فصلنامه انرژی ایران، دوره ۲۵،شماره۴ زمستان ۱۴۰۱،صفحه ۳۴-۵۴

بازارهای برق محلی حافظ حریم خصوصی تفاضلی

میلاد حسین‌پور
دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران
m.hoseinpour@modares.ac.ir

محمودرضا حقی‌فام*
دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران
haghifam@modares.ac.ir

تاریخ دریافت:
۱۴۰۱/۱۰/۳

تاریخ پذیرش:
۱۴۰۱/۱۰/۱۰

کلمات کلیدی:
حریم خصوصی تفاضلی،
بازارهای برق محلی،
طراحی مکانیسم،
شبکه‌های هوشمند

چکیده

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، این بازارها امکان انتشار آماری خروجی‌های بازار و به اشتراک‌گذاری آن‌ها را نیز فراهم می‌کنند، که منجر به انتفاع جامعه خواهد شد. این مقاله با استفاده از مفهوم حریم خصوصی تفاضلی، طراحی یک بازار برق برای شبکه‌های انرژی محلی که به شکلی قابل اثبات حفاظت از حریم خصوصی شرکت‌کنندگان در بازار را تضمین کند، پیگیری می‌کند. مدل پیشنهادی ضمن دستیابی به یک پاسخ بهینه‌ی تقریبی و حفاظت از حریم خصوصی شرکت‌کنندگان در بازار، منفعت داده‌ها را نیز برای انتشارهای آماری حفظ می‌کند. ماهیت تصادفی مورد نیاز حریم خصوصی تفاضلی نیز با استفاده از نویزهای تصادفی با توزیع احتمال گاوسی در هر تکرار از الگوریتم گرادیان افزایشی، در فرایند بهینه‌سازی مساله تسویه بازار، تعبیه می‌شود. در بخش مطالعات عددی، تاثیر پارامتر حفاظت از حریم خصوصی تفاضلی را بر توزیع‌های احتمال خروجی‌های مساله تسویه بازار و سود بازیگران بررسی می‌کنیم. 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.

۱. مقدمه

پیشرفت‌های اخیر مرتبط با منابع انرژی تجدیدپذیر[۱] (RESs)، تمرکززدایی، و هوشمندسازی در سیستم‌های قدرت، مسیر را برای پیدایش بازارهای برق محلی هموار کرده است (جارگوو[۲] و همکاران، ۲۰۲۱). بازارهای برق محلی در حال ظهور یک منبع عظیم از داده‌های شرکت‌کنندگان در بازار، مانند داده‌های اقتصادی و مبادلات الکتریکی، محسوب می‌شوند (تساوسوگلو[۳] و همکاران، ۲۰۲۲). انتشار عمومی این داده‌ها و ایجاد دسترسی برای محققین، صاحبان کسب‌وکار، سیاست‌گذاران، و سایرین، گستره‌ی وسیعی از مزایای اقتصادی، فنی، و اجتماعی را در پی دارد. به عنوان نمونه، ایجاد هماهنگی میان بازارهای برق و حرارت از طریق تبادل داده‌ها میان این دو بازار منجر به افزایش رفاه اجتماعی و بهره‌وری انرژی خواهد شد. هم‌چنین، انتشار عمومی این داده‌ها، گامی اساسی در راستای شفافیت[۴] در بازارهای برق محلی محسوب می‌شود. در واقع، شفافیت در بازارهای برق، ارتقای ماهیت رقابتی آن را به دنبال دارد، که خود زمینه‌ی جذب مشترکین بیشتری را به بازارهای برق محلی فراهم می‌کند. بنابراین، انتشار خروجی‌های مساله تسویه بازار، ابزاری کارآمد در جهت نظارت مستمر بر عملکرد بازار و کشف موقعیت‌های انحصارطلبانه تلقی می‌شود .

اما، این مجموعه‌داده‌های جزئی و غنی می‌توانند منجر به نقض حریم خصوصی شرکت‌کنندگان در بازار شوند. در واقع، انتشار این مجموعه‌داده‌ها می‌تواند اطلاعات حساسی را درباره‌ی شرکت‌کنندگان در بازار آشکار کند، و منجر به پیامدهای نامطلوبی برای این افراد شود؛ پیامدهایی که در صورت عدم مشارکت آن‌ها در بازار کمتر محتمل بوده‌اند (سامی[۵] و همکاران، ۲۰۲۱). برای مثال، مبادلات انرژی الکتریکی در بازار، الگوی مصرف شرکت‌کنندگان در بازار را آشکار می‌کند، که می‌تواند با هدف نظارت بر رفتار[۶] و تبلیغات بیش از اندازه شخصی‌سازی‌شده[۷] توسط شرکت‌های بازاریابی مورد استفاده قرار گیرد. به همین دلیل، دغدغه‌های ناشی از حریم خصوصی خاستگاه انگیزه‌ای برای رفتار راهبردی[۸] شرکت‌کنندگان در بازار، از طریق گزارش اطلاعات نادرست به مکانیسم بازار، و یا حتی خروج آن‌ها از بازار محسوب می‌شود. از طرف دیگر، قوانین مرتبط با حفاظت از حریم خصوصی، مانند مقررات عمومی حفاظت از داده‌ها[۹] (GDPR) در اتحادیه اروپا، از لحاظ قانونی بازارهای برق را ملزم به حفاظت از داده‌های خصوصی شرکت‌کنندگان در بازارهای برق محلی می‌کند (لی[۱۰] و همکاران، ۲۰۲۱).

بنابراین، چالش حریم خصوصی در بازارهای برق محلی ریشه در ایجاد تعادل میان ارزش به اشتراک‌گذاری داده‌ها و ریسک نقض حریم خصوصی افراد دارد. در همین راستا، سوال اصلی که در پی یافتن پاسخ آن هستیم، این است که چگونه می‌توان دسترسی نامحدودی به داده‌های افراد برای بهره‌برداران قابل اعتماد بازار فراهم کرد و به آن‌ها اجازه داد که خروجی‌های بازار را به شکلی عمومی با هدف انتفاع جامعه منتشر کنند. برای پرداختن به این پرسش، هدف این مقاله طراحی یک بازار برق محلی است که تضمینی قابل اتکا برای حفاظت از

[۱] Renewable Energy Sources (RESs)
[۲] Bjarghov
[۳] Tsaousoglou
[۴] Trasparency
[۵] Samy
[۶] Behavioral surveillance
[۷] Hyper personalization
[۸] Strategic behavior
[۹] General Data Protection Regulation (GDPR)
[۱۰] Lee

حریم خصوصی افراد ارائه می‌دهد، ارزش کاربردی خروجی‌های بازار را برای مطالعات آماری حفظ می‌کند، و در عین حال، به رفاه اجتماعی نزدیک به بهینه[۱] دست می‌یابد. در راستای این اهداف، ما از مفهوم حریم خصوصی تفاضلی[۲] (DP) بهره می‌گیریم، که چارچوبی برای استدلال کمی درباره‌ی حریم خصوصی و ریسک افشای اطلاعات خصوصی شرکت‌کنندگان در بازار را فراهم می‌کند. مکانیسم‌های حریم خصوصی تفاضلی به‌طور معمول مصالحه‌ای میان سطح حفاظت از حریم خصوصی افراد حاضر در یک مجموعه‌داده و دقت محاسبات بر روی آن مجموعه داده را ایجاد می‌کنند (نیسیم[۳]، ۲۰۲۱). علاوه‌براین، برخلاف سایر روش‌های حفاظت از حریم خصوصی، حریم خصوصی تفاضلی در برابر تمامی پساپردازش‌ها[۴] مقاوم است و هیچگونه پیش‌فرضی درباره‌ی توان محاسباتی و اطلاعات جانبی طرف‌های متخاصم ندارد (دومینگو-انریچ[۵] و همکاران، ۲۰۲۲).

۲. پیشینه تحقیق و نوآوری‌های مقاله

حریم خصوصی تفاضلی و مبانی نظری آن در کارهای تحقیقاتی متعددی مورد بررسی قرار گرفته است. هم‌چنین، دیدگاه حریم خصوصی تفاضلی به عنوان یک فناوری پیش‌رو برای حفاظت از داده‌های حساس افراد به شکلی گسترده توسط شرکت‌هایی مانند اپل، گوگل و مایکروسافت اتخاذ شده است. با این‌حال، به‌کارگیری حریم خصوصی تفاضلی در سیستم‌های قدرت و شبکه‌های هوشمند در مراحل آغازین خود بوده، و در سال‌های اخیر بیش‌تر مورد توجه قرار گرفته است. فیورتو[۶] و همکاران (۲۰۱۹) مکانیسمی حافظ حریم خصوصی تفاضلی برای انتشار آماری داده‌های حساس سیستم‌های قدرت، مانند پارامترهای خطوط انتقال و ترانسفورماتورها، ارائه داده است. مکانیسم پیشنهادی تضمین می‌کند که استفاده از داده‌های منتشرشده در مساله پخش‌بار بهینه[۷] (OPF)، منجر به پاسخ‌های غیرمجاز نخواهد شد، و شکاف میان پاسخ بهینه‌ی مساله OPF و پاسخ مساله OPF تحت قیود حفاظت از حریم خصوصی خللی در تحلیل عملکرد سیستم ایجاد نمی‌کند. در دیورکین[۸] و همکاران (۲۰۲۰)، یک مکانیسم OPF حافظ حریم خصوصی تفاضلی ارائه شده است. در این مکانیسم پیشنهادی طرف‌های متخاصمی که به خروجی‌های مساله OPF، مانند ولتاژ گره‌ها و جریان خطوط، دسترسی دارند، قادر به استخراج اطلاعات خصوصی مشترکین نخواهند بود. در ژو[۹] و همکاران (۲۰۱۹)، نویسندگان مکانیسمی حافظ حریم خصوصی برای انتشار داده‌های مساله DC-OPF ارائه داده‌اند. علاوه‌براین، در این مقاله تشریح می‌شود که مکانیسم حافظ حریم خصوصی پیشنهادی به ساختار شبکه وابسته است. ماک[۱۰] و همکاران (۲۰۲۰) مکانیسمی حافظ حریم خصوصی برای مساله OPF در سیستم‌های قدرت توزیع‌شده ارائه می‌دهد. مکانیسم پیشنهادی با به‌کارگیری نسخه‌ی نویزی الگوریتم ADMM از اطلاعات خصوصی مشترکین، شامل بار مصرفی آن‌ها، حفاظت می‌کند. هم‌چنین، این مکانیسم تضمین می‌کند که خروجی‌های مساله OPF در ناحیه مجاز قرار دارد. در کار تحقیقاتی دیگری، مصالحه‌ی میان منفعت ناشی از انتشار داده‌ها در

[۱] Near optimal
[۲] Differential Privacy (DP)
[۳] Nissim
[۴] Post-processing
[۵] Domingo-Enrich
[۶] Fioretto
[۷] Optimal Power Flow (OPF)
[۸] Dvorkin
[۹] Zhou
[۱۰] Mak

چارچوبی حافظ حریم خصوصی تفاضلی و حفاظت از حریم خصوصی افراد ارائه شده است (یانگ[۱] و همکاران، ۲۰۱۷). علاوه‌براین، یانگ و همکاران (۲۰۱۷) اثرگذاری نویز تزریقی، برای حفاظت از حریم خصوصی، بر قیمت‌های محلی برق و پخش‌بار شبکه بررسی می‌کنند.

در گروه دیگری از کارهای تحقیقاتی، حریم خصوصی مشترکین متصل به کنتورهای هوشمند مورد بررسی قرار گرفته است. سانتوس[۲] و همکاران (۲۰۲۱) و لو[۳] و همکاران (۲۰۲۰)، الگوریتم‌های حافظ حریم خصوصی تفاضلی برای حفاظت از داده‌های مصرفی مشترکین ارائه شده است. هم‌چنین، به دلیل ماهیت تصادفی الگوریتم‌های پیشنهادی، آثار داده‌های استخراج‌شده بر عملکرد سیستم نیز ارزیابی شده است. در ادامه نیز، هزینه‌های مازاد ناشی از اعمال قید حریم خصوصی با استفاده از مکانیسم‌های مبتنی بر نظریه بازی‌های همکارانه، به مشترکین تخصیص داده شده است. بروجنی[۴] و همکاران (۲۰۱۹) با به‌کارگیری نسخه‌ی توسعه‌یافته‌ای از حریم خصوصی تفاضلی، مکانیسمی را برای افزودن نویز به داده‌های مصرفی مشترکین، پیش از انتشار آن‌ها، ارائه می‌دهد، تا از این طریق مانع از افشای الگوی مصرفی و هم‌چنین حضور و یا عدم حضور آن‌ها در خانه گردد. مکانیسم پیشنهادی ژاو[۵] و همکاران (۲۰۱۴) نیز برای پنهان کردن الگوی مصرف حقیقی مشترکین از عوامل خارجی، از روشی ترکیبی مبتنی بر ذخیره‌سازهای انرژی و حریم خصوصی تفاضلی بهره می‌گیرد.

به منظور تشویق مشترکین حساس به حریم خصوصی برای مشارکت در بازارهای برق محلی و جلوگیری از رفتار راهبردی آنان، بایستی دغدغه‌ی حریم خصوصی آنان مورد توجه قرار گیرد. در همین راستا، هدف این مقاله معرفی یک مکانیسم حافظ حریم خصوصی برای بازارهای برق محلی در چارچوب حریم خصوصی تفاضلی است. نوآوری‌های کلیدی این مقاله را می‌توان به صورت زیر خلاصه نمود:

- ارائه‌ی یک مکانیسم حافظ حریم خصوصی تفاضلی برای بازارهای برق محلی 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،
- تعبیه‌ی نویز مورد نیاز در جهت تضمین حفاظت از حریم خصوصی در الگوریتم بهینه‌سازی گرادیان افزایشی و پرهیز از روش‌های مبتنی بر مبهم‌سازی داده‌های ورودی که منجر به انحراف شدید پاسخ مساله از نقطه‌ی بهینه می‌گردد،
- تحلیل تلفات حریم خصوصی تفاضلی در فرایند بهینه‌سازی مساله تسویه بازار و هم‌چنین محاسبه‌ی پرداختی‌های شرکت‌کنندگان در بازار،
- بکارگیری سازوکاری در فرایند بهینه سازی برای تضمین قرارگیری خروجی‌های مساله تسویه بازار حافظ حریم خصوصی در ناحیه مجاز.

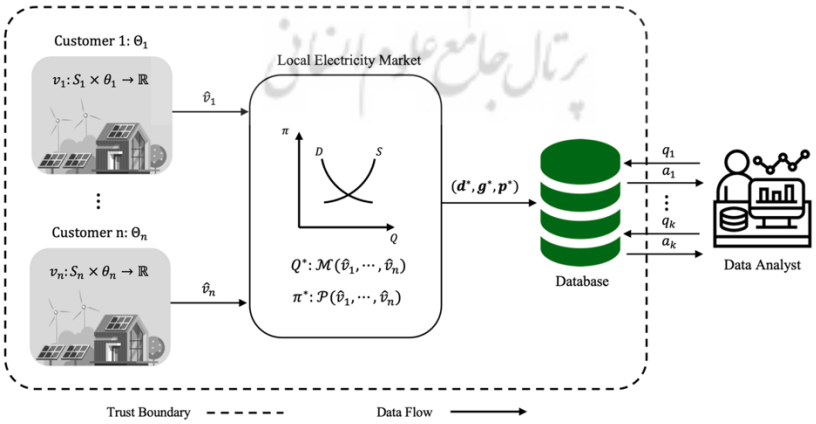
در ادامه‌ی مقاله، در بخش ۳ به بیان چارچوب مساله خواهیم پرداخت. بخش ۴ به مرور مبانی حریم خصوصی تفاضلی اختصاص دارد. مکانیسم پیشنهادی و بازارهای برق گاوسی در بخش ۵ ارائه خواهد شد. نتایج عددی و تفسیر آن‌ها در بخش ۶ ارائه می‌شوند. در نهایت، در بخش ۷ ، به بیان نتایج خواهیم پرداخت.

[۱] Yang
[۲] Santos
[۳] Lou
[۴] Boroujeni
[۵] Zhao

۳. چارچوب مساله

در این بخش ما مساله‌ی تسویه‌ی بازار برق متمرکز در یک شبکه انرژی محلی با مجموعه‌ای از شرکت‌کنندگان Ω، شامل تولیدکنندگان Ω^p و مصرف‌کنندگان Ω^c، را در نظر می‌گیریم. 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 $d_i \in \left[\underline{d_i}, \overline{d_i}\right]$ و میزان تولید $g_i \in \left[\underline{g_i}, \overline{g_i}\right]$ 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، توابع ارزش‌گذاری شرکت‌کنندگان در بازار را نرمالیزه می‌کنیم، به‌نحوی که در محدوده‌ی [۰،۱] قرار می‌گیرند.



شکل ۱: نمای کلی چارچوب مساله تسویه بازار برق حافظ حریم خصوصی تفاضلی

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 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 $p = (p_i)_{i\in\Omega}$. در بازارهای برق، الگوریتم تخصیص 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:

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

$$s.t.$$

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

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

$$\sum_{i\in\Omega^p} g_i - \sum_{i\in\Omega^c} d_i = ۰, \quad (۴)$$

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، و شرکت‌های بیمه، است، خواهان دسترسی به این پایگاه داده حاوی خروجی‌های مساله تسویه بازار هستند. این در حالی است که شرکت‌کنندگان در بازار هیچگونه پیش‌فرضی درباره اهداف گوناگون طرف‌های ثالث ندارند. هدف یک تحلیل‌گر داده غیرمتخاصم این است که از طریق طرح پرسمان‌ها[۱] $\{q_j\}_{j=۱}^{k}$ و دریافت پاسخ‌های $\{a_j\}_{j=۱}^{k}$ اماره‌ها[۲] و اطلاعات مفیدی را در مورد جامعه اماری شرکت‌کنندگان در بازار کسب کند. بااین‌حال، با انتشار عمومی داده‌های خروجی مساله تسویه بازار افراد متخاصم نیز به این داده‌های غنی دسترسی خواهند داشت و شرکت‌کنندگان در بازار در معرض نقض حریم خصوصی قرار خواهند گرفت. بنابراین، بازارهای حافظ حریم خصوصی بایستی به منظور حفاظت از حریم خصوصی شرکت‌کنندگان در بازار و بطور هم‌زمان انتشار عمومی داده‌های خروجی بازار در راستای انتفاع جامعه، تضمین کنند که هر فردی خارج از محدوده‌ی اعتماد تعیین‌شده قادر به کسب اطلاعاتی در سطح فردی شرکت‌کنندگان در بازار نخواهد شد.

۴. مروری بر مبانی مدل پیشنهادی

[۱] Queries
[۲] Statistics

۱،۴. حریم خصوصی تفاضلی

یک راهکار شناخته شده برای ایجاد تعادل میان هزینه‌های ناشی از نقض حریم خصوصی و مزایای به اشتراک‌گذاری داده‌ها، استفاده از مفهوم حریم خصوصی تفاضلی است. حریم خصوصی تفاضلی یک استاندارد ریاضی با قابلیت اثبات نظری برای حفاظت از حریم خصوصی افراد محسوب می‌شود. بر خلاف سایر روش‌های حفاظت از حریم خصوصی، مانند ناشناسی[۱] $k-$، که نسبت به اطلاعات جانبی و حملات پیوندی[۲] آسیب‌پذیر هستند، حریم خصوصی تفاضلی در برابر تمامی مجموعه داده‌های موجود در گذشته، حال، و آینده مقاوم است. به بیانی دیگر، طرف‌های متخاصم با ترکیب و ادغام این مجموعه داده‌ها موفق به شناسایی داده‌های گمنام‌سازی شده و کسب اطلاعاتی مفید در سطح افراد نخواهند شد. در واقع، حریم خصوصی تفاضلی این تضمین را به افراد می‌دهد، که آن‌ها با مشارکت و به اشتراک‌گذاری داده‌های خود در هرگونه الگوریتم، تحلیل، و یا محاسبه، در معرض هیچ‌گونه آسیبی نخواهند بود (تروکس[۳] و همکاران، ۲۰۱۹).

مبنای این روش تعیین یک کران بالا برای میزان حساسیت خروجی یک الگوریتم به داده‌ی ورودی هر یک از افراد است. در واقع، 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 (وود[۴] و همکاران، ۲۰۱۸). ایده‌ی اصلی برای دستیابی به چنین مشخصه‌ای، ایجاد نوعی آشفتگی[۵] در الگوریتم از طریق افزودن مقدار کالیبره شده‌ای 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 $\epsilon \geq 0$، الگوریتم تصادفی $\mathcal{M}: \mathcal{X}^n \to \mathcal{R}$ را $\epsilon - DP$ گویند اگر برای هر زوج از مجموعه داده‌های همسایه[۶] $x \sim x' \in \mathcal{X}^n$ (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 (دورک[۷] و همکاران، ۲۰۱۴):

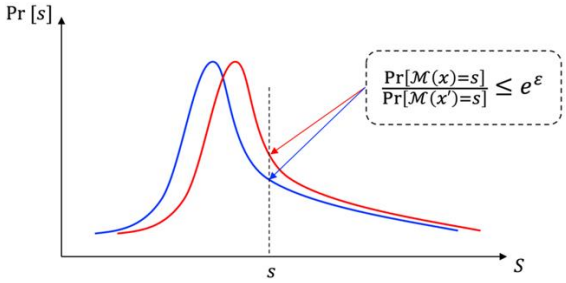
$$\Pr[\mathcal{M}(x) \in S] \leq e^{\epsilon}.\Pr[\mathcal{M}(x') \in S]. \quad (۵)$$

که در آن احتمال از ماهیت تصادفی الگوریتم ناشی می‌شود.

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 $\epsilon - DP$ (حافظ حریم خصوصی تفاضلی با پارامتر ϵ) 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

[۱] K-anonymity
[۲] Linkage attack
[۳] Truex
[۴] Wood
[۵] Perturbation
[۶] Neighboring
[۷] Dwork

نزدیکی از طریق کران بالای نسبت این توزیع‌های احتمال، یعنی e^{ϵ}، منعکس می‌گردد. شکل ۲ نمایی از چگونگی عملکرد الگوریتم‌های $\epsilon - DP$ بر روی مجموعه داده‌های همسایه‌ی $x \sim x' \in \mathcal{X}^n$ را نشان می‌دهد.



شکل ۲: نگاه کلی به عملکرد الگوریتم‌های $\epsilon - DP$

هنگامی که $\epsilon = 0$ است، توزیع‌های احتمال بر روی تمامی مجموعه داده‌های همسایه، در خروجی الگوریتم $\mathcal{M}$، کاملا مشابه یکدیگر خواهند بود. به عبارتی، داده‌ی هر یک از افراد در خروجی الگوریتم کاملا بی‌تاثیر خواهد بود و حریم خصوصی بطور مطلق حفظ می‌گردد. اما، بهای چنین سطحی از حفاظت برای حریم خصوصی، غیرقابل استفاده گشتن خروجی الگوریتم است. چراکه، خروجی الگوریتم به شکلی کاملا تصادفی و بدون توجه به داده‌های ورودی تعیین می‌گردد و حاوی هیچ اطلاعات مفیدی نیست. از طرف دیگر، هنگامی که $\epsilon = \infty$ است، هیچ کرانی برای نسبت توزیع‌های احتمال خروجی الگوریتم $\mathcal{M}$ بر روی مجموعه داده‌های همسایه وجود ندارد و هیچ محدودیتی متوجه میزان تاثیرگذاری داده‌ی هر یک از افراد در خروجی الگوریتم نیست. از همین روی، در چنین حالتی هیچ تضمینی برای حفاظت از حریم خصوصی وجود ندارد. بنابراین، هر چقدر میزان ϵ کاهش یابد تضمین بیشتری برای حفظ حریم خصوصی وجود دارد. همانگونه که مطرح شد، بایستی تعادلی میان میزان حفاظت از حریم خصوصی و سودمندی داده‌ها برقرار گردد. به همین منظور، در عمل معمولا پارامتر حریم خصوصی مقادیر کوچکی در محدوده‌ی $\epsilon \lesssim 1$ را اختیار می‌کند. با این حال، انتخاب ϵ بسیار وابسته به حوزه‌ی کاربرد آن و میزان حساسیت داده‌های مورد نظر است، و بیش از اینکه ریشه در جنبه‌های فنی داشته باشد، ریشه در مسائل اجتماعی دارد.

۱،۱،۴. حریم خصوصی تفاضلی تقریبی

در این بخش، حریم خصوصی تفاضلی تقریبی[۱] (ADP) را معرفی می‌کنیم، که نسبت به حریم خصوصی تفاضلی تضمین ضعیف‌تری برای حفظ حریم خصوصی محسوب می‌شود. در واقع، ADP اجازه‌ی وقوع رخدادهای ناقض حریم خصوصی اما بسیار نامحتمل را می‌دهد. در ادامه، با اصلاح تعریف اولیه‌ی حریم خصوصی تفاضلی، به ارائه‌ی تعریف ADP خواهیم پرداخت. این تعریف، علاوه بر معیار ضریب نسبی برای بیان نزدیکی توزیع‌های احتمال خروجی الگوریتم، شامل معیار افزایشی[۲] نیز می‌شود.

[۱] Approximate Differential Privacy (ADP)
[۲] Additive

تعریف ۲ (حریم خصوصی تفاضلی تقریبی). برای $\epsilon \geq ۰$ و $۰ \leq \delta \leq ۱$، 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 (دورک و همکاران، ۲۰۱۴):

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

زمانی که $\delta = ۰$، $(\epsilon, ۰) - DP$ معادل تعریف استاندارد حریم خصوصی تفاضلی خواهد بود، که آن را حریم خصوصی تفاضلی محض می نامند. با توجه به تعریف فوق، δ معادل احتمال نقض کامل حریم خصوصی است، بنابراین، تمایل داریم که مقدار δ بسیار کم باشد، مانند $\delta = ۲^{-۲۰}$. لازم به ذکر است که ADP نیز تمامی ویژگی‌های کاربردی حریم خصوصی تفاضلی را که پیش‌تر ذکر شد، دارا است.

۲,۴. دست‌یابی به حریم خصوصی تفاضلی

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[۱] برای دستیابی به حریم خصوصی تفاضلی می‌پردازیم. پیش از آن، بایستی مفهوم مهمی تحت عنوان حساسیت سراسری[۲] (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 ۳ (حساسیت $\ell_۲$-). برای تابع $f: \mathcal{X}^n \to \mathbb{R}^k$، حساسیت-$\ell_۲$ بر روی هر زوج از مجموعه داده‌های همسایه $x \sim x' \in \mathcal{X}^n$ برابر است با

$$\Delta(f) = \max_{x \sim x' \in \mathcal{X}^n} \|f(x) - f(x')\|_۲. \quad (۷)$$

که در آن $\|\cdot\|_۲$ نشانگر نرم-$\ell_۲$ است (ودهان[۳]، ۲۰۱۷).

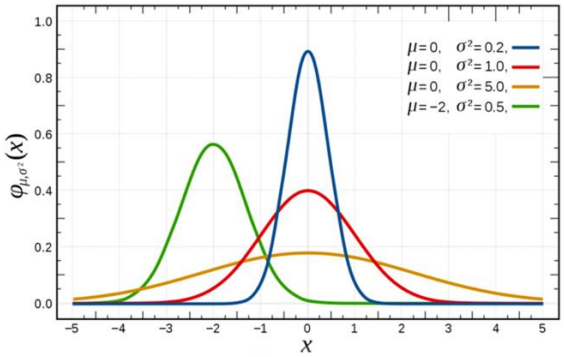
لازم به ذکر است که در نظر گرفتن حساسیت سراسری در ارتباط با مفهوم حریم خصوصی تفاضلی و پیاده‌سازی آن امری بدیهی محسوب می‌شود. در واقع، همانگونه که پیش‌تر اشاره شد، حریم خصوصی تفاضلی سعی می‌کند که اثر حضور و یا عدم حضور هر یک از افراد در مجموعه داده‌ی ورودی یک الگوریتم را پنهان کند. برای انجام چنین کاری، تعیین کران بالایی برای میزان تغییرات خروجی یک الگوریتم با توجه به تغییرات داده‌ی هر یک از افراد گامی کلیدی محسوب می‌شود. با توجه به عنوان مکانیسم گاوسی، نویز مورد نیاز در این مکانیسم از طریق توزیع احتمال گاوسی ایجاد می‌گردد. در ادامه به تعریف توزیع احتمال گاوسی می‌پردازیم.

[۱] Gaussian Mechanism
[۲] Global Sensitivity (GS)
[۳] Vadhan

تعریف ۴ (توزیع احتمال گاوسی). توزیع احتمال گاوسی $\mathcal{N}(\mu, \sigma^2)$ با میانگین μ و واریانس σ^2، دارای چگالی احتمال زیر است (دورک[1] و همکاران، ۲۰۱۴):

$$p(x) = \frac{1}{\sqrt{2\pi\sigma^2}} exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right). \quad (8)$$

در شکل ۳ نمایی از توابع چگالی احتمال توزیع گاوسی به ازای پارامترهای مختلف ارائه شده است.



شکل ۳: وابع چگالی احتمال توزیع گاوسی به ازای پارامترهای مختلف

تعریف ۵ (مکانیسم گاوسی). اگر $f: \mathcal{X}^n \to \mathbb{R}^k$، آنگاه مکانیسم گاوسی به شکل زیر تعریف می‌گردد (دورک[2] و همکاران، ۲۰۱۴):

$$\mathcal{M}(x) = f(x) + (Y_1, \cdots, Y_k), \quad (9)$$

که Y_iها اعداد تصادفی مستقل با توزیع احتمال $\mathcal{N}(0, 2\log(1.25/\delta)\Delta_2^2/\epsilon^2)$ هستند.

۵. مدل پیشنهادی

در این بخش به معرفی مکانیسمی مبتنی بر الگوریتم بهینه‌سازی گرادیان افزایشی[3]، برای دستیابی به حریم خصوصی تفاضلی در بازارهای برق محلی می‌پردازیم. 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 به‌شکلی 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. در واقع، افزودن محتاطانه‌ی نویز به مقادیر خروجی، که در آن میزان نویز بر اساس تحلیل‌های بدبینانه صورت می‌گیرد، می‌تواند به کاهش بسیار شدید رفاه اجتماعی منجر شود. بنابراین، بایستی برای افزودن نویز و دستیابی به حریم خصوصی تفاضلی

[1] Dwork
[2] Dwork
[3] Gradient Ascent

با ظرافت بیشتری عمل کرد. به همین منظور، در مکانیسم پیشنهادی، با بکارگیری الگوریتم گرادیان افزایشی، ماهیت تصادفی مورد نیاز برای حریم خصوصی تفاضلی ر،ا با استفاده از مکانیسم گاوسی، در فرایند بهینه‌سازی اعمال می‌کنیم. پیش از پرداختن به الگوریتم گرادیان افزایشی نویزی، ابتدا مروری بر الگوریتم گرادیان افزایشی خواهیم داشت.

۱,۵. الگوریتم گرادیان افزایشی

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

$$\underset{s\in\mathcal{O}}{\text{argmax}}\ \text{sw}(v,s)=\sum_{i=۱}^{n} v_i(s_i). \qquad (۱۰)$$

ایده‌ی اصلی در الگوریتم گرادیان افزایشی برای یافتن پاسخ بهینه‌ی مساله‌ی فوق، بهبود مکرر یک پاسخ اولیه $s.$ با بروزرسانی این پاسخ از طریق گام‌هایی در راستای گرادیان تابع هدف $\text{sw}(v,s)$ است. در واقع، $\nabla\text{sw}(v,s)$ ضرایب بهترین تقریب خطی تابع هدف $\text{sw}(v,s)$ در پیرامون نقطه‌ی s را ارائه می‌کند. بنابراین، حرکت در راستای گرادیان در این نقطه برابر است با حرکت در راستایی که $\text{sw}(v,s)$ بیشترین افزایش را خواهد داشت. هم‌چنین، از آنجاکه ممکن است در حین بروزرسانی، متغیرهای تصمیم‌گیری از ناحیه‌ی مجاز مساله تسویه بازار $\mathcal{O}$ خارج شوند، نگاشت $\Pi_{\mathcal{O}}(\cdot)$ به منظور انتقال دوباره‌ی این متغیرها به ناحیه‌ی مجاز در الگوریتم گرادیان افزایشی تعبیه شده است. الگوریتم ۱ به تشریح گام‌های الگوریتم گرادیان افزایشی و پیاده‌سازی آن اختصاص دارد.

الگوریتم ۱: الگوریتم گرادیان افزایشی

ورودی‌ها: مجموعه‌ی توابع ارزش‌گذاری شرکت‌کنندگان در بازار $v=(v_i)_{i\in\Omega}$، تابع رفاه اجتماعی $\text{sw}(v,s)=\sum_{i=۱}^{n} v_i(s_i)$، مجموعه‌ی پاسخ‌های مجاز $\mathcal{O}\subseteq\mathbb{R}^n$، تعداد تکرار T، گام بروزرسانی η.

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

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

۲: **برای هر** $t\in[T]$:

۳: محاسبه‌ی گرادیان تابع رفاه اجتماعی برای هر شرکت‌کننده در بازار $g_t=\nabla_s\text{sw}(v,s_{t-۱})$

۴: بروزرسانی متغیرها:

$$u_t=s_{t-۱}+\eta g_t$$

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

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

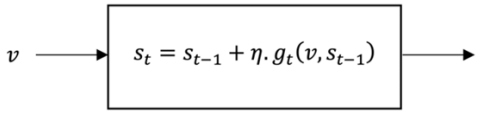
۶: **پایان حلقه**

۷: **بازگشت** s_T.

۲,۵. مکانیسم تسویه بازار پیشنهادی

همانطورکه اشاره شد، برای تحقق حریم خصوصی تفاضلی نویز مورد نیاز را در فرایند بهینه‌سازی مساله تسویه بازار، که مبتنی بر الگوریتم گرادیان افزایشی است، تعبیه می‌کنیم. در واقع، بایستی مقدار تنظیم‌شده‌ای نویز با توزیع گاوسی را به قاعده‌ی بروزرسانی متغیرها در هر تکرار

الگوریتم گرادیان افزایشی اضافه کنیم. شکل ۴ بلوک محاسباتی که بایستی، با بکارگیری مکانیسم گاوسی، حافظ حریم خصوصی داده‌های شرکت‌کنندگان در بازار باشد را نمایش می‌دهد.



شکل ۴: بروزرسانی متغیرهای تصمیم‌گیری شرکت‌کنندگان در بازار در گام tام

همانطورکه می‌دانیم، نویز مورد نیاز بایستی با توجه به حساسیت محاسبه‌ی مورد نظر در شکل ۴ تعیین گردد. هرچه میزان این حساسیت به داده‌های عامل‌ها کمتر باشد، نویز کمتری مورد نیاز است. به عبارتی، دستیابی به حریم خصوصی تفاضلی در الگوریتم گرادیان افزایشی از طریق مکانیسم گاوسی نیازمند محدودسازی تاثیر داده‌های هر یک از عامل‌ها در محاسبه‌ی گرادیان g_t در هر تکرار است.در این بلوک، $g_t(v, s_{t-1})$ تنها مولفه‌ای است که از داده‌های ورودی v بهره می‌گیرد، بنابراین، تنها بایستی توجه خود را معطوف به محاسبه‌ی حساسیت $g_t(v, s_{t-1})$ و افزودن نویز مورد نیاز برای محاسبه‌ی حافظ حریم خصوصی تفاضلی $g_t(v, s_{t-1})$ کنیم. در واقع، با توجه به خاصیت پساپردازشی حریم خصوصی تفاضلی، خروجی بلوک شکل ۴ حافظ حریم خصوصی تفاضلی خواهد بود. چراکه، s_t ترکیب خطی از $g_t(v, s_{t-1})$ است، که نیازمند ارجاع دوباره به داده‌های ورودی v نیست.

به دلیل اینکه در اکثر موارد کران محدودی برای حساسیت اشاره‌شده وجود ندارد، بایستی راهکار دیگری اتخاذ کنیم. در این راهکار که مبتنی بر قضیه ۱ برای الگوریتم گرادیان افزایشی است، 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 است. بر اثر این شیوه‌ی محدودسازی اندازه‌ی گرادیان‌ها، اگر $\|g\|_2 \leq C$، انگاه گرادیان g بدون تغییر خواهد ماند. درحالی‌که، اگر $\|g\|_2 \geq C$، با تغییر مقیاس گرادیان g اندازه‌ی ان برابر با $\|g\|_2 = C$ خواهد شد. بنابراین، حساسیت $g_t(v, s_{t-1})$، با توجه به نامساوی مثلثی، برابر است با:

$$\Delta = \max_{v \sim v'} \|\nabla \mathrm{sw}(v, s_{t-1}) - \nabla \mathrm{sw}(v', s_{t-1})\|_2 \leq \max_{v \sim v'} (\|\nabla \mathrm{sw}(v, s_{t-1})\|_2 - \|\nabla \mathrm{sw}(v', s_{t-1})\|_2) = 2. \qquad (11)$$

حال، با توجه به اعمال مکانیسم گاوسی، برای اینکه بلوک بروزرسانی متغیرهای تصمیم‌گیری در شکل ۴ حافظ حریم خصوصی تفاضلی با پارامترهای (ϵ', δ') باشد، کافی است نویزی با مقیاس $\sigma \geq \frac{2}{n\epsilon'} \sqrt{2 \ln\left(\frac{1.25}{\delta'}\right)}$ به گرادیان محاسبه‌شده $g_t(v, s_{t-1})$ در هر تکرار اضافه کنیم.. الگوریتم ۲ چگونگی تسویه بازارهای برق گاوسی را نشان می‌دهد (آبادی[1] و همکاران، ۲۰۱۶).

[1] Abadi

الگوریتم ۲: الگوریتم گرادیان افزایشی نویزی

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 $s.$ 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.

۳،۵. مکانیسم تعیین پرداختی‌های شرکت‌کنندگان در بازار

در کنار مقادیر تسویه بازار، پرداختی‌های شرکت‌کنندگان در بازار نیز به شکلی عمومی منتشر خواهد شد. بدین ترتیب، فرد متخاصمی که در تلاش برای کسب اطلاعات خصوصی شرکت‌کنندگان در بازار است، به این پرداختی‌ها دسترسی دارد. از انجاکه، این پرداختی‌ها نیز بر اساس محاسباتی بر روی داده‌های افراد تعیین شده است، امکان افشای اطلاعات خصوصی افراد از طریق دسترسی به آن‌ها وجود دارد. بنابراین، با به‌کارگیری حریم خصوصی تفاضلی، بایستی از امکان تشخیص و تمایز در پرداختی‌های بازار $p = (p_1(v), \cdots, p_n(v))$ توسط فرد متخاصم جلوگیری کنیم. در همین راستا، برای هر زوج پروفایل ارزش‌گذاری همسایه $v \sim v' \in V^n$ و هر پروفایل پرداختی $p \in \mathcal{P}$، قید مبتنی بر حریم خصوصی تفاضلی پیش رو بایستی برقرار باشد:

$$\Pr[\, p_1(v), \cdots, p_n(v) \in \mathcal{P}] \leq e^{\epsilon}.\Pr[\, p_1(v'), \cdots, p_n(v') \in \mathcal{P}]. \qquad (۱۲)$$

در این مقاله تعیین پرداختی‌های شرکت‌کنندگان در بازار 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 ۳، 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 (تساوسوگلو[۱] و همکاران، ۲۰۲۱)

الگوریتم ۳: تعیین پرداختی‌های VCG عامل‌ها 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:

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

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.

همانگونه که در الگوریتم ۳ اشاره شد، برای محاسبه‌ی پرداختی‌های مکانیسم VCG، نیازمند محاسبه‌ی رفاه اجتماعی هستیم. از همین روی، برای تضمین حفاظت از حریم خصوصی پرداختی‌ها، نیازی به پیاده‌سازی یک مکانیسم حافظ حریم خصوصی تفاضلی جدید نیست، و تنها کافی‌ست که الگوریتم ۲ را برای محاسبه‌ی پرداختی‌های مکانیسم VCG به کار گیریم، که در ادامه به چگونگی آن اشاره می‌کنیم.

الگوریتم ۴ به محاسبه‌ی پرداختی‌ها تحت حفاظت حریم خصوصی تفاضلی اختصاص دارد. در گام نخست، الگوریتم ۳ اقدام به فراخوانی الگوریتم ۲ با ورودی $v = (v_i)_{i\in\Omega}$ می‌کند و توزیع احتمال خروجی $\mathcal{D}^*$ را که در ادامه برای محاسبه‌ی مقدار 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 ۲ تعیین می‌کند، تا با بهره‌گیری از توزیع احتمال خروجی $\mathcal{D}_{-i}$، 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 پرداختی‌های p شرکت‌کنندگان در بازار را محاسبه کند.

الگوریتم ۴: محاسبه‌ی پرداختی‌های VCG حافظ حریم خصوصی

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

خروجی‌ها: مقدار انتظاری پرداختی‌های شرکت‌کنندگان در بازار p.

۱: **فراخوانی** الگوریتم ۲:

ورودی‌ها: $v = (v_i)_{i\in\Omega}$، ϵ، n_s

[۱] Tsaousoglou

خروجی‌ها: $r \sim \mathcal{D}$

۲: **برای هر** $i \in \Omega$:

۳: فراخوانی الگوریتم ۲:

ورودی‌ها: n_s ،ϵ ،$v = \left(v_j\right)_{j\in\Omega, j\neq i}$

خروجی‌ها: $r \sim \mathcal{D}_{-i}$

۴: $\mathrm{sw}_{-i}(\mathcal{D}_{-i}) = \mathbb{E}_{r\sim\mathcal{D}_{-i}}\left[\sum_{j\neq i} v_j(r)\right]$

۵: $\mathrm{sw}_{-i}(\mathcal{D}) = \mathbb{E}_{r\sim\mathcal{D}}\left[\sum_{j\neq i} v_j(r)\right]$

۶: $p_i = \mathrm{sw}_{-i}(\mathcal{D}_{-i}) - \mathrm{sw}_{-i}(\mathcal{D})$

۷: **پایان حلقه**

۸: **بازگشت** p.

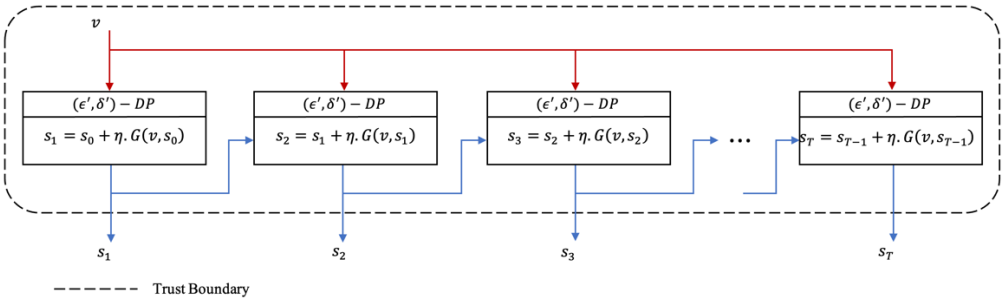
۴,۵. تحلیل تلفات حریم خصوصی مکانیسم پیشنهادی

برای تحلیل مکانیسم بازارهای برق محلی گاوسی از منظر تلفات حریم خصوصی، بایستی الگوریتم‌های تسویه بازار و تعیین پرداختی‌ها را به صورت مجزا بررسی کنیم. در این بخش، ابتدا توجه خود را به الگوریتم تسویه بازار، که مبتنی بر گرادیان افزایشی نویزی است، معطوف می‌کنیم و سپس به تحلیل تلفات حریم خصوصی در محاسبه‌ی پرداختی‌های بازار در مکانیسم پیشنهادی می‌پردازیم.

۱,۴,۵. تلفات حریم خصوصی در مکانیسم تسویه بازار

برای تحلیل تلفات حریم خصوصی در این الگوریتم، می‌توانیم از خاصیت ترکیب‌بندی حریم خصوصی تفاضلی بهره گیریم. بدین نحو که کل فرایند مبتنی بر تکرار الگوریتم گرادیان افزایشی را به عنوان مجموعه‌ای از محاسبه‌های متوالی حافظ حریم خصوصی تفاضلی تلقی کنیم، و با استفاده از خاصیت ترکیب‌بندی، پارامترهای حریم خصوصی تفاضلی کل فرایند را محاسبه کنیم. شکل ۵ T تکرار از الگوریتم گرادیان افزایشی نویزی را نمایش می‌دهد، که در آن $s_t, \forall t \in [T]$ بیانگر متغیرهای تصمیم‌گیری شرکت‌کنندگان در بازار در تکرار tام، η ضریب گام بروزرسانی الگوریتم، و $G(v, s_t)$ محاسبه‌ی گرادیان تابع رفاه اجتماعی حافظ حریم خصوصی تفاضلی است. لازم به ذکر است که نحوه‌ی محاسبه‌ی $G(v, s_t)$ در الگوریتم ۲ ذکر گردید.

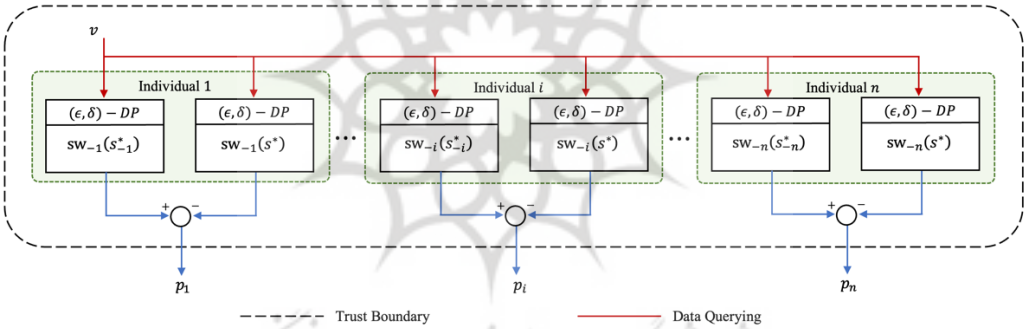
با توجه شکل ۵، مشاهده می‌کنیم که خروجی بلوک بروزرسانی تصمیم‌گیری در تکرار $(t-1)$ام الگوریتم به عنوان ورودی بلوک بروزرسانی تصمیم‌گیری در تکرار tام الگوریتم مورد استفاده قرار می‌گیرد. بنابراین، اگر در هر تکرار از الگوریتم، مقادیر متغیرهای تصمیم‌گیری به‌روزرسانی شده را منتشر کنیم، الگوریتم نهایی ما حاصل ترکیب‌بندی تطبیقی بلوک‌های بروزرسانی، که هر یک حافظ حریم خصوصی تفاضلی هستند، خواهد بود. در واقع، بروزرسانی متغیرهای تصمیم‌گیری در تکرار t ام به تکرار $(t-1)$ام وابسته است و اگر هر یک از آن‌ها حافظ حریم خصوصی تفاضلی باشند، الگوریتم نهایی نیز که متشکل از T بلوک بروزرسانی است، طبق قضیه‌ی ترکیب‌بندی پیشرفته حافظ حریم خصوصی تفاضلی خواهد بود. با توجه به قضیه‌ی ترکیب‌بندی پیشرفته، برای اینکه الگوریتم نهایی $(\epsilon, \delta) - DP$ باشد، مقدار نویزی که در هر تکرار بایستی به بلوک‌های بروزرسانی متغیرها تزریق گردد دارای مقیاسی معادل $\sigma \geq \frac{۲}{n\epsilon}\sqrt{۲\ln\left(\frac{۱.۲۵}{\delta}\right)}$ است.



شکل ۵: ترکیب‌بندی T بلوک $(\epsilon', \delta') - DP$ بروزرسانی متغیرهای تصمیم‌گیری

۱،۴،۵. تلفات حریم خصوصی در مکانیسم تعیین پرداختی‌ها

شکل ۶ ترکیب‌بندی بلوک‌های محاسبه‌ی پرداختی‌های VCG را نمایش می‌دهد. همانطورکه پیش‌تر گفته شد، محاسبه‌ی پرداختی VCG برای هر شرکت‌کننده‌ی در بازار نیازمند دسترسی به داده‌های خصوصی ورودی (توابع ارزش‌گذاری شرکت‌کنندگان در بازار) به منظور محاسبه‌ی $\mathrm{sw}_{-i}(s^*_{-i})$ و $\mathrm{sw}_{-i}(s^*)$ است. می‌دانیم که مکانیسم پیشنهادی برای بیشینه‌سازی رفاه اجتماعی و محاسبه‌ی مقادیر تسویه بازار $(\epsilon, \delta) - DP$ است. بنابراین، محاسبه‌ی پرداختی VCG برای هر شرکت‌کننده در بازار، با توجه به خاصیت ترکیب‌بندی، $(۲\epsilon, ۲)-DP$ خواهد بود. از انجاکه، تعداد کل شرکت‌کنندگان در بازار n است، محاسبه‌ی تمامی پرداختی‌های $(-۲, ۲\epsilon)$ DP خواهد بود.



شکل ۶: ارزیابی تلفات حریم خصوصی در محاسبه‌ی پرداختی‌های VCG بازارهای برق گاوسی

٦. مطالعات عددی

در این بخش با هدف انعکاس مشخصه‌های نظری مکانیسم حافظ حریم خصوصی تفاضلی پیشنهادی برای بازارهای برق محلی، نتایج مطالعات عددی را ارائه خواهیم کرد. به همین منظور، یک شبکه انرژی محلی متشکل از ۳ تولیدکننده و ۳ مصرف‌کننده را با توجه به سیستم تست استفاده‌شده در مرجع () تهیه می‌کنیم. تابع هزینه تولیدکننده i و تابع منفعت مصرف‌کننده i در قالب توابع درجه‌ی دو هستند، و به ترتیب عبارتند از $C_{i,\theta_i}(\cdot) := a_i^g g_i^۲ + b_i^g g_i + c_i^g$ و $U_{i,\theta_i}(\cdot) := a_i^u d_i^۲ + b_i^u d_i + c_i^u$. پارامترهای مورد نیاز برای توابع هزینه و منفعت در جدول۱ ارائه شده است.

جدول۱ : پارامترهای اقتصادی و فیزیکی شرکت‌کنندگان در بازار

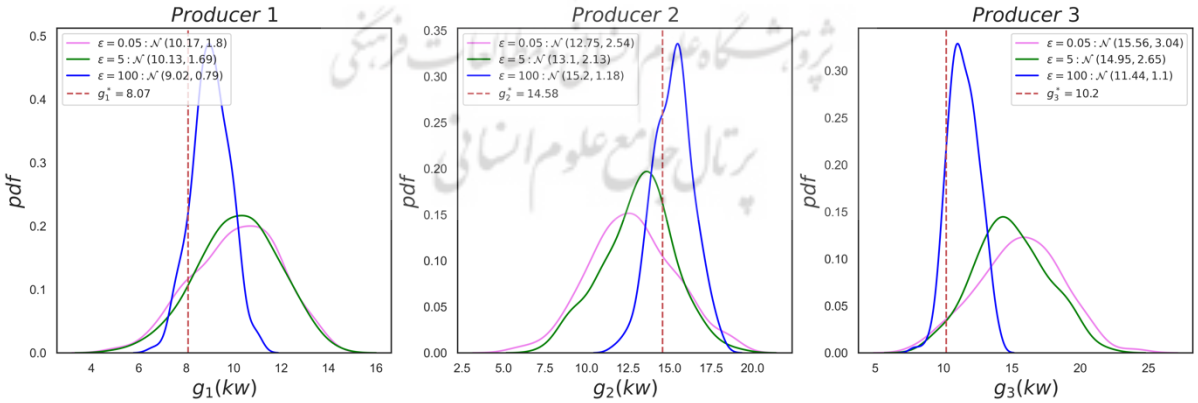
	a_i^g	b_i^g	c_i^g	$\underline{g_i}$	$\overline{g_i}$
Producers	($/kWh^۲)	($/kWh)	($)	(kW)	(kW)

۱	۰,۰۱۵	۰,۰۳۸	۰	۰	۲۰
۲	۰,۰۰۸	۰,۰۴۷	۰	۰	۲۵
۳	۰,۰۱۱	۰,۰۵۶	۰	۰	۳۰

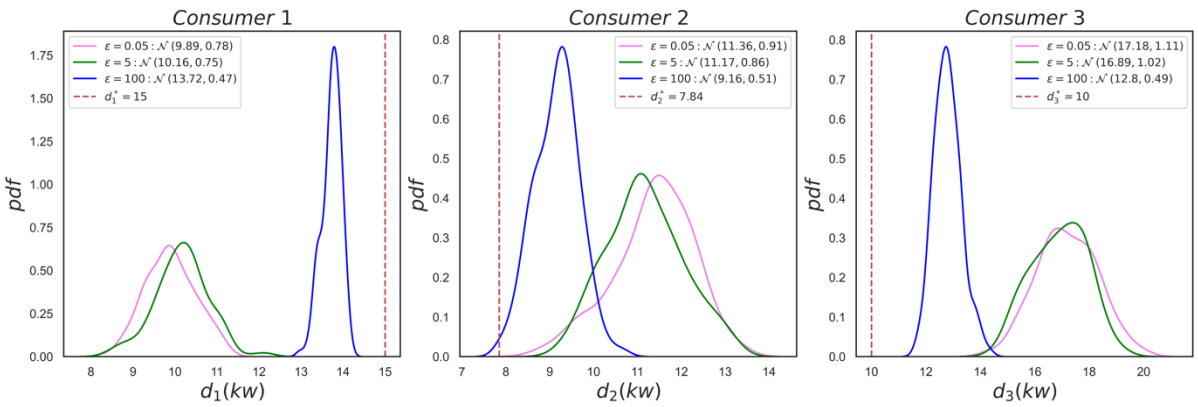
Consumers	a_i^u ($/kWh^2)	b_i^u ($/kWh)	c_i^u ($)	$\underline{d_i}$ (kW)	$\overline{d_i}$ (kW)
۱	-۰,۰۰۸	۰,۸	۰	۵	۱۵
۲	-۰,۰۱۴	۰,۵	۰	۵	۱۸
۳	-۰,۰۰۹	۰,۴	۰	۱۰	۲۵

۱,۶. مقادیر تسویه بازار

همانگونه که انتظار داریم، خروجی‌های یک مساله تسویه بازار حافظ حریم خصوصی تفاضلی ماهیتی تصادفی دارند و در قالب یک توزیع احتمال خواهند بود. در این بخش، به بررسی توزیع‌های احتمال متغیرهای تصمیم‌گیری مربوط به هر یک از تولیدکنندگان و مصرف‌کنندگان، تحت سیاست‌های حفاظت از حریم خصوصی متفاوت، خواهیم پرداخت. برای این منظور ۳ مقدار $\epsilon = ۰.۰۵$، $\epsilon = ۵$، و $\epsilon = ۱۰۰$ که به ترتیب با سطح حفاظت زیاد، متوسط، و کم متناسب هستند، مورد بررسی قرار گرفته است. در شکل ۷ و شکل ۸ چگالی‌های توزیع احتمال برای مقادیر تسویه بازار تولیدکنندگان و مصرف‌کنندگان، به ازای پارامترهای ϵ ذکرشده، ترسیم شده است. لازم به ذکر است که چگالی‌های توزیع احتمال ترسیم‌شده حاصل ۲۰۰ نمونه‌برداری از توزیع احتمال حقیقی مقادیر تسویه بازار است. هم‌چنین، پارامترهای میانگین μ و واریانس σ^2 مربوط به هر یک از چگالی‌های توزیع احتمال، $\mathcal{N}(\mu, \sigma^2)$، به تفکیک پارامتر ϵ تعیین شده است.



شکل ۷: چگالی توزیع احتمال مقادیر تسویه بازار تولیدکنندگان

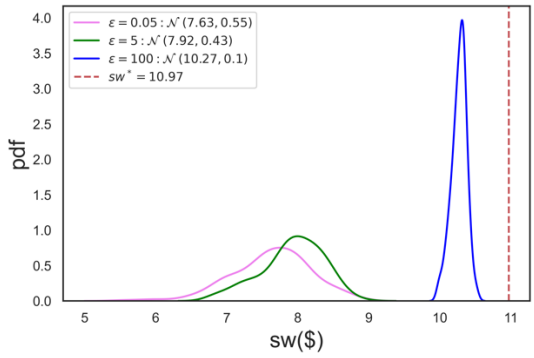


شکل ۸: چگالی توزیع احتمال مقادیر تسویه بازار مصرف‌کنندگان

مطابق انتظار، با کاهش ϵ، یا به عبارتی افزایش سطح حفاظت از حریم خصوصی، واریانس چگالی توزیع احتمال مقادیر تسویه بازار افزایش می‌یابد. در واقع، این افزایش واریانس به مفهوم افزایش دامنه‌ی تولید نویز و انحراف مقادیر حافظ حریم خصوصی از مقادیر بهینه در راستای حفاظت از حریم خصوصی شرکت‌کنندگان در بازار است. از طرف دیگر، مشاهده می‌کنیم که با افزایش ϵ مقدار متوسط چگالی توزیع احتمال مقادیر مساله تسویه بازار به سمت مقادیر بهینه خود در غیاب قیود حریم خصوصی تفاضلی متمایل می‌شوند. به عبارت دیگر، با افزایش مقدار ϵ به مقادیر خیلی بالا، چگالی‌های توزیع احتمال با واریانسی قابل چشم‌پوشی در مجاورت مقادیر بهینه تسویه بازار قرار می‌گیرند، و عملکرد بهینه بازار نسبت به حفاظت از حریم خصوصی اولویت می‌یابد.

۲,۶. هزینه حفاظت از حریم خصوصی

تمرکز این بخش بر روی ارزیابی مصالحه‌ی میان رفاه اجتماعی مساله تسویه بازار و سطح حفاظت از حریم خصوصی شرکت‌کنندگان در بازار قرار دارد. همانطورکه می‌دانیم، بهای تامین حریم خصوصی شرکت‌کنندگان در بازار در قالب کاهش رفاه اجتماعی منعکس می‌گردد. در واقع، این کاهش رفاه اجتماعی ریشه در افزودن نویز به فرایند بهینه‌سازی مساله تسویه بازار دارد، که منجر به انحراف مقادیر تسویه بازار از مقادیر بهینه می‌شود. می‌توان انتظار داشت که هرچه مقدار میزان نویز تزریق‌شده به فرایند بهینه‌سازی مساله تسویه بازار بیشتر باشد، رفاه اجتماعی نیز بیشتر کاهش می‌یابد. شکل ۹ چگالی توزیع احتمال رفاه اجتماعی را به ازای ۳ مقدار متفاوت برای ϵ نمایش می‌دهد. مشاهده می‌کنیم که به ازای $\epsilon = ۰.۰۵$، متناظر با سطح بالایی از حفاظت از حریم خصوصی، مقدار انتظاری رفاه اجتماعی معادل $\mathbb{E}[sw] =$ ۷.۶۳ $ است. این مقدار در مقایسه با مقدار بهینه‌ی رفاه اجتماعی $sw^* =$ ۱۰.۹۷ $ کاهش چشم‌گیری محسوب می‌شود.



شکل ۹: چگالی توزیع احتمال رفاه اجتماعی

با افزایش پارامتر تلفات حریم خصوصی به $\epsilon = ۱۰۰$ مقدار انتظاری چگالی توزیع احتمال رفاه اجتماعی معادل $\mathbb{E}[sw] = ۱۰.۲۷$ می‌شود، که بسیار نزدیک به مقدار بهینه‌ی رفاه اجتماعی است. بااین‌حال، این بهبود رفاه اجتماعی با بهای چشم‌پوشی از حریم خصوصی شرکت‌کنندگان در بازار حاصل می‌شود. نمودارهای چگالی توزیع احتمال رفاه اجتماعی ابزار خوبی برای بهره‌بردار بازار در جهت انتخاب آگاهانه‌ی پارامتر ϵ محسوب می‌شوند. به عنوان مثال، همانطور که در شکل ۹ مشاهده می‌کنیم، چگالی‌های توزیع احتمال رفاه اجتماعی به ازای $\epsilon = ۰.۰۵$ و $\epsilon = ۵$ تقریبا مشابه یکدیگر هستند. از همین روی، در صورتی که شرکت‌کنندگان در بازار حساسیت بالایی نسبت به حریم خصوصی خود داشته باشند، می‌توان $\epsilon = ۰.۰۵$ را در مقایسه با $\epsilon = ۵$، بدون نگرانی از اختلاف چشمگیر هزینه‌های حریم خصوصی، برگزید.

۳,۶. منفعت شرکت‌کنندگان در بازار

در این بخش منفعت شرکت‌کنندگان در بازار و نحوه‌ی اثرگذاری قید حریم خصوصی تفاضلی بر آن را بررسی خواهیم کرد. میزان منفعت u_i برای هر عامل $i \in \Omega$ شرکت‌کننده‌ی در بازار، مطابق با رابطه‌ی زیر است:

$$u_i(s_i) = v_i(s_i) - p_i(v), \qquad (۱۳)$$

که در آن v_i و p_i به ترتیب تابع ارزش‌گذاری و میزان پرداختی عامل i در بازار خواهند بود.

جدول۲ مقادیر انتظاری و انحراف معیار توزیع احتمال منفعت تولیدکنندگان، u_i^p، و مصرف‌کنندگان، u_i^c، را تحت سطوح حفاظتی متفاوت حریم خصوصی، ϵ، نمایش می‌دهد. لازم به ذکر است که پارامترهای فوق بر اساس ۲۰۰ نمونه‌برداری از توزیع‌های احتمال متناظر با توابع منفعت هر یک از شرکت‌کنندگان در بازار محاسبه شده است. همانطور که پیش‌تر اشاره کردیم، به ازای مقادیر بالای پارامتر حریم خصوصی تفاضلی، مانند $\epsilon = ۵۰۰$، خروجی‌های بازار تقریبا مشابه حالتی است که قید حریم خصوصی تفاضلی وجود ندارد. بنابراین، ستون $\epsilon = ۵۰۰$ در جدول۲ مقادیر بهینه‌ی منفعت هر یک از شرکت‌کنندگان در بازار را نمایش می‌دهد. هم‌چنین، مشاهده می‌کنیم که مقدار انحراف معیار در این حالت نیز بسیار اندک است، که نشان از خروجی‌های تقریبا قطعی دارد. در نقطه‌ی مقابل، به ازای مقادیر کوچک پارامتر حریم خصوصی تفاضلی، مانند $\epsilon = ۰.۵$، مکانیسم تسویه بازار پیشنهادی، تقریبا به شکلی کاملا تصادفی، مقادیری را به عنوان خروجی‌ها تعیین خواهد کرد. همانگونه که در ستون $\epsilon = ۰.۵$ جدول۲ مشاهده می‌کنیم، مقادیر انتظاری منفعت شرکت‌کنندگان در بازار تفاوت چشم‌گیری با مقادیر بهینه،

$\epsilon = ۵۰۰$، دارند. علاوه‌براین، انحراف معیار توزیع احتمال منفعت شرکت‌کنندگان در بازار نیز مقدار زیادی دارد، که بر ماهیت بسیار تصادفی بازار در راستای تامین سطح بالایی از حفاظت حریم خصوصی دلالت دارد.

جدول۲ : مقادیر انتظاری و انحراف معیار منفعت شرکت‌کنندگان در بازار تحت ملاحظات حریم خصوصی ($)

	$\epsilon = ۰.۵$		$\epsilon = ۵$		$\epsilon = ۵۰$		$\epsilon = ۵۰۰$	
	μ	σ	μ	σ	μ	σ	μ	σ
u_1^c	۳,۹	۰,۶۲	٤,۳	۰,۶۱	٥,۶۲	۰,۳٥	٦,٥٨	۰,۰٥٥
u_2^c	-۰,۰۷	۰,۶۱	۰,۳	۰,٥۹	۰,۹۳	۰,٤٤	۱,۰۸	۰,۰٦٥
u_3^c	-۱,٤	۰,٥٥	-۰,۹	۰,٥۲	۰,۰۱	۰,۳۹	۰,٥٦	۰,۰٤
u_1^p	۱,۰۲	۰,۷۷	۱,۲۷	۰,۷۱	۱,٤۷	۰,٤۸	۱,۱۹	۰,۰۷
u_2^p	۲,٤٤	۰,۷۱	۲,۷	۰,٦۹	۳,۰۲	۰,٤٥	۲,٦۸	۰,۰۸۲
u_3^p	۰,۷	۰,٦	۱,۰۸	۰,٥٥	۱,۷۲	۰,٤٥	۱,٥۲	۰,۰۷۲

لازم به ذکر است که هزینه‌ی بالای تامین حریم خصوصی به ازای $\epsilon = ۰.۵$ منجر به منفی شدن منفعت مصرف‌کنندگان ۲ و ۳ می‌شود. در واقع می‌توان گفت، که این سطح از حفاظت از حریم خصوصی برای این شرکت‌کنندگان توجیه اقتصادی ندارد. اما، از انجاکه پارامتر حریم خصوصی تفاضلی به شکل متمرکز تعیین می‌گردد، به ناچار همه‌ی شرکت‌کنندگان در بازار متحمل هزینه‌های ناشی از آن خواهند شد، حتی اگر حساسیت آن‌ها نسبت به حریم خصوصی یکسان نباشد.

۷. نتیجه‌گیری

در این مقاله یک مکانیسم تسویه بازار حافظ حریم خصوصی تفاضلی برای بازارهای برق محلی ارائه شد. مکانیسم پیشنهادی در چارچوب بازارهای برق متمرکز ارائه شده است و از مکانیسم VCG نیز برای تعیین پرداختی‌های بازار استفاده می‌شود. این مقاله با تکیه بر حریم خصوصی تفاضلی کران بالایی قابل اثبات برای ریسک مرتبط با نقض حریم خصوصی شرکت‌کنندگان در بازار ارائه می‌کند. برای دست‌یابی به حریم خصوصی تفاضلی، از مکانیسم گاوسی برای مبهم‌سازی الگوریتم گرادیان افزایشی در فرایند بهینه‌سازی مساله تسویه بازار استفاده می‌شود. هم‌چنین، برای اطمینان از قرار گرفتن خروجی‌های مساله تسویه بازار در ناحیه مجاز، سازوکاری برای تصویر کردن متغیرهای بروزرسانی‌شده، در الگوریتم گرادیان افزایشی، به ناحیه مجاز اعمال می‌شود. در بخش مطالعات عددی مشاهده کردیم که حفاظت از حریم خصوصی شرکت‌کنندگان در بازار منجر به کاهش رفاه اجتماعی شرکت‌کنندگان در بازار می‌گردد، و یک مصالحه‌ی ذاتی میان حفاظت از حریم خصوصی و رفاه اجتماعی وجود دارد. هم‌چنین، مشاهده کردیم که با افزایش پارامتر حریم خصوصی تفاضلی به مقادیر بسیار بالا، که متناظر با سطح حفاظت بسیار پایین است، خروجی‌های مساله تسویه بازار حافظ حریم خصوصی تفاضلی به سمت خروجی‌های بهینه سوق پیدا می‌کنند، و قید حریم خصوصی تفاضلی بی‌اثر می‌گردد. در نقطه‌ی مقابل نیز با کاهش پارامتر حریم خصوصی تفاضلی به مقادیر بسیار پایین، مکانیسم تسویه بازار مقادیری کاملا تصادفی را، بی‌توجه به داده‌های ورودی و در راستای حفاظت حداکثری از حریم خصوصی شرکت‌کنندگان در بازار، به عنوان خروجی‌های مساله تسویه بازار تعیین می‌کند.

منابع

A. Samy, et al. (۲۰۲۱), "Spets: Secure and privacy- preserving energy trading system in microgrid," Sensors, vol. ۲۱, no. ۲۳, p. ۸۱۲۱.

A. Wood, et al. (۲۰۱۸), "Differential privacy: A primer for a non-technical audience," Vand. J. Ent. & Tech. L., vol. ۲۱, p. ۲۰۹.

C. Domingo-Enrich, et al. (۲۰۲۲), "Auditing differential privacy in high dimensions with the kernel quantum renyi divergence," arXiv preprint arXiv:۲۲۰۵,۱۳۹٤۱.

C. Dwork, et al. (۲۰۱٤), "The algorithmic foundations of differential privacy." Found. Trends Theor. Comput. Sci., vol. ۹, no. ۳-٤, pp. ۲۱۱– ٤۰۷.

D. Lee, et al. (۲۰۲۱), "Data privacy and residential smart meters: Comparative analysis and harmonization potential," Utilities Policy, vol. ۷۰, p. ۱۰۱۱۸۸.

F. Fioretto, et al. (۲۰۱۹), "Differential privacy for power grid obfuscation," IEEE Transactions on Smart Grid, vol. ۱۱, no. ۲, pp. ۱۳۵٦–۱۳٦٦.

F.Zhou, et al. (۲۰۱۹),"Differentialprivacyofaggregated dc optimal power flow data," in ۲۰۱۹ American Control Conference (ACC). IEEE, pp. ۱۳۰۷–۱۳۱٤.

G. Tsaousoglou, et al. (۲۰۲۱), "Mech- anism design for fair and efficient dso flexibility markets," IEEE transactions on smart grid, vol. ۱۲, no. ۳, pp. ۲۲٤۹–۲۲٦۰.

G.Tsaousoglou, et al. (۲۰۲۲),"Marketmechanisms for local electricity markets: A review of models, solution concepts and algorithmic techniques," Renewable and Sustainable Energy Reviews, vol. ۱۵٦, p. ۱۱۱۸۹۰.

J. Zhao, et al. (۲۰۱٤), "Achieving differential privacy of data disclosure in the smart grid," in IEEE INFOCOM ۲۰۱٤-IEEE Conference on Computer Communications. IEEE, pp. ۵۰٤–۵۱۲.

K. Nissim (۲۰۲۱), "Privacy: From database reconstruction to legal theorems," in Proceedings of the ٤۰th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems, pp. ۳۳–٤۱.

M. Abadi, et al. (۲۰۱٦). "Deep learning with dif- ferential privacy". In Proceedings of the ۲۰۱٦ ACM SIGSAC Conference on Computer and Communications Security, pages ۳۰۸–۳۱۸. ACM.

M. B. Gough, et al. (۲۰۲۱), "Preserving privacy of smart meter data in a smart grid environment," IEEE Transactions on Industrial Informatics, vol. ۱۸, no. ۱, pp. ۷۰۷–۷۱۸.

M.G.Boroujeni, et al. (۲۰۱۹),"Privacy of real-time pricing in smart grid," in ۲۰۱۹ IEEE ۵۸th Conference on Decision and Control (CDC). IEEE, pp. ۵۱٦۲–۵۱٦۷.

S. Bjarghov, et al. (۲۰۲۱), "Devel- opments and challenges in local electricity markets: A comprehensive review," *IEEE Access*, vol. ۹, pp. ۵۸ ۹۱۰–۵۸ ۹٤۳.

S. Truex, et al. (۲۰۱۹), "A hybrid approach to privacy-preserving federated learning," in Proceedings of the ۱۲th ACM workshop on artificial intelligence and security, pp. ۱–۱۱.

S. Vadhan (۲۰۱۷), "The complexity of differential privacy," in Tutorials on the Foundations of Cryptography. Springer, pp. ۳٤۷–٤۵۰.

T. W. Mak, et al. (۲۰۲۰), "Privacy-preserving obfuscation for distributed power systems," Electric Power Systems Research, vol. ۱۸۹, p. ۱۰٦۷۱۸.

V.Dvorkin, et al. (۲۰۲۰), "Differentially private optimal power flow for distribution grids," IEEE Transactions on Power Systems, vol. ۳٦, no. ۳, pp. ۲۱۸٦–۲۱۹٦.

X. Lou, et al. (۲۰۲۰), "Cost and pricing of differen- tial privacy in demand reporting for smart grids," IEEE Transactions on Network Science and Engineering, vol. ۷, no. ۳, pp. ۲۰۳۷–۲۰۵۱.

Z. Yang, et al. (۲۰۱۷), "Differential-privacy preserving optimal power flow in smart grid," IET Generation, Transmission & Distribution, vol. ۱۱, no. ۱۵, pp. ۳۸۵۳–۳۸٦۱.