مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۵۹-۴۵

یک پروتکل احراز هویت خصوصی گمنام متقابل جهت به‌کارگیری در سامانه‌های بازشناسی از طریق امواج رادیویی

کبری طالقانی‌زاده[۱]، مهدی گل‌سرخ‌تبار امیری[۲*]

۱- کارشناس ارشد، گروه کامپیوتر، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران

۲- استادیار، گروه کامپیوتر، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران

(دریافت: ۱۳۹۶/۰۹/۱۲، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

سامانه بازشناسی از طریق امواج رادیویی، مزایای فراوانی در زمینه شناسایی در مقیاس وسیع، افزایش سرعت و کاهش هزینه دارد. به همین دلیل این سامانه کاربرد بسیاری در جهان مدرن دارد و می‌توان از آن به عنوان یک ابزار ضروری برای بهبود زندگی بشر بهره جست. از آنجا که این فناوری با چالش‌های جدی در زمینه امنیت و حفظ حریم خصوصی روبروست، کاربرد آن همراه با نگرانی‌های امنیتی و تاخیر در استانداردسازی محدود شده است. با توجه به کاربرد وسیع فناوری RFID در سامانه‌های با مقیاس بزرگ و اهمیت حفظ حریم خصوصی در این سامانه‌ها، این مقاله به معرفی یک پروتکل احراز هویت خصوصی گمنام متقابل (MAPAP) با ویژگی‌های حفظ حریم خصوصی و مقیاس-پذیری توأم با احراز هویت متقابل پروتکل می‌پردازد. سپس میزان حریم خصوصی در آن با استفاده از معیار نشت اطلاعات اندازه‌گیری شده و ملاحظه می‌شود میزان اطلاعات افشا شده به‌وسیله این پروتکل زمانی که به خطر افتاده است نسبت به احراز هویت مبتنی بر گروه به مقدار قابل‌توجهی کمتر می‌باشد. چنانچه، در یک سامانه با تعداد 2^{20} برچسب ملاحظه می‌شود با افزایش تعداد برچسب‌های به خطر افتاده، اختلاف میزان نشت اطلاعات بین این پروتکل و پروتکل احراز هویت مبتنی بر گروه افزایش می‌یابد به‌طوری‌که وقتی تعداد برچسب‌های به خطر افتاده در این سامانه به ۱۵۰ عدد می‌رسد پروتکل پیشنهادی به میزان ۶۵٪ کمتر از احراز هویت مبتنی‌بر گروه، اطلاعات را افشا می‌نماید و این اختلاف با افزایش اندازه سامانه افزایش می‌یابد.

واژه‌های کلیدی: بازشناسی از طریق امواج رادیویی، احراز هویت متقابل، حریم خصوصی، امنیت، گمنامی

۱- مقدمه

شناسایی فرکانس رادیویی (RFID[1])، یک فناوری ارتباطی است که به‌وسیله امواج رادیویی و بدون تماس فیزیکی، قادر به شناسایی و ردیابی افراد و اشیاء می‌باشد. تحرک زیاد اجزای سامانه RFID و طبیعت باز آن، همچنین ارتباطات بی‌سیم در RFID موجب شده‌است تا این سامانه نسبت به انواع تهدیدات و خطرات، آسیب‌پذیر باشد. قابلیت ذاتی شناسایی دقیق و قابل‌انعطاف این سامانه باعث شده تا در حوزه برنامه‌های کاربردی ردیابی جذب شوند. این پتانسیل می‌تواند حریم خصوصی و امنیت سامانه‌های مذکور را در معرض خطر قرار دهد. توسعه فناوری RFID به‌دلیل وجود چنین نگرانی‌هایی محدود شده است. همچنین عدم وجود استاندارد و مقررات قانونی پیرامون موضوعات حریم خصوصی و امنیت، این فناوری را با چالش‌هایی مواجه کرده است که کاربرد آن را توام با نگرانی‌های امنیتی محدود ساخته است. از طرف دیگر، با توجه به محدودیت‌های بسیار زیادی که برچسب‌ها در تأمین منابع خود دارند، می‌بایست قبل از گسترش تعداد زیادی از برچسب های RFID در محیط، به رفع مشکلات امنیتی و حفظ حریم خصوصی در این سامانه‌ها پرداخت.

از جمله اقدامات کلیدی در راستای امنیت و حفظ حریم خصوصی در سامانه‌های RFID ، به‌کارگیری پروتکل‌های احراز هویت با رعایت اصول امنیت اطلاعات و همچنین استفاده از روش‌هایی چون الگوریتم‌های رمزنگاری شده در آن می‌باشد. به دلیل پایین بودن هزینه برچسب‌ها، امکان به‌کارگیری الگوریتم‌های پیچیده رمزنگاری بر روی برچسب‌ها امکان‌پذیر نمی‌باشد. در نتیجه عمده فعالیت‌ها در راستای تأمین امنیت، بر روی پروتکل‌ها متمرکز شده است.

از آن‌جا که فناوری RFID کاربرد وسیعی در سامانه‌های با مقیاس بزرگ دارد و به دلیل اهمیت حفظ حریم خصوصی در

*رایانامه نویسنده پاسخگو: golesorkh@baboliau.ac.ir

1- Radio frequency Identification

این سامانه‌ها، در این مقاله یک پروتکل احراز هویت خصوصی گمنام متقابل (MAPAP[1]) با ویژگی‌های حفظ حریم خصوصی، مقیاس‌پذیری و دوطرفه (متقابل) بودن پروتکل معرفی می‌شود و سعی در جهت تحقق امور زیر دارد:

- این مقاله، با استفاده از تعریف حریم خصوصی در سامانه‌های RFID از منظر قابلیت عدم ارتباط‌پذیری[2] در میان برچسب‌های متفاوت سامانه، نشان می‌دهد با برقراری قابلیت‌عدم ارتباط‌پذیری، حریم خصوصی برچسب‌ها حفظ می‌شود و مهاجم نمی‌تواند با احتمال بهتر از حدس زدن تصادفی قابلیت عدم ارتباط‌پذیری را بشکند یا به حریم خصوصی حمله نماید.
- پروتکل احراز هویت خصوصی گمنام متقابل (MAPAP) یک پروتکل احراز هویت گروهی است که علاوه بر دارا بودن ویژگی‌ها و مزایای طرح احراز هویت مبتنی‌بر گروه، در آن از روش‌های گمنامی و متقابل بودن به منظور حفظ حریم خصوصی بهتر و اطمینان از امنیت بیشتر در یک سامانه RFID استفاده شده است. پروتکل MAPAP از رمزنگاری کلید متقارن استفاده می‌کند.
- پروتکل MAPAP حریم خصوصی برچسب‌های RFID را حفظ می‌نماید و همچنین قابلیت عدم ارتباط‌پذیری را فراهم نموده و باعث حفظ حریم خصوصی می‌شود. مهاجم نمی‌تواند با پاسخ‌های برچسب ارتباط برقرار نماید، حتی اگر بتواند بخش اول پاسخ را رمزگشایی کند و شناسه‌ای که برچسب‌ها برای تولید پاسخ استفاده کرده‌اند را یاد بگیرد. همچنین، پروتکل MAPAP جهت افزایش امنیت بیشتر و در نتیجه حفظ بهتر حریم خصوصی، پس از مرحله احراز هویت برچسب، صحت یا عدم‌صحت کارت‌خوان را مورد بررسی قرار داده و در صورت درستی کارت‌خوان، هویت آن را احراز می‌نماید.

ساختار این مقاله به این شرح است: بخش ۲، شامل تحقیق‌های انجام شده مرتبط می‌باشد. بخش ۳، ضمن ارایه یک تعریف قوی از حریم خصوصی به تعیین راه حل مناسب برای انتقال اطلاعات مهم در سامانه‌های RFID با مقیاس بزرگ همزمان با حفظ حریم خصوصی در آنها می‌پردازد. پروتکل پیشنهادی در بخش ۴، ارائه می‌شود. بخش ۵، پروتکل پیشنهادی را تحلیل می‌کند و نشان می‌دهد چگونه در این روش حریم خصوصی حفظ می‌شود و قابلیت عدم ارتباط‌پذیری فراهم می‌شود. سطح حریم خصوصی ارایه شده در پروتکل، در بخش ۶، اندازه‌گیری می‌شود. در نهایت بخش ۷، شامل نتیجه‌گیری مقاله خواهد بود.

۲- کارهای مرتبط

پروتکل‌های احراز هویت با کارایی بالا ویژگی مقیاس‌پذیر بودن پروتکل را فراهم می‌نمایند. بررسی روش‌های حفاظت از حریم خصوصی در سامانه‌های RFID نشان می‌دهد تعدادی ازاین روش‌ها دارای پیچیدگی $O(N)$ هستند (N تعداد کل برچسب‌ها در سامانه است). این میزان از پیچیدگی در محیط‌های با مقیاس بزرگ قابل مدیریت نبوده و ناکارآمد هستند. این روش‌ها را می‌توان به دو دسته روش‌های مبتنی‌بر غیردرخت و روش‌های مبتنی‌بر درخت تقسیم نمود [۲-۱].

پروتکل‌های مبتنی‌بر غیردرخت معمولا برای پیدا کردن یک برچسب، جستجوی خطی انجام می‌دهند. پیچیدگی جستجو در این نوع از پروتکل‌ها $O(N)$ است که N تعداد برچسب‌ها می‌باشد. بدیهی است جستجوی خطی در سامانه‌های RFID با مقیاس بزرگ که تعداد زیادی برچسب دارد کارآمد نیست [۱].

در روش چکیده‌ساز- قفل که از روش‌های مبتنی‌بر غیردرخت است، مقدار چکیده‌ساز یک کلید، برای شناسایی یک برچسب استفاده می‌شود. پروتکل RAC[3] از این‌روش برای احراز هویت استفاده می‌کند. در این‌روش کارت‌خوان برای شناسایی یک برچسب به جستجوی کامل در بین همه ID ها نیاز دارد [۱]. این پروتکل باعث حملات بازپخشی و جعل هویت می‌شود.

در روش چکیده‌ساز- زنجیره [۳] امکان به‌روز رسانی کلید با استفاده از تابع چکیده‌ساز فراهم می‌شود. در این روش بعد از هر احراز هویت، برچسب و کارت‌خوان مقدار چکیده‌ساز کلید قبلی را به‌عنوان کلید جدید در نظر می‌گیرند. با توجه به ویژگی یک‌طرفه بودن تابع چکیده‌ساز، حتی اگر مهاجم کلید فعلی را در دست داشته باشد، نمی‌تواند کلیدهای قبلی را به‌دست آورد. روش چکیده‌ساز- زنجیره پیچیدگی جستجو را به $O(N^{2/3})$ کاهش می‌دهد [۴]. این روش از حملات ناهم‌زمانی رنج می‌برد [۲]. دی‌میتریوس [۵] برای مقابله با حملات ناهم‌زمانی در روش چکیده‌ساز- زنجیره، پروتکل D[4] را پیشنهاد می‌نماید که به‌روزرسانی کلیدها در برابر این حملات، تنها پس از احراز هویت موفقیت‌آمیز انجام می‌شود. با این حال، حمله ردیابی ممکن است بین شناسایی موفقیت‌آمیز باشد، زیرا هیچ عملیات به‌روزرسانی در این فواصل صورت نمی‌گیرد. پروتکل D اگرچه برای شناسایی و احراز هویت برچسب به $O(1)$ عمل احتیاج دارد ولی در برابر حملات ردیابی و DoS[5] امن نیست و دارای مشکلات بحرانی امنیتی است. هنری‌چی و مولر [۶] با استفاده از روش

1- Mutual Anonymous Private Authentication Protocol
2- Unlinkability
3- Randomized Access Control
4- Dimitriou
5- Denial of Service

چکیده‌ساز- زنجیره سعی در حفظ حریم خصوصی مکان برچسب با استفاده از تغییر شناسه برچسب بعد از هر احراز هویت موفق می‌نمایند. این طرح نیز تا حدودی باعث ردیابی برچسب می‌شود، زیرا برچسب قبل از احراز هویت موفقیت‌آمیز بعدی، با مقدار ثابت چکیده‌ساز شناسه، پاسخ را ارسال می‌نماید [۷]. در پروتکل ارایه شده توسط یون [۸] که از توابع چکیده‌ساز و تولید اعداد شبه تصادفی استفاده می‌نماید نیز قابلیت ردیابی وجود دارد. همچنین این پروتکل در برابر حمله DoS، جعل هویت سرور پشتی، جعل برچسب و جعل اطلاعات مقاوم نیست [۹]. در پروتکل اسریواستاوا و همکاران [۱۰] با استفاده از توابع چکیده‌ساز و تولید اعداد شبه تصادفی و به‌روزرسانی راز مخفی برچسب توسط سرور، سعی شده‌است حریم خصوصی پروتکل حفظ شده و از مشکلات جعل جلوگیری نماید. این پروتکل در برابر حملاتی مانند حمله مردی در میان، امن نیست. اما می‌توان با استفاده از کد احراز هویت پیام[1] این پروتکل را در برابر این گونه حملات امن نمود. این پروتکل برای پیدا کردن برچسب باید تمام شناسه‌های برچسب‌های موجود را مورد بررسی قرار دهد.

اشکال اصلی روش‌های مبتنی بر غیردرخت بهره‌وری کم جستجو است. برای رفع این مشکل طرح احراز هویت مبتنی‌بر درخت مطرح شده است [۱۱]. این طرح پیچیدگی را از $O(N)$ به $O(LogN)$ کاهش می‌دهد و این امر باعث افزایش کارایی پروتکل می‌شود ولی این افزایش در کارایی، سطح حریم خصوصی طرح را کاهش می‌دهد. محققین برای پیداکردن یک مصالحه بین میزان پیچیدگی و سطح حریم خصوصی ارایه شده به‌وسیله طرح مبتنی‌بر درخت تحقیقاتی انجام داده‌اند. از جمله این کارها می‌توان به تحقیقات [۴] و [۱۲] اشاره کرد. نویسندگان مقاله [۱۲] دریافته‌اند از دست رفتن حریم خصوصی زمانی که برخی از برچسب‌ها به خطر می‌افتند می‌تواند توسط طراحی دقیق درخت به حداقل برسد و یک اصل مهم در طراحی عملی این درخت، حداکثرسازی فاکتور انشعاب در سطح اول درخت است به‌گونه‌ای که سامانه بتواند حداکثر میزان تاخیر برای احراز هویت را قبول نماید. آنها نتیجه می‌گیرند درخت‌های کلیدی که دارای فاکتورهای انشعاب مختلف در سطوح مختلف درخت هستند می‌توانند سطح بالاتری از حریم خصوصی را فراهم آورند و با تعداد برچسب‌های داده شده و بیشترین مقدار پیچیدگی ممکن برای احراز هویت در یک سامانه، یک الگوریتم برای تعیین درخت کلید بهینه پیشنهاد می‌کنند.

اما ازآنجاکه در طرح مبتنی‌بر درخت، برچسب‌ها کلیدها را با برخی از برچسب‌های دیگر سامانه به اشتراک می‌گذارند [۱۱]، هر زمان که یک برچسب تحت کنترل مهاجم قرار گیرد همه برچسب‌هایی که حداقل یک کلید مشترک با برچسب تحت کنترل مهاجم دارند حریم خصوصی آنها قربانی می‌شود. در نتیجه این طرح اگرچه کارایی را افزایش می‌دهد ولی باعث کاهش حریم خصوصی می‌شود.

چن و همکاران [۱۳] یک طرح احراز هویت مبتنی‌بر توکن پویا را مورد بحث قرار می‌دهند. این پروتکل گمنامی و احراز هویت را از طریق مقداردهی اولیه تصادفی توکن‌ها فراهم می‌کند. توکن‌ها به صورت پویا از طریق استفاده از توکن پایه به‌روزرسانی می‌شوند. این طرح نیاز به ذخیره‌سازی بیشتر روی برچسب برای به‌روزرسانی‌ها دارد و مستعد حمله ناهمزمانی است.

رحمان و همکاران [۱۴] یک پروتکل مبتنی‌بر تابع PRNG[2] را مطرح کردند. اما این پروتکل فرض می‌کند کارت‌خوان تمام رازها را قبل از شروع فرآیند احراز هویت می‌داند و کاربردهای آن را محدود می‌نماید.

اولین بار اوین و همکاران [۱۵] یک طرح احراز هویت براساس ساختار گروهی را بیان نمودند که مشکل حریم خصوصی پروتکل‌های مبتنی‌بر ساختار درختی را حل می‌کرد. این طرح مصالحه بین مقیاس‌پذیری و حریم خصوصی را با تقسیم برچسب‌ها به تعدادی گروه بهبود بخشیده است و حفاظت از حریم خصوصی را نیز به میزان قابل توجهی افزایش می‌دهد. در طرح مبتنی بر ساختار گروهی مجموعه برچسب‌ها به گروه‌هایی با اندازه یکسان تقسیم می‌شوند و به همه برچسب‌ها در یک گروه یک کلید گروه اختصاص داده می‌شود که این کلید گروه برای هر گروه، منحصربه‌فرد است. کلید گروه مخفی است و فقط اعضای گروه و کارت‌خوان از مقدار آن آگاه هستند اما شناسه‌های برچسب‌ها به صورت عمومی اعلان می‌شود. برای جلوگیری از جعل هویت برچسب در یک گروه یکسان، هر برچسب دارای یک کلید یکتای مخفی نیز می‌باشد. این کلید فقط بین برچسب و کارت‌خوان به اشتراک گذاشته شده است.

در پروتکل‌های احراز هویت مبتنی‌برگروه، در فرآیند احراز هویت برچسب، کارت‌خوان یک پیام به عنوان پیام چالشی برای برچسب ارسال می‌کند. پاسخ هر برچسب دو قسمت دارد، در قسمت اول برچسب یک پیام رمز شده با کلید گروهی را به عنوان پاسخ برای کارت‌خوان ایجاد می‌کند که محتوای پیام، مقدار چالشی دریافتی از کارت‌خوان به همراه یک نانس تصادفی و شناسه خود است. در قسمت دوم برچسب مقدار چالشی دریافتی به همراه یک نانس تصادفی را با کلید مخفی خود

1- Message Authentication Code (MAC)

2- Pseudorandom number generator

رمزگذاری می‌کند و به عنوان پاسخ برای کارت‌خوان ارسال می‌نماید. کارت‌خوان پس از دریافت این مقدار ابتدا توسط بررسی تمام کلیدهای گروه، قسمت اول پیام را رمزگشایی می‌کند. کارت‌خوان در صورت رمزگشایی بخش اول پیام، بخش دوم پیام را با کلید خصوصی برچسب رمزگشایی نموده و به این ترتیب برچسب را احراز هویت می‌نماید [۱۵]. بدون قسمت دوم، هر برچسب می‌تواند هر برچسب دیگری را در گروه جعل هویت نماید.

این طرح پیچیدگی کارت‌خوان و برچسب را کاهش می‌دهد. برچسب همیشه باید دو رمزگذاری انجام دهد. در بدترین حالت کارت‌خوان باید به تعداد Y+1 رمزگذاری انجام دهد که Y تعداد گروه‌ها در سامانه است. به‌علاوه هر برچسب فقط نیاز به ذخیره کردن دو کلید برای احراز هویت دارد.

اشکالی که در طرح مبتنی‌بر گروه وجود دارد این است که اگر مهاجم یک برچسب را تحت کنترل خود قرار دهد، آنگاه مهاجم تمام اعضای آن گروه را تحت تاثیر قرار می‌دهد. زیرا مهاجم پس از تحت کنترل قرار دادن یک برچسب، کلید گروه و کلید خصوصی برچسب را به‌دست می‌آورد. حال مهاجم می‌تواند هر پیامی که توسط همان گروه ارسال می‌شود را شناسایی نماید، زیرا مهاجم می‌تواند شناسه هر برچسب را توسط رمزگشایی قسمت اول به‌دست آورد. به این ترتیب با به خطر افتادن یک برچسب در یک گروه تمام برچسب‌های آن گروه به خطر می‌افتند. در این طرح سایر گروه‌ها که هیچ برچسبی در آنها تحت کنترل مهاجم قرار نگرفته است هیچ آسیبی نمی‌بینند.

پروتکل AnonPri[1] توسط رحمان و همکاران [۱۶] ارائه شده است. این پروتکل ویژگی گمنامی را به طرح احراز هویت براساس ساختار گروهی اضافه می‌نماید. پروتکل AnonPri ویژگی عدم ارتباط‌پذیری برچسب‌ها را برقرار می‌نماید و مهاجم حتی با رمزگشایی بخش اول پاسخ برچسب و به‌دست آوردن شناسه آن نمی‌تواند پیام را به برچسبی که پیام را ارسال کرده است لینک نماید. در این پروتکل مهاجم نمی‌تواند خروجی‌های بین دو برچسب را از یکدیگر تشخیص دهد.

در این طرح هر برچسب دارای تعدادی شناسه یکتا است. هر برچسب تعدادی از این شناسه‌ها را با بعضی از اعضای گروه به اشتراک می‌گذارد. بنابراین، این پروتکل با استفاده از افزایش عدم قطعیت باعث عدم ردیابی توسط مهاجم می‌شود.

در این پروتکل برای احراز هویت برچسب، کارت‌خوان مقدار عدد تصادفی n_r را برای برچسب ارسال می‌کند. برچسب پس از دریافت این مقدار یک عدد تصادفی n_t را تولید کرده سپس یک شناسه مانند $ID_{i.j_x}$ (x امین شناسه برچسب j که در گروه i قرار دارد) را از مجموعه شناسه‌های خود انتخاب می‌کند و با محاسبه مقدار $u = E_{k_{Gi}}(n_r \,||\, n_t \,||\, ID_{i,j_x})$ و مقدار $v = E_{k_{Tj}}(n_r \,||\, n_t)$، این مقادیر را به‌عنوان پاسخ برای کارت‌خوان ارسال می‌نماید. $E_k()$ یک رمزنگاری متقارن با کلید k را نشان می‌دهد. کارت‌خوان پس از دریافت پاسخ در بین تمامی کلیدهای گروه‌ها جستجو انجام می‌دهد تا کلید درست را پیدا کند و به‌درستی قسمت اول پاسخ (u) را رمزگشایی کند. اگر کارت‌خوان شناسه $ID_{i.j_x}$ را که برچسب در پاسخ استفاده کرده است به‌دست آورد بخش دوم پاسخ (v) را توسط مجموعه کلیدهای مربوط به شناسه $ID_{i.j_x}$ رمزگشایی می‌کند. پس از پیدا کردن کلید درست، کارت‌خوان می‌تواند برچسب را شناسایی نماید.

در پروتکل AnonPri کارت‌خوان طی فرآیندی که توضیح داده شده برچسب را احراز هویت می‌نماید. اما در این پروتکل با توجه به فرض صحت کارت‌خوان مکانیزمی برای احراز هویت کارت‌خوان وجود ندارد. در پروتکل پیشنهادی (MAPAP) برای آزاد بودن از قید سالم بودن کارت‌خوان، علاوه بر احراز هویت برچسب، احراز هویت کارت‌خوان نیز صورت می‌گیرد. به عبارت دیگر پروتکل پیشنهادی علاوه بر دارا بودن ویژگی‌های پروتکل AnonPri دارای احراز هویت متقابل نیز می‌باشد. با احراز هویت برچسب توسط کارت‌خوان و همچنین احراز هویت کارت‌خوان توسط برچسب، میزان اعتماد بین برچسب و کارت‌خوان افزایش می‌یابد. وجود این ویژگی، پروتکل پیشنهادی را نسبت به آسیب‌پذیری‌ها و تهدیدات ممکن در حوزه امنیت و حریم خصوصی ایمن‌تر می‌نماید. بدون احراز هویت متقابل، این امکان وجود دارد که هر یک از طرفین به غلط هویت خود را معرفی نمایند.

۳- حریم خصوصی و مقیاس‌پذیری در سامانه‌های RFID

در این بخش ابتدا یک تعریف دقیق از حریم خصوصی در سامانه‌های RFID جهت اندازه‌گیری و سنجش این پارامتر مهم در پروتکل احراز هویت بیان می‌شود. پس از آن برای حفظ حریم خصوصی در سامانه‌های با مقیاس بزرگ، راه حل مناسب برای انتقال اطلاعات مهم و کلیدی و در نتیجه حفظ حریم خصوصی همزمان با افزایش اندازه سامانه مورد بررسی قرار می‌گیرد.

تاکنون تعاریف مختلفی از حریم خصوصی ارائه شده است. اما یک تعریف قوی از حفظ حریم خصوصی، برقراری قابلیت عدم‌ارتباط‌پذیری است. عدم‌ارتباط‌پذیری به این معناست که

1- Anonymous Private

مهاجم نتواند پاسخ‌های مربوط به یک برچسب را از پاسخ‌های بقیه برچسب‌های سامانه تشخیص دهد. به عبارت دیگر، مهاجم نمی‌تواند بین دو برچسب با احتمال بهتر از حدس زدن تصادفی تمایز قائل شود. به همین دلیل فراهم کردن قابلیت عدم‌ارتباط‌پذیری حریم خصوصی قوی‌تری را تضمین می‌نماید [۱۷].

سطح حریم خصوصی هر پروتکل می‌تواند توسط مجموعه گمنامی اندازه‌گیری شود. مجموعه گمنامی به همه فرستنده‌ها (گیرنده‌ها)ی بالقوه پیام گفته می‌شود. گمنامی به این معناست که شناسه فرد در گروه مورد نظر افشا نشود. برای دست‌یابی به گمنامی بیشتر باید مجموعه گمنامی بزرگتر شود. گمنامی کامل درصورتی برقرار می‌شود که مجموعه گمنامی شامل همه اعضای قادر به ارسال (دریافت) پیام در سامانه باشد [۱۸].

تضمین حریم خصوصی در یک پروتکل، پیچیدگی بیشتری را روی کارت‌خوان تحمیل می‌کند و باعث افزایش پیچیدگی در کارت‌خوان می‌شود به عبارت دیگر افزایش کارایی پروتکل برای حفظ قابلیت گسترش‌پذیری ممکن است باعث ضربه زدن به حریم خصوصی آن شود.

برای افزایش ضریب امنیت و حفظ بیشتر حریم خصوصی در سامانه‌های RFID ، از روش‌های رمزنگاری در ساختار پروتکل‌های احراز هویت استفاده می‌شود. از این رو، به‌صورت مختصر به شرح روش‌های رمزنگاری متقارن و رمزنگاری کلیدعمومی (نامتقارن) پرداخته می‌شود.

رمزنگاری متقارن یک نوع راهکار رمزنگاری است که از یک کلید یکسان برای رمزنگاری و رمزگشایی استفاده می‌کند. در روش رمزنگاری متقارن، فرستنده و گیرنده یک کلید خصوصی را به اشتراک می‌گذارند. فرستنده هنگام ارسال پیام به گیرنده از کلید به اشتراک گذاشته‌شده برای رمزگذاری متن استفاده می‌کند. گیرنده با دریافت متن رمزشده، آن را با همان کلید رمزگشایی می‌کند. رمزنگاری متقارن دارای ویژگی‌های منحصربه فردی است. اولا پروسه رمزنگاری و رمزگشایی با سرعت انجام می‌شود و برای سخت‌افزار نیز به صورت کارا پیاده‌سازی می‌شود. دوما کلید استفاده شده کوتاه است و تنها یک کلید برای رمزنگاری و رمزگشایی احتیاج است [۱۹]. بنابراین، در این رمزنگاری مشکل انتقال کلید به صورت امن مطرح می‌شود.

رمزنگاری کلید عمومی (نامتقارن)، برخلاف رمزنگاری متقارن از یک جفت کلید، برای رمزنگاری و رمزگشایی استفاده می‌نماید. موجودیتی که برای دریافت پیام در نظر گرفته شده است، یک جفت کلید می‌سازد که یکی از این کلیدها را کلید عمومی و دیگری را کلید خصوصی می‌نامند. کلید خصوصی را به صورت مخفی نگه می‌دارد و کلید عمومی را به صورت عمومی انتشار می‌دهد. بنابراین، هر موجودیتی که می‌خواهد برای او پیامی بفرستد می‌تواند پیام را با کلید عمومی رمزگذاری نماید. پس از دریافت متن رمزشده، دریافت‌کننده توسط کلید خصوصی خود آن را رمزگشایی می‌کند [۲۰].

روش رمزنگاری کلید عمومی در مقایسه با رمزگذاری متقارن، دارای نقاط قوت و ضعف مختلفی است. در رمزنگاری کلید عمومی تنها کلید خصوصی باید مخفی نگه داشته شود. فرآیند انتقال کلید در مقایسه با رمزنگاری متقارن راحت‌تر انجام می‌گیرد. به‌علاوه، از رمزنگاری کلید عمومی می‌توان برای طراحی امضای دیجیتال استفاده کرد. در ارتباطات شبکه، رمزنگاری کلید عمومی به کلیدهای کمتری نسبت به رمزنگاری متقارن احتیاج دارد. رمزنگاری کلید عمومی از کارایی کمتر و طول کلید بیشتری برخوردار است [۱۹].

راه‌کارهای رمزنگاری کلید عمومی یک‌روش بهتر برای حل مشکل حفظ حریم خصوصی و قابلیت گسترش‌پذیری هستند. در این روش‌ها برچسب توسط کلید عمومی کارت‌خوان، پیام خود را رمزگذاری می‌کند که در این صورت فقط کارت‌خوان قادر به رمزگشایی آن خواهد بود و می‌تواند برچسب را شناسایی کند. اما روش‌های رمزنگاری کلید عمومی برای برچسب‌های باهزینه کم، بسیار گران هستند [۱۶]. در سامانه‌های RFID با توان محدود، بیشتر از رمزنگاری کلید متقارن به جای الگوریتم‌های کلید عمومی استفاده می‌کنند، چون روش‌های رمزنگاری متقارن توان کمتری مصرف می‌کنند و سطح امنیتی مناسب را فراهم می‌نمایند [۲۱] ازاین‌رو، در پروتکل پیشنهادی از روش رمزنگاری متقارن استفاده شده است که کلیدها بین برچسب و کارت‌خوان به‌اشتراک گذاشته می‌شود.

از آنجا که در پروتکل پیشنهادی از روش رمزنگاری متقارن استفاده شده است مشکل انتقال کلید به صورت امن و حفاظت از حریم خصوصی مطرح می‌شود. احراز هویت خصوصی می‌تواند یک راه حل مطلوب برای رفع مشکلات حریم خصوصی باشد. در روش احراز هویت خصوصی، یک طرف به عنوان اثبات کننده (برچسب)، هویت خود را به طرف دیگر که تصدیق کننده (کارت‌خوان) است اثبات می‌نماید، بطوری که مهاجم نتواند اثبات کننده را شناسایی و ردیابی نماید. مشکل احراز هویت خصوصی این است که چگونه دو طرف می‌توانند یک کلید احراز هویت را در اختیار یکدیگر قرار دهند بدون این‌که هویت خود را به مهاجم نشان دهند. به عبارت دیگر هر چند یک برچسب می‌تواند پیامش را برای مخفی کردن هویت خود از استراق سمع رمزگذاری نماید،

ولی نمی‌تواند به کارت‌خوان راجع به کلیدی که برای رمزگذاری استفاده کرده است هیچ اشاره‌ای داشته باشد. چون چنین اشاره‌ای می‌تواند توسط مهاجم برای شکستن حریم خصوصی برچسب استفاده شود. به‌این دلیل کارت‌خوان باید در بین مجموعه‌ای از کلیدهای منتخب جستجو نماید تا کلید درستی که پیام برچسب را به درستی رمزگشایی می‌کند، پیدا نماید [۱۵].

۴- پروتکل پیشنهادی

در این بخش یک پروتکل احراز هویت خصوصی گمنام متقابل (MAPAP) براساس ساختار گروهی معرفی می‌شود. از آنجا که پروتکل پیشنهادی بر مبنای ساختار گروهی است، برچسب‌ها در مدل سامانه به گروه‌هایی باندازه یکسان تقسیم می‌شوند. اگر N تعداد کل برچسب‌ها در سامانه و τ تعداد گروه‌ها باشد، بنابراین تعداد اعضای گروه $n=\frac{N}{\tau}$ است. پارامترها و اجزای گروه در سامانه به شرح زیر بیان می‌شوند.

صادرکننده: صادرکننده با ذخیره اطلاعات در حافظه هر برچسب، آن را مقداردهی اولیه می‌نماید. هرگروه یک کلید یکتا و یک استخر از شناسه‌ها از صادرکننده دریافت می‌کند.

گروه: هرگروه دارای n برچسب است. صادرکننده یک کلید گروهی یکتا k_{G_i} را به گروه i ام اختصاص می‌دهد. این کلید بین اعضای گروه به اشتراک گذاشته می‌شود. هر گروه یک استخر از شناسه‌ها ξ را نیز از صادرکننده دریافت می‌کند. استخرهای شناسه هیچ دو گروهی، شناسه یکسان ندارند. به هر برچسب گروه G_i، یک گروه از شناسه‌های ξ_i اختصاص داده می‌شود.

برچسب: همه برچسب‌ها به τ گروه تقسیم می‌شوند. هر برچسب یک کلید گروهی و یک کلید یکتای منحصربه‌فرد را دریافت می‌کند و دارای یک مجموعه از شناسه‌ها است. فرض کنید برچسب T_j به گروه G_i تعلق دارد. در این صورت برچسب T_j دارای یک کلید گروهی k_{G_i} است، یک کلید خصوصی k_{T_j} دارد و مجموعه‌ای از شناسه‌ها که با نماد Ω_{ij} نشان داده می‌شوند. هر کلید از θ بیت تشکیل شده است که θ پارامتر امنیتی مربوط به کلید متقارن است.

هر شناسه برچسب به صورت تصادفی از استخر شناسه‌های گروه انتخاب می‌شود. هیچ کدام از شناسه‌های یک برچسب با هم برابر نیستند. شناسه‌ها به‌گونه‌ای به برچسب‌ها اختصاص داده می‌شوند که حداقل یک شناسه مشترک بین هر دو عضو یک گروه وجود داشته باشد.

M یک پارامتر سامانه است و به تعداد شناسه‌های اختصاص داده‌شده به گروه خاص اشاره دارد. m به‌تعداد شناسه‌های اختصاص داده‌شده به هر برچسب اشاره دارد. مقدار m از مقدار M کوچکتر است. با افزایش مقدار M شکستن حریم خصوصی برای مهاجم سخت‌تر است. البته نمی‌توان مقدار M را یک عدد خیلی بزرگ در نظر گرفت به طوری که سامانه کند شود.

جدول (۱): نمادهای استفاده شده در پروتکل پیشنهادی

T_j	برچسب j ام
G_i	گروه i ام
$ID_{i,x}$	شناسه x ام در گروه i
ξ_i	استخر شناسه‌های گروه i
Ω_{ij}	مجموعه شناسه‌های برچسب j ام گروه i ام
k_{G_i}	کلید گروهی گروه i ام
k_{T_j}	کلید خصوصی برچسب j ام
N	تعداد کل برچسب‌ها در سامانه
τ	تعداد گروه‌های سامانه
n	تعداد برچسب‌های هر گروه
M	تعداد شناسه‌های اختصاص داده شده به گروه
m	تعداد شناسه‌های اختصاص داده شده به هر برچسب
σ_i	نگاشت شناسه‌های موجود در استخر ξ_i با مخفی برچسب‌ها
π_x	مجموعه کلیدهای مخفی متناظر با $ID_{i,x}$ برچسب
n_r	تولید یک عدد تصادفی به‌عنوان نانس توسط کارت‌خوان
n_t	تولید یک عدد تصادفی به‌عنوان نانس توسط برچسب
$\|\|$	عمل الحاق
$E_k()$	تابع رمزنگاری متقارن با کلید k

کارت‌خوان: کارت‌خوان به سرور متصل است. در پروتکل پیشنهادی فرض براین است که کانال بین کارت‌خوان و سرور امن است. صادرکننده به هر کارت‌خوان یک مجموعه از کلیدها را اختصاص می‌دهد که شامل کلید گروه k_{G_i} و نگاشت σ_i شناسه‌های موجود در استخر ξ_i با کلیدهای برچسب است. مقادیر σ_i را می‌توان به‌صورت دقیق‌تر به شکل رابطه (۱) بیان نمود:

$$\sigma_i = \{< ID_{i,x}, \pi_x > | 1 \le x \le M \; and \; ID_{i,x} \in \xi_i\} \quad (۱)$$

که در آن، π_x مجموعه کلیدهای مخفی متناظر با $ID_{i,x}$ برچسب است. به عبارت دیگر، π_x مجموعه کلیدهای مخفی برچسب‌هایی است که شامل شناسه $ID_{i,x}$ هستند. π_x در صورتی که هیچ کلیدی متناظر با $ID_{i,x}$ وجود نداشته باشد برابر تهی است.

پارامترهای سامانه: از آن‌جایی که هر برچسب m شناسه دارد که به‌صورت تصادفی از استخر شناسه‌ها با اندازه M انتخاب می‌شوند و با توجه به استراتژی توزیع ID می‌توان بیان کرد هر برچسب حداقل یک شناسه مشترک با دو عضو از گروه دارد.

پروتکل پیشنهادی در شکل (۱) نشان داده شده و نمادهای آن در جدول (۱) آمده است. در این پروتکل ابتدا، کارت‌خوان

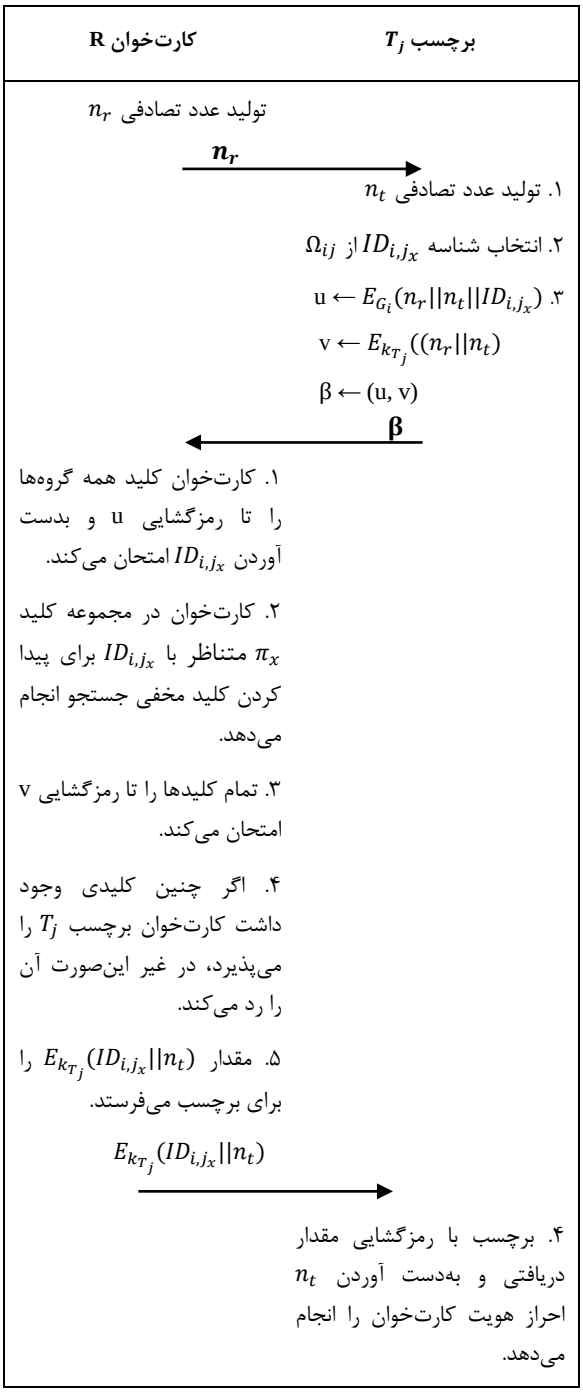
برای احراز هویت برچسب، پرس‌وجوی برچسب را با نانس n_r شروع می‌کند. برچسب پس از دریافت آن یک نانس دیگر مانند n_t را تولید می‌نماید. در مرحله دوم برچسب یک شناسه مانند $ID_{i,x}$ را از مجموعه شناسه‌های خود یعنی Ω_{ij} انتخاب می‌کند. سپس برچسب مقدار β را به شرح زیر محاسبه می‌نماید.

- مقادیر نانس n_r، نانس n_t و شناسه ID_{i,j_x} را با یکدیگر الحاق نموده و مقدار بدست آمده را با کلید گروهی برچسب k_{G_i} رمزگذاری نموده و آن را به u نسبت می‌دهد.
- مقادیر نانس n_r و نانس n_t را پس از الحاق با یکدیگر با کلید اختصاصی برچسب k_{T_j} رمزگذاری نموده و به v نسبت می‌دهد.
- برچسب دو مقدار u و v را به β داده و با پیام β به کارت‌خوان پاسخ می‌دهد.

$E_k()$ نشان دهنده رمزنگاری متقارن با کلید k است. برچسب با پیام β پاسخ داده است. حال کارت‌خوان تمامی کلیدهای گروه‌ها را تا پیدا کردن کلید درست برای رمز گشایی قسمت اول پیام یعنی u مورد بررسی قرار می‌دهد. اگر کارت‌خوان بتواند شناسه ID_{i,j_x} که برچسب ارسال کرده است را بازیابی کند می‌تواند قسمت دوم پیام یعنی v را توسط کلیدهای خصوصی π_x مربوط به ID_{i,j_x} رمزگشایی نماید. در صورت وجود چنین کلیدی، کارت‌خوان برچسب T_j را احراز هویت می‌کند در غیر این‌صورت برچسب احراز هویت نشده و رد می‌شود. به اشتراک گذاشتن تعدادی از شناسه‌های برچسب با دیگر اعضای گروه باعث برقراری عدم ارتباط‌پذیری برچسب می‌شود، حتی درصورتی‌که برچسب تحت کنترل مهاجم قرار دارد.

پس از آن که احراز هویت برچسب به اتمام رسید و برچسب مورد تایید کارت‌خوان قرار گرفت، مرحله احراز هویت کارت‌خوان آغاز می‌شود. به این منظور کارت‌خوان که در این مرحله کلید خصوصی برچسب احراز هویت شده را می‌داند مقادیر n_t و ID_{i,j_x} را با یکدیگر الحاق نموده و آن را با کلید خصوصی برچسب T_j احراز هویت شده، رمزگذاری می‌کند و در آخر، مقدار حاصل یعنی $E_{k_{T_j}}(ID_{i,j_x}||n_t)$ را جهت احراز هویت متقابل به برچسب ارسال می‌نماید.

با انتخاب مقدار $E_{k_{T_j}}(ID_{i,j_x}||n_t)$ جهت احراز هویت کارت‌خوان، اولا به‌دلیل تصادفی بودن n_t، این مقدار در هر نشست متفاوت خواهد بود و این کار از حمله برچسب‌زدن[1] جلوگیری می‌نماید.



شکل (۱). پروتکل احراز هویت پیشنهادی MAPAP

ثانیا استفاده از ID_{i,j_x} و n_t نشان می‌دهد سرور کلید گروهی مربوط به برچسب و گروه برچسب را داشته است. زیرا با رمزگشایی قسمت اول پیام برچسب، مقادیر ID_{i,j_x} و n_t را به‌دست آورده است. نکته مهم‌تر این است که رمزگذاری مقدار $E_{k_{T_j}}(ID_{i,j_x}||n_t)$ با کلید خصوصی برچسب k_{T_j} نشان می‌دهد کلید خصوصی برچسب نیز در اختیار کارت‌خوان است. زیرا سرور

1 Tagging Attack

با به‌دست آوردن شناسه ID_{i,j_x} توانسته است در مجموعه کلیدهای π_x متناظر با شناسه ID_{i,j_x} کلید خصوصی برچسب را پیدا نماید و مقدار $(ID_{i,j_x}||n_t)$ را با کلید خصوصی برچسب رمزگذاری کند.

در نهایت، برچسب با دریافت مقدار $E_{k_{T_j}}(ID_{i,j_x}||n_t)$ از طرف کارت‌خوان، آن را با کلید خصوصی خود رمزگشایی می‌کند. سپس درستی مقدار n_t را مورد بررسی قرار می‌دهد. درصورت درستی این مقدار احراز هویت کارت‌خوان نیز صورت می‌گیرد. باید در نظر داشت مهاجم برای تولید مقدار $E_{k_{T_j}}(ID_{i,j_x}||n_t)$ باید هم کلید گروهی و هم کلید خصوصی برچسب را بداند. همچنین با شنود مقادیر رد و بدل شده بین برچسب و کارت‌خوان نمی‌تواند حملات برچسب‌زدن را انجام دهد.

۵- تحلیل و ارزیابی

حال پروتکل پیشنهادی مورد تحلیل و ارزیابی قرار می‌گیرد. برای این منظور، ابتدا این پروتکل از نقطه نظر مسایل امنیتی تحلیل شده و چگونگی حفظ حریم خصوصی و فراهم نمودن قابلیت عدم‌ارتباط‌پذیری در آن نشان داده می‌شود. پس از آن عملکرد پروتکل پیشنهادی تحلیل خواهد شد.

۵-۱- تحلیل امنیتی

در این بخش به صورت رسمی ثابت می‌شود پروتکل پیشنهادی حریم خصوصی و قابلیت عدم ارتباط‌پذیری را فراهم می‌نماید. برای این کار از مدل اوراکل تصادفی استفاده می‌شود. مدل اوراکل یک ابزار قدرتمند است که به منظور فراهم نمودن «اثبات امنیت» دقیق، برای پروتکل‌های رمزنگاری خاص استفاده می‌شود. به طور معمول این مدل یک تابع چکیده‌ساز است که توسط یک اوراکل تصادفی مدل‌سازی شده است. به‌صورت غیررسمی به این معنی است که یک تابع چکیده‌ساز H را به عنوان یک جعبه سیاه در نظر می‌گیرد و با دادن یک مقدار تصادفی به یک پرس‌وجو برای مقدار چکیده‌ساز رشته بیت M، پاسخ می‌دهد. اوراکل برای هر پرس‌و جو، یک انتخاب تصادفی مستقل را ایجاد می‌کند [۲۲]. همچنین در این بخش، حفظ حریم خصوصی این پروتکل در برابر بعضی از حالات حمله مورد بررسی قرار می‌گیرد.

ابتدا یک مدل حمله در نظر گرفته شده و فرض می‌شود $\hat{A}$ مهاجم فعالی است که می‌تواند در ارتباط بین برچسب‌ها و کارت‌خوان استراق سمع نماید و همچنین مستقیما با برچسب و کارت‌خوان ارتباط برقرار کند، اما پیام‌هایی که بین آنها ارسال می‌شود را تغییر نمی‌دهد به عنوان مثال مهاجم می‌تواند یک برچسب را جعل هویت کند و با یک کارت‌خوان معتبر ارتباط برقرار کند. مهاجم حتی می‌تواند یک پرس‌وجو را از برچسب شروع کند و پاسخ‌های مربوطه را دریافت نماید. فرض براین است که مهاجم بر تعدادی از کارت‌خوان‌ها و برچسب‌ها نیز کنترل دارد. هر برچسب و کارت‌خوان کنترل شده توسط مهاجم به ترتیب با نمادهای $\hat{T}$ و $\hat{R}$ نشان داده می‌شوند. $\hat{R}$ نمی‌تواند به هیچ برچسبی دسترسی داشته باشد زیرا دارای هیچ کلید خصوصی نیست. به صورت مشابه $\hat{T}$ نیز معتبر شمرده نمی‌شود زیرا کلید و شناسه برچسب را ندارد اما یک کارت‌خوان مانند $\hat{R}$ می‌تواند با یک برچسب معتبر ارتباط برقرار کند. همچنین یک برچسب جعلی مانند $\hat{T}$ نیز می‌تواند با یک کارت‌خوان مجاز ارتباط برقرار کند. در هر دو مورد هدف مهاجم ردیابی برچسب‌ها در سامانه RFID است. همچنین فرض می‌شود مهاجم، کارت‌خوان متخاصم و برچسب متخاصم، منابع محدود دارند. به‌علاوه، مهاجم می‌تواند حملات فیزیکی راه‌اندازی نماید.

حال برای این‌که حفظ حریم خصوصی و قابلیت عدم ارتباط‌پذیری پروتکل پیشنهادی به صورت رسمی ثابت شود ابتدا به‌صورت تئوری تعریف می‌شود چگونه پروتکل پیشنهادی حریم خصوصی را حفظ می‌کند و قابلیت عدم‌ارتباط‌پذیری را تضمین می‌نماید. برای این منظور از یک تعریف مبتنی‌بر تجربه و آزمایش [۱۷]، برای رسمی کردن حریم خصوصی استفاده می‌شود و نتیجه‌گیری می‌شود مهاجم حتی در صورت رمزگشایی قسمت اول پیام نمی‌تواند پاسخ‌ها را به برچسب‌ها ارتباط داده و شناسه برچسب را شناسایی نماید. مهاجم فقط با احتمالی نزدیک به حدس تصادفی می‌تواند شناسه‌ها را به‌دست آورد. در این سامانه، اوراکل به‌صورت زیر وجود دارد:

O_{pick} یک اوراکل است که به‌صورت تصادفی تعدادی برچسب را از کل برچسب‌ها (N) انتخاب می‌کند.

$O_{encrypt}$ یک برچسب مانند T را به عنوان ورودی دریافت می‌کند و با داشتن نانس n_T، کلید گروهی k_G، کلید خصوصی برچسب k_T، مجموعه شناسه‌ها Ω و یک شناسه تصادفی انتخاب شده مانند $ID\epsilon\Omega$، یک نانس دیگر تولید می‌نماید و پس از آن پاسخ $\beta = (u.v)$ را تولید کرده و خروجی β را ایجاد می‌کند.

O_{query} یک اوراکلی است که برچسب را مورد پرس‌وجو قرار می‌دهد و β را دریافت می‌کند.

O_{filp} اوراکلی است که از بین دو برچسب T_0 و T_1، یکی را به صورت تصادفی انتخاب می‌کند و توسط اوراکل O_{query} آن برچسب را مورد پرس‌وجو قرار می‌دهد. خروجی برابر β_b خواهد بود که در آن $b \in \{0.1\}$ است.

۵-۱-۱- حریم خصوصی اطلاعات در برابر مهاجم

با داشتن برچسب T، مجموعه شناسه‌های Ω که در برچسب T ذخیره شده است و شناسه ID یک مهاجم درصورتی می‌تواند حریم خصوصی این پروتکل را از بین ببرد که بتواند تشخیص دهد برچسب T از شناسه ID استفاده کرده است یا خیر. θ پارامتر امنیتی و $t \epsilon N$ بیشترین تعداد دفعاتی است که مهاجم می‌تواند برچسب T را مورد پرس‌وجو قرار دهد:

- **آزمایش $Exp_{\hat{A}}^{priv}[\theta, t]$:**

۱. راه‌اندازی: صادرکننده، N برچسب را توسط کلیدهای خصوصی هر برچسب، کلید گروه و مجموعه شناسه‌ها پس از تقسیم به τ گروه راه‌اندازی اولیه می‌کند. همه این اطلاعات مخفی فقط با کارت‌خوان به اشتراک گذاشته می‌شود.

۲. یادگیری: O_{pick} یک برچسب مانند T را انتخاب می‌کند. مهاجم این برچسب را t بار مورد پرس‌وجو قرار می‌دهد و هر پاسخ به لیست L اضافه می‌شود. لیست در ابتدا خالی است.

۳. حدس‌زدن: حال، مهاجم برچسب T را به همراه نانس به اوراکل $O_{encrypt}$ می‌دهد و پاسخ β را از اوراکل دریافت می‌کند. مهاجم یک شناسه ID انتخاب می‌کند. با توجه به t پاسخ در لیست L اگر مهاجم حدس بزند β با استفاده از ID تولیدشده است خروجی یک و در غیر این صورت خروجی صفر را ایجاد می‌کند. مهاجم در صورتی موفق است که حدس او درست باشد.

براساس آزمایش انجام شده $Exp_{\hat{A}}^{priv}[\theta, t]$ و برای رسمی‌کردن حریم خصوصی پروتکل، یک تعریف از حریم خصوصی پروتکل پیشنهادی، مطابق با تعریف (۱) ارائه می‌شود.

تعریف (۱): پروتکل پیشنهادی حریم خصوصی اطلاعات را با پارامتر امنیتی θ و در زمان چندجمله‌ای $poly(\theta)$ حفظ می‌کند، درصورتی که رابطه (۲) برقرار باشد.

$$\forall \hat{A}, \Pr\left[Exp_{\hat{A}}^{priv}[\theta, t] succeeds\right] \leq \frac{1}{2} + \frac{1}{poly(\theta)} \qquad (۲)$$

۵-۱-۲- قابلیت عدم ارتباط‌پذیری در برابر مهاجم

مهاجم نباید بتواند بین دو پاسخ متفاوت از یک برچسب یکسان، تمایز قایل شود.

- **آزمایش $Exp_{\hat{A}}^{unlink}[\theta, t]$:**

۱. راه‌اندازی: صادرکننده، N برچسب را توسط کلیدهای خصوصی هر برچسب، کلید گروه و مجموعه شناسه‌ها پس از تقسیم به τ گروه، راه‌اندازی اولیه می‌کند. این کلیدها فقط با کارت‌خوان به اشتراک گذاشته می‌شود.

۲. یادگیری: O_{pick} دو برچسب T_0 و T_1 را از یک گروه یکسان انتخاب می‌کند. مهاجم هریک از این برچسب‌ها را t بار مورد پرس‌وجو قرار می‌دهد و پاسخ‌های β_0 و β_1 را در لیست L قرار می‌دهد. در ابتدا لیست خالی است.

۳. حدس زدن: مهاجم دو برچسب T_0 و T_1 را به اوراکل O_{filp} می‌دهد. مهاجم $\hat{A}$ از این اوراکل پاسخ β_b را دریافت می‌کند. با داشتن لیست L از پاسخ‌ها و β_b، مهاجم مقدار b را حدس می‌زند. مهاجم $\hat{A}$، در صورتی موفق می‌شود که حدس او درست باشد.

براساس آزمایش انجام شده $Exp_{\hat{A}}^{unlink}[\theta, t]$ و برای رسمی‌کردن عدم ارتباط‌پذیری پروتکل، یک تعریف از قابلیت عدم ارتباط‌پذیری پروتکل پیشنهادی مطابق با تعریف (۲) ارائه می‌شود.

تعریف (۲): پروتکل پیشنهادی، قابلیت عدم‌ارتباط‌پذیری را با پارامتر امنیتی θ و در زمان چندجمله‌ای $poly(\theta)$ حفظ می‌کند، در صورتی که رابطه (۳) برقرار باشد.

$$\forall \hat{A}. \Pr\left[Exp_{\hat{A}}^{unlink}[\theta, t] succeeds\right] \leq \frac{1}{2} + \frac{1}{poly(\theta)} \qquad (۳)$$

چون مهاجم راهی بهتر از حدس‌زدن برای موفق بودن در تمایز برچسب‌ها ندارد در نتیجه احتمال موفقیت در تمایز برچسب‌ها کمتر یا مساوی $\frac{1}{2}$ است. به عنوان مثال وقتی مهاجم دو ورودی اوراکل m_0 و m_1 را می‌فرستد، اوراکل یکی از آنها را به‌طور تصادفی انتخاب کرده و یک خروجی (Out_0) را محاسبه می‌کند. سپس خروجی را به مهاجم می‌فرستد. اینجا اوراکل به‌عنوان جعبه سیاه کار می‌کند. به عبارت دیگر، مهاجم اطلاعاتی غیر از m_0، m_1 و Out_0 ندارد. حال اگر مهاجم بتواند با موفقیت دریابد Out_0 متعلق به کدام ورودی است او قادر است حریم خصوصی را بشکند. به‌هرحال، از آنجا که مهاجم اطلاعات دیگری ندارد بهترین شانس، انتخاب یکی از ورودی‌ها به‌طور تصادفی و با احتمال $\frac{1}{2}$ است. اگر ورودی انتخاب شده واقعا ورودی متناظر با Out_0 باشد دراینصورت مهاجم حریم خصوصی سامانه را از بین می‌برد. به عبارت دیگر مهاجم با احتمال $\frac{1}{2}$ قادر به تمایز برچسب است.

حال به‌صورت رسمی ثابت می‌شود پروتکل پیشنهادی حریم خصوصی و قابلیت عدم‌ارتباط‌پذیری را فراهم می‌کند.

قضیه (۱): پروتکل پیشنهادی حریم خصوصی اطلاعات را در برابر مهاجم $\hat{A}$ حفظ می‌کند.

اثبات: فرض کنید O_{pick}، برچسب T را انتخاب می‌کند. مهاجم $\hat{A}$ این برچسب را به همراه نانس n_1 به $O_{encrypt}$ می‌دهد. سپس $O_{encrypt}$ پاسخ β را می‌فرستد.

حال مهاجم $\hat{A}$ شناسه ID را انتخاب می‌کند. برای شکستن حریم خصوصی داده‌ها مهاجم $\hat{A}$ باید تشخیص دهد β توسط شناسه ID تولید شده است یا خیر. این کار به‌این معناست که مهاجم $\hat{A}$ باید ورودی را فقط با دانستن متن رمز شده شناسایی کند. مهاجم $\hat{A}$ در دو صورت موفق می‌شود. روش اول، بازیابی ورودی‌ها از خروجی‌های اوراکل تصادفی است اما این روش با فرض مسئله در تناقض است زیرا در اوراکل از روی خروجی نمی‌توان ورودی را به‌دست آورد. روش دوم، مهاجم کلیدهای برچسب T را بداند. این روش نیز به این معناست که مهاجم بدون دانستن کلیدها از روی متن رمز شده کلیدها را به‌دست آورد که در این صورت راه‌کارهای رمزنگاری متقارن نیز شکسته می‌شود. پس این روش نیز ممکن نیست. بنابراین، مهاجم $\hat{A}$ نمی‌تواند حریم خصوصی را با احتمالی بیشتر از حدس تصادفی بشکند. پس تعریف (۱) اثبات می‌شود. بنابراین پروتکل پیشنهادی حریم خصوصی داده‌ها را حفظ می‌نماید.

قضیه (۲): پروتکل پیشنهادی قابلیت عدم لینک پذیری را در برابر مهاجم $\hat{A}$ حفظ می‌کند.

اثبات: فرض کنید که O_{pick} دو برچسب T_0 و T_1 را از یک گروه یکسان برای مهاجم $\hat{A}$ فراهم می‌کند. این دو برچسب وارد مرحله یادگیری می‌شوند. $\hat{A}$ این دو برچسب را به O_{filp} می‌دهد و O_{filp} خروجی β_b را تولید می‌کند.

حال برای شکستن قابلیت عدم‌ارتباط‌پذیری، مهاجم $\hat{A}$ باید مقدار b را بگوید. فرض نمایید حدس مهاجم درست باشد. به عبارت دیگر، مهاجم بتواند با توجه به پاسخ‌های یاد گرفته شده از دو برچسب T_0 و T_1 تعیین نماید β_b توسط کدام یک از برچسب‌های T_0 و یا T_1 تولید شده است. از آنجا که در این پروتکل وجود یک نانس در سمت برچسب باعث می‌شود هر پاسخ برچسب با تمام پاسخ‌های قبلی نشئت گرفته از همان برچسب متفاوت باشد، در نتیجه پاسخ‌های یک برچسب نمی‌تواند به‌عنوان امضای برچسب تلقی شود. بنابراین، می‌توان گفت مهاجم می‌بایست کلیدهای ذخیره شده بر روی این دو برچسب (کلید گروهی و کلید خصوصی) را می‌دانسته و به دلیل این دانستن توانسته است حدس درستی بزند. یعنی مهاجم، بدون دستکاری برچسب‌های T_0 و T_1، فقط با مشاهده متن‌های رمز شده باید کلیدهای ذخیره شده روی این برچسب‌ها را تشخیص دهد. اما این با امنیت معنایی رمزنگاری کلید متقارن در تضاد است. بنابراین مهاجم نمی‌تواند قابلیت عدم‌لینک‌پذیری را با احتمالی بیشتر از حدس زدن تصادفی بشکند. پس تعریف ۲ اثبات می‌شود یعنی پروتکل پیشنهادی قابلیت عدم‌ارتباط‌پذیری را برقرار می‌نماید.

۵-۱-۳- حمله فیزیکی

حال اثرات حمله فیزیکی مورد بحث و بررسی قرار گرفته و نشان داده می‌شود چگونه پروتکل احراز هویت گمنام متقابل قابلیت عدم‌ارتباط‌پذیری را فراهم می‌نماید حتی در صورتی که مهاجم شناسه استفاده شده در پاسخ را یاد بگیرد.

حمله‌ای را تصور کنید که مهاجم $\hat{A}$ می‌تواند در یک سامانه با N برچسب، هر برچسب را با احتمال 1/N به خطر بیندازد. هر زمان یک برچسب T_j به خطر بیفتد مهاجم همه اطلاعات شخصی ذخیره شده روی برچسب T_j را یاد می‌گیرد. بنابراین مهاجم می‌تواند مقدار u در هر پاسخ β که بوسیله بقیه اعضای گروه G_i تولید شده است را رمزگشایی کند. در نتیجه مهاجم $\hat{A}$ می‌تواند شناسه‌ای که یک برچسب برای تولید پاسخ خود از آن استفاده کرده است را با رمزگشایی u یاد بگیرد. به عنوان مثال یک گروه G_i با چهار برچسب T_3, T_2, T_1 و T_4 را در نظر گرفته و فرض نمایید مهاجم، برچسب T_3 را به خطر می‌اندازد. دراین صورت مهاجم کلید گروه، کلید مخفی برچسب T_3 و مجموعه شناسه‌های برچسب T_3 را یاد می‌گیرد. از این به بعد مهاجم می‌تواند بخش u همه پاسخ‌هایی که از برچسب‌های T_2, T_1 و T_4 ایجاد شده است را با استفاده از کلید گروه رمزگشایی نماید. اما از آنجا که مهاجم کلیدهای مخفی این برچسب‌ها را در اختیار ندارد هنوز نمی‌تواند بخش v این پاسخ‌ها را رمزگشایی کند. مهاجم با اطلاعات یادگرفته‌شده (کلید گروه و مجموعه شناسه‌های برچسب T_3) سعی می‌کند بقیه برچسب‌های گروه را ردیابی نماید. با توجه به این که مهاجم قادر است بخش u هر پاسخ را رمزگشایی کند، بنابراین می‌تواند شناسه‌ای که در متن رمزی u وجود دارد را یاد بگیرد. به‌عبارت دیگر او می‌تواند کشف کند کدام شناسه برای تولید یک پاسخ مورد استفاده قرار گرفته است. طبق این پروتکل حتی اگر مهاجم شناسه استفاده شده در یک پاسخ را بداند نمی‌تواند نتیجه بگیرد کدامیک از برچسب‌های بالقوه، فرستنده این پاسخ است. به عبارت دیگر مهاجم هیچ دانشی درباره این‌که برچسب T_3 کدامیک از شناسه‌های خود را با دیگر برچسب‌ها به اشتراک گذاشته است ندارد. حتی مهاجم نمی‌داند چند تا از شناسه‌های Ω_3 به اشتراک گذاشته شده‌اند. بنابراین، وقتی مهاجم یک برچسب از یک گروه با n برچسب را مورد حمله قرار می‌دهد

پروتکل پیشنهادی یک مجموعه گمنامی با اندازه ۱ و مجموعه گمنامی دیگری با اندازه n-1 را از این گروه تشکیل می‌دهد. در صورتی‌که در چنین شرایطی در پروتکل احرازهویت مبتنی‌بر گروه n مجموعه گمنامی با اندازه ۱ تشکیل می‌شود [۱۵]. این بخش قابل‌توجه، سطح حریم خصوصی تهیه شده به‌وسیله این پروتکل را نسبت به احرازهویت گروهی، بهبود می‌بخشد. چون (N-n) برچسب باقیمانده سامانه، مجموعه گمنامی دیگری را تشکیل می‌دهد که این در هر دو پروتکل مشابه است. پس پروتکل احراز هویت گمنام متقابل از نفوذ مهاجم از ردیابی با استفاده از به خطر انداختن یک برچسب پیشگیری می‌کند.

با به خطر افتادن برچسب دیگری از این گروه، مهاجم همچنان نمی‌تواند مطمئن باشد کدام یک از برچسب‌های باقیمانده بالقوه، شناسه مورد نظر مهاجم را ارسال کرده است. بنابراین، نتیجه‌گیری می‌شود در این پروتکل مجموعه گمنامی در یک گروه که تحت حمله فیزیکی است با اندازه (n-c) تشکیل می‌شود جایی که n اندازه گروه و c تعداد برچسب‌های به‌خطر افتاده در گروه مورد نظر است.

۵-۲- تحلیل عملکرد

در پروتکل MAPAP پیچیدگی کل کارت‌خوان در بدترین حالت، $\tau + |\pi_x|$ است که در بهترین حالت، اندازه π_x برابر ۳ و در بدترین حالت می‌تواند به مقدار اندازه گروه یعنی n باشد. میزان پیچیدگی کارت‌خوان در پروتکل پیشنهادی نسبت به طرح مبتنی بر گروه، که پیچیدگی کارت‌خوان در بدترین حالت آن $\tau + 1$ است افزایش کمی دارد. به‌منظور ارائه بهبود در حفاظت از حریم خصوصی، باید این افزایش کوچک در پیچیدگی کارت‌خوان را پذیرفت. با توجه به قدرت بیشتر کارت‌خوان‌ها نسبت به برچسب‌ها می‌توان گفت کارت‌خوان‌ها می‌توانند این افزایش در پیچیدگی جستجو را مدیریت نمایند.

سربار ذخیره‌سازی: برچسب‌ها نیاز به ذخیره m عدد شناسه همراه با کلید گروه و کلید مخفی منحصربه‌فرد خود دارند. اگرچه برچسب‌ها محدودیت منابع دارند ولی افزایش نیاز به حافظه از افزایش در پیچیدگی محاسبات و ارتباطات قابل قبول‌تر است. برچسب‌های هوشمند RFID، ظرفیت حافظه ۳۲ کیلو بایت یا بیشتر دارند [۲۳]. همچنین برچسب‌های RFID با ظرفیت حافظه توسعه یافته در بازار در دسترس هستند که می‌توان از آنها در این پروتکل استفاده نمود.

هزینه عملیات: هزینه محاسباتی در برچسب‌های سامانه RFID یک چالش است و ایجاد مشکل می‌نماید [۱۴]. از این رو در این پروتکل از برچسب‌های با هزینه کم که توانایی استفاده از رمزنگاری متقارن را دارند استفاده شده‌است. در پروتکل پیشنهادی هزینه محاسبات برچسب شامل دو عملیات رمزنگاری و یک عملیات رمزگشایی است.

جدول (۲): سربار پروتکل پیشنهادی (MAPAP)

سربار	شرح
ذخیره‌سازی	$(k_0.k_1.\ldots.k_x).n_t$
عملیات	انتخاب یک شناسه ID_{i,j_x} از استخر شناسه گروه ۲ عملیات رمزنگاری ۱ عملیات رمزگشایی
ارتباطی	۳

سربار ارتباطی: در پروتکل پیشنهادی برای احراز هویت موفقیت‌آمیز، برچسب فقط یک پیام به کارت‌خوان ارسال می‌کند. تعداد کل پیام‌های ردوبدل شده بین برچسب و کارت‌خوان در این پروتکل سه پیام است. دو پیام دیگر توسط کارت‌خوان به برچسب ارسال می‌شود که یکی از آنها جهت احراز هویت برچسب می‌باشد و پیام دیگر کارت‌خوان به برچسب باعث می‌شود برچسب بتواند کارت‌خوان را احراز هویت نماید.

۶- اندازه‌گیری حریم خصوصی

به منظور اندازه‌گیری حریم خصوصی پروتکل، سطح حریم خصوصی پروتکل به عنوان یک تابع از تعداد کل برچسب‌های به خطر افتاده اندازه گرفته می‌شود. این کار را با استفاده از دو روش انجام می‌گیرد. روش اول، اندازه‌گیری حریم خصوصی مبتنی‌بر مجموعه گمنامی است [۱۵]، روش دوم، مقدار اطلاعات فاش شده توسط پروتکل می‌باشد [۲۴].

۶-۱- اندازه‌گیری حریم خصوصی مبتنی بر مجموعه گمنامی

سطح حریم خصوصی یک سامانه RFID در یک زمان مشخص، یک تابع از تعداد کل برچسب‌های به خطر افتاده در آن زمان است. وقتی در یک سامانه بعضی از برچسب‌ها به خطر افتاده‌اند مجموعه همه برچسب‌ها به مجموعه‌های گمنامی اعضای خودشان تبدیل می‌شوند. سطح حریم خصوصی مبتنی‌بر مجموعه گمنامی که با $\wp$ نشان داده می‌شود می‌تواند به عنوان متوسط اندازه مجموعه گمنامی اندازه‌گیری شود. با استفاده از رابطه (۴) سطح حریم خصوصی مبتنی‌بر مجموعه گمنامی محاسبه می‌شود [۱۵].

$$\wp = \frac{1}{N}\sum_i |p_i|\frac{|p_i|}{N} = \frac{1}{N^2}\sum_i |p_i|^2 \qquad (۴)$$

در رابطه فوق، $|P_i|$ اندازه بخش P_i است و $|P_i|/|N|$ احتمالی است که یک برچسب انتخاب شده به‌طور تصادفی به بخش P_i تعلق داشته باشد.

در این پروتکل وقتی برچسب‌ها به‌خطر می‌افتد یک نوع مشابه از بخش‌ها تشکیل می‌شود. به این ترتیب که اگر c_i تعداد برچسب‌های به خطر افتاده در گروه G_i باشد، سپس مجموعه برچسب‌های داخل این گروه به c_i مجموعه گمنامی با اندازه یک و مجموعه گمنامی دیگر با اندازه $(n - c_i)$ تقسیم می‌شوند.

در این صورت سطح حریم خصوصی مبتنی‌بر مجموعه گمنامی در پروتکل پیشنهادی با استفاده از رابطه (۵) قابل محاسبه است.

$$\wp = \frac{1}{N^2}\left((n(\tau - |C|))^2 + \sum_{each\ c_i \epsilon C}(c_i + (n - c_i)^2)\right) \qquad (۵)$$

در رابطه فوق، N تعداد کل برچسب‌ها در سامانه، n تعداد کل برچسب‌های داخل یک گروه و τ تعداد کل گروه‌ها در سامانه است. در این رابطه C مجموعه همه c_iها یعنی تعداد کل برچسب‌های به خطر افتاده است $(C = \sum_{each\ c_i \epsilon C} c_i)$ و $|C|$ تعداد کل گروه‌های به خطر افتاده می‌باشد.

۶-۲- اندازه‌گیری حریم خصوصی مبتنی‌بر نشت اطلاعات

میزان نشت اطلاعات بر حسب بیت براساس نظریه اطلاعات شانون اندازه‌گیری می‌شود [۲۵]. اگر یک گروه از برچسب‌ها با اندازه S داشته باشیم و مهاجم این گروه را به دو زیرگروه مجزا با اندازه S/2 تقسیم کند یک بیت اطلاعات از $\log_2 S$ بیت افشا می‌شود. در صورت تقسیم گروه به دو زیرگروه با اندازه‌های مختلف، که در آن، s/a برچسب‌ها در یک زیرگروه و بقیه برچسب‌ها یعنی (1-1/a)S در زیرگروه دیگر قرار گیرند، مقدار متوسط اطلاعات افشا شده برحسب بیت با استفاده از رابطه (۶) قابل اندازه‌گیری است.

$$I = \frac{1}{\mathrm{a}}\log_2(a) + \frac{a-1}{\mathrm{a}}\log_2\left(\frac{\mathrm{a}}{a-1}\right) \qquad (۶)$$

بنابراین، در حالت کلی اگر مهاجم همه N برچسب سامانه را به k بخش مجزا تقسیم کند مقدار متوسط اطلاعات افشا شده بر حسب بیت با استفاده از رابطه (۷) قابل اندازه‌گیری است.

$$I = \sum_{i=1}^{k} \frac{|p_i|}{\mathrm{N}} . \log_2\left(\frac{N}{|p_i|}\right) \qquad (۷)$$

$|P_i|$ اندازه بخش P_i را نشان می‌دهد.

مطابق با پروتکل پیشنهادی وقتی برچسب‌ها به خطر می‌افتد اگر c_i تعداد برچسب‌های به خطر افتاده در گروه G_i باشد، مجموعه برچسب‌های داخل این گروه به c_i مجموعه گمنامی با اندازه یک و مجموعه گمنامی دیگر با اندازه $(n - c_i)$ تقسیم می‌شوند.

در چنین صورتی مقدار نشت اطلاعات I برحسب بیت با استفاده از رابطه (۸) محاسبه می‌شود.

$$I = \left(\frac{n(\tau - |C|)}{\mathrm{N}}\log_2\left(\frac{\mathrm{N}}{n(\tau - |C|)}\right)\right) + \sum_{each\ c_i \epsilon C}\left(c_i\frac{1}{\mathrm{N}}\log_2 N + \left(\frac{\mathrm{n} - c_i}{N}\right)\log_2\left(\frac{N}{\mathrm{n} - c_i}\right)\right) \qquad (۸)$$

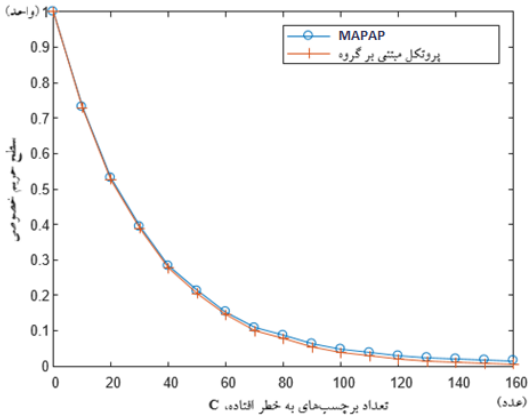
در رابطه فوق N تعداد کل برچسب‌ها در سامانه، n تعداد کل برچسب‌های داخل یک گروه و τ تعداد کل گروه‌ها در سامانه است. در این رابطه C مجموعه همه c_iها یعنی تعداد کل برچسب‌های به خطر افتاده می‌باشد $(C = \sum_{each\ c_i \epsilon C} c_i)$ و $|C|$ تعداد کل گروه‌های به خطر افتاده می‌باشد.

۶-۳- نتایج عملی

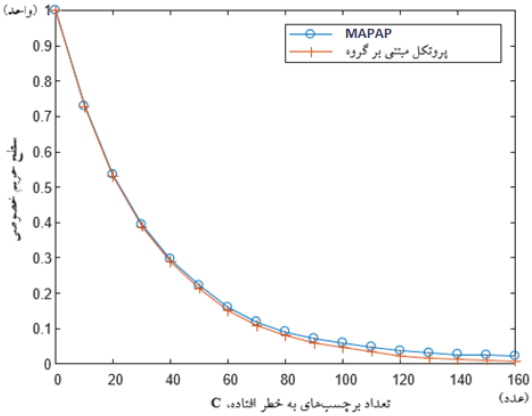
از آنجا که پروتکل پیشنهادی مبتنی‌بر ساختار گروهی است میزان حریم خصوصی ارائه شده در این پروتکل با حریم خصوصی طرح مبتنی‌بر گروه، مقایسه می‌شود. برای انجام این‌کار از شبیه‌ساز متلب استفاده شده است. در این آزمایش سه سامانه با مشخصات $N=2^{20}$, τ=64، $N=2^{16}$, τ=64، $N=2^{10}$, τ=64 درنظر گرفته شدند که با یک توزیع تصادفی یکنواخت به خطر افتادند. تعداد برچسب‌های در معرض خطر در محدوده ۰ تا ۱۶۰ می‌باشد و این آزمایش ۱۰۰ بار اجرا شد. متوسط $\wp$ به دست آمده توسط هر دو پروتکل به عنوان تابعی از تعداد کل برچسب‌های به خطر افتاده C محاسبه شد.

نتایج حاصل از شبیه‌سازی نشان می‌دهد سطح حریم خصوصی ایجاد شده بوسیله پروتکل پیشنهادی بالاتر از احراز هویت مبتنی بر گروه است. همانطور که در نمودارهای (۱)، (۲) و (۳) اندازه‌گیری سطح حریم خصوصی نشان داده می‌شود وقتی تعداد برچسب‌های به خطر افتاده بیشتر از ۳۰ برچسب می‌باشد افزایش کم در سطح حریم خصوصی پروتکل پیشنهادی قابل مشاهده است. در این آزمایش مقدار متوسط نشت اطلاعات I نیز برای هر دو پروتکل محاسبه شد. در نمودار (۴) که تعداد برچسب‌ها در سامانه 2^{10} می‌باشد وقتی مقدار برچسب‌های به خطر افتاده به ۱۵۰ عدد می‌رسد، احراز هویت مبتنی‌بر گروه حدود ۹ بیت از ۱۰ بیت اطلاعات را افشا می‌کند، در حالی که پروتکل پیشنهادی حدود ۷ بیت از اطلاعات را افشا می‌نماید. به عبارت دیگر، احراز هویت مبتنی‌بر گروه حدود ۲۰ درصد بیشتر از

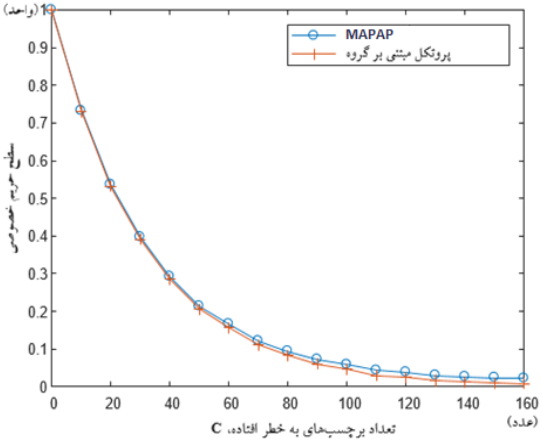
پروتکل پیشنهادی اطلاعات را افشا می‌کند. نمودار (۵) که تعداد برچسب‌های سامانه در آن 2^{16} می‌باشد وقتی مقدار برچسب‌های به خطر افتاده به ۱۵۰ عدد می‌رسد، احراز هویت مبتنی‌بر گروه حدود ۱۵ بیت از ۱۶ بیت اطلاعات را افشا می‌کند، در حالی که پروتکل پیشنهادی حدود ۶ بیت از اطلاعات را افشا می‌نماید.



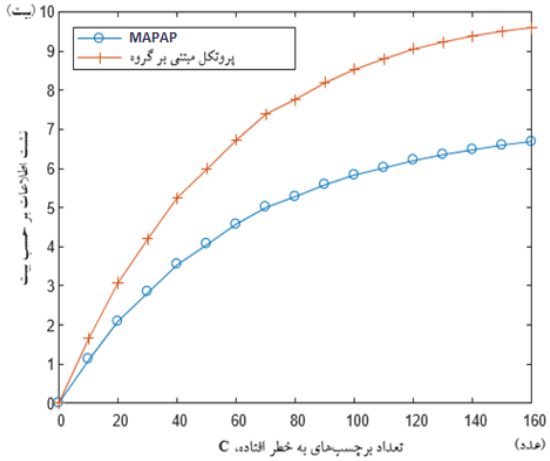
نمودار (۱): مقایسه سطح حریم خصوصی مبتنی‌بر گمنامی با $N=2^{10}$ و $\tau = 64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی‌بر گروه.



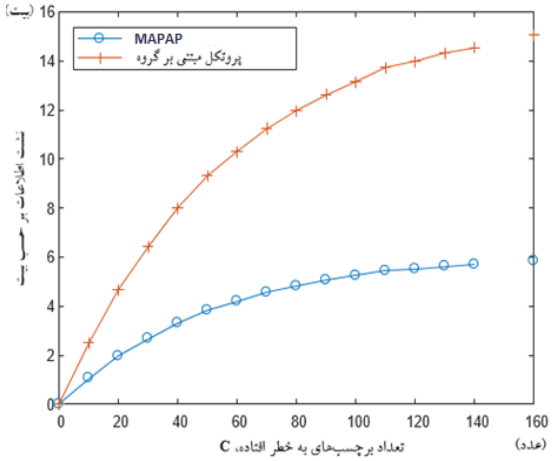
نمودار (۲): مقایسه سطح حریم خصوصی مبتنی‌بر گمنامی با $N=2^{16}$ و $\tau=64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی بر گروه.



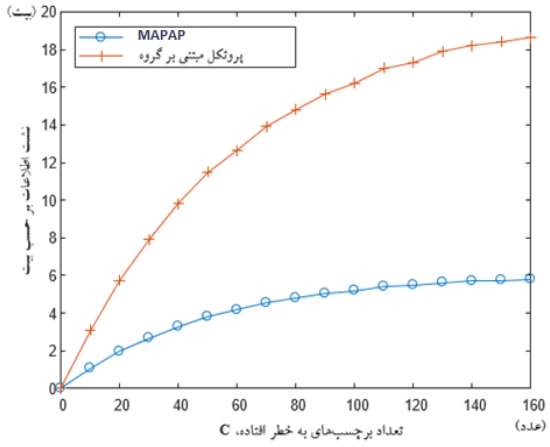
نمودار (۳): مقایسه سطح حریم خصوصی مبتنی بر گمنامی با $N=2^{20}$ و $\tau=64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی بر گروه



نمودار (۴): مقایسه میزان نشت اطلاعات برحسب بیت با $N=2^{10}$ و $\tau=64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی بر گروه



نمودار (۵): مقایسه میزان نشت اطلاعات بر حسب بیت با $N=2^{16}$ و $\tau=64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی‌بر گروه



نمودار (۶): مقایسه میزان نشت اطلاعات بر حسب بیت با $N=2^{20}$ و $\tau=64$ در پروتکل پیشنهادی (MAPAP) و احراز هویت مبتنی‌بر گروه.

به عبارت دیگر، احراز هویت مبتنی‌بر گروه حدود ۵۶/۲۵ درصد بیشتر از پروتکل پیشنهادی اطلاعات را افشا می‌کند. بر اساس نتایج شبیه‌سازی، نتیجه می‌شود میزان اطلاعات افشا شده به‌وسیله پروتکل احراز هویت مبتنی بر گروه با بزرگ شدن اندازه سامانه افزایش می‌یابد. چنانچه نمودار (۶) که میزان نشت اطلاعات را در یک سامانه که تعداد برچسب‌های آن به 2^{20} برچسب افزایش یافته است، این نتیجه را تصدیق می‌نماید. در این نمودار پروتکل احراز هویت مبتنی‌بر گروه، زمانی که تعداد ۱۵۰ برچسب به خطر می‌افتد تقریبا ۱۹ بیت از ۲۰ بیت اطلاعات را افشا می‌نماید در حالی که پروتکل پیشنهادی حدود ۶ بیت از اطلاعات را افشا می‌کند. در چنین شرایطی، پروتکل احراز هویت مبتنی‌بر گروه ۶۵ درصد بیشتر از پروتکل پیشنهادی اطلاعات را افشا می‌نماید.

مطابق با نمودارهای (۴)، (۵) و (۶) ملاحظه می‌شود پروتکل پیشنهادی با افشای کمتر اطلاعات در سامانه‌های با مقیاس بزرگ، حفاظت از حریم خصوصی را به مقدار قابل توجهی نسبت به طرح احراز هویت مبتنی‌بر گروه بهبود می‌بخشد و هر چه تعداد برچسب‌ها در سامانه بیشتر می‌شود تفاوت مقدار اطلاعات افشا شده در پروتکل پیشنهادی نسبت به طرح احراز هویت مبتنی‌بر گروه بیشتر می‌شود. همچنین نمودارهای مربوط به نشت اطلاعات نشان می‌دهد با افزایش تعداد کل برچسب‌های به خطر افتاده C، مقدار متوسط اطلاعات افشا شده توسط طرح احراز هویت مبتنی بر گروه کاملا بالاتر از اطلاعات افشا شده در پروتکل پیشنهادی است. از این رو پروتکل احراز هویت پیشنهادی انتخاب بهتری برای حفظ حریم خصوصی در سامانه‌های با مقیاس بزرگ می‌باشد.

نشت اطلاعات یک معیار بهتر از مجموعه گمنامی برای نشان دادن تهدیدات حریم خصوصی در سامانه RFID است [۱۵]. در این آزمایش اگرچه بهبود سطح حریم خصوصی ارائه شده توسط پروتکل پیشنهادی در برابر طرح احراز هویت مبتنی‌بر گروه قابل توجه نیست ولی بر اساس نتایج حاصل از مقدار اطلاعات افشا شده بوسیله این دو پروتکل می‌توان گفت پروتکل پیشنهادی حفاظت از حریم خصوصی را به میزان قابل توجهی بهتر از طرح احراز هویت مبتنی‌بر گروه فراهم می‌نماید.

۷- نتیجه‌گیری

با توجه به برتری روش احراز هویت مبتنی‌بر گروه، ضمن ارائه یک پروتکل احراز هویت خصوصی گمنام متقابل مبتنی‌بر گروه، حریم خصوصی و امنیت آن مورد بحث و بررسی قرار گرفت. بررسی و تحلیل رسمی پروتکل MAPAP نشان داد این پروتکل اطلاعات حریم خصوصی و همچنین قابلیت عدم‌ارتباط‌پذیری را حفظ می‌نماید. همچنین زمانی که مهاجم برخی از برچسب‌ها را به خطر می‌اندازد، این پروتکل سطح بالاتری از حریم خصوصی را نسبت به طرح مبتنی‌بر گروه ایجاد می‌کند. حریم خصوصی پروتکل پیشنهادی در مقایسه با طرح احراز هویت مبتنی‌بر گروه با دو معیار "سطح حریم خصوصی" و "نشت اطلاعات" طی یک آزمایش عملی مورد سنجش قرار گرفتند. نتایج حاصل نشان داد گرچه افزایش سطح حریم خصوصی ارائه شده در پروتکل پیشنهادی نسبت به طرح احراز هویت مبتنی‌بر گروه افزایش کمی داشت ولی بر اساس نتایج حاصل از مقدار اطلاعات افشا شده به‌وسیله این دو پروتکل می‌توان گفت پروتکل پیشنهادی حفاظت از حریم خصوصی را به میزان قابل توجهی نسبت به طرح احراز هویت مبتنی‌بر گروه بهبود می‌بخشد. بنابراین، نتیجه می‌شود پروتکل پیشنهادی با افشای کمتر اطلاعات در سامانه های با مقیاس بزرگ، حفاظت از حریم خصوصی را به مقدار قابل توجهی نسبت به طرح احراز هویت مبتنی‌بر گروه بهبود می‌بخشد و هر چه تعداد برچسب‌ها در سامانه بیشتر می‌شود تفاوت مقدار اطلاعات افشا شده در پروتکل پیشنهادی با طرح احراز هویت مبتنی‌بر گروه نیز بیشتر می‌شود. از این رو پروتکل احراز هویت پیشنهادی انتخاب بهتری برای حفظ حریم خصوصی در سامانه‌های با مقیاس بزرگ می‌باشد.

از جمله موضوعاتی که می‌توان در ارتقاء پروتکل احراز هویت خصوصی گمنام متقابل به عنوان کارهای تحقیقاتی آینده اشاره نمود، کاهش بیشتر هزینه‌های پیچیدگی و ذخیره‌سازی پروتکل، افزایش مقیاس‌پذیری و ایجاد مکانیزمی برای بازنوسازی کلیدها جهت جلوگیری از حملات *Dos* می‌باشد. از دیگر کارهای آینده می‌توان به تعیین مصالحه بهینه بین پیچیدگی احراز هویت و میزان ذخیره‌سازی مورد نیاز اشاره نمود.

۸- منابع

[1] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," Security in Pervasive Computing, pp. 201-212, 2004.

[2] Q. Yao, Y. Qi, J. Han, J. Zhao, X. Li, and Y. Liu, "Randomizing RFID private authentication," in Proceedings of the Pervasive Computing and Communications Workshop (PerCom Workshops 2009), pp. 1–10, 2009.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," RFID privacy workshop, vol. 82, 2003.

[4] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," Selected Areas in Cryptography, vol. 3897, 2005.

[5] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), IEEE, 2005.

[6] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," IEEE Annual Conference on Pervasive Computing and Communications Workshops, Proceedings of the Second, IEEE, 2004.

[7] H. Y. Chien and C. H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," Computer Standards & Interfaces, vol. 29.2, pp. 254-259, 2007.

[8] E. J. Yoon, "Improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard," Expert Systems with Applications, vol. 39.1, pp. 1589-1594, 2012.

[9] A. Mohammadali, Z. Ahmadian, and M. R. Aref, "Analysis and Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard," IACR Cryptology ePrint Archive, p. 66, 2013.

[10] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. C. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system," Journal of medical systems, vol. 39.1, p. 153, 2015.

[11] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," Proceedings of the 11th ACM conference on Computer and communications security, ACM, 2004.

[12] L. Buttyán, T. Holczer, and I. Vajda, "Optimal key-trees for tree-based private authentication," Privacy Enhancing Technologies, Springer Berlin/Heidelberg, 2006.

[13] M. Chen and S. Chen, "An efficient anonymous authentication protocol for RFID systems using dynamic tokens," Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference on. IEEE, 2015.

[14] M. Rahman, R. V. Sampangi, and S. Sampalli, "Lightweight protocol for anonymity and mutual authentication in RFID systems," Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE, IEEE, 2015.

[15] G. Avoine, L. Buttyant, T. Holczer, and I. Vajda, "Group-based private authentication," World of Wireless, Mobile and Multimedia Networks, WoWMoM 2007. IEEE International Symposium on a, IEEE, pp. 1-6, 2007.

[16] F. Rahman, M. E. Hoque, and S. I. Ahamed, "Anonpri: A secure anonymous private authentication protocol for RFID systems," Information Sciences, vol. 379, pp. 195-210, 2017.

[17] A. Juels and S. A. Weis, "Defining strong privacy for RFID," ACM Transactions on Information and System Security (TISSEC), vol. 13.1, p. 7, 2009.

[18] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," International Workshop on Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2002.

[19] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC press, 1996.

[20] W. Diffie and ME. Hellman, "Multiuser cryptographic techniques," Proceedings of the June 7-10, National Computer Conference and Exposition, ACM, 1976.

[21] G. N. Khan and Z. Guangyu, "Secure RFID authentication protocol with key updating technique," Computer Communications and Networks (ICCCN), 2013 22nd International Conference on, IEEE, 2013.

[22] N. Koblitz and A. J. Menezes, "The random oracle model: a twenty-year retrospective," Designs, Codes and Cryptography, vol. 77.2-3, pp. 587-610, 2015.

[23] A. Laurie, "Practical attacks against RFID," Network Security 2007, vol. 9, pp. 4-7, 2007.

[24] K. Nohl and D. Evans, "Quantifying information leakage in tree-based hash protocols (short paper)," Information and Communications Security, pp. 228-237, 2006.

[25] C. E. Shannon, "A mathematical theory of communication," ACM SIGMOBILE Mobile Computing and Commnuications Review, vol. 5.1, pp. 3-55, 2001.

Journal of Electronical & Cyber Defence
Vol. 6, No. 4, 2019, Serial No. 24

A Mutual Anonymity Private Authentication Protocol to Use in Radio-Frequency Identification Systems

K. Taleghanizadeh, M. Golsorkhtabaramiri*

Department of Computer Engineering, Babol Branch, Islamic Azad University, Babol, Iran

(Received: 03/12/2017, Accepted: 27/05/2018)

ABSTRACT

Radio frequency identification (RFID) has many advantages in the field of large-scale identification, including speed increase and cost reduction.For this reason, this system has many applications in the modern world and can be used as an essential tool for improving human life. Since this technology faces serious challenges in the field of security and privacy, its applications has been limited due to security concerns and delays in standardization. Given the widespread use of RFID technology in large-scale systems, and importance of privacy in these systems, this article introduces a mutual anonymous private authentication protocol (MAPAP); a protocol which adds privacy and scalability features to a mutual authentication protocol. In this new protocol the privacy is measured using the information leakage criterion and it is seen that the amount of information disclosed by this protocol when compromised is significantly less than group-based authentication. In a system with 2^{20} tags, with the increase in the number of compromised tags, the difference in information leakage between this protocol and the group-based authentication protocol increases, such that, when the number of compromised tags in this system reaches 150, information disclosed by the proposed protocol is about 65 percent less than group-based authentication and this difference increases with increasing system size.

Keywords: RFID, Mutual Authentication, Privacy, Security, Anonymity

* Corresponding Author Email: golesorkh@baboliau.ac.ir