلاً بیشتر از ۱۰٪)، این سهم‌ها و فرستنده‌های آن‌ها هم به سرگروه معرفی‌شده و در فهرست خاکستری قرار می‌گیرند.

۳-۳-۵ ارسال پاسخ

پس از بازسازی کامل راز و استخراج اطلاعات سنجیده شده، درصورتی‌که بسته حاوی درخواستی از سوی مشارکت‌کننده باشد، خدمت‌دهنده به‌سادگی پاسخ پیام را برای سرگروه ارسال می‌کند. این پاسخ برای جلوگیری از شنود توسط افراد غیرمجاز با کلید عمومی سرگروه رمزی و سپس با کلید خصوصی خدمت‌دهنده امضاء می‌شود. به‌علاوه مقدار مُهر زمانی بستهٔ سنجیده‌شده که توسط مولد بسته تولید شده بود نیز به این بستهٔ پاسخ ضمیمه می‌شود. ساختار بستهٔ پاسخ در رابطهٔ (۳) آمده است.

$$Msg = Sign_{SP}(Enc_G(Answer \parallel Timestamp)) \qquad (۳)$$

مدیر گروه پس از دریافت بسته و کنترل امضای خدمت‌دهنده، محتوای آن را استخراج می‌نماید و با توجه به مقدار مُهر زمانی موجود در بسته، فرستنده را شناسایی و پاسخ را برای او ارسال می‌کند. با توجه به این‌که سرگروه‌ها برای شروع چالش، یک مدت زمان تصادفی صبر کرده و سپس آن را آغاز می‌کنند و از آنجا که زمان حل چالش با توجه به منابع و محدودیت‌های اعضای گروه، متفاوت است، مُهر زمانی موجود در بسته‌های هر گروه برای هر بسته با احتمال بسیار بالایی یکتا است. حتی اگر یکتا هم نباشد این پاسخ برای همهٔ اعضای گروه می‌تواند ارسال شود، تا خود گره‌ای که ارسال‌کنندهٔ بسته است، پاسخ را دریافت کند. الگوریتم (۳) مراحل مختلف فرایند دریافت سهم‌ها، بازیابی بسته و پاسخ به درخواست‌های کاربران در روش پیشنهادی را بیان می‌کند.

۳-۳-۶ سازوکارهای تشویقی

در روش پیشنهادی، خدمت‌دهنده پس از دریافت سهم‌ها و بازیابی بسته، امتیاز گروه ارسال‌کننده را افزایش می‌دهد و این امتیاز را در قالب گواهینامه برای سرگروه ارسال و اعتبار او را افزایش می‌دهد. البته برای این‌که تبادل این گواهی‌ها ترافیک شبکه را زیاد نکند، می‌توان مثلاً به ازای هر m بسته یک‌بار امتیاز گروه‌ها را افزایش داد. هرچه امتیاز گروهی بیشتر باشد، مشارکت‌کنندگان جدید بیشتر به عضویت در آن‌ها تمایل دارند، چون اعضای این گروه‌ها در صورت نیاز به استفاده از خدمت‌های موجود در خدمت‌دهنده زودتر از گروه‌های دیگر خدمت می‌گیرند. در روش پیشنهادی، خدمت‌دهنده به تمام کاربرانی که از آن‌ها سهمی را دریافت کرده است و این سهم‌ها در بازسازی راز موفق به‌کار گرفته شده‌اند، پاداش می‌دهد. بنابراین همهٔ کاربران در گروه تلاش می‌کنند تا بسته‌های سهم را زودتر به خدمت‌دهنده برسانند. با این روش هر عضوِ گروه به اندازهٔ تلاشی که انجام می‌دهد و منابعی که صرف می‌کند، پاداش می‌گیرد. البته می‌توان برای روش پیشنهادی از سازوکارهای تشویقی وزن‌دار و پیچیده‌تر که نمونه‌های آن در [۲۵، ۲۶] آمده است نیز استفاده کرد که پرداختن به جزئیات آن خارج از حوصلهٔ این نوشتار است. هرچه تعداد همکاری‌ها بیشتر شود بسته‌های بیشتری در زمان مشابه به خدمت‌دهنده می‌رسد و گروه‌های فعال‌تر، امتیاز بیشتری خواهند داشت.

۴- شبیه‌سازی و تحلیل

در این بخش پارامترها و نتایج شبیه‌سازی‌ها به همراه تحلیل‌های امنیتی بیان‌شده است.

۴-۱ پارامترها و نتایج شبیه‌سازی

برای اثبات قابلیت به‌کارگیری و گسترش‌پذیریِ روش پیشنهادی، ابتدا با کمک شبیه‌سازی، حداکثر زمان ارسال بسته‌ها از هنگام تولید تا رسیدن حداقل تعداد t سهم از کل سهم‌ها به خدمت‌دهنده با شبیه‌سازی محاسبه و در شکل

(۳) نمایش داده شـــده است. برای انجام این شبیه‌سازی‌ها از نرم‌افـــزار متلب به کمک رایانهٔ Sony VAIO Core i7 با ۸ گیگابایت RAM و سیســـتم‌عامل ویندوز ۱۰ استفاده شده اســـت. محیط شبیه‌ســـازی منطقه‌ای با ابعاد ۱۰۰ در ۱۰۰ متر، الگوریتم رمز نامتقارن RSA 1024 و الگوریتم امضای رقمی اســـتاندارد نیز RSA با خروجی امضای ۵۱۲ بیت در نظر گرفته شـــده است. در شبیه‌ســـازی‌ها مشابه آنچه در [۱۷] آمده، اندازهٔ بســـته‌های ارسالی ۲۵۰ کیلوبایت و برد ارتباطی وای‌فای ۱۵ متر در نظر گرفته شـــده اســـت. برای عضویت دســـتگاه‌ها برای فرایند تولید کلید از خم بیضوی secp256k1 استفاده شده است.

الگوریتم (۳): الگوریتم دریافت سهم‌ها، بازیابی بسته‌ها و ارسال پاسخ

ورودی: سهم‌ها
خروجی: بستهٔ بازیابی شده و درصورت نیاز پاسخ بسته
محل اجرا: خدمت‌دهنده (درصورت ارسال پاسخ: سرگروه و مشارکت‌کننده)

۱- اصالت هر سهم را با کنترل امضای آن بررسی کنید.
۲-شناسهٔ گروه و مقادیر n و t را از سهم‌های دریافتی استخراج کنید.
۳-با روی‌هم قرار دادن حداقل t سهم (OR بیتی) بستهٔ اولیه را بازیابی کنید.
۴-بسته را رمزگشایی و محتویات آن (داده‌های حس‌شده و مُهرزمانی) را بازیابی کنید.
۵-اگر اطلاعات صحیح بود با توجه به سیاست‌های تشویقیِ از پیش تعیین‌شده، امتیاز گروه را افزایش داده، به گام ۱۰ بروید.
۶-اگر اطلاعات بسته نادرست و یا جعلی بود، به سرگروه اطلاع داده شود.
۷-سرگروه با بررسیِ دلایل ارائه‌شده از طرف خدمت‌دهنده مبنی بر جعلی بودن بسته، از روی مقادیر مُهرزمانی و ID ذخیره‌شـــده، مولد آن را شناســـایی و با توجه به سابقهٔ خطاها او را در فهرست خاکستری یا سیاه قرار می‌دهد.
۸-گزارش فعالیت انجام‌شـــده و شناســـهٔ مولد خاطی به خدمت‌دهنده ارسال و به گام ۱۴ بروید.
۹-اگر ســـرگروه نتواند مولد خاطی را شناســـایی و معرفی نماید، خود او در فهرســـت خاکستری یا سیاه خدمت‌دهنده قرار خواهد گرفت.
۱۰-اگر بسته نیاز به پاسخ ندارد، به گام ۱۴ بروید.
۱۱-بستهٔ پاسخ مطابق رابطهٔ (۳) تولید و برای سرگروه فرستاده شود.
۱۲-سرگروه پاسخ را با توجه به مقدار مُهرزمانی برای مشارکت‌کنندهٔ مرتبط با آن ID (یا در صورت وجود چند عضو) از گروه می‌فرستد.
۱۳-اعضای گروه با توجه به مقدار مُهرزمانی متوجه می‌شوند، پاسخی که آمده مربوط به کدام درخواست آن‌ها است.
۱۴-پایان.

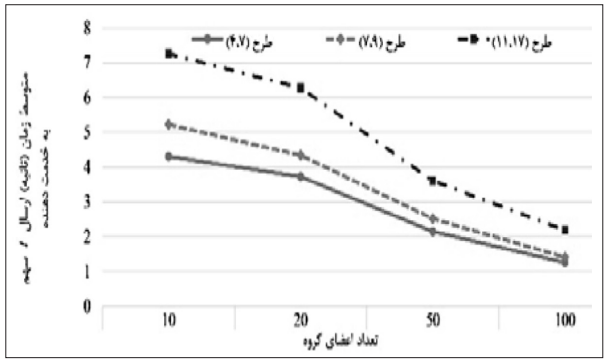
در این پیاده‌ســـازی اطلاعات سنجیده شده به‌صورت بایت برای تولید سهم‌ها استفاده شده و بازیابی راز از روی سهم‌ها تنها با روی‌هم قرار دادن سهم‌ها و عملیات OR انجام می‌شود. شبیه‌سازی‌ها با سه حالت مختلف تسهیم راز (۷، ٤)، (۹، ۷) و (۱۷، ۱۱) برای تولید سهم انجام شده است. از سوی دیگر احتمال اتصال دستگاه‌ها به اینترنت ۵۰٪ فرض شده است. نحوهٔ حرکت گره‌ها با فرایند راه رفتن تصادفی و زمان انجام عملیات سنجش توســـط کاربران با کمک فرایند پواسون با پارامتر $\lambda = 2$ و به‌صورت زمان رسیدن ضربه‌های پواسون در نظر گرفته شده است. ایجاد چالش بین سرگروه و سایر اعضای گروه نیز با صفـــر کردن بیت‌های انتهایی یک تابع درهم‌ساز پیاده‌سازی شده، تا بتوان یک چالش درهم‌سازی[۲۵] ایجاد نمـــود. چالش درهم‌ســـازی از الگوریتـــم SHA-512 استفاده می‌کند و برای همهٔ کاربران تعداد بیت‌های تصادفی بین ۷ تا ۱۰ بیت در نظر گرفته شـــده است. زمان تصادفی انتظار برای شروع چالش در ســـرگروه‌ها عددی تصادفی بیـــن ۱۰۰ تا ۲۰۰ میلی‌ثانیه فرض شـــده اســـت. با افزایش تعداد اعضای گروه، امکان اتصال تعداد بیشـــتری از آن‌ها به اینترنت وجود دارد. افزایش این احتمال باعث می‌شود تا بسته‌های سهم زودتر به خدمت‌دهنده برسد و زمان بازیابی اطلاعات با استفاده از سهم‌های دریافت شده کاهش یابد. در شبیه‌سازی‌ها متوســـط زمان انتقال t سهم موردنیاز برای بازیابی بســـته‌های سنجیده شـــده در طرح‌های تسهیم راز (۷، ٤)، (۹، ۷) و (۱۷، ۱۱) برای ۱۰۰ بار اجرا به ترتیب برابر ۲/۸۶۳، ۳/۳۷۵ و ٤/۸۳۵ ثانیه است.

برای بررسی دقیق‌تر زمان اجرای چالش درهم‌سازی، شـــش تابع درهم‌ســـاز SHA-256، SHA-1، MD5، MD2، SHA-512، SHA-384 با صفر کردن بیت‌های انتهایی چکیده پیام شبیه‌سازی شده است. زمان آغاز چالش‌ها برای این توابـــع حداکثر برابر ۰/۰٦ میلی‌ثانیه اســـت. میانگین زمان حل این چالش به ازای ۱۰۰ بار اجرا در محیط شبیه‌سازی برحســـب تعداد بیت‌های چالش و توابع مختلف در جدول (۳) آمده اســـت. همان‌طور که مشاهده می‌شود با افزایش تعـــداد بیت‌های صفر شـــده در چالش، زمـــان حل آن نیز به‌صورت کاملاً مشـــهودی افزایش می‌یابد. البته در جدول (۳) برای نمایش میزان سختی حل چالش هم‌سازی، مقادیر زمان مورد نیاز تا ۲۰ بیت محاســـبه و نمایش داده شـــده است. اما در شبیه‌سازی‌ها و نمونه‌های آزمایشگاهی تعداد بیت‌ها حداکثر ۱۰ بیت انتخاب‌شـــده تا تأثیر سایر مؤلفه‌ها نیز در فرایند ارسال بسته‌ها قابل‌محاسبه باشد.

25- Hash Puzzle Challenge

جدول ۳: متوسط زمان (میلی‌ثانیه) حل چالش چکیده‌سازی به ازای تعداد بیت‌های مختلف

الگوریتم چکیده‌سازی	تعداد بیت‌های صفر شده چالش چکیده‌سازی																	میانگین
	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	
MD2	۰/۲۵	۰/۵۰	۱/۰۱	۲/۰۱	۴/۰۲	۸/۰۴	۱۶/۰۸	۳۲/۱۷	۶۴/۳۳	۱۲۸/۶۷	۲۵۷/۳۳	۵۱۴/۶۶	۱۰۲۹/۳۳	۲۰۵۸/۶۶	۴۱۱۷/۳۱	۸۲۳۴/۶۲	۱۶۴۶۹/۲۵	۳۲۹۳۸/۴۹	۳۶۵۹/۸۲
MD5	۰/۲۰	۰/۴۱	۰/۸۲	۱/۶۳	۳/۲۷	۶/۵۳	۱۳/۰۷	۲۶/۱۴	۵۲/۲۸	۱۰۴/۵۵	۲۰۹/۱۰	۴۱۸/۲۱	۸۳۶/۴۱	۱۶۷۲/۸۲	۳۳۴۵/۶۴	۶۶۹۱/۲۸	۱۳۳۸۲/۵۶	۲۶۷۶۵/۱۲	۲۹۷۳/۸۹
SHA-1	۰/۱۷	۰/۳۳	۰/۶۶	۱/۳۲	۲/۶۴	۵/۲۸	۱۰/۵۶	۲۱/۱۲	۴۲/۲۴	۸۴/۴۹	۱۶۸/۹۸	۳۳۷/۹۵	۶۷۵/۹۰	۱۳۵۱/۸۰	۲۷۰۳/۶۰	۵۴۰۷/۲۰	۱۰۸۱۴/۴۰	۲۱۶۲۸/۸۰	۲۴۰۳/۱۹
SHA-256	۰/۱۶	۰/۳۲	۰/۶۵	۱/۲۹	۲/۵۸	۵/۱۶	۱۰/۳۲	۲۰/۶۴	۴۱/۲۹	۸۲/۵۸	۱۶۵/۱۵	۳۳۰/۳۱	۶۶۰/۶۱	۱۳۲۱/۲۳	۲۶۴۲/۴۵	۵۲۸۴/۹۱	۱۰۵۶۹/۸۱	۲۱۱۳۹/۶۳	۲۳۴۸/۸۴
SHA-384	۰/۱۷	۰/۳۵	۰/۶۹	۱/۳۸	۲/۷۷	۵/۵۴	۱۱/۰۷	۲۲/۱۴	۴۴/۲۸	۸۸/۵۷	۱۷۷/۱۳	۳۵۴/۲۷	۷۰۸/۵۴	۱۴۱۷/۰۷	۲۸۳۴/۱۵	۵۶۶۸/۳۰	۱۱۳۳۶/۵۹	۲۲۶۷۳/۱۹	۲۵۱۹/۲۳
SHA-512	۰/۱۷	۰/۳۵	۰/۶۹	۱/۳۸	۲/۷۶	۵/۵۲	۱۱/۰۵	۲۲/۱۰	۴۴/۲۰	۸۸/۴۰	۱۷۶/۷۹	۳۵۳/۵۸	۷۰۷/۱۶	۱۴۱۴/۳۲	۲۸۲۸/۶۵	۵۶۵۷/۲۹	۱۱۳۱۴/۵۸	۲۲۶۲۹/۱۶	۲۵۱۴/۳۴
میانگین	۰/۱۹	۰/۳۸	۰/۷۵	۱/۵۰	۳/۰۱	۶/۰۱	۱۲/۰۳	۲۴/۰۵	۴۸/۱۰	۹۶/۲۱	۱۹۲/۴۱	۳۸۴/۸۳	۷۶۹/۶۶	۱۵۳۹/۳۲	۳۰۷۸/۶۳	۶۱۵۷/۲۷	۱۲۳۱۴/۵۳	۲۴۶۲۹/۰۷	۲۷۳۶/۵۵



شکل ۳: نتایج شبیه‌سازی طرح پیشنهادی و محاسبه میانگین زمان (ثانیه) لازم برای ارسال و بازیابی بسته‌های سنجیده شده.

متوسط زمان لازم برای اجرای هرکدام از بخش‌های روش پیشنهادی در شبیه‌سازی‌های انجام‌شده و نتایج به‌دست‌آمده در پیاده‌سازی‌های آزمایشگاهی به همراه مقایسه با روش‌های مطرح‌شده در [۱۷] و [۱۸] در جدول (٤) آمده است. همان‌گونه که مشاهده می‌شود، استفاده از تسهیم رازِ مطرح‌شده در الگوریتم (۲) به‌منظور تولید سهم‌ها، موجب افزایش سرعت در مراحل مختلف روش پیشنهادی شده است. به‌علاوه در کنار توانایی تحمل تأخیر در شبکه، سرعت انتقال بسته‌های سنجیده شده نیز در مقایسه با روش‌های مطرح‌شده در [۱۷] و [۱۸] بیشتر است.

۵- ارزیابی آزمایشگاهی و مقایسه

در این بخش به بیان ویژگی‌های محیط آزمایشگاهی و نتایج حاصل از ارزیابی‌ها و همچنین مقایسهٔ روش پیشنهادی با چند روش دیگر پرداخته می‌شود.

۵-۱ ارزیابی کارایی

به‌منظور انجام ارزیابی آزمایشگاهی در محیط پژوهشکدهٔ فضای مجازی دانشگاه شهید بهشتی، عملیات عضویت، تولید سهم، رمزگذاری، رمزگشایی، تولید و بازشناسی امضاء، از هفت گوشی هوشمند (نکسوس ۵، هواوی P8، ایسوس زنفون ۳، هواوی هانور ۸، سامسونگ +S8، نوت ٤ و نوت ۵) با امکان اتصال به اینترنت استفاده شده است. مشخصات توابع رمزگذاری، امضاء و خم بیضوی نیز مشابه بخش شبیه‌سازی‌ها بوده و پیاده‌سازی آن‌ها با استفاده از کتابخانهٔ متن‌باز Themis [۲۷] انجام شده است. استفادهٔ مستقیم از اینترنت و یا ارسال برای دستگاه مجاور نیز به‌صورت تصادفی با احتمال ۵۰٪ و طرح تسهیم راز بیتی (۵، ۳) در نظر گرفته شده است.

چالش درهم‌سازی نیز با همان تابع SHA-512 و با صفر کردن ۱۰ بیت انتهایی درهم شدهٔ پیام، پیاده‌سازی شده است. زمان انتظار برای شروع چالش نیز مقادیری تصادفی بین ۱۰۰ تا ۲۰۰ میلی‌ثانیه در نظر گرفته شده است. اگرچه در مستندات، سرعت انتقال وای‌فای ۲۵۰ مگابیت بر ثانیه ذکر شده است [۱۹]، اما در آزمون آزمایشگاهی انجام شده این سرعت کمتر بود و هر بستهٔ یک کیلوبایتی (بدون در نظر گرفتن عملیات رمزنگاری و تولید امضاء) از طریق این گوشی‌های هوشمند به‌طور متوسط در زمان ۰/۰٤ میلی‌ثانیه از طریق انتقال وای‌فای منتقل گردید.

کاربـــران برنامه برای تولید بســـته، اقدام به ســـنجش اطلاعـــات مکانی (از طریق GPS) و همچنین میزان شـــدت ســـیگنال‌های وای‌فای موجـــود در محیط (با اســـتفاده از کتابخانه WifiManager در اندروید استودیو) نمودند. این فرایند روی هرکدام از گوشی‌های هوشمند ذکرشده یک‌صد بار اجرا شده است. متوســـط زمان مورد نیاز برای انجام هریـــک از هفت فرایندِ عضویت و تولیـــد کلید، رمزگذاری، رمزگشـــایی، امضاء، تصدیق هویت (با بررســـی امضاء)، تولید سهم و بازیابی بسته برحسب میلی‌ثانیه روی بستهٔ داده‌ای به‌اندازه ۲۵۰ کیلوبایت محاسبه گردید. این نتایج در جدول (٤) در کنار مقادر حاصل از شبیه‌ســـازی‌ها نشان داده شده است.

در پیاده‌سازی‌های آزمایشـــگاهی با تابع درهم‌ساز و گوشی‌های ذکرشـــده به ازای چالشی با صفر شدن تعداد ۱۰ بیت، حداکثر و میانگین زمان لازم برای شـــروع چالش هم‌ســـازی از زمان درخواست مشـــارکت‌کننده تا دریافت پارامترها از ســـرگروه نیز به ترتیب برابـــر ۰/۱۸ و ۰/۱۲ میلی‌ثانیه اندازه‌گیری شـــده است. حداکثر و میانگین زمان موردنیاز برای حل این چالش در گوشـــی‌های هوشـــمند حاضـــر در گـــروه نیز به ترتیـــب برابـــر ٤۲/۲۳ و ۲۲/٦٥ میلی‌ثانیه اندازه‌گیری شـــده اســـت. بنابراین نسبت زمان شـــروع چالش به حل آن به‌طور تقریبی در حالت بیشـــینه برابـــر ۲۳٥=۰/۱۸÷٤۲/۲۳ و در حالـــت متوســـط برابـــر ۱۸۹=۰/۱۲÷۲۲/٦٥ اســـت. واضح است که این نسبت‌ها با افزایش تعداد بیت‌های چالش بســـیار بیشـــتر می‌شود. در ارزیابی‌های آزمایشـــگاهی میانگین زمان انتقال بسته‌های سنجیده شـــده برابر ۲۸۲/۸ میلی‌ثانیه و در بدترین حالت برابر ٤۸۰/۸ میلی‌ثانیه محاسبه گردید.

۵-۲ ارزیابی امنیتی

ابتـــدا دو مورد از اولین چالش‌هـــای امنیتی مربوط به سرگروه‌ها یعنی ســـرگروه کنجکاو و سرگروه بدخواه را تشریح می‌کنیم. در مورد سرگروه کنجکاو، با توجه به رمزی شـــدن اطلاعات سنجیده شده با کلید عمومی خدمت‌دهنده، سرگروه امکان کشـــف اطلاعات و محتوای آن‌ها را ندارد. در مورد سرگروه بدخواه نیز اگر سرگروهی اقدام به تولید و ارسال بسته‌های جعلی در گروه نماید، چون این بسته‌ها درنهایت توسط خدمت‌دهنده شناسایی می‌شوند، عضویت او باطل‌شـــده و گروهی که ایجاد کرده از بین می‌رود. در ادامهٔ این بخش با توجه به تهدیدات امنیتی مطرح‌شـــده در جدول (۱) و مـــدل تهدیدات مطرح‌شـــده در بخش ۳-۳ به بررسی و تحلیل امنیتی روش پیشنهادی پرداخته می‌شود.

۱) **شـــنود**: با توجه به این‌که در طرح پیشنهادی برای ارتباط بیـــن اعضای گروه از هر دو روش ارتباط وای‌فای و ارتباط اینترنتی استفاده می‌شود و زمان ارسال بسته‌ها و ســـهم‌ها کاملاً در اختیار اعضاء اســـت، ایـــن حمله نیز برای مهاجم بســـیار پیچیده و پرهزینه خواهد بود، چرا که باید همهٔ بســـترهای ارتباطی اینترنت و وای‌فای را شـــنود و تمام بســـته‌ها را دخیره نمایـــد. بنابراین مهاجم می‌تواند روی شنود بخشی از شبکه ســـرمایه‌گذاری کند. به‌علاوه ازآنجاکه محتوای بسته‌ها از ابتدا توسط مشارکت‌کننده با کلید عمومیِ خدمت‌دهنده رمزی می‌شود، پس تنها توسط خدمت‌دهنده قابل بازیابی خواهد بود. بنابراین سرگروه یا شـــنود کنندگان خارجی حتی با جمع‌آوری تعداد کافی از بســـته‌ها قادر به کشف محتویات آن‌ها نخواهند بود و حل این مسئله وابسته به پیچیدگی الگوریتم رمزگذاری و امنیت آن است.

۲) **تولید** و ارســـال بســـتهٔ جعلی: در روش پیشنهادی هیچ یک از اعضاء (مولد بســـته، سرگروه، اعضای گروه و خدمت‌دهنده) قادر به تولید بستهٔ جعلی نیستند. تولیدکنندهٔ بستهٔ ســـنجشِ جمعی نمی‌تواند بستهٔ جعلی بسازد چراکه توسط سرگروه‌ها شناسایی‌شده و در فهرست سیاه قرار می‌گیرد (گام ٦ از الگوریتم (۱)). سرگروه نمی‌تواند بستهٔ جعلی تولید کند، چرا که اگر این بستهٔ جعلی به خدمت‌دهنده برسد و سرگروه نتواند مولد بسته را معرفی نماید، عضویت خودش لغو می‌شـــود (گام ۱۳ از الگوریتم (۲)). ازآنجاکه سهم‌های تولید شـــده توسط سرگروه‌ها امضاء می‌شوند،

اعضـــای گروه نیز توانایی تولید ســـهم جعلی را ندارند. با توجه این‌که در فرایند تولید کلید معرفی‌شده، خدمت‌دهنده کلید خصوصی اعضاء را نـــدارد، او نیز نمی‌تواند به‌جای آن‌ها بسته تولید و امضاء نماید.

۳) گمنامی: درروش پیشـــنهادی گمنامیِ کاربر به‌طور کامل در بین اعضای گروه حفظ می‌شـــود و خدمت‌دهنده امکان شناســـایی کاربر مولد بسته را ندارد و فقط می‌داند که عضو کدام گروه اســـت. هم‌گروهی‌ها و اعضای گروه نیز حتی با جمع‌آوری تمام ســـهم‌ها قـــادر به بازیابی و یا شناسایی مولد بســـته نخواهند بود، پس گمنامی در میان اعضای گروه حفظ می‌شـــود. به‌علاوه ساختار DTN باعث ایجاد تأخیر در فرایند ارسال بسته‌ها می‌شود. این ساختار ماننـــد روش‌های تأخیـــری تصادفی مطرح‌شـــده در [۱۸] می‌تواند باعث افزایش سطح گمنامی کاربران شود.

۴) کارایی: مشارکت بیشـــتر باعث افزایش کارایی در روش‌های مشارکتی می‌شـــود [۲۵، ۲۶]. همان‌گونه که در بخش شبیه‌سازی‌ها مشاهده شـــد، افزایش تعداد کاربران علاوه بـــر افزایش تعداد مشـــارکت‌کنندگان در ســـنجش جمعـــی، باعث کاهش زمان ارســـال بســـته‌ها و در نتیجه کاهش زمان پاسخ به درخواست‌ها می‌گردد. سازوکارهای تشـــویقی و افزایش اعتبار تعریف‌شـــده، اعضای گروه و مشـــارکت‌کنندگان را به اســـتفاده از منابع خود در فرایند سنجش جمعی و همچنین تبادل بسته‌ها تشویق می‌کند.

۵) منع خدمت: با وجود ســـازوکار چالش هم‌سازی بین اعضای گروه و سرگروه‌ها و همچنین وجود زمان تصادفی برای شـــروع این چالش، احتمال انجـــام حملات منع خدمت از ســـوی آن‌ها برای به مخاطره انداختن ســـرگروه‌ها کمتر می‌شود. از سوی دیگر، امکان ارسال سهم جعلی نیز توسط اعضاء وجود ندارد چراکه هر عضو گروه به‌محض دریافت سهم، ابتدا اصالت آن و امضای سرگروه را کنترل می‌کند.

۶) ارســـال بسته و ســـهم تکراری: با توجه به ماهیت شـــبکه‌های DTN این امر ممکن اســـت اتفاق افتد اما چون درنهایت این بســـته‌ها برای خدمت‌دهنده ارسال می‌شوند، امکان شناسایی آن‌ها توسط خدمت‌دهنده وجود دارد. این شناسایی و همچنین وجود فهرست‌های خاکستری و سیاه، روش پیشـــنهادی را در مقابل حملات منع خدمت با روش تکرار بسته، مقاوم می‌نماید.

۷) تبانی کاربران و اعضای گروه: ازآنجاکه کاربران به‌صورت نیمه-مطمئن هستند، فرض می‌شود امکان تبانی آن‌هـــا نیز با یکدیگر وجـــود دارد. اما با توجه به این‌که هر بستهٔ سنجیده شـــده باید از کانال سرگروه‌ها عبور کند و ســـهم تولید شده توسط آن‌ها امضاء شـــود، امکان تبانی تنها با وجود سرگروه بدخواه امکان‌پذیر خواهد بود. اما با توجه به آنچه در بخش دریافت و بازیابی بسته‌ها (۳-٤-٤) توضیح داده شد، این امر نیز میسر نخواهد شد.

۸) تبانی خدمت‌دهنده و ســـرگروه: چون سرگروه‌ها ثابت نیستند و در طول فرایند سنجش جمعی به‌مرورزمان با توجه به روش‌هـــای رأی‌گیری محرمانه در داخل گروه تغییر می‌کنند، این کار نیـــز عملاً به معنای تبانی با تک‌تک کاربران حاضر در گروه اســـت. برای تحقق چنین تبانی‌ای خدمت‌دهنـــده باید اطلاعات مکانی، هویتی و محرمانهٔ تمام افراد گروه را بشناسد. لذا حفظ حریم خصوصی مکان در مقابـــل این خدمت‌دهنده که چنین اطلاعاتی از اعضاء دارد، بی‌معنی می‌شود.

۹) تغییر و دســـت‌کاری اعتماد: بـــا توجه به امضای گواهی‌های هر گروه توســـط خدمت‌دهنده، امکان تغییر و دســـت‌کاری امتیاز گروه‌ها بدون داشـــتن کلید خصوصی خدمت‌دهنده وجود ندارد.

۱۰) اخلال در فرایند انتخاب سرگروه: همان‌گونه که در بند انتهای بخش ۳-۳-۱ اشـــاره شد، روش پیشنهادی از الگوریتم اجماع RAFT برای انتخاب ســـرگروه اســـتفاده می‌کند. در این روش بـــرای ایجاد اختلال در روند انتخاب سرگروه باید بیش از یک‌سوم اعضای گروه بدخواه باشند. برای کســـب نتیجهٔ بهتر می‌توان از سایر روش‌های اجماع ماننـــد روش‌های بازگشـــتی که امنیت روش پیشـــنهادی را مســـتقل از بحث انتخاب ســـرگروه می‌نماید، اســـتفاده

نمود. یا بـا کمک روش گراف‌های جهـت‌دار بدون دور[۲۶] (DAG-Base) مقیاس‌پذیری و سـرعت روش پیشنهادی را افزایش داد. البته ذکر جزئیات این موارد خارج از حوصلهٔ این نوشتار است.

۱۱) **اخلال در تعداد اعضـای گروه:** مهاجم نمی‌تواند روی تعداد اعضـای گروه و درنتیجه بـر میزان گمنامی کاربران تأثیرگذار باشد. اعضای گروه با توجه به خواست و علاقه‌مندی‌های خود وارد گروه می‌شـوند و ارتباط بین آن‌ها و سـایر اعضای طرح پیشنهادی، وابسته به منابع و سلیقهٔ خودشان است. بنابراین اگر مهاجمان با دستگاه‌های متعـدد و منابع نامتناهی نیز وارد گروهی شـوند، اگر در فرایند ارسال بسته‌ها شرکت نکنند، امتیاز گروه موردنظر تغییری نمی‌کند. البته با همکاری مثبت باعث افزایش امتیاز گروه می‌شـوند. هرچند خـود این همکاری بـرای فرایند سنجش جمعی بسیار ایده‌آل است، اما مهاجمان می‌توانند بعد از بالا بردن امتیـاز کاذب گروه‌ها آن‌ها را ترک کرده و سایر کاربران را در انتخاب گروه ایده‌آل خود به چالش کشـانند. برای حل این مشـکل نیز سازوکارهای تشویقی بازخورد پذیر و امتیازات پویا توصیه می‌شود [۲۸].

در ادامـه دو مورد امنیتی که در نتایج آزمایشـگاهی محاسبه‌شده بیان می‌شود.

الف) یک مهاجم پیش از افشـای هویـت خود، حداکثر قادر به تولید چند بسـتهٔ جعلی است. همان‌طور که در نتایج ارزیابی‌های آزمایشگاهی بیان شد، میانگین زمان لازم برای ارسـال بسـته‌ها برابر ۲۸۲/۸ میلی‌ثانیه و در بدترین حالت برابر ٤٨٠/٨ میلی‌ثانیه اسـت. بنابراین به‌طور متوسط پس از گذشت این زمان، بستهٔ جعلی مهاجم توسط خدمت‌دهنده شناسـایی و لغو عضویت می‌شـود. ازآنجاکه در طول این مدت، مهاجم برای حل هر چالش درهم‌سازی به‌طور متوسط ۲۲/٦٥ میلی‌ثانیـه زمان صرف می‌کند، لـذا مهاجم پیش از افشای هویت خود به‌طور متوسط می‌تواند $65/22^{(ms)}÷8/282^{(ms)}$ بسته ارسـال نماید. این مقدار در بدترین حالت برابر $65/22^{(ms)}÷8/480^{(ms)}=23/21$ خواهد بود.

ب) فرض کنید مهاجم توسـط خدمت‌دهنده شناسایی نشـود. همان‌طور که در بخش شبیه‌سـازی‌ها محاسـبه شـد، میانگین زمـان لازم برای حل چالش درهم‌سـازی برابر ۲۲/٦٥ میلی‌ثانیه اسـت و مهاجم باید برای هر بستهٔ ارسـالی به طور متوسـط این مقدار زمان را صرف کند. بنابرایـن اگر فرض کنیـم مهاجم قصد ارسـال یک هزار بسـتهٔ جعلی را دارد، باید تعداد یک هزار بار این چالش را حل نماید. از سـوی دیگر اگر زمـان تصادفی انتظار برای شـروع چالش نیز به‌طور متوسـط برابـر ۱۵۰ میلی‌ثانیه فرض شـود. مهاجم برای ارسـال هر بسـته باید حدود $150^{(ms)}+22/65^{(ms)}=172/65^{(ms)}<173^{(ms)}$ میلی‌ثانیـه صبـر کند. به‌علاوه ازآنجاکه سـرگروه‌ها بسته تکراری دریافت نمی‌کنند، بنابراین مهاجم باید برای تولید هر بسته عملیات امضاء و رمزنگاری را انجام دهد. همان‌طور که در جدول (٤) مشـاهده می‌شـود این مقادیر به طور متوسط برابر ۲/٦٤ و ۱٦/٦۳ میلی‌ثانیه است. هرچند مجموع زمان انجام ایـن دو فرایند کمتر از ۱۷۳ میلی‌ثانیه اسـت، اما مصرف انرژی و حافظهٔ خاص خود را دارد. بنابراین برای ارسـال یک هزار بسته، مهاجم به‌طور متوسط به ۱۷۳۰ ثانیه (حدود ۲۹ دقیقه) زمان احتیاج دارد (اما به دلیل آن‌که سرگروه‌ها تنها مأمور به گرفتن بسـته از یک عضو نیستند، این زمان قطعاً بیشتر است). البته لازم به ذکر است مهاجمان معمولاً علاقه‌ای به‌صرف هزینه‌های زیاد برای حملات کم‌اهمیت از خود نشان نمی‌دهند [۲۹، ۳۰].

۵-۳ مقایسهٔ روش پیشـنهادی با روش‌های مطرح شده در [۱۵]، [۱۷] و [۱۸]

در این بخش به مقایسـهٔ روش پیشـنهادی با تعدادی از روش‌های مشـارکتی مطرح‌شـده در ادبیـات پرداخته می‌شـود. نتایج نشان می‌دهند طرح پیشـنهادی علاوه بر محیط شبیه‌سازی، در محیط آزمایشگاهی نیز به‌خوبی کار می‌کند. با توجه به شبیه‌سازی‌های انجام‌شده و ارزیابی‌های آزمایشـگاهی، ابتدا به ارائهٔ نتایج مربوط به میانگین زمان اجرای هرکدام از بخش‌های طرح پیشنهادی در مقایسه با

26- Directional Acyclic Graph Base (DAG-Base)

جدول ۴: متوسط زمان (میلی‌ثانیه) اجرای بخش‌های مختلف روش پیشنهادی در مقایسه با روش‌های [۱۷] و [۱۸] در محیط شبیه‌سازی و ارزیابی‌های آزمایشگاهی.

فرایند	محیط					
	شبیه‌سازی			ارزیابی آزمایشگاهی		
	[۱۷]	[۱۸]	پیشنهادی	[۱۷]	[۱۸]	پیشنهادی
رمزنگاری	۱۸/۷۲	–	۳/۳۲	۹۰/۳۲	–	۱۶/۶۳
رمزگشایی	۱۱/۸۶	–	۱/۱۵	۷۹/۵۸	–	۵/۲۵
امضاء	۰/۵۲	–	۰/۵۳	۲/۶۱	–	۲/۶۴
تصدیق امضاء	۰/۹۲	–	۰/۸۴	۴/۱۳	–	۴/۲۱
تولید سهم	–	۲۴/۷۶	۱۹/۰۷	–	۷۴/۳۷	۵۷/۲۹
بازیابی بسته	–	۱۰/۸۹	۰/۸۶	–	۴۳/۵۲	۳/۲۱
مدت زمان ارسال	۲۷۳/۷	۲۵۲/۴	۲۵۳/۴	۲۸۹/۵	۲۹۳/۴	۲۸۲/۸

بخش‌های موجود در طرح‌های مشارکتی [۱۷] و [۱۸] برای یکصد بار اجرا پرداخته می‌شود. در این مقایسه، اندازهٔ بسته‌های ارسالی همان ۲۵۰ کیلوبایت و اندازهٔ کلید و نوع توابع رمزگذاری مشابه طرح پیشنهادی در نظر گرفته شده و برای همهٔ طرح‌ها تعداد مشارکت‌کنندگان در انتقال بسته برابر k=5 فرض شده است. برای طرح [۱۷] تعداد ویژگی‌های موردنیاز برای رمزگذاری p=3 در نظر گرفته شده است (با توجه به این‌که نویسندگان در [۱۷] به‌کفایت این مقدار اعتقاد دارند). نتایج به‌دست آمده در جدول (٤) نشان داده شده است. بخش‌هایی که در برخی خانه‌های جدول با خط تیره مشخص‌شده‌اند، به‌معنای عدم وجود این بخش‌ها در آن روش است. به‌عنوان مثال، طرح پیشنهاد شده در [۱۷] فاقد مراحل تسهیم راز و تولید سهم است.

همان‌طور که مشاهده می‌شود، زمان لازم برای فرایند رمزگذاری و رمزگشایی در طرح پیشنهادی از زمان لازم در [۱۷] کمتر است. دلیل این اختلافِ زمان ازآنجا است که در روش پیشنهادی [۱۷] فرایند رمزگذاری و رمزگشایی یک مرتبه روی بسته‌ها با الگوریتم رمز RSA و p مرتبه با زنجیرهٔ بلوک رمزی و الگوریتم AES 27 (AES-CBC) روی بلوک‌های به‌دست‌آمده از بسته انجام می‌شود. به‌علاوه یک‌بار هم عملیات رمزگذاری و رمزگشایی روی مقدار پوشش مکانی انجام می‌شود. اما در روش پیشنهادی یک‌بار عملیات رمزگذاری/رمزگشایی و یک‌بار فرایند تولید سهم و بازیابی آن‌ها انجام می‌شود.

در روش تسهیم راز مطرح‌شده در [۱۸] برای بازیابی راز از سهم‌های دریافت‌شده باید $n(r-1)$ بار عمل جمع و $(n-r)(r-1)$ بار عمل ضرب انجام شود. بنابراین فرایند بازیابی بستهٔ راز در روش پیشنهادی به‌مراتب از روش مطرح شده در [۱۸] کمتر است. به‌علاوه وجود بسته‌های جعلی در [۱۸] برای ایجاد گمنامی و لزوم شناسایی آن‌ها توسط خدمت‌دهنده این زمان را افزایش داده است. در ضمن از آنجاکه در روش [۱۸] فرایند رمزگذاری و رمزگشایی وجود ندارد و گمنامی با تولید بسته‌های جعلی ایجاد می‌شود، وجود گره‌های بدخواه می‌تواند امنیت این روش را با چالش روبرو کند. به همین دلیل و همچنین عدم وجود سازوکار لازم برای ارسال پاسخ به گره‌ها، این روش برای کاربردهای سنجش جمعی استفاده نمی‌شود و در شبکه‌های حسگر بی‌سیم به کار گرفته شده است. اما از آنجاکه در روش مطرح‌شده در [۱۸] اندازهٔ هر سهم تولید شده برابر با $1/r$ اندازهٔ پیام اولیه است، ترافیک این روش از سایر روش‌ها کمتر است. جدول (۵) برخی تفاوت‌های کمّی روش پیشنهادی و روش‌های مطرح‌شده در [۱۵]، [۱۷] و [۱۸] را نشان می‌دهد.

۶- نتیجه‌گیری

رویکرد تحمل تأخیر، امکان استفادهٔ کارآمد از پهنای باند را فراهم می‌کند، به‌طوری‌که کاربران می‌توانند هر زمان خطوط اینترنتی مناسب داشتند، اقدام به ارسال سهم‌هایی که در اختیار دارند، نمایند. وجود گروه‌های متحرک با تعداد اعضای متفاوت باعث ایجاد گمنامی کاربران شده است. از سوی دیگر با توجه به نوع ارتباط بین اعضاء که

27- AES-Cipher Block Chaining (AES-CBC)

جدول ۵: مقایسهٔ کمّی روش پیشنهادی با روش‌های [۱۵]، [۱۷] و [۱۸].

مشخصه / روش	[۱۵]	[۱۷]	[۱۸]	روش پیشنهادی
کاربرد	شبکهٔ خودرویی	فرایندهای مبتنی بر مکان	شبکهٔ حسگر بی‌سیم	سنجش جمعی و فرایندهای مبتنی بر مکان
بیشترین سربار محاسباتی	امضای حلقوی و افزایش بار محاسباتی در خودروها	رمزنگاری مبتنی بر ویژگی	محاسبات و بازیابی سهم‌ها	عضویت و تولید کلید
تحمل تأخیر	ندارد	ندارد	دارد	دارد
نوع محرمانگی	گمنامی	پوشش مکانی و گمنامی	گمنامی	گمنامی
کارساز قابل‌اعتماد	دارد	ندارد	دارد	ندارد
هزینه بازیابی سهم	ندارد	ندارد	ضرب و جمع	OR
مدیریت کلیدها (تعداد کلیدهای نگهداری شده توسط هر عضو)	کلید خصوصی هر عضو و مجموعه‌ای از کلیدهای مربوط به اعضای گروه	کلیدهای هر عضو برای رمزنگاری اولیه و کلیدهای تصادفی رمزنگاری‌های زنجیره بلوک رمزی	کلیدهای عضو	کلیدهای عضو
بیشترین محاسبات	گره مولد	گره مولد	گره مولد	سرگروه

می‌تواند با استفاده از وای‌فای و یا اینترنت باشد، هم‌گروهی لزوماً به معنای هم‌مکانی نبوده و روش پیشنهادی باعث حفظ حریم‌خصوصی مکان مشارکت‌کنندگان می‌شود. با توجه به تحلیل‌های انجام شده، گام عضویت و رمزگذاری که برای حفظ امینت داده‌ها در روش پیشنهادی به کار می‌رود، یکی از مراحل زمان‌بر این روش است. این فرایند برای هر دستگاهِ صادق، عملاً یک‌بار برای عضویت و یک‌بار به ازای هر بار سنجش اتفاق می‌افتد. از آنجاکه بارِ پردازشی بخش‌های پرتکرارِ روش پیشنهادی کم است، اجرای آن برای دستگاه‌هایی با توان پردازشی و منابع محدود، مناسب است. در روش پیشنهادی ممکن است گرهی با اینترنت ارتباط مستقیم نداشته باشد و یا به دلیل نگرانی از مصرف انرژی، تمایلی به اتصال از خود نشان ندهد. در چنین مواردی استفاده از روش تسهیم راز باعث افزایش کارایی روش پیشنهادی شده و سهم‌های تولید شده از مسیرهای دیگری به خدمت‌دهنده می‌رسد. این تحمل تأخیر برای کاربردهای سنجش جمعی که در آن‌ها رویکردهای برخط وجود ندارد، بسیار مناسب است. نتایج شبیه‌سازی‌ها و ارزیابی‌های آزمایشگاهی نشان می‌دهد طرح پیشنهادی توانایی حفاظت از حریم خصوصی مشارکت‌کنندگان در فرایند سنجش جمعی را دارد. به‌علاوه با توجه به استفاده از ترکیب روش رمزگذاری و ساختار تسهیم راز، محرمانگی داده‌ها حفظ می‌شود و روش پیشنهادی تحمل ایجاد تأخیر به دلیل خرابی، قطع اتصال یا عدم دخالت اعضای گروه‌ها در ارسال سهم را دارد.

به‌عنوان پیشنهاد برای کارهای آتی، می‌توان بر روش‌های تسهیم رازی که در آن‌ها اندازهٔ سهم‌ها از راز کوچک‌تر است تمرکز نمود و ترافیک شبکه را کاهش داد. این کار سبب کاهش تأخیر در روش پیشنهادی می‌شود. گام دوم در کارهای آینده تغییر روش انتخاب سرگروه است، که در بخش تحلیل امنیتی تعدادی از آن‌ها بیان شد.

مراجع

[1] Kouicem, D. E., Bouabdallah, A., Lakhlef, H. "Internet of Things Security: A Top-Down Survey," Computer Networks, vol. 141, pp. 199-221, 2018.

[2] Vergara-Laurens, I. J., Jaimes, L. G., Labrador, M. A. "Privacy-Preserving Mechanisms for Crowdsensing: Survey and Research Challenges," IEEE Internet of Things Journal Special Issue on Privacy Issues in The Internet of Things, vol. 4, no. 4, pp. 855-869, 2016.

[3] Mao, Y., Zhou, C., Ling, Y., Lloret, J. "An Optimized Probabilistic Delay Tolerant Network (DTN) Routing Protocol Based on Scheduling Mechanism for Internet of Things

(IoT)," Sensors, vol. 19, no. 2, pp. 243-259, 2019.
[4] Quercia, D., Leontiadis, I., McNamara, L., Mascolo, C., Crowcroft, J. "Spotme if You Can: Randomized Responses for Location Obfuscation on Mobile Phones," 31th IEEE International Conference on Distributed Computing Systems (ICDCS), pp. 363–372, 2011.
[5] Alikhani, N., Moghtadaiee, V., Sazdar, A. M., Ghorashi, S. A. "A Privacy Preserving Method for Crowdsourcing in Indoor Fingerprinting Localization." 8th IEEE International Conferences Computer Knowledge Engineering. (ICCKE), pp. 58-62, 2018.
[6] Ojha, G., Singh, R., Shukla, A. "Improved Identity Anonymization Using Hashed-TOR Network," Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 185-192, 2016.
[7] Xiao, M., Wu, J., Zhang, S., Yu, J. "Secret-Sharing-Based Secure User Recruitment Protocol for Mobile Crowdsensing," IEEE Conference on Computer Communications (INFOCOM), pp. 1-9, 2017.
[8] Vergara-Laurens, I. J., Mendez, D., Jaimes, L. G., Labrador, M. "A-PIE: An Algorithm for Preserving Privacy, Quality of Information, and Energy Consumption in Participatory Sensing Systems," Pervasive and Mobile Computing, vol.32, pp. 93–112, 2016.
[9] Meng, G., Liu, Y., Zhang, J., Pokluda, A., Boutaba, R. "Collaborative security: A Survey and Taxonomy," ACM Computing Surveys (CSUR), vol. 48, pp. 1–42, 2015.
[10] Castro-Jul, F., Diaz-Redondo, R. P., Fernandez-Vilas, A. "Collaboratively Assessing Urban Alerts in Adhoc Participatory Sensing," Computer Networks, vol. 131, pp. 129–143, 2018.
[11] Loomba, R., Shi, L., Jennings, B., Friedman, R., Kennedy, J., Butler, J. "Energy-Aware Collaborative Sensing for Multiple Applications in Mobile Cloud Computing," Sustainable Computing: Informatics and Systems, vol. 8, pp. 47–59, 2015.
[12] Lyu, L., Law, Y. W., Erfani, S. M., Leckie, C., Palaniswami, M. "An Improved Scheme for Privacy-Preserving Collaborative Anomaly Detection," IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 1–6, 2016.
[13] Santos, F., Humbert, M., Shokri, R., Hubaux, J. P., "Collaborative Location Privacy with Rational Users," International Conference on Decision and Game Theory for Security, pp. 163–181, 2011.
[14] Hashem, T., Datta, S., Islam, T. U., Ali, M. E., Kulik, L., Tanin, E. "A Unified Framework for Authenticating Privacy Preserving Location Based Services," Second International ACM Workshop on Managing and Mining Enriched Geo-Spatial Data, pp. 13-18, 2015.
[15] Mei, Y., Jiang, G., Zhang, W., Cui, Y. "A Collaboratively Hidden Location Privacy Scheme for Vanets," International Journal of Distributed Sensor Networks, vol. 10, no. 3, 2014.
[16] Petrillo, A., Pescape, A., Santini, S. "A Collaborative Approach for Improving the Security of Vehicular Scenarios: The Case of Platooning," Computer Communications, vol. 122, pp. 59–75, 2018.
[17] Dargahi, T., Ambrosin, M., Conti, M., Asokan, N. "ABAKA: A Novel Attribute-Based k-Anonymous Collaborative Solution for LBSs," Computer Communications, vol. 85, pp. 1-13, 2016.
[18] Wang, N., Fu, J., Li, J., Bhargava, B. K. "Source-Location Privacy Protection Based on Anonymity Cloud in Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 100-114, 2019.
[19] Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., Ott, J. "Security and Privacy in Device-to-Device (d2d) Communication: A Review," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1054–1079, 2017.
[20] Zhao, C., Yang, S., Yang, X., McCann, J. A. "Rapid, User-Transparent, and Trustworthy Device Pairing for D2D-Enabled Mobile Crowdsourcing," IEEE Transactions on Mobile Computing, vol. 16, no 7, pp. 2008–2022, 2017.
[21] Shokri, R. Freudiger, J., Hubaux, J.P. "A Unified Framework for Location Privacy," Technical Report, 2010.
[22] Huang, D., Ma, X., Zhang, S. "Performance Analysis of the RAFT Consensus Algorithm for Private Blockchains," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 172-181, 2020.
[23] Nguyen, G. T., Kim, K. "A Survey About Consensus Algorithms Used in Blockchain," Journal of Information processing systems, vol. 14, no. 1, pp. 101-128, 2018.
[24] Noureddine, M. A., Fawaz, A. M., Hsu, A., Guldner, C., Vijay, S., Başar, T., Sanders, W. H. "Revisiting Client Puzzles for State Exhaustion Attacks Resilience," 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 617-629, 2019.
[25] Zhan, Y., Xia, Y., Zhang, J. "Incentive Mechanism in Platform-Centric Mobile Crowdsensing: A One-to-Many Bargaining Approach," Computer Networks, vol. 132, pp. 40–52, 2018.
[26] Restuccia, F., Das, S. K., Payton, J. "Incentive Mechanisms for Participatory Sensing: Survey and Research challenges," ACM Transactions on Sensor Networks (TOSN), vol. 12, no. 2, pp. 13–50, 2016.
[27] Liu, R., Liu, H., Kwak, D., Xiang, Y., Borcea, C., Nath, B., Iftode, L. "Themis: A Participatory Navigation System for Balanced Traffic Routing," IEEE Vehicular Networking Conference (VNC), pp. 159-166, 2014.
[28] Bergemann, D., Välimäki, J. "Dynamic Mechanism Design: An Introduction," Journal of Economic Literature, vol. 57, no. 2, pp. 235-74, 2019.
[29] Yan, Q., Yu, F. R. "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing," IEEE Communications Magazine, vol. 53, no. 4, pp. 52–59, 2015.
[30] Laurens, V., El-Saddik, A., Nayak, A. "Requirements for Client Puzzles to Defeat the Denial of Service and the Distributed Denial of Service Attacks," International Arabian Journal of Information Technology, vol. 3, no. 4, pp. 326–333, 2006.