نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

مدلسازی و تحلیل پروتکل رای گیری F.O.O با ابزارهای تحلیل صوری

قادر ابراهیم پور[۱]، علیرضا رنجبران[۲]، بابک صادقیان[۳]

[۱] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران،
ebrahimpour.g@aut.ac.ir

[۲] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران،
ranjbaran@aut.ac.ir

[۳] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران،
basadegh@aut.ac.ir

چکیده

پروتکل‌های رای‌گیری گام‌هایی را مشخص می‌کنند که افراد با پیمودن آن می‌توانند در رای‌گیری شرکت کرده و رای خود را به ثبت برسانند و در عین حال از صحت انتخابات نیز مطمئن باشند. بنابراین این پروتکل‌ها بایستی خواسته‌های امنیتی خاصی را برآورده کنند. در این مقاله سعی داریم با مدلسازی پروتکل F.O.O با ابزارهای صوری، برخی از ویژگی‌های امنیتی آن را تحلیل کنیم. همچنین نشان می‌دهیم که برخلاف ادعای [2] این پروتکل در محیط‌هایی با مقیاس وسیع تنها در شرایط ایده‌آل (و در برخی موارد نزدیک به ایده‌آل) قابل استفاده است، اما در حالت کلی برای محیطی که مقیاس وسیعی را دربرمی‌گیرد، قابل استفاده نخواهد بود.

کلمات کلیدی

رای‌گیری الکترونیکی، پروتکل امنیتی، تحلیل صوری، خواسته‌های امنیتی، PRISM

۱- مقدمه

رای‌گیری الکترونیکی به استفاده از تجهیزات رایانه‌ای برای دادن رای در یک انتخابات اشاره دارد [1]. پروتکل‌های رای‌گیری الکترونیکی روشی مناسب، موثر و قابل اعتماد برای جمع‌آوری و شمارش آرا محسوب می‌شود که از اشتباهات انسانی در هنگام رای‌گیری، شمارش آرا و نیز خطاهای عمدی جلوگیری می‌کنند اما می‌توانند در برابر حملات متعددی آسیب‌پذیر باشند. بنابراین استفاده از رای‌گیری الکترونیکی می‌تواند بسیاری از مسائل اخلاقی و سیاسی را در پی داشته باشد [3].

پروتکل‌های رای‌گیری الکترونیکی برای اطمینان از صحت انتخابات، بایستی خواسته‌های امنیتی مورد نیاز را برآورده کنند. در این مقاله سعی داریم با استفاده از ابزارهای صوری برخی از این خواسته‌های امنیتی را بر روی پروتکل رای‌گیری F.O.O بررسی کنیم. همچنین نشان می‌دهیم که پروتکل F.O.O تنها با وجود شرایطی نزدیک به ایده‌آل، خواسته‌های امنیتی مورد نیاز را برآورده می‌کند. بنابراین این پروتکل برخلاف آن چیزی که در [2] ادعا شده است، در مقیاس‌های بزرگ قابل استفاده نخواهد بود.

۱-۱- خواسته‌های امنیتی پروتکل‌های رای‌گیری

پروتکل‌های رای‌گیری بایستی خواسته‌های امنیتی مورد نیاز را برآورده کنند. این خواسته‌های امنیتی مطابق [4] عبارتند از:

تایید صلاحیت (Eligibility): تنها رای‌دهندگان مجاز توان رای دادن داشته باشند.

حریم خصوصی: تمام رای‌ها بایستی محرمانه باقی بماند و هیچ کس نتواند تعیین کند که یک شخص به چه کسی رای داده است.

عدم قابلیت استفاده مجدد (Unreusability): هیچ کس نتواند دو بار رای دهد و نیز نتواند رای شخص دیگری را تکرار کند.

قابلیت بررسی (Verifiability): هیچ کس نتواند رای کس دیگری را تغییر دهد بدون آنکه معلوم گردد.

جامعیت (Completeness): تمام آراء معتبر بایستی به درستی در جمع‌بندی نهایی دخالت داده شوند.

مانعیت (Soundness): رای‌دهندگان متقلب نتوانند فرآیند رای‌گیری را دچار اخلال کنند.

انصاف (Fairness): هیچ کس (در اینجا مسؤولین انتخابات) نبایستی بتواند نتیجه‌ی انتخابات را تغییر دهد.