بازارهای برق محلی حافظ حریم خصوصی تفاضلی با قابلیت شخصی‌سازی سطح حفاظت از حریم خصوصی

میلاد حسین‌پور[1]، محمودرضا حقی‌فام[2]، استاد

۱- دانشکده مهندسی برق و کامپیوتر- دانشگاه تربیت مدرس- تهران- ایران

m.hoseinpour@modares.ac.ir

۲- دانشکده مهندسی برق و کامپیوتر- دانشگاه تربیت مدرس - تهران- ایران

haghifam@modares.ac.ir

چکیده: انتشار عمومی داده‌های بازارهای برق محلی گستره‌ی وسیعی از مزایای اقتصادی، فنی، و اجتماعی را به دنبال دارد. همچنین، دسترسی عمومی به این داده‌ها گامی اساسی در راستای شفافیت در بازارهای برق محلی و ارتقای ماهیت رقابتی آن‌ها محسوب می‌شود. با این حال، مشترکین حساس به حریم خصوصی دغدغه‌ی افشای اطلاعات خصوصی خود را از طریق انتشار داده‌های خروجی بازارهای برق محلی دارند. این مقاله، با استفاده از مفهوم حریم خصوصی تفاضلی، در پی طراحی مکانیسمی برای بازارهای برق محلی است، که به شکلی قابل اثبات حفاظت از حریم خصوصی شرکت‌کنندگان در بازار را تضمین کند، و همچنین تمایلات حریم خصوصی آن‌ها را نیز مد نظر قرار دهد. در گام نخست، ماهیت تصادفی مورد نیاز حریم خصوصی تفاضلی با استفاده از الگوریتم گرادیان افزایشی نویزی در فرایند بهینه‌سازی مساله تسویه بازار تعبیه می‌شود. سپس به منظور ایجاد امکان شخصی‌سازی سطح حفاظت از حریم خصوصی، مکانیسمی مبتنی بر نمونه‌برداری در سطح مجموعه‌داده‌ی ورودی مساله تسویه بازار پیشنهاد می‌گردد. در بخش مطالعات عددی، تاثیر پارامترهای حریم خصوصی تفاضلی بر خروجی‌های مساله تسویه بازار ارزیابی می‌شود. همچنین، مصالحه‌ی ذاتی میان حفاظت از حریم خصوصی و رفاه اجتماعی در مساله تسویه بازار نیز تحت سیاست‌های مختلف حفاظت از حریم خصوصی مورد توجه قرار می‌گیرد.

واژه های کلیدی: بازارهای برق محلی، طراحی مکانیسم، حریم خصوصی داده، حریم خصوصی تفاضلی

نوع مقاله: پژوهشی

تاریخ ارسال مقاله : ۱۴۰۲/۳/۲۶

تاریخ پذیرش مقاله : ۱۴۰۳/۴/۱۵

نام نویسنده‌ی مسئول : دکتر محمودرضا حقی‌فام

نشانی نویسنده‌ی مسئول : ایران – تهران – خیابان جلال آل‌احمد – پل نصر– دانشگاه تربیت مدرس – دانشکده‌ی مهندسی برق و کامپیوتر

۱-مقدمه

تحول دیجیتال در سیستم‌های توزیع و به دنبال آن جمع‌آوری، ذخیره‌سازی، مدیریت، تحلیل، و استفاده از کلان‌داده‌ها منجر به تسهیل ادغام منابع انرژی پراکنده با سیستم‌های توزیع و بهبود عملکرد این سیستم‌ها می‌گردد. منابع اولیه این کلان‌داده‌ها اغلب عبارتند از داده‌های بهره‌برداری حاصل از ابزارهای اندازه‌گیری سطح شبکه، داده‌های بازار برق حاصل از تسویه‌ی بازار و تراکنش‌های مالی، و داده‌های مشترکین

حاصل از کنتورهای هوشمند [۱]. دسترسی به این داده‌ها توسعه‌ی ابزارهای قدرتمند تصمیم‌گیری مبتنی بر مدل‌های یادگیری ماشین را در حوزه شبکه‌های توزیع در پی خواهد داشت [۲]. الگوریتم‌ها و مدل‌های توسعه‌یافته بر مبنای این داده‌ها منجر به ارتقای بهره‌وری، قابلیت اطمینان، و امنیت سیستم‌های توزیع خواهند شد. همچنین، انتشار این داده‌ها و به اشتراک‌گذاری آن‌ها منشاء فواید متعددی برای جامعه، از جمله توسعه عدالت اجتماعی، شفافیت، و بهبود خدمات، خواهد بود [۳].

انتشار عمومی داده‌های بازارهای برق محلی، مانند داده‌های اقتصادی و مبادلات انرژی الکتریکی، گستره‌ی وسیعی از مزایای اقتصادی، فنی، و اجتماعی را به دنبال دارد. با این حال، دغدغه‌ی حریم خصوصی خاستگاه انگیزه‌ای برای رفتار راهبردی شرکت‌کنندگان در بازارهای برق و یا حتی خروج آن‌ها از بازارهای برق محسوب می‌شود. در همین راستا، بازارهای برق حافظ حریم خصوصی، با اطمینان‌بخشی به مشترکین در زمینه‌ی حفاظت از داده‌های حساس آن‌ها، نقشی محوری در ترغیب مشترکین برای مشارکت در بازارهای برق محلی ایفا می‌کنند. همچنین، قوانینی نیز در جهت الزام به انتشار داده‌های بازارهای برق وجود دارد. به عنوان نمونه، قانون اقدامات شفافیت در اتحادیه اروپا بازارهای برق را، با هدف افزایش سطح نفوذ منابع انرژی تجدیدپذیر و تسهیل ورود آن‌ها به بازار، ملزم به انتشار داده‌های خروجی بازار می‌کند. در واقع، دسترسی به داده‌های بازار برق سیگنال‌های اقتصادی مفیدی را برای مشترکین و طرف‌های ثالث به منظور ارزیابی بازار و سرمایه‌گذاری در بخش منابع انرژی پراکنده فراهم می‌کند. بنابراین، مشترکین تمایل بیشتری برای سرمایه‌گذاری در بخش منابع انرژی پراکنده، به ویژه منابع انرژی تجدیدپذیر ، و مشارکت در بازارهای برق محلی خواهند داشت، که خود منجر به افزایش سیالیت بازار و ارتقای ماهیت رقابتی آن می‌گردد [۴]. علاوه بر این، انتشار خروجی‌های مساله تسویه بازار، ابزاری کارآمد در جهت نظارت مستمر بر عملکرد بازار و کشف موقعیت‌های انحصارطلبانه تلقی می‌شود [۵].

با این وجود، این مجموعه‌داده‌های جزئی و غنی می‌توانند منجر به نقض حریم خصوصی شرکت‌کنندگان در بازار شوند. انتشار این مجموعه‌داده‌ها می‌تواند اطلاعات حساسی را درباره‌ی شرکت‌کنندگان در بازار آشکار کند، و منجر به پیامدهای نامطلوبی برای این افراد شود؛ پیامدهایی که درصورت عدم مشارکت آن‌ها در بازار کمتر محتمل بوده‌اند. برای مثال، مبادلات انرژی الکتریکی در بازار، الگوی مصرف شرکت‌کنندگان در بازار را آشکار می‌کند، که می‌تواند با هدف نظارت بر رفتار و تبلیغات بیش از اندازه شخصی‌سازی‌شده توسط شرکت‌های بازاریابی مورد استفاده قرار گیرد. از طرف دیگر، قوانین مرتبط با حفاظت از حریم خصوصی، مانند مقررات عمومی حفاظت از داده‌ها (GDPR)[1] در اتحادیه اروپا و قانون حفظ حریم خصوصی نیویورک (NYPA)[2]، بازارهای برق را ملزم به رفتاری مسئولانه در قبال حریم خصوصی شرکت‌کنندگان در بازار می‌کند [۶]. بر اساس این قوانین، حفاظت از حریم خصوصی بایستی مبتنی بر طراحی[3] (PbD) باشد. این بدان معناست که تمامی نهادها و مجموعه‌هایی که داده‌های افراد را در اختیار دارند بایستی حریم خصوصی را از ابتدا در توسعه و طراحی خدمات خود مد نظر قرار دهند، بطوری که حفاظت از حریم خصوصی بخشی از ماهیت وجودی آن خدمات باشد. در رویکرد PbD جنبه‌های فنی سیستم به نحوی طراحی می‌شود که افشای اطلاعات و استفاده‌ی غیرمجاز از داده‌های افراد تقریبا غیرممکن می‌گردد، و در صورت بروز چنین اتفاقی نیز پیامدهای آن بسیار اندک و قابل چشم‌پوشی خواهد بود.

با توجه به مطالب فوق، انتشار عمومی داده‌های خروجی مساله تسویه بازار بایستی ضمن تضمین حفاظت از حریم خصوصی شرکت‌کنندگان در بازار صورت گیرد. هدف این مقاله طراحی یک بازار برق محلی است که به شکلی قابل اثبات حفاظت از حریم خصوصی شرکت‌کنندگان در بازار را تضمین، و در عین حال ارزش کاربردی داده‌های خروجی بازار را به منظور انتشار عمومی حفظ کند. علاوه بر این، در این مقاله امکان شخصی‌سازی سطح حفاظت از حریم خصوصی بر حسب میزان حساسیت و تمایل شرکت‌کنندگان در بازار فراهم می‌شود. در راستای این اهداف، این مقاله از مفهوم حریم خصوصی تفاضلی[4] بهره می‌گیرد، که چارچوبی برای استدلال کمی درباره‌ی حریم خصوصی و ریسک افشای اطلاعات خصوصی شرکت‌کنندگان در بازار را فراهم می‌کند. ایده‌ی اصلی در حریم خصوصی تفاضلی، تعبیه‌ی مقدار تنظیم‌شده‌ای نویز تصادفی در محاسبه‌ی مورد نظر است. مکانیسم‌های حریم خصوصی تفاضلی بطور معمول مصالحه‌ای میان سطح حفاظت از حریم خصوصی افراد حاضر در یک مجموعه‌داده و دقت محاسبات بر روی آن مجموعه داده را ایجاد می‌کنند. علاوه بر این، برخلاف سایر روش‌های حفاظت از حریم خصوصی، حریم خصوصی تفاضلی در برابر تمامی پساپردازش‌ها مقاوم است و هیچگونه پیش‌فرضی درباره‌ی توان محاسباتی و اطلاعات جانبی طرف‌های متخاصم ندارد.

۲-پیشینه تحقیق و نوآوری‌های مقاله

کارهای تحقیقاتی متعددی در حوزه‌ی رمزنگاری برای حفاظت از داده‌های مشترکین در بازارهای برق ارائه شده است. در مرجع [۷] یک پروتکل غیرمتمرکز مبتنی بر محاسبه چندجانبه امن[5] (MPC) برای بازارهای برق محلی مطرح می‌شود. در پروتکل پیشنهادی، تعیین مقادیر تسویه بازار و محاسبه‌ی قیمت تسویه بازار به صورت امن و بدون آشکارسازی داده‌های شرکت‌کنندگان در بازار انجام می‌پذیرد. در راستای نگرانی‌های امنیتی مرتبط با سیستم‌های انرژی مبادلاتی، یک پلتفرم مبادلات بازاری مبتنی بر رمزنگاری در مرجع [۸] پیشنهاد می‌شود. در پلتفرم پیشنهادی، اطلاعات مالی شرکت‌کنندگان در بازار در فرایند تعاملات بازاری با استفاده از الگوی رمزنگاری Paillier حفاظت می‌گردد. علاوه بر این، راهکار حفاظتی پیشنهادی در برابر هرگونه تزریق اطلاعات نادرست مقاوم است. در مرجع [۹] ، یک مکانیسم مناقصه‌ی دوجانبه‌ی

امن برای بازارهای برق محلی ارائه شده است. در راستای عدم شناسایی و حفاظت از حریم خصوصی شرکت‌کنندگان در بازار، هویت اصلی آن‌ها حذف و اطلاعات مالی آن‌ها نیز توسط رمزنگاری Paillier حفاظت می‌گردد. مرجع [۱۰] یک پلتفرم مبادلات انرژی P2P حافظ حریم خصوصی را ارائه می‌دهد. اطلاعات خصوصی شرکت‌کنندگان در بازار، شامل قیمت پیشنهادی فروشندگان و میزان تقاضای خریداران، بر مبنای رمزنگاری هم‌ریختی[۶] (HE) حفاظت شده‌اند. به منظور توسعه‌ی منابع انرژی پراکنده و تمرکززدایی از سیستم قدرت، مرجع [۱۱] چارچوبی حافظ حریم خصوصی برای بازارهای برق توزیع‌شده ارائه می‌دهد. در چارچوب پیشنهادی، عامل‌های شرکت‌کننده در بازار قادر هستند در غیاب یک نهاد واسط و به کمک یک دستورالعمل رمزنگاری نوین، قیمت و توان مبادلاتی دوجانبه را با سایر عامل‌ها تعیین کنند. مکانیسم پیشنهادی بر اساس یک بازی غیرهمکارانه توسعه یافته است، و مشخصه‌های مطلوب در طراحی مکانیسم را مورد بررسی قرار می‌دهد. مرجع [۱۲] نیز به نگرانی‌های حریم خصوصی در بازارهای برق همتا به همتا[۷] (P2P) و عدم تمایل مشترکین برای مشارکت در پلتفرم‌های انرژی مبادلاتی، به دلیل این نگرانی‌ها، می‌پردازد. مدل پیشنهادی در این مقاله بر اساس یک بازار برق P2P روز-پیش رو مبتنی بر MPC توسعه یافته و از برنامه‌های پاسخگویی بار نیز در راستای افزایش سطح مبادلات انرژی بهره می‌جوید. در مرجع [۱۳]، تحلیلی کلی از چالش‌های امنیت داده و حریم خصوصی در بازارهای برق P2P آتی ارائه شده است. در ادامه، مطالعات موردی برای ساختارهای متفاوت بازارهای برق P2P صورت می‌گیرد، و آسیب‌پذیری این ساختارها در مقابل حملات گوناگون ارزیابی می‌شود.

در گروه دیگری از کارهای تحقیقاتی، روش‌های گمنام‌سازی داده‌ها برای حفاظت از حریم خصوصی داده‌های شرکت‌کنندگان در بازارهای برق اتخاذ شده است. در مرجع [۱۴]، روشی مبتنی بر ناشناسی مرتبه‌ی- k برای حفاظت از حریم خصوصی مشترکین خانگی پیشنهاد شده است. بطور مشخص، این مقاله بر روی هزینه‌ی تامین حریم خصوصی، شامل پیامدهای محیط زیستی و هزینه‌ی تحمیلی بر شرکت‌کنندگان در بازار، تحت گمنام‌سازی داده‌ها تمرکز می‌کند. مرجع [۱۵] یک مکانیسم تسویه بازار حافظ حریم خصوصی برای ممانعت از شناسایی و کسب اطلاعات توسط رقبا از یکدیگر ارائه می‌کند. در این مقاله، واحدهای تولیدی و نهادهای تامین‌کننده‌ی بار داده‌های واقعی خود را پیش از گزارش به بهره‌بردار بازار در یک عدد تصادفی ضرب می‌کنند، تا نوعی پوشش و گمنام‌سازی برای اطلاعات خود ایجاد نمایند. مرجع [۱۶] اثرگذاری حریم خصوصی شرکت‌کنندگان در بازارهای برق P2P را بر نقطه‌ی تعادل بازار بررسی می‌کند. مدل پیشنهادی در این مقاله بر اساس یک بازی غیرهمکارانه توسعه داده شده است، که در آن همتاها اطلاعات حقیقی خود را با افزودن ماهیت تصادفی برای تعامل با سایر همتاها گزارش می‌کنند. در واقع، ایجاد ماهیت تصادفی محلی و فرد-محور امکان شخصی‌سازی حریم خصوصی را برای همتاها فراهم می‌کند. همچنین، مدل پیشنهادی وجود و یکتایی نقطه‌ی تعادل بازار تحت قیود حریم خصوصی را اثبات می‌کند، و رابطه‌ای را نیز برای هزینه‌ی حریم خصوصی ارائه می‌دهد. تضمین حریم خصوصی در این گروه از مقالات قابل اتکا و اثبات نیست. علاوه‌براین، این راهکارها در برابر اطلاعات جانبی و حملات بازیابی[۸] آسیب‌پذیر هستند.

همانطور که مشاهده می‌کنیم اغلب کارهای پژوهشی فوق بر روی امنیت داده‌ها و منع هرگونه دسترسی به آن‌ها متمرکز هستند، و از راهکارهای مبتنی بر رمزنگاری، مانند HE و MPC بهره می‌گیرند. این در حالی است، که هدف اصلی این مقاله ترویج به اشتراک‌گذاری و انتشار داده‌های خروجی بازارهای برق محلی، ضمن حفاظت از حریم خصوصی شرکت‌کنندگان در بازار، است. در دسته‌ای دیگر از کارهای پژوهشی برای محافظت از حریم خصوصی در بازارهای برق از راهکارهای گمنام‌سازی داده‌ها[۹] و مبهم‌سازی[۱۰] آن‌ها استفاده شده است. با این حال، راهکارهای اتخاذ شده تضمینی قابل اثبات برای حفاظت از حریم خصوصی ارائه نمی‌دهند و در برابر اطلاعات جانبی آسیب‌پذیر هستند. در همین راستا، تمرکز این رساله بر روی خلاء تحقیقاتی موجود در حوزه بازارهای برق حافظ حریم خصوصی تفاضلی خواهد بود.

مهم‌ترین نوآوری‌های این مقاله را می‌توان به صورت زیر خلاصه نمود:

- در این مقاله یک مکانیسم حافظ حریم خصوصی تفاضلی برای بازارهای برق محلی پیشنهاد می‌شود که ضمن تعیین خروجی بهینه‌ی تقریبی مساله تسویه بازار، تضمین می‌کند که این خروجی‌ها تقریبا هیچ‌گونه اطلاعاتی را در مورد شرکت‌کنندگان در بازار افشا نخواهند کرد. همچنین، ماهیت حفاظتی راهکار پیشنهادی منفعت داده‌های خروجی بازارهای برق محلی را نیز حفظ خواهد کرد.
- در این مقاله قرارگیری خروجی‌های مساله تسویه بازار در ناحیه مجاز و همچنین کیفیت خروجی‌های بازار تحت ماهیت تصادفی ناشی از قیود حریم خصوصی تفاضلی تضمین می‌شود. در این راستا، بر خلاف راهکارهای مبتنی بر افزودن مستقیم نویز به خروجی‌های مساله تسویه بازار، که ممکن است به پاسخ‌های نامطلوب و غیرمجاز منجر شود، رفاه اجتماعی مساله تسویه بازار در ایجاد ماهیت تصادفی مورد نیاز مکانیسم‌های حافظ حریم خصوصی تفاضلی مورد توجه قرار می‌گیرد.
- در این مقاله امکان شخصی‌سازی سطح حفاظت از حریم خصوصی شرکت‌کنندگان در بازار برق با توجه به ناهمگونی تمایلات حریم خصوصی شرکت‌کنندگان در

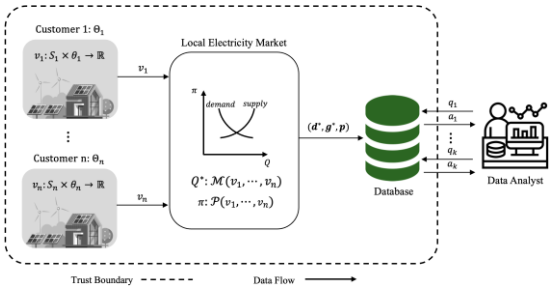
بازار برق فراهم می‌شود. شخصی‌سازی سطح حفاظت از حریم خصوصی مانع از تامین حفاظت مازاد برای برخی از شرکت‌کنندگان در بازار خواهد شد. این رویکرد ارتقای کیفیت خروجی‌ها و کارایی بازار را به دنبال خواهد داشت.

در ادامه، در بخش ۳ به بیان چارچوب مساله و مدل تهدید مورد نظر خواهیم پرداخت. بخش ۴ به مرور مبانی حریم خصوصی تفاضلی اختصاص دارد. در بخش ۵ مدل پیشنهادی را معرفی می‌کنیم. بطور مشخص در این بخش، مکانیسم تسویه بازار و همچنین تعیین پرداختی‌های بازار در چارچوب حریم خصوصی تفاضلی تشریح می‌گردد. در ادامه، مکانیسم پیشنهادی، مبتنی بر نمونه‌برداری در سطح مجموعه‌داده‌ی ورودی، به منظور شخصی‌سازی سطح حفاظت از حریم خصوصی شرکت‌کنندگان در بازار معرفی می‌گردد. نتایج عددی و تفسیر آن‌ها در بخش ۶ ارائه می‌شوند. در بخش ۷، به بیان نتایج و کارهای آتی خواهیم پرداخت.

۳-چارچوب مساله

مساله‌ی تسویه‌ی بازار برق مورد نظر در این مقاله دارای ساختاری متمرکز است، و در یک شبکه انرژی محلی با مجموعه‌ای از شرکت‌کنندگان Ω، شامل تولیدکنندگان Ω^p و مصرف‌کنندگان Ω^c، تعریف می‌شود. به منظور پرهیز از نمایه‌های اضافی، روابط پیش رو، به جز مواردی که صریحا بیان شده است، بدون تمایز میان تولیدکننده و مصرف‌کننده، برای یک عامل شرکت‌کننده‌ی در بازار ارائه می‌شود. در این مساله، مجموعه‌ای از تصمیم‌های اجتماعی ممکن $S = \prod_{i=1}^{n} S_i$ وجود دارد، که در آن $S_i \subset R^{|s_i|}$ دامنه‌ی تصمیم‌های محلی (انفرادی) عامل i را نشان می‌دهد. بنابراین، تصمیم‌های محلی $s\_i \in S_i$ مصرف‌کننده‌ی i و تولیدکننده‌ی i، به ترتیب، با میزان تقاضای $d_i \in [\underline{d_i}, \overline{d_i}]$ و میزان تولید $g_i \in [\underline{g_i}, \overline{g_i}]$ مشخص می‌شوند.

هر عامل $i \in \Omega$ دارای اطلاعات خصوصی $\theta_i \in \Theta_i$ است، که نوع عامل نامیده می‌شود، و بیانگر ترجیحات عامل i بر روی تصمیم‌های اجتماعی S است. در ازای نوع θ_i، ترجیحات عامل i از طریق تابع ارزش‌گذاری $v_i: S \times \theta_i \to \mathbb{R}$ ارزیابی می‌شود، که $v_i(s, \theta_i)$ ارزش تصمیم $s \in S$ را برای عامل i منعکس می کند. همچنین، از آنجاکه در بازارهای برق ارزش‌گذاری عامل i تنها به تصمیم‌های محلی خودش وابسته است، در ادامه $v_i(s, \theta_i) = v_i(s_i, \theta_i)$ خواهد بود. تابع ارزش‌گذاری مصرف‌کننده‌ی i منفعت ناشی از میزان تقاضای d_i را منعکس می‌کند، و به‌صورت $v_i(d_i, \theta_i) = U_{i,\theta_i}(d_i)$ نشان داده می‌شود. همچنین، برای تولیدکننده‌ی i نیز تابع ارزش‌گذاری معادل قرینه‌ی هزینه‌ی تولید توان اکتیو g_i است، به‌صورت $v_i(g_i, \theta_i) = -C_{i,\theta_i}(g_i)$ نشان داده می‌شود. لازم به ذکر است که $U_{i,\theta_i}(\cdot)$ و $C_{i,\theta_i}(\cdot)$، به ترتیب، تابع منفعت مصرف‌کننده‌ی i و تابع هزینه‌ی تولیدکننده‌ی i هستند. علاوه‌براین، به منظور سهولت مدل سازی‌ها و بدون خلل در اعتبار آن‌ها،



شکل ۱: نمای کلی از چارچوب مساله تسویه بازار برق حافظ حریم خصوصی تفاضلی و مدل تهدید

توابع ارزش‌گذاری شرکت‌کنندگان در بازار را نرمالیزه می‌کنیم، به‌نحوی که در محدوده‌ی $[0,1]$ قرار می‌گیرند.

شکل ۱ نمایی کلی از چارچوب مساله را نمایش می‌دهد. همانطور که مشاهده می‌شود، هر عامل $i \in \Omega$ تابع ارزش‌گذاری خود v_i را به بازار گزارش می‌کند. با توجه به پروفایل ارزش‌گذاری شرکت‌کنندگان در بازار $v = (v_i)_{i\in\Omega}$، بهره‌بردار بازار از یک الگوریتم تخصیص $\mathcal{M}(v)$ برای تعیین مقادیر تولیدی و مصرفی در تسویه بازار، $d^* = (d_i^*)_{i\in\Omega^c}$ و $g^* = (g_i^*)_{i\in\Omega^p}$، و یک الگوریتم تعیین پرداختی‌ها $\mathcal{P}(v)$ برای تعیین پرداختی‌های شرکت‌کنندگان در بازار $p = (p_i)_{i\in\Omega}$ استفاده خواهد کرد. در بازارهای برق، الگوریتم تخصیص $\mathcal{M}(v)$ از طریق بیشینه‌سازی تابع رفاه اجتماعی $\mathrm{sw}(v,s) = \sum_{i\in\Omega} v_i(s_i)$ تحت قیود فنی شرکت‌کنندگان در بازار و قید تسویه بازار، مقادیر تسویه بازار را تعیین می‌کند. با جایگذاری توابع ارزش‌گذاری مصرف‌کنندگان و تولیدکنندگان در $\mathrm{sw}(v,s)$، الگوریتم تخصیص $\mathcal{M}(v)$ برابر است با:

$$(d^*, g^*) \in \arg\max_{d,g} \sum_{i\in\Omega^c} U_{i,\theta_i}(d_i) - \sum_{i\in\Omega^p} C_{i,\theta_i}(g_i) \qquad (۱)$$

$$s.t.$$

$$\underline{d_i} \le d_i \le \overline{d_i}\ , \forall i \in \Omega^c \qquad (۲)$$

$$\underline{g_i} \le g_i \le \overline{g_i}\ , \forall i \in \Omega^p \qquad (۳)$$

$$\sum_{i\in\Omega^p} g_i - \sum_{i\in\Omega^c} d_i = 0, \qquad (۴)$$

که در آن قیود (۲) و (۳) محدودیت‌های میزان تقاضای مصرف‌کنندگان و عرضه‌ی مصرف‌کنندگان را نمایش می‌دهند. همچنین، قید (۴) به تعادل عرضه و تقاضا در تسویه بازار اشاره دارد.

بدین ترتیب، خروجی مساله تسویه بازار آرایه‌ای مانند (d^*, g^*, p) است که در یک پایگاه داده ذخیره می‌شود. با توجه به شکل ۱، تحلیل‌گر داده که نمادی از تمامی طرف‌های ثالث، مانند تامین‌کنندگان خدمات بهره‌وری انرژی، سیاست‌گذاران، پژوهشگران، و زیرساخت‌های شهری، است، خواهان دسترسی به این پایگاه داده حاوی خروجی‌های مساله تسویه بازار است.

هدف یک تحلیل‌گر داده غیرمتخاصم این است که از طریق طرح پرسمان‌ها و دریافت پاسخ‌های مربوطه، آماره‌ها و اطلاعات مفیدی را در مورد جامعه آماری شرکت‌کنندگان در بازار کسب کند. با این حال، با ایجاد دسترسی آزاد و انتشار عمومی داده‌های خروجی مساله تسویه بازار، طرف‌های متخاصم نیز قادر به بهره‌گیری از این مجموعه‌داده‌ها به منظور

کسب اطلاعات و استنتاج در سطح فردی خواهند بود. لازم به ذکر است که مفهوم طرف‌های متخاصم علاوه بر بازیگران خارج از بازار به بازیگران داخل بازار نیز که به خروجی‌های انتشاریافته‌ی مساله تسویه بازار دسترسی دارند و در پی ارتقاء مزیت رقابتی خود هستند، اطلاق می‌گردد. همچنین، طرف‌های متخاصم ممکن است که لزوما از بازیگران بازار نباشند، و هر فرد، نهاد، یا مجموعه‌ای با هدف کسب اطلاعات شرکت‌کنندگان در بازار در سطح فردی را می‌توان در این نقش متصور شد. این در حالی است که شرکت‌کنندگان در بازار نسبت به افشای اطلاعات خصوصی خود حساسیت دارند، و هیچ‌گونه پیش‌فرضی درباره اهداف گوناگون طرف‌های ثالث ندارند. در واقع، انتشارهای آماری خروجی‌های مساله تسویه بازار، شرکت‌کنندگان در بازار را در معرض ریسک نقض حریم خصوصی توسط طرف‌های ثالث متخاصم قرار می‌دهد. بطوری که، فرد متخاصم با مشاهده‌ی خروجی‌های مساله تسویه بازار در پی استخراج نوع شرکت‌کنندگان در بازار $\theta' \in \Theta$ است، که در صورت موفقیت، نوع استخراج‌شده‌ی θ' منطبق بر نوع حقیقی θ شرکت‌کنندگان در بازار خواهد بود. به بیان ریاضی، می‌توان هدف کلی فرد متخاصم را در یافتن پاسخی برای مساله‌ی بهینه‌سازی پیش رو منعکس نمود:

$$\min_{\theta' \in \Theta} \left\| \operatorname*{argmax}_{s \in S} \mathrm{sw}(\theta', s) - s^* \right\|, \qquad (۵)$$

که در آن s^* خروجی منتشرشده‌ی مساله‌ی تسویه بازار، $s \in S$ متغیرهای تصمیم‌گیری در مساله‌ی تسویه بازار، $\theta' \in \Theta$ نوع شرکت‌کنندگان در بازار، $\mathrm{sw}(\cdot)$ تابع رفاه اجتماعی، و $\|\cdot\|$ معیار فاصله را منعکس می‌کند. همانطور که در مساله‌ی بهینه‌سازی فوق مشاهده می‌شود، شخص متخاصم در تلاش است که $\theta' \in \Theta$ را چنان تعیین کند که خروجی مساله‌ی تسویه بازار حاصل از آن دارای کمترین فاصله از خروجی مشاهده‌شده‌ی s^* باشد. در واقع، می‌توان نتیجه گرفت که امکان استخراج اطلاعات خصوصی شرکت‌کنندگان در بازار و نقض حریم خصوصی آنان، به واسطه‌ی انتشارهای آماری خروجی‌های بازار وجود دارد. بنابراین، طراحی یک مکانیسم تسویه بازار حافظ حریم خصوصی، که تضمین کند هر عاملی خارج از محدوده‌ی اعتماد قادر به کسب اطلاعاتی در سطح افراد و نقض حریم خصوصی آنان نیست، امری ضروری محسوب می‌شود.

۴-مروری بر مبانی حریم خصوصی تفاضلی

حریم خصوصی تفاضلی یک راهکار شناخته‌شده برای کمی‌سازی و بیان ریاضی مفهوم حفاظت از حریم خصوصی محسوب می‌شود. گذشته از این، بر خلاف سایر روش‌های حفاظت از حریم خصوصی که امکان به اشتراک‌گذاری داده‌ها را فراهم نمی‌کنند، حریم خصوصی تفاضلی امکان انتشار عمومی خروجی‌های یک محاسبه، مانند مساله تسویه بازار برق، را ضمن حفاظت از حریم خصوصی افراد حاضر در آن محاسبه فراهم می‌کند. به بیان دیگر، حریم خصوصی تفاضلی ایجاد تعادل میان هزینه‌های ناشی از نقض حریم خصوصی و مزایای به اشتراک‌گذاری داده‌ها را ممکن می‌سازد. مبنای این روش تعیین یک کران بالا برای میزان حساسیت خروجی یک الگوریتم به داده‌ی ورودی هر یک از افراد است. به بیان دقیق‌تر، حریم خصوصی تفاضلی اطمینان حاصل می‌کند که خروجی یک الگوریتم با حضور و یا عدم حضور هر یک از افراد تقریبا بدون تغییر باقی می‌ماند، و به واسطه‌ی همین عدم حساسیت، توانایی طرف‌های متخاصم برای استنتاج در مورد داده‌های افراد را محدود می‌کند[۱۷]. ایده‌ی اصلی برای دستیابی به چنین مشخصه‌ای، ایجاد نوعی آشفتگی در الگوریتم از طریق افزودن مقدار کالیبره‌شده‌ای نویز تصادفی است، تا بتوان نقش هر یک از افراد در الگوریتم را پنهان نمود. در ادامه، تعریف رسمی حریم خصوصی تفاضلی و تفسیر آن را ارائه خواهیم کرد.

تعریف ۱ (حریم خصوصی تفاضلی). برای $0 \le \epsilon \ge 0$ و $0 \le \delta \le 1$، الگوریتم تصادفی $\mathcal{M}: \mathcal{X}^n \to \mathcal{R}$ را $(\epsilon, \delta) - DP$ گویند اگر برای هر زوج از مجموعه داده‌های همسایه $x \sim x' \in \mathcal{X}^n$ (x و x' تنها در یک عنصر با یکدیگر تفاوت دارند) و برای هر زیرمجموعه‌ای از محدوده خروجی الگوریتم $S \subseteq \mathcal{R}$، رابطه‌ی زیر برقرار باشد [۱۸]:

$$\Pr[\mathcal{M}(x) \in S] \le e^{\epsilon}.\Pr[\mathcal{M}(x') \in S] + \delta. \qquad (۶)$$

تعریف فوق در مورد رفتار الگوریتم $\mathcal{M}$ است، و این تضمین را می‌دهد که داده‌ی هیچ یک از افراد تاثیر قابل توجهی در خروجی الگوریتم نخواهد داشت. به بیان دیگر، هنگامی که یک الگوریتم $(\epsilon, \delta) - DP$ (حافظ حریم خصوصی تفاضلی با پارامتر ϵ و δ) بر روی دو مجموعه داده‌ی همسایه اجرا می‌گردد، توزیع‌های احتمال حاصل بر روی محدوده‌ی خروجی الگوریتم بسیار به یکدیگر نزدیک خواهند بود، و میزان این نزدیکی از طریق کران بالای نسبت این توزیع‌های احتمال، یعنی e^{ϵ}، و پارامتر افزایشی δ منعکس می‌گردد.

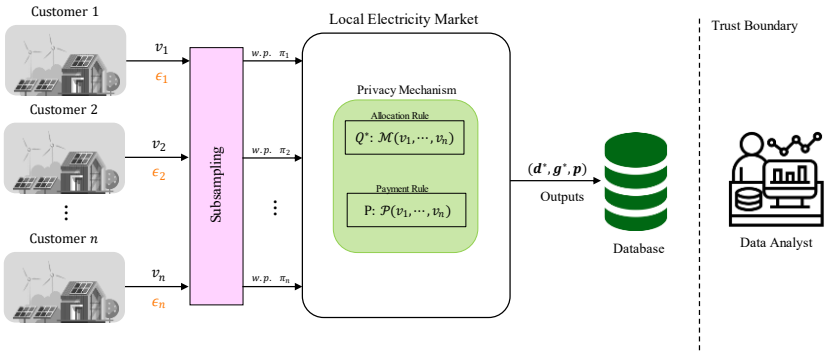
یکی از روش‌های افزودن ماهیت تصادفی به یک محاسبه و یا الگوریتم، اضافه کردن نویز به خروجی مورد نظر است. این خروجی می‌تواند یک عدد حقیقی و یا یک بردار از اعداد حقیقی باشد. در این بخش به معرفی مکانیسم گاوسی[11] برای دستیابی به حریم خصوصی تفاضلی می‌پردازیم. پیش از آن، بایستی مفهوم مهمی تحت عنوان حساسیت سراسری[12] (GS) را تعریف کنیم. می‌توان گفت که نویز مورد نیاز برای تامین شرایط حریم خصوصی تفاضلی بر اساس مقدار حساسیت سراسری الگوریتم تعیین می‌گردد.

تعریف ۲ (حساسیت ℓ_2-). برای تابع $f: \mathcal{X}^n \to \mathbb{R}^k$، حساسیت-$\ell_2$ بر روی هر زوج از مجموعه داده‌های همسایه $x \sim x' \in \mathcal{X}^n$ برابر است با

$$\Delta(f) = \max_{x \sim x' \in \mathcal{X}^n} \|f(x) - f(x')\|_2, \qquad (۷)$$

که در آن $\|\cdot\|_2$ نشانگر نرم-ℓ_2 است [۱۸].

با توجه به عنوان مکانیسم گاوسی، نویز مورد نیاز در این مکانیسم از طریق توزیع احتمال گاوسی ایجاد می‌گردد. ایده‌ی اصلی مکانیسم



شکل ۲: نمای کلی از مدل پیشنهادی برای بازارهای برق حافظ حریم خصوصی تفاضلی با قابلیت شخصی‌سازی سطح حفاظت از حریم خصوصی

گاوسی، که در دسته‌ی مکانیسم‌های نویز-افزایشی قرار دارد، افزودن مقدار تنظیم‌شده‌ای نویز تصادفی با توزیع احتمال گاوسی به خروجی محاسبه‌ی مورد نظر است. در ادامه تعریف رسمی مکانیسم گاوسی ارائه می‌گردد.

تعریف ۳ (مکانیسم گاوسی). اگر $f: \mathcal{X}^n \to \mathbb{R}^k$، آنگاه مکانیسم گاوسی به شکل زیر تعریف می‌گردد:

$$\mathcal{M}(x) = f(x) + (Y_1, \cdots, Y_k), \qquad (۸)$$

که Y_iها اعداد تصادفی مستقل با توزیع احتمال $\mathcal{N}(0, 2\ln(1.25/\delta)\Delta_2^2/\epsilon^2)$ هستند. با افزودن اعداد تصادفی Y_i به خروجی محاسبه مورد نظر $f(x)$، خروجی‌های حاصل $(\epsilon, \delta) - DP$ خواهد بود [۱۹].

۵-مدل پیشنهادی

در این بخش به معرفی مکانیسمی عمومی مبتنی بر نمونه‌برداری برای دستیابی به حریم خصوصی شخصی‌سازی‌شده می‌پردازیم. مبنای این مکانیسم تعبیه‌ی دو منبع تصادفی در محاسبات مورد نظر است: (۱) نمونه‌برداری تصادفی غیریکنواخت در سطح مجموعه‌داده، که در آن احتمال عضویت داده‌های هر فرد به تمایلات حریم خصوصی‌اش و آستانه‌ی حفاظت یکنواخت عمومی وابسته است، و (۲) ماهیت تصادفی برای تامین حریم خصوصی تفاضلی مجموعه‌داده‌ی نمونه‌برداری‌شده، که در آن پارامتر حریم خصوصی ϵ به t وابسته است. با ترکیب این دو ماهیت تصادفی، سطح حریم خصوصی مورد نیاز هر فرد حاضر در مجموعه‌داده تامین خواهد شد. شکل ۲ نمایی کلی از عملکرد مکانیسم پیشنهادی برای تحقق حریم خصوصی شخصی‌سازی‌شده را نمایش می‌دهد.

در ادامه‌ی این بخش، ابتدا مکانیسم پیشنهادی به منظور دستیابی به سطحی یکنواخت از حریم خصوصی را ارائه خواهیم نمود. بطور مشخص، مکانیسم‌های پیشنهادی برای تسویه بازار و همچنین تعیین پرداختی‌های بازار را در چارچوب حریم خصوصی تفاضلی معرفی خواهیم نمود. در گام بعدی، راهکار پیشنهادی به منظور شخصی‌سازی سطح حفاظت از حریم خصوصی تشریح می‌گردد.

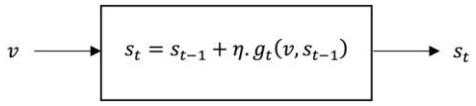
۵-۱- مکانیسم تسویه بازار

همانطور که پیش‌تر اشاره شد، افزودن نویز به شکل مستقیم به خروجی‌های مساله تسویه بازار ممکن است منجر به خروجی‌هایی شود که قیود مساله را نقض می‌کنند. مهم‌تر از آن، به دلیل اینکه تابع هدف مساله به شکلی صریح در فرایند تولید و افزودن نویز لحاظ نشده است، هیچ‌گونه معیاری از میزان نزدیکی مقادیر نویزی تسویه بازار و پرداختی‌ها به مقادیر بهینه آن‌ها وجود ندارد. به عبارتی، عدم توجه به تابع هدف مساله تسویه بازار و قیود مساله بهینه‌سازی در تامین نویز مورد نیاز، عدم کنترل بر روی کیفیت خروجی‌های مساله تسویه بازار را به دنبال دارد. بنابراین، بایستی برای افزودن نویز و دستیابی به حریم خصوصی تفاضلی با ظرافت بیشتری عمل کرد. به همین منظور، در مکانیسم پیشنهادی، با بکارگیری الگوریتم گرادیان افزایشی[۱۳]، ماهیت تصادفی مورد نیاز برای حریم خصوصی تفاضلی را با استفاده از مکانیسم گاوسی، در فرایند تخصیص مقادیر تسویه بازار $\mathcal{M}(v)$ تعبیه می‌کنیم.

بیان ریاضی مساله‌ی تسویه بازار مورد نظر، که در پی حل آن از طریق الگوریتم گرادیان افزایشی هستیم، به صورت زیر خواهد بود:

$$\underset{s \in \mathcal{O}}{\text{argmax}}\ \text{sw}(v, s) = \sum_{i=1}^{n} v_i(s_i). \qquad (۹)$$

برای دستیابی به حریم خصوصی تفاضلی در مکانیسم تسویه بازار پیشنهادی، از مکانیسم حریم خصوصی گاوسی استفاده می‌شود. برای این منظور، بایستی مقدار تنظیم‌شده‌ای نویز با توزیع گاوسی را به قاعده‌ی بروزرسانی متغیرها در هر تکرار از الگوریتم گرادیان افزایشی اضافه کنیم. شکل ۳ بلوک محاسباتی که بایستی، با بکارگیری مکانیسم گاوسی، حافظ حریم خصوصی داده‌های شرکت‌کنندگان در بازار باشد را نمایش می‌دهد. در این بلوک $g_t = \nabla_s \text{sw}(v, s_{t-1})$ و η گام بروزرسانی متغیرها را نشان می‌دهد.



شکل ۳: بروزرسانی متغیرهای تصمیم‌گیری شرکت‌کنندگان در بازار در گام tام

در بلوک شکل ۳، $g_t(v, s_{t-1})$ تنها بخشی از محاسبات است که به داده‌های ورودی v وابسته است. بنابراین، تنها بایستی $g_t(v, s_{t-1})$ را در چارچوب حریم خصوصی تفاضلی محاسبه کنیم. در همین راستا، حساسیت سراسری $g_t(v, s_{t-1})$ برابر است با:

$$\begin{aligned}\Delta &= \max_{v\sim v'\in V^n} \left\|\nabla\left(\mathrm{sw}(v, s_{t-1}) - \mathrm{sw}(v', s_{t-1})\right)\right\|_2 \\ &= \max_{v\sim v'\in V^n} \left\|\nabla\left(\sum_{j\neq i}^{n} v_j + v_i - \sum_{j\neq i}^{n} v_j - v_i'\right)\right\|_2 \\ &= \max_{v\sim v'\in V^n} \|\nabla(v_i - v_i')\|_2.\end{aligned} \quad (10)$$

حال بایستی کران بالایی برای $\|\nabla(v_i - v_i')\|_2$ تعیین گردد. با این حال، چنین کرانی در اغلب موارد با توجه به داده‌های ورودی مساله تسویه بازار وجود ندارد. به همین منظور، برای تعیین حساسیت مورد نیاز از روش برش گرادیان استفاده می‌شود. گرادیان‌ها در هر تکرار الگوریتم، $g_t(v, s_{t-1})$، را با توجه به یک کران دلخواه مانند C محدود می‌سازیم. بنابراین، بردار گرادیان g بایستی با $g/\max(1, \|g\|_2/C)$ جایگزین گردد، که در آن C معیار برش گرادیان‌ها[۱۴] است [۲۰]. بر اثر این شیوه‌ی محدودسازی اندازه‌ی گرادیان‌ها، اگر $\|g\|_2 \leq C$، آنگاه گرادیان g بدون تغییر خواهد ماند. درحالی‌که، اگر $\|g\|_2 \geq C$، با تغییر قیاس گرادیان g اندازه‌ی آن برابر با $\|g\|_2 = C$ خواهد شد. بنابراین، حساسیت $g_t(v, s_{t-1})$، با توجه به نامساوی مثلثی، برابر است با:

$$\begin{aligned}\Delta &= \max_{v\sim v'} \|\nabla \mathrm{sw}(v, s_{t-1}) - \nabla \mathrm{sw}(v', s_{t-1})\|_2 \\ &\leq \max_{v\sim v'} (\|\nabla \mathrm{sw}(v, s_{t-1})\|_2 \\ &\quad - \|\nabla \mathrm{sw}(v', s_{t-1})\|_2) = 2C.\end{aligned} \quad (11)$$

با توجه به اعمال مکانیسم گاوسی، برای اینکه بلوک بروزرسانی متغیرهای تصمیم‌گیری در شکل ۳ حافظ حریم خصوصی تفاضلی با پارامترهای (ϵ', δ') باشد، کافی است نویزی با مقیاس $\sigma \geq \frac{2C}{n\epsilon'}\sqrt{2\ln\left(\frac{1.25}{\delta'}\right)}$ به گرادیان محاسبه‌شده $g_t(v, s_{t-1})$ در هر تکرار اضافه کنیم. الگوریتم ۱ چگونگی پیاده‌سازی مکانیسم تسویه بازار پیشنهادی را نشان می‌دهد. همچنین، شکل ۵ روندنمای نحوه پیاده‌سازی مکانیسم تسویه بازار حافظ حریم خصوصی تفاضلی پیشنهادی از طریق الگوریتم ۱ را نمایش می‌دهد. لازم به ذکر است که خروجی هر حلقه محاسباتی در شکل ۵، s_t، حافظ حریم خصوصی تفاضلی با پارامترهای (ϵ', δ') است. افزون بر این، مطابق گام ۷ در الگوریتم ۱، در صورت عدم قرارگیری متغیرهای تصمیم‌گیری s_t در هر تکرار از الگوریتم پیشنهادی، از نگاشت $\Pi_{\mathcal{O}}(\cdot)$ برای انتقال متغیر مورد نظر به ناحیه مجاز استفاده خواهد شد.

الگوریتم ۱: مکانیسم تسویه بازار پیشنهادی

ورودی‌ها: مجموعه‌ی توابع ارزش‌گذاری شرکت‌کنندگان در بازار $v = (v_i)_{i\in\Omega}$، تابع رفاه اجتماعی $\mathrm{sw}(v, s) = \sum_{i=1}^{n} v_i(s_i)$، مجموعه‌ی پاسخ‌های مجاز $\mathcal{O} \subseteq \mathbb{R}^n$، تعداد تکرار T، گام بروزرسانی η، مقیاس نویز σ، کران گرادیان C.

خروجی‌ها: متغیرهای تصمیم‌گیری شرکت‌کنندگان در بازار در گام T، s_T.

۱: مقداردهی اولیه‌ی s_0 با نقطه‌ای دلخواه در $\mathcal{O}$

۲: **برای هر** $t \in [T]$:

۳: محاسبه‌ی گرادیان تابع رفاه اجتماعی برای هر شرکت‌کننده در بازار $g_t = \nabla_s \mathrm{sw}(v, s_{t-1})$

۴: برش گرادیان با توجه به کران C:

$$g_t^{clip} = \frac{g_t}{max(1, \|g_t\|_2/C)}$$

۵: افزودن نویز:

$$\tilde{g}_t = g_t^{clip} + \mathcal{N}(0, \sigma^2 I_n)$$

۶: بروزرسانی متغیرها:

$$u_t = s_{t-1} + \eta.\, \tilde{g}_t$$

۷: نگاشت متغیرها به ناحیه مجاز $\mathcal{O}$:

$$s_t = \Pi_{\mathcal{O}}(u_t)$$

۸: **پایان حلقه**

۹: **بازگشت** s_T.

الگوریتم ۲: تعیین پرداختی‌های VCG شرکت‌کنندگان در بازار

ورودی‌ها: مجموعه‌ی توابع ارزش‌گذاری $v = (v_i)_{i\in\Omega}$

خروجی‌ها: مقادیر تسویه‌ی بازار $s^* = (d^*, g^*) \in S$ و پرداختی‌های شرکت‌کنندگان در بازار $p = (p_i)_{i\in\Omega}$

۱: مساله‌ی بیشینه‌سازی رفاه اجتماعی را حل کنید:

$$s^* \in \underset{s\in S}{\mathrm{argmax}} \sum_{i\in\Omega} v_i(s_i).$$

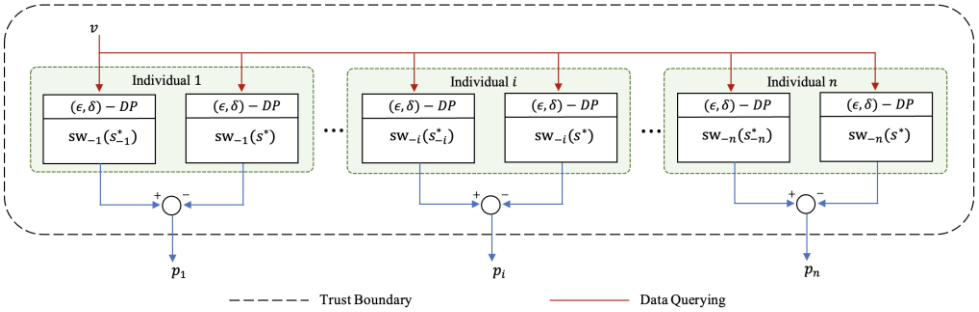
۲: **برای هر** $i \in \Omega$:

۳: پرداختی تخصیص‌یافته به شرکت‌کننده‌ی i را تعیین کنید:

$$p_i(v_i, v_{-i}) = \max_{s\in S} \sum_{j\neq i\in\Omega} v_j(s_j) - \sum_{j\neq i\in\Omega} v_j(s^*).$$

۴: **پایان حلقه**

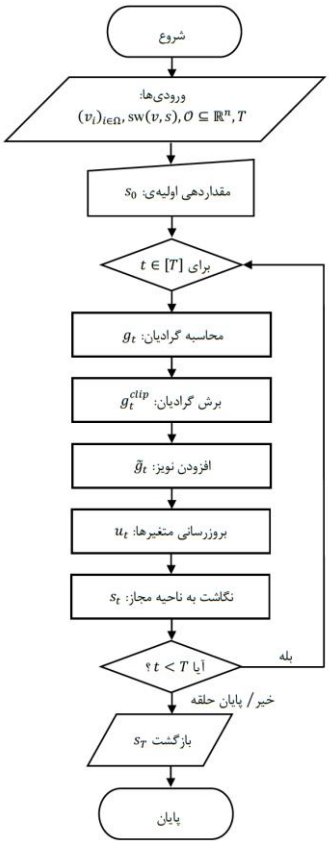
۵: **بازگشت** مقادیر s^* و p.



شکل ۴: نمای کلی از پیاده‌سازی الگوریتم ۳ برای محاسبه پرداخت‌های VCG در چارچوب حریم خصوصی تفاضلی

همانطور که در الگوریتم ۲ مشاهده می‌شود، پرداختی‌های VCG نیز بر اساس محاسباتی بر روی داده‌های افراد تعیین می شوند، بنابراین امکان افشای اطلاعات خصوصی افراد از طریق دسترسی به آن‌ها وجود دارد. به همین دلیل، بایستی با به‌کارگیری حریم خصوصی تفاضلی، از امکان تشخیص و تمایز در پرداختی‌های بازار $p=(p_i)_{i\in\Omega}$ توسط فرد متخاصم جلوگیری شود. مطابق الگوریتم ۲، محاسبه‌ی پرداختی VCG برای شرکت‌کننده‌ی i در بازار تنها نیازمند محاسبه‌ی رفاه اجتماعی در دو حالت است: (۱) رفاه اجتماعی سایر شرکت‌کنندگان در بازار در حالت عدم حضور i در بازار، $\mathrm{sw}_{-i}(s^*_{-i})$، و (۲) رفاه اجتماعی سایر شرکت‌کنندگان در بازار در حالت حضور i در بازار، $\mathrm{sw}_{-i}(s^*)$. بنابراین، برای تضمین حفاظت از حریم خصوصی پرداختی‌های VCG، تنها کافی‌ست که رفاه اجتماعی مطابق الگوریتم ۱ در چارچوب حریم خصوصی تفاضلی محاسبه گردد. لازم به ذکر است، که حاصل ترکیب دو محاسبه‌ی $\mathrm{sw}_{-i}(s^*_{-i})$ و $\mathrm{sw}_{-i}(s^*)$ با استفاده از الگوریتم ۱، بر اساس خاصیت ترکیب‌بندی حریم خصوصی تفاضلی، حافظ حریم خصوصی تفاضلی خواهد بود.

الگوریتم ۳ به محاسبه‌ی پرداختی‌ها تحت حفاظت حریم خصوصی تفاضلی اختصاص دارد. در گام نخست، الگوریتم ۳ اقدام به فراخوانی الگوریتم ۱ با ورودی $v=(v_i)_{i\in\Omega}$ می‌کند و توزیع احتمال خروجی $\mathcal{D}$ را بر روی s^* محاسبه می‌کند، که در ادامه برای محاسبه‌ی مقدار انتظاری رفاه اجتماعی سایر عامل‌ها در حضور عامل $i\in\Omega$ مورد استفاده قرار می‌گیرد، $\mathrm{sw}_{-i}(\mathcal{D})$. آنگاه، برای هر عامل $i\in\Omega$، الگوریتم ۳ با حذف آن عامل پروفایل ارزش‌گذاری $v=(v_j)_{j\in\Omega,j\neq i}$ را به عنوان ورودی الگوریتم ۱ تعیین می‌کند، تا با بهره‌گیری از توزیع احتمال خروجی $\mathcal{D}_{-i}$ بر روی s^*_{-i}، مقدار انتظاری رفاه اجتماعی سایر عامل‌ها را در غیاب عامل i محاسبه کند، $\mathrm{sw}_{-i}(\mathcal{D}_{-i})$. در نهایت، با محاسبه‌ی اختلاف $\mathrm{sw}_{-i}(\mathcal{D})$ از $\mathrm{sw}_{-i}(\mathcal{D}_{-i})$ برای هر عامل $i\in\Omega$ پروفایل مقدار انتظاری پرداختی‌های p شرکت‌کنندگان در بازار محاسبه می‌شود. شکل ۴ چگونگی پیاده‌سازی الگوریتم ۳ و محاسبه‌ی پرداختی‌های VCG در چارچوب حریم خصوصی تفاضلی را نشان می‌دهد.



شکل ۵: روندنمای پیاده‌سازی الگوریتم ۱

۵-۲- مکانیسم تعیین پرداختی‌های شرکت‌کنندگان در بازار

در این مقاله تعیین پرداختی‌های شرکت‌کنندگان در بازار $p=(p_i)_{i\in\Omega}$ بر اساس مکانیسم Vickerly-Clarke-Groves (VCG) صورت می‌گیرد، که در این بخش به چگونگی محاسبه‌ی آن‌ها تحت ملاحظات حریم خصوصی تفاضلی می‌پردازیم. با توجه به الگوریتم ۲، عامل‌ها پروفایل ارزش‌گذاری خود $v=(v_i)_{i\in\Omega}$ را به بهره‌بردار بازار گزارش می‌کنند، و مکانیسم VCG خروجی s^* را در راستای بیشینه‌سازی رفاه اجتماعی شرکت‌کنندگان در بازار انتخاب می‌کند. سپس، مکانیسم میزان پرداختی هر عامل i را بر اساس هزینه‌ی تحمیلی آن بر اجتماع شرکت‌کنندگان در بازار تعیین می‌کند، که معادل اختلاف میان رفاه اجتماعی دیگران در حالت وجود و یا عدم وجود عامل i در مساله تسویه بازار است.

الگوریتم ۳: محاسبه‌ی پرداختی‌های VCG حافظ حریم خصوصی تفاضلی

ورودی‌ها: مجموعه‌ی توابع ارزش‌گذاری $v = (v_i)_{i\in\Omega}$، پارامتر حریم خصوصی ϵ، δ.

خروجی‌ها: مقدار انتظاری پرداختی‌های شرکت‌کنندگان در بازار p.

فراخوانی الگوریتم ۱:
ورودی‌ها: $v = (v_i)_{i\in\Omega}$، ϵ، δ
خروجی‌ها: $s^* \sim \mathcal{D}$
برای هر $i \in \Omega$:
فراخوانی الگوریتم ۲:
ورودی‌ها: $v = (v_j)_{j\in\Omega, j\neq i}$، ϵ، δ
خروجی‌ها: $s^*_{-i} \sim \mathcal{D}_{-i}$
$\mathsf{SW}_{-i}(\mathcal{D}_{-i}) = \mathbb{E}_{r\sim\mathcal{D}_{-i}}\left[\sum_{j\neq i} v_j(r)\right]$
$\mathsf{SW}_{-i}(\mathcal{D}) = \mathbb{E}_{r\sim\mathcal{D}}\left[\sum_{j\neq i} v_j(r)\right]$
$p_i = \mathsf{SW}_{-i}(\mathcal{D}_{-i}) - \mathsf{SW}_{-i}(\mathcal{D})$
پایان حلقه
بازگشت p.

۵-۳- شخصی‌سازی سطح حفاظت از حریم خصوصی

یکی از محدودیت‌های مکانیسم تسویه بازار پیشنهادی در بخش ۱-۵ تامین سطح یکنواختی از حفاظت برای حریم خصوصی شرکت‌کنندگان در بازار است. در صورتی که، شرکت‌کنندگان در بازار ممکن است حساسیت‌های متفاوتی نسبت به مساله حفظ حریم خصوصی داده‌های خود داشته باشند. بنابراین، مکانیسم پیشنهادی ممکن است منجر به حفاظت ناکافی از حریم خصوصی برخی از افراد شود، در حالی که حفاظت بیش از اندازه‌ای، که مورد تقاضا نیست، برای دیگران ارائه کند. با توجه به عدم یکنواختی تمایلات حریم خصوصی شرکت‌کنندگان در بازار، امکان دستیابی به رفاه اجتماعی بالاتری در مساله تسویه بازار از طریق عدم تامین حفاظت مازاد برای آن دسته از افرادی که چنین تقاضایی ندارند، وجود دارد. برای این منظور، ما در این بخش از مفهوم حریم خصوصی تفاضلی شخصی سازی‌شده[15] (PDP) بهره می‌گیریم [۲۱].

شخصی‌سازی حریم خصوصی را می‌توان به صورت مجموعه‌ای از زوج مرتب‌های $\Phi = \{(u_1, \epsilon_1), (u_2, \epsilon_2), \cdots\}$ نمایش داد، که در آن $u_i \in \mathcal{U}$ نشانگر شرکت‌کننده i در بازار و $\epsilon_i \in \mathbb{R}_+$ نشانگر تمایل حریم خصوصی مربوطه است. در عمل، ممکن است انتظار اینکه افراد درکی نسبت به مقدار پارامتر حریم خصوصی ϵ و تصمیم‌گیری در مورد مقادیر آن داشته باشند، غیرمنطقی به‌نظر برسد. در همین راستا، فرض می شود که با ایجاد یک رابط کاربری مناسب، افراد ترجیح خود برای سطح حفاظت از حریم خصوصی را بطور کیفی منعکس کنند، برای مثال در قالب گزینه‌هایی مانند کم، متوسط، و زیاد.

با توجه به راهکار پیشنهادی در شکل ۲ به منظور دست‌یابی به سطح حفاظت شخصی‌سازی‌شده در بازارهای برق حافظ حریم خصوصی، بایستی ورودی مکانیسم تسویه بازار پیشنهادی در بخش ۵-۱ بر اساس نمونه‌برداری غیریکنواخت از مجموعه‌داده‌ی اصلی تعیین گردد. در ادامه به مکانیسم نمونه‌برداری پیشنهادی اشاره می‌کنیم.

تعریف ۴ (مکانیسم نمونه‌برداری). تابع $f: \mathcal{D} \to \mathcal{R}$، مجموعه‌داده $D \in \mathcal{D}$، و شخصی‌سازی حریم خصوصی Φ را در نظر بگیرید. آنگاه $RS(D, \Phi, t)$ بیانگر فرایندی است که به شکل مستقل از داده‌های هر فرد حاضر در مجموعه‌داده $x \in D$ با احتمال پیش رو نمونه می‌گیرد:

$$\pi_x = \begin{cases} \dfrac{e^{\Phi^x} - 1}{e^t - 1}, & if\ \Phi^x < t \\ 1, & otherwise \end{cases}, \qquad (۱۲)$$

که در آن $\min_u \Phi^u \le t \le \max_u \Phi^u$ آستانه‌ای قابل تنظیم و π_x احتمال حضور داده‌ی $x \in D$ در محاسبه‌ی $f: \mathcal{D} \to \mathcal{R}$ است. حال می‌توانیم مکانیسم نمونه‌برداری را مطابق زیر تعریف کنیم:

$$S_f(D, \Phi, t) = DP_t^f\big(RS(D, \Phi, t)\big) \qquad (۱۳)$$

که در آن DP_t^f هرگونه مکانیسم $t - DP$ است که تابع f از طریق آن محاسبه می‌شود. بنابراین، با اعمال ماهیت تصادفی ناشی از $RS(D, \Phi, t)$ بر روی داده‌های شرکت‌کنندگان در بازار در قالب بلوک نمونه‌برداری در شکل ۲، تمایلات حریم خصوصی شرکت‌کنندگان در بازار منعکس می‌گردد. در گام بعدی بایستی ماهیت تصادفی مورد نیاز برای تضمین حریم خصوصی تفاضلی با سطح حفاظت یکنواخت $\epsilon = t$ از طریق مکانیسم تسویه بازار پیشنهادی تامین گردد. پس از طی این دو مرحله، می توان گفت که مکانیسم تسویه بازار پیشنهادی امکان دستیابی به حریم خصوصی تفاضلی شخصی‌سازی‌شده $\Phi - PDP$ را فراهم می‌کند.

مکانیسم پیشنهادی برای شخصی‌سازی سطح حفاظت از حریم خصوصی ریشه در دو نوع فرایند تصادفی دارد، و به همین دلیل در محاسبه‌ی تابع f در چارچوب این مکانیسم با دو نوع خطا مواجه می‌شویم. برای ایجاد تعادل میان این دو نوع خطا و کنترل آن‌ها می‌توانیم از پارامتر t، که آستانه‌ی سطح حفاظت از حریم خصوصی است، استفاده کنیم. مقادیر کوچک t منجر به حذف تعداد کمتری از داده‌های افراد در گام نمونه‌برداری می‌شود و خطای نمونه‌برداری را کاهش می‌دهد. اما، با این حال، نویز بیشتری به الگوریتم محاسبه‌ی f در راستای تامین شرایط DP_t^f افزوده خواهد شد. در نقطه‌ی مقابل، هنگامی که $t = \max_u \Phi^u$، خطای نمونه‌برداری بیشینه خواهد بود و هر یک از افراد دقیقا سطح مورد تقاضای حریم خصوصی خود را دریافت خواهند کرد. با این حال، هرچند که در چنین شرایطی نویز تصادفی کمتری به سیستم افزوده می‌شود، به دلیل خطای نمونه برداری بالا، تضمینی برای حصول بهترین نتایج از منظر دقت در محاسبات وجود ندارد. در واقع، ممکن است با انتخاب آستانه‌ی t کوچک‌تر، خطای نمونه‌برداری را به‌شکلی چشم‌گیر کاهش دهیم، در حالی که نویز زیادی به الگوریتم جهت تضمین حریم خصوصی افزوده نخواهد شد. همچنین، لازم به ذکر است که به‌ازای $t = \min_u \Phi^u$ مکانیسم نمونه‌برداری به

مکانیسم کمینه‌ی پایه تبدیل می‌شود، که در آن حفاظتی یکنواخت برابر با بیشترین سطح حفاظت مورد تقاضای افراد حاضر در مجموعه‌داده تامین می‌گردد.

۶-مطالعات عددی

در این بخش نتایج مطالعات عددی مربوط به مصالحه‌ی میان سطح حفاظت از حریم خصوصی و رفاه اجتماعی در مساله تسویه بازار، و همچنین تاثیر شخصی‌سازی سطح حفاظت از حریم خصوصی بر کاهش هزینه‌ی تامین حریم خصوصی را بررسی خواهیم کرد. به همین منظور، یک شبکه انرژی محلی متشکل از ۳ تولیدکننده و ۳ مصرف‌کننده را مد نظر قرار می‌دهیم. تابع هزینه تولیدکننده i و تابع منفعت مصرف‌کننده i در قالب توابع درجه‌ی دو هستند، و به ترتیب عبارتند از $C_{i,\theta_i}(\cdot) := a_i^g g_i^2 + b_i^g g_i + c_i^g$ و $U_{i,\theta_i}(\cdot) := a_i^u d_i^2 + b_i^u d_i + c_i^u$.

پارامترهای مورد نیاز برای توابع هزینه و منفعت تولیدگنندگان و مصرف‌کنندگان در جدول۱ و جدول ۲ ارائه شده است.

۶-۱- هزینه حفاظت از حریم خصوصی

شکل ۶ نحوه‌ی اثرگذاری پارامترهای δ و ϵ بر مقدار متوسط و بازه‌ی تغییرات رفاه اجتماعی مساله تسویه بازار را نشان می‌دهد. این شکل برای ۳ مقدار متفاوت δ به ازای ۲۰۰ نمونه از توزیع چگالی احتمال رفاه اجتماعی خروجی مساله تسویه بازار، در بازه‌ی $[0.1,100]$ برای ϵ، ترسیم شده است. همانگونه که انتظار داریم، با افزایش ϵ خروجی‌های مساله تسویه بازار حافظ حریم خصوصی تفاضلی به مقادیر بهینه خود متمایل می‌شوند، و بنابراین رفاه اجتماعی افزایش می‌یابد. همانطورکه در شکل ۶ مشاهده می‌شود، مقدار متوسط رفاه اجتماعی با افزایش ϵ افزایش می‌یابد و به مقدار بهینه، مشخص شده در شکل، نزدیک می‌شود.

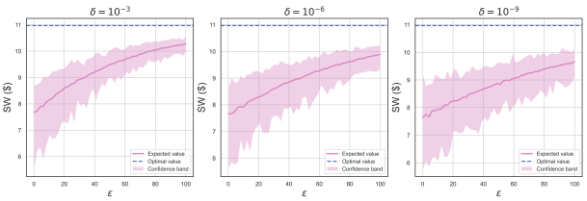
انعطاف‌پذیری ناشی از مقادیر کوچک پارامتر δ امکان دست‌یابی به خروجی‌هایی با رفاه اجتماعی بالاتر را بدون تحمیل خدشه‌ای جدی به سطح حفاظت از حریم خصوصی شرکت‌کنندگان در بازار فراهم می‌کند. در همین راستا، در شکل ۶ مشاهده می‌کنیم که با افزایش مقدار δ از 10^{-9} به 10^{-3} مقدار انتظاری رفاه اجتماعی به ازای هر ϵ افزایش می‌یابد و به مقدار بهینه نزدیک‌تر می‌شود. همچنین، بازه‌ی تغییرات رفاه اجتماعی نیز، که معادل فاصله‌ی میان بیش‌ترین و کم‌ترین مقدار رفاه اجتماعی در میان ۲۰۰ نمونه‌ی برداشته‌شده از توزیع احتمال رفاه اجتماعی است، با افزایش δ کاهش می‌یابد.

جدول۱: پارامترهای اقتصادی و فیزیکی تولیدکنندگان در بازار

Producers	a_i^g ($/kWh^2)	b_i^g ($/kWh)	c_i^g ($)	$\underline{g_i}$ (kW)	$\overline{g_i}$ (kW)
1	0.015	0.038	0	0	20
2	0.008	0.047	0	0	25
3	0.011	0.056	0	0	30

جدول ۲: پارامترهای اقتصادی و فیزیکی مصرف‌کنندگان در بازار

Consumers	a_i^u ($/kWh^2)	b_i^u ($/kWh)	c_i^u ($)	$\underline{d_i}$ (kW)	$\overline{d_i}$ (kW)
1	- 0.008	0.8	0	5	15
2	- 0.014	0.5	0	5	18
3	- 0.009	0.4	0	10	25



شکل ۶: اثرگذاری پارامترهای δ و ϵ بر مقدار متوسط و بازه‌ی تغییرات رفاه اجتماعی مساله تسویه بازار

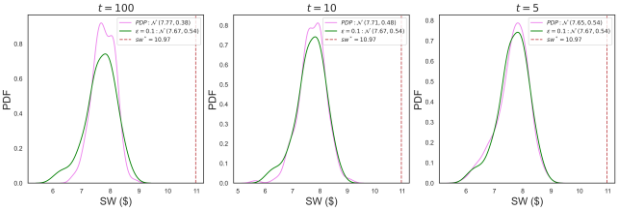
۶-۲- تاثیر شخصی‌سازی سطح حفاظت از حریم خصوصی بر رفاه اجتماعی

همان‌طورکه پیش‌تر اشاره شد، شرکت‌کنندگان در بازار حساسیت یکسانی برای حفاظت از حریم خصوصی خود ندارند، و از این موضوع می‌توان در جهت کاهش هزینه‌ی تامین حریم خصوصی و افزایش رفاه اجتماعی در مساله تسویه بازار بهره برد. چراکه، در چنین شرایطی می‌توان با عدم تامین حفاظت مازاد برای آن گروه از شرکت‌کنندگان در بازار که دغدغه‌ی کمتری نسبت به حریم خصوصی دارند، نویز تصادفی کمتری به مساله تسویه بازار تزریق نمود.

برای این منظور، سناریویی را در نظر می‌گیریم که طی آن شرکت‌کنندگان در بازار تمایلات گوناگونی نسبت به حفاظت از حریم خصوصی خود دارند، و با اعمال مکانیسم نمونه‌برداری به بررسی خروجی‌های مساله تسویه بازار خواهیم پرداخت. شخصی‌سازی حریم خصوصی تولیدکنندگان Φ^p و مصرف‌کنندگان Φ^c در بازار به ترتیب از طریق $\Phi^p = \{(p_1, 2), (p_2, 10), (p_3, 100)\}$ و $\Phi^c = \{(c_1, 0.1), (c_2, 1), (c_3, 5)\}$ تعیین شده است. برای تعیین سطح حفاظت یکنواخت و بدون شخصی‌سازی، مقدار پارامتر ϵ بایستی به صورت متمرکز توسط بهره‌بردار بازار و برابر با $\min\left\{\min_c \Phi^c, \min_p \Phi^p\right\} = 0.1$ تعیین گردد، تا حفاظت مطلوب تمامی شرکت‌کنندگان در بازار تامین شود. روشن است که در این شرایط برخی از شرکت‌کنندگان در بازار، مانند تولیدکننده ۳ با $\Phi^{p_3} = 100$، از حفاظتی بیش از حد مورد انتظار برخوردار می‌شوند.

برای اعمال شخصی‌سازی سطح حفاظت از حریم خصوصی، مقدار آستانه‌ای قابل تنظیم، t، برای پارامتر حریم خصوصی در نظر می‌گیریم. با توجه به این مقدار آستانه t، شرکت‌کنندگانی که خواهان سطح بالاتری از حفاظت باشند، سطح حفاظت از حریم خصوصی آن‌ها شخصی‌سازی خواهد شد، و سایر شرکت‌کنندگان در بازار سطح یکنواختی از حفاظت را با پارامتر $\epsilon = t$ دریافت خواهند کرد. شکل ۷ چگالی‌های توزیع احتمال رفاه اجتماعی شرکت‌کنندگان در بازار را با توجه به

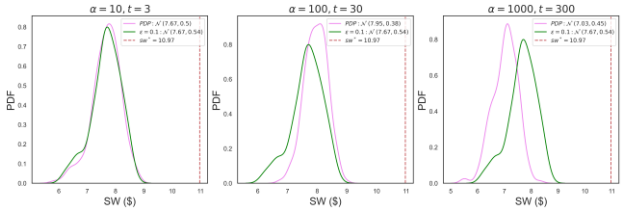
شخصی‌سازی سطح حفاظت، به ازای مقادیر متفاوت t در مقایسه با سطح یکنواخت حفاظت به ازای $\epsilon = 0.1$، نشان می‌دهد. مطابق انتظار، به ازای $t = 100$، که متناظر با شخصی‌سازی سطح حفاظت از حریم خصوصی برای تمامی شرکت‌کنندگان است، بیش‌ترین بهبود در عملکرد مکانیسم تسویه بازار حاصل می‌شود. در این حالت، مقدار انتظاری رفاه اجتماعی $\mathbb{E}[\mathrm{sw}] = 7.77$ است، که با کاهش t این مقدار انتظاری رفاه اجتماعی نیز کاهش خواهد یافت. چراکه، کاهش t مترادف با حرکت به سمت تامین سطح یکنواختی از حفاظت از حریم خصوصی است. علاوه بر این، مشاهده می‌کنیم که با کاهش t انحراف معیار چگالی توزیع احتمال رفاه اجتماعی افزایش می‌یابد، که این مشاهده ریشه در افزایش ماهیت تصادفی مورد نیاز برای تامین سطح یکنواختی از حفاظت (و یا کاهش شخصی‌سازی سطح حفاظت از حریم خصوصی) دارد.



شکل ۷: اثر شخصی‌سازی سطح حفاظت از حریم خصوصی بر رفاه اجتماعی

در ادامه به بررسی تاثیر میزان ناهمگونی تمایلات حریم خصوصی شرکت‌کنندگان در بازار بر کارایی شخصی‌سازی سطح حفاظت از حریم خصوصی خواهیم پرداخت. در همین راستا، سناریوهای گوناگونی را برای شخصی‌سازی حریم خصوصی ϕ شرکت‌کنندگان در بازار مد نظر قرار می‌دهیم. این سناریوها میزان ناهمگونی تمایلات حریم خصوصی را بر اساس انحراف معیار میان تمایلات حریم خصوصی شرکت‌کنندگان در بازار منعکس می‌کنند. به همین منظور، سناریوهای شخصی‌سازی حریم خصوصی تولیدکنندگان و مصرف‌کنندگان را با توجه به رابطه‌ی $\Phi_\alpha^p = \alpha\Phi^c$ تعیین می‌کنیم، که در آن α ضریبی مشخص، Φ^c شخصی‌سازی حریم خصوصی مصرف‌کنندگان، و Φ_α^p شخصی‌سازی حریم خصوصی تولیدکنندگان به ازای ضریب α است. در بررسی پیش رو، مقادیر تمایلات حریم خصوصی شرکت‌کنندگان در بازار، به ترتیب، معادل $\Phi^c = \{(c_1, 0.1), (c_2, 0.2), (c_3, 0.3)\}$ و $\Phi_\alpha^p = \{(p_1, 0.1\alpha), (p_2, 0.2\alpha), (p_3, 0.3\alpha)\}$ برای مصرف‌کنندگان و تولیدکنندگان خواهد بود. همچنین، مقدار آستانه‌ی پارامتر حریم خصوصی t به منظور شخصی‌سازی سطح حفاظت را معادل بیشینه تمایلات حریم خصوصی شرکت‌کنندگان در بازار، $\max\left\{\max_c \Phi^c, \max_p \Phi_\alpha^p\right\}$، انتخاب می‌کنیم.

شکل ۸ مقایسه‌ی چگالی توزیع احتمال رفاه اجتماعی شرکت‌کنندگان در بازار را در حالت شخصی‌سازی سطح حفاظت از حریم خصوصی با حالت سطح حفاظت یکنواخت نشان می‌دهد. مشاهده می‌کنیم که برای $\alpha = 10$ شخصی‌سازی سطح حفاظت از حریم خصوصی تغییر محسوسی در چگالی توزیع احتمال رفاه اجتماعی ایجاد نمی‌کند.



شکل ۸: اثر میزان ناهمگونی تمایلات حریم خصوصی بر کارایی شخصی‌سازی سطح حفاظت از حریم خصوصی

در واقع، به ازای $\alpha = 10$ تمایلات حریم خصوصی تولیدکنندگان و مصرف‌کنندگان، به ترتیب، معادل $\Phi_{\alpha=10}^p = \{(p_1, 1), (p_2, 2), (p_3, 3)\}$ و $\Phi^c = \{(c_1, 0.1), (c_2, 0.2), (c_3, 0.3)\}$ خواهد بود. همانطورکه مشاهده می‌کنیم، در این حالت تقریبا تمامی شرکت‌کنندگان در بازار خواهان سطح بالایی از حریم خصوصی هستند، و اختلاف چشم‌گیری میان تمایلات آن‌ها وجود ندارد. به همین دلیل، شخصی‌سازی سطح حفاظت از حریم خصوصی نیز کارایی چندانی نخواهد داشت. با افزایش α به مقدار 100، مشاهده می‌کنیم که اثرگذاری شخصی‌سازی سطح حفاظت از حریم خصوصی نیز محسوس خواهد بود. در این حالت، مصرف‌کنندگان، با توجه به $\Phi^c = \{(c_1, 0.1), (c_2, 0.2), (c_3, 0.3)\}$، در مقایسه‌ی با تولیدکنندگان، $\Phi_{\alpha=100}^p = \{(p_1, 10), (p_2, 20), (p_3, 30)\}$، دغدغه‌ی بسیار بیشتری نسبت به حریم خصوصی خود دارند. از این‌رو، شخصی‌سازی سطح حفاظت از حریم خصوصی، مانع از تامین حفاظت مازاد برای تولیدکنندگان خواهد شد، که این موضوع کاهش ماهیت تصادفی مکانیسم تسویه بازار را به دنبال دارد. با این حال، وقتی α به مقدار 1000 افزایش می‌یابد، بر خلاف انتظار، کارایی شخصی‌سازی سطح حفاظت از حریم خصوصی در مقایسه‌ی با سطح حفاظت یکنواخت کاهش می‌یابد. در شکل ۸ مشاهده می‌کنیم که برای $\alpha = 1000$ و $t = 300$، مقدار انتظاری رفاه اجتماعی معادل $\mathbb{E}[\mathrm{sw}] = 7.03$ \$. درحالی‌که، این مقدار تحت حفاظت یکنواخت معادل $\mathbb{E}[\mathrm{sw}] = 7.67$ \$ است. علت چنین رخدادی، به خطای نمونه‌برداری بازمی‌گردد.

۷-نتیجه‌گیری

در این مقاله به طراحی بازارهای برق محلی حافظ حریم خصوصی تفاضلی با قابلیت شخصی‌سازی سطح حفاظت از حریم خصوصی پرداختیم. بطور مشخص برای تضمین حفاظت از حریم خصوصی شرکت‌کنندگان در بازار، مکانیسم‌هایی را برای محاسبه‌ی مقادیر تسویه بازار و همچنین پرداختی‌های شرکت‌کنندگان در بازار در چارچوب حریم خصوصی تفاضلی ارائه کردیم. در ادامه، توجه خود را معطوف به شخصی‌سازی سطح حفاظت از حریم خصوصی نمودیم، و ناهمگونی تمایلات حریم خصوصی شرکت‌کنندگان در بازار را به عنوان فرصتی برای کاهش ماهیت تصادفی بازارهای برق حافظ حریم خصوصی تفاضلی مطرح کردیم. در همین راستا، با معرفی یک مکانیسم نمونه‌برداری، در سطح مجموعه‌داده‌ی ورودی مساله تسویه بازار، امکان انعکاس تمایلات حریم خصوصی شرکت‌کنندگان در بازار را فراهم نمودیم. در بخش مطالعات عددی تاثیر پارامترهای حریم خصوصی تفاضلی و

شخصی‌سازی سطح حفاظت از حریم خصوصی را بر رفاه اجتماعی شرکت‌کنندگان در بازار ارزیابی نمودیم. همچنین، مشاهده کردیم که افزایش آستانه‌ی شخصی‌سازی، منجر به افزایش مقدار انتظاری چگالی توزیع احتمال رفاه اجتماعی و کاهش انحراف معیار آن می‌گردد. علاوه بر این، تاثیر میزان ناهمگونی تمایلات حریم خصوصی شرکت‌کنندگان در بازار و خطای نمونه‌برداری بر کارایی شخصی‌سازی سطح حفاظت از حریم خصوصی بررسی گردید.

مراجع

[۱] ضیائی، رشیدی‌نژاد، عبداللهی، پیرمرادی، "یک معماری برای برنامه‌ریزی تولید در بازار تجدیدساختار شده با زیرساخت اینترنت اشیاء"، نشریه مهندسی برق و الکترونیک ایران، دوره ۱۹، صفحات ۱۷۵-۱۶۱، تهران، ۱۴۰۱.

[۲] عمادالاسلامی، مجیدی، حقی‌فام " ارائه یک مدل دومرحله‌ای جهت تشخیص تقلب در شبکه توزیع به‌وسیله یادگیری عمیق"، نشریه مهندسی برق و الکترونیک ایران، دوره ۱۹، صفحات ۱۳-۲۲، تهران، ۱۴۰۱.

[۳] سالک گیلانی، فریدونیان، "مدلسازی داده‌رانه مدت زمان تداوم وقفه در شبکه توزیع برق با در نظر گرفتن نگهداری و تعمیرات پیشگیرانه و تحلیل اثر آن"، نشریه مهندسی برق و الکترونیک ایران، دوره ۱۹، صفحات ۱-۱۱، تهران، ۱۴۰۱.

[4] Y. Yang, M. Bao, Y. Ding, Y. Song, Z. Lin, and C. Shao, "Review of Information Disclosure in Different Electricity Markets," *Energies (Basel)*, vol. 11, no. 12, p. 3424, 2018.

[5] D. Brown, A. Eckert, and J. Lin, "Information and Transparency in Wholesale Electricity Markets: Evidence from Alberta," *SSRN Electronic Journal*, vol. 54, pp. 292–330, 2018.

[6] M. Rhahla, S. Allegue, and T. Abdellatif, "Guidelines for GDPR compliance in Big Data systems," *Journal of Information Security and Applications*, vol. 61, p. 102896, 2021.

[7] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An MPC-based privacy-preserving protocol for a local electricity trading market," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, doi: 10.1007/978-3-319-48965-0_40, 2016.

[8] Y. Lu, J. Lian, M. Zhu, and K. Ma, "Transactive Energy System Deployment over Insecure Communication Links," doi: arXiv preprint arXiv:2008.00152, 2020.

[9] R. Sarenche, M. Salmasizadeh, M. H. Ameri, and M. R. Aref, "A secure and privacy-preserving protocol for holding double auctions in smart grid," *Inf Sci (N Y)*, vol. 557, 2021.

[10] K. Erdayandi, A. Paudel, L. Cordeiro, and M. A. Mustafa, "Privacy- friendly peer-to-peer energy trading: A game theoretical approach," *arXiv preprint*, doi: arXiv:2201.01810, 2022.

[11] S. Xie, H. Wang, Y. Hong, and M. Thai, "Privacy preserving distributed energy trading," in *Proceedings - International Conference on Distributed Computing Systems*, pp. 322–332, 2020.

[12] F. Zobiri, M. Gama, S. Nikova, and G. Deconinck, "A Privacy-Preserving Three-Step Demand Response Market Using Multi-Party Computation," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, pp. 1–5, 2022.

[13] M. Montakhabi, A. Madhusudan, S. van der Graaf, A. Abidin, P. Ballon, and M. A. Mustafa, "Sharing Economy in Future Peer-to-peer Electricity Trading Markets: Security and Privacy Analysis", Energy Sources, Part B: Economics, Planning, and Policy, vol. 17, 2022.

[14] E. Buchmann, S. Kessler, P. Jochem, and K. Bohm, "The costs of privacy in local energy markets," in *Proceedings - 2013 IEEE International Conference on Business Informatics, IEEE CBI 2013*, pp. 198–207, 2013.

[15] L. Wu and J. Li, "Privacy-Preserving Economic Dispatch in Competitive Electricity Market," in *Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference*, pp. 1–5, 2018.

[16] I. Shilov, H. le Cadre, and A. Busic, "Privacy impact on generalized Nash equilibrium in peer-to-peer electricity market," *Operations Research Letters*, vol. 49, no. 5, 2021.

[17] I. Dekel, R. Cummings, O. Heffetz, and K. Ligett, "The Privacy Elasticity of Behavior: Conceptualization and Application," Cambridge, MA, doi: 10.3386/w30215, 2022.

[18] J. P. Near and X. He, "Differential Privacy for Databases," *Foundations and Trends® in Databases*, vol. 11, no. 2, pp. 109–225, 2021.

[19] S. Vadhan, "The complexity of differential privacy," in *Information Security and Cryptography*, pp. 347–450, 2017.

[20] M. Abadi *et al.*, "Deep learning with differential privacy," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 308–318, 2016.

[21] B. Niu, Y. Chen, B. Wang, Z. Wang, F. Li, and J. Cao, "AdaPDP: Adaptive Personalized Differential Privacy," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, IEEE, pp. 1–10., 2021.

زیرنویس‌ها

[1] General Data Protection Regulation (GDPR)
[2] New York Privacy Act (NYPA)
[3] Privacy by Design (PbD)
[4] Differential privacy
[5] Multi Party Computation (MPC)
[6] Homomorphic Encryption (HE)
[7] Peer-to-Peer electricity markets
[8] Reconstruction attacks
[9] Data anonymization
[10] Obfuscation
[11] Gaussian mechanism
[12] Global Sensitivity (GS)
[13] Gradient ascent
[14] Gradient clipping
[15] Personalized Differential Privacy (PDP)