مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال دوم، شماره ۲، تابستان ۱۳۹۳، ص ۳۱-۲۳

تحلیل محرمانگی و امنیت پروتکل احراز هویت دوسویه در سامانه‌های RFID مبتنی بر توابع چکیده‌ساز

سیدمحمد علوی[۱]، بهزاد عبدالملکی*[۲]، کریم باقری[۳]

۱- استادیار، دانشگاه جامع امام‌حسین(ع)

۲و۳- آزمایشگاه سامانه‌های یادگیری برمبنای نظریه اطلاعات(سینا)، دانشگاه شاهد

(دریافت: ۹۳/۰۱/۱۶، پذیرش: ۹۳/۵/۱۵)

چکیده

فناوری شناسایی با استفاده از امواج رادیویی (RFID)، یک فناوری نوین است که در زمینه‌های متفاوت، جهت شناسایی و احراز هویت مورد استفاده قرار می‌گیرد. در اکثر کاربردها، امنیت این سامانه‌ها بسیار اهمیت دارد. در سال‌های اخیر برای حفظ امنیت این سامانه‌ها، پروتکل‌های احراز هویت متفاوتی پیشنهاد شده است. این مقاله، به تحلیل امنیتی یک پروتکل احراز هویت متقابل سامانه‌های RFID که توسط آقای کیم در سال ۲۰۱۳ ارائه شده است پرداخته و نشان می‌دهد برخلاف اینکه طراح سعی کرده است که پروتکل امنی را طراحی کند، اما همچنان ضعف‌هایی بر آن وارد است و در مقابل حمله‌هایی نظیر جعل برچسب، ردیابی و ردیابی پسرو ضعف دارد. برای تحلیل‌های امنیتی، از مدل محرمانگی اوفی- فان استفاده شده و حمله‌های ردیابی و ردیابی پسرو در قالب این مدل انجام شده است. در ادامه، نسخه بهبودیافته از پروتکل کیم پیشنهاد شده، که ضعف‌های پروتکل کیم در آن حذف شده است. امنیت و محرمانگی پروتکل پیشنهادشده با برخی از پروتکل‌های مشابه مقایسه شده و نشان داده شده است که امنیت و محرمانگی پروتکل پیشنهادشده کامل است.

واژه‌های کلیدی: امنیت سامانه‌های RFID، پروتکل‌های احراز هویت، سامانه‌های RFID، پروتکل‌های احراز هویت دوسویه

۱. مقدمه

فناوری شناسایی از طریق امواج رادیویی(RFID)، یک فناوری جدید است که برای شناسایی اشیاء و موجودات زنده به‌کار گرفته می‌شود. به‌دلیل مزایای زیادی همچون کاهش هزینه‌ها، افزایش سرعت و انجام شناسایی در مقیاس وسیع، این فناوری مورد توجه بسیاری قرار گرفته و روزبه‌روز بر دامنه کاربران آن افزوده می‌شود.

برای نخستین بار، در جنگ جهانی دوم از فناوری شناسایی از طریق امواج رادیویی استفاده شد. کاربرد این فناوری، در شناسایی هواپیماهای خودی و دشمن بود که به این کاربرد اصطلاحاً شناسایی دوست یا دشمن [۱](IFF) گفته می‌شد. هنگامی که یک هواپیما در حوزه شناسایی و تشخیص رادارهای خودی قرار می‌گرفت، به کمک پیام‌های مشخصی که از هواپیما منتشر می‌شد رادارها می‌توانستند دوست یا دشمن بودن آن را تشخیص دهند [۱]. در دهه نود میلادی حوزه‌های دیگری چون سامانه‌های کنترل دسترسی [۲] و همچنین استفاده در عوارضی بزرگراه‌ها نیز به کاربردهای RFID اضافه شد. با پیشرفت چشمگیر فناوری مدارهای مجتمع در ده سال اخیر و در نتیجه، کاهش هزینه‌های استفاده از فناوری RFID، شاهد رشد چشم‌گیر و به‌کارگیری سامانه‌های RFID در حوزه‌های مختلفی چون استفاده در ترابری و پشتیبانی قوای نظامی [۳]، بارکدهای الکترونیکی، بلیط‌های حمل‌ونقل عمومی و گذرنامه‌های الکترونیکی [۴] بوده‌ایم.

به‌طورکلی، یک سامانه RFID از سه جزء تشکیل‌شده است[۵]:

رایانامه نویسنده مسئول: b.abdolmaleki.ir@ieee.org

1. Identify Friend or Foe

۱. برچسب‌ها [1]

۲. کارت‌خوان‌ها [2]

۳. سرویس‌دهنده نهایی [3]

نحوه عملکرد این سامانه‌ها بدین گونه است که به هر برچسب، یک شناسه منحصر به‌فرد اختصاص داده می‌شود و این شناسه در حافظه او ذخیره می‌شود. هر برچسب دارای یک تراشه بسیار کوچک نیز هست که ابزارهای محاسباتی و پردازشی در این تراشه واقع می‌شوند. این برچسب‌ها بر روی اهداف موردنظر برای شناسایی که می‌تواند کالا، انسان و یا حیوان باشد، کار گذاشته می‌شوند. دستگاه‌های کارت‌خوان نیز در مکان‌های مناسبی نصب می‌شوند. کارت‌خوان‌ها از طریق یک کانال به سرویس‌دهنده نهایی متصل می‌شوند. در سرویس‌دهنده نهایی نیز اطلاعات مربوط به همه برچسب‌ها در یک حافظه امن و بزرگ ذخیره می‌شود.

برای امن کردن ارتباطات در سامانه‌های RFID، پروتکل‌های زیادی در سال‌های اخیر مطرح شده‌اند [۶-۱۰]. این پروتکل‌ها از توابع متعددی نظیر توابع چکیده‌ساز برای افزایش امنیت تبادل داده استفاده می‌کنند. توابع چکیده‌ساز کاربردهای متعددی در مخابرات دارند[۱۱-۱۲].که امروزه این توابع در رمزنگاری‌های سبک نیز بسیار مورد توجه واقع شده است. در همین راستا، اوکابو[4] و همکاران یک پروتکل احراز هویت مبتنی بر توابع چکیده‌ساز ارائه کردند اما آن دارای آسیب‌پذیری‌های امنیتی بود [۱۳]. تسودیک[5] یک پروتکل احراز هویت به‌نام YA-TRAP ارائه کرد و ادعا نمود که در برابر حمله ردیابی و دیگر حملات مقاوم می‌باشد [۱۴]. اما نشان داده شد که این ادعا درست نمی‌باشد. سپس تسودیک پروتکل احراز هویت *YA– TRAP را در [۱۵] ارائه کرد که بعدها ثابت شد که این پروتکل نیز دارای ضعف امنیتی است. اخیراً چو[6] و همکارانش یک پروتکل احراز هویت دوسویه مبتنی بر توابع چکیده‌ساز را پیشنهاد کردند [۱۶] و ادعا کردند که یک پروتکل امن می‌باشد. در سال ۲۰۱۳، کیم[7] نشان داد که پروتکل چو و همکارانش در مقابل حمله ناهمزمان‌سازی آسیب‌پذیر می‌باشد و در ادامه، یک پروتکل احراز هویت دوسویه[8] (MAPS)مبتنی بر توابع چکیده‌ساز ارائه و ادعا کرد که پروتکل پیشنهادی‌اش، امنیت و محرمانگی داده‌ها را حفظ می‌کند و همچنین در مقابل حمله جعل هویت، حمله ردیابی و حمله ردیابی پیشرو مقاوم است [۱۷]. در این مقاله، ما نشان خواهیم داد که پروتکل کیم نه‌تنها ویژگی‌های امنیتی را برآورده نمی‌سازد، بلکه ازلحاظ محرمانگی نیز آسیب‌پذیر می‌باشد. ما در ابتدا به‌طور خلاصه پروتکل مورد بحث را مرور و سپس حملات خود یعنی حمله جعل هویت برچسب، حمله ردیابی و حمله ردیابی پیشرو را بر روی آن ارائه می‌کنیم. در ادامه، جهت رفع ضعف‌های پروتکل کیم، نسخه بهبودیافته ای از آن را ارائه می‌کنیم و نشان می‌دهیم که پروتکل پیشنهادشده از امنیت کافی برخوردار است.

در این مقاله، در بخش ۲، به بازبینی پروتکل احراز هویت MAPS پرداخته شده و در بخش ۳، تحلیل امنیتی پروتکل MAPS و ضعف‌های آن مورد بررسی قرار گرفته و حملات جعل هویت برچسب، ردیابی و ردیابی پیشرو بر روی آن انجام می‌شود. سپس جهت تأمین امنیت کاربران RFID یک پروتکل بهبودیافته از MAPS پیشنهاد می‌شود که در بخش ۴ آورده شده است. در بخش ۵، به تحلیل امنیتی پروتکل پیشنهادشده پرداخته شده است. همچنین مقایسه تحلیل امنیتی پروتکل پیشنهادشده با چند پروتکل مشابه، در این بخش آورده شده و درنهایت، نتیجه‌گیری از مقاله در بخش ۶ ذکر شده است.

۲. بازبینی پروتکل MAPS

در سال ۲۰۱۳، آقای کیم پروتکل احراز هویت متقابل MAPS را برای سیستم‌های RFID ارائه کرد [۱۷]. این پروتکل از دو مرحله تشکیل‌شده است. در مرحله نخست، برچسب و سرویس‌دهنده نهایی مقداردهی اولیه می‌شوند. در مرحله دوم، پروتکل وارد مرحله شناسایی و احراز اصالت می‌شود. در شکل ۱ روند کار پروتکل MAPS نمایش داده‌شده است. در ادامه، این پروتکل را به‌صورت مختصر بازبینی می‌کنیم.

الف) مرحله اولیه

این مرحله قبل از شروع عملیات سامانه انجام و در طی آن، یک تابع چکیده‌ساز بین برچسب و سرویس‌دهنده نهایی به اشتراک گذاشته می‌شود. در سرویس‌دهنده برای هر برچسب چندتایی (ID_k, S_j, DATA, S_{j+1}) ذخیره می‌شود. در برچسب و کارت‌خوان یک تابع تولید اعداد تصادفی کار گذاشته می‌شود.

1. Tags
2. Readers
3. Back-end Server
4. Ohkubo
5. Tsudik
6. Cho
7. Kim
8. Mutual Authentication Protocol Based on Synchronized Secret (MAPS)

ب) مرحله احراز هویت

این مرحله از تبادل اطلاعات بین برچسب، کارت‌خوان و سرویس‌دهنده نهایی به‌صورت زیر انجام می‌شود:

۱) ابتدا کارت‌خوان عدد تصادفی R_r را تولید کرده و به همراه یک درخواست به برچسب ارسال می‌کند.

۲) پس از دریافت پیام، برچسب عدد تصادفی R_t و همچنین مقدار RID_i را تولید کرده و پیام‌های زیر را تولید می‌کند:

$$RID_i = \left(R_t - R_t \bmod s_j + 1\right)_{(0:47)} \| \left(R_t + s_j - R_t mods_j\right)_{(48:95)}$$
$$\alpha = H\left(ID_k \oplus R_t \oplus R_r \oplus RID_i\right)$$
$$\beta = s_{(0:47)} \| ID_{k_{(48:95)}} \quad (1)$$

سپس پیام $(\alpha, R_t \oplus \beta)$ را به کارت‌خوان ارسال می‌کند.

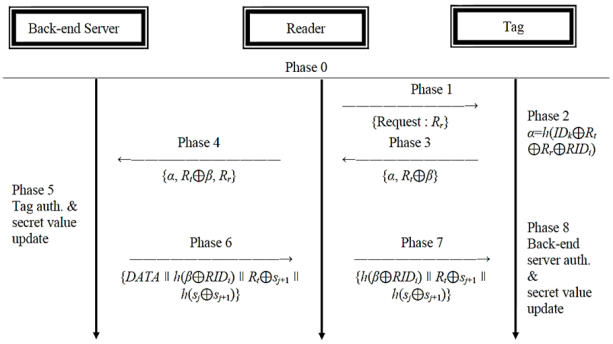
۳) کارت‌خوان پیام دریافتی از برچسب را به‌همراه R_r برای سرویس‌دهنده نهایی ارسال می‌کند.

۴) در سرویس‌دهنده بعد از دریافت پیام به‌ازای همه $(ID_k, S_{old}, S_{new}, DATA)$ موجود در پایگاه داده خود، مقدار β را محاسبه کرده و سپس مقدار R_t و RID'_i را محاسبه می‌کند. در ادامه، مقدار $\alpha' = h\left(ID_k \oplus R_t \oplus R_r \oplus RID'_i\right)$ و با پیام دریافتی مقایسه می‌کند و در صورت برابری، هویت برچسب تأیید می‌شود و کلید مخفی S_j را به S_{j+1} به‌روزرسانی می‌کند. در نهایت، پیام زیر را محاسبه کرده و به کارت‌خوان ارسال می‌کند:

$$\{DATA \| h(\beta \oplus RID_i) \| R_t \oplus S_{j+1} \| h\left(S_j \oplus S_{j+1}\right)\}$$

۵) کارت‌خوان اطلاعات مربوط به برچسب یعنی DATA را از پیام دریافتی جدا کرده و سپس پیام را به برچسب می‌فرستد. پیام:

$$\{h(\beta \oplus RID_i) \| R_t \oplus S_{j+1} \| h\left(S_j \oplus S_{j+1}\right)\}$$



شکل ۱. پروتکل MAPS [۱۷]

۶) برچسب بعد از دریافت پیام ابتدا تابع چکیده متناظر با پیام دریافتی $h\left(S_j \oplus S_{j+1}\right)$ و $h(\beta \oplus RID_i)$ محاسبه کرده و در صورت برابری، کلید خود را مانند سرویس‌دهنده نهایی به‌روزرسانی می‌کند.

۳. تحلیل امنیتی و حمله به پروتکل MAPS

کیم در [۱۷] ادعا کرده است که پروتکل MAPS دارای ویژگی‌های امنیتی مطلوب است. اما نتایجی که ما به دست می‌آوریم نشان می‌دهد که این پروتکل در برابر حملات گوناگون آسیب‌پذیر است. در ادامه، حمله‌هایی بر روی پروتکل MAPS ارائه می‌شوند که این حمله‌ها شامل جعل هویت برچسب، حمله ردیابی و حمله ردیابی پسرو است. حمله‌های ردیابی و ردیابی پسرو در قالب مدل اوفی- فان انجام شده است. لذا در ادامه، در ابتدا اشاره مختصری به مدل اوفی- فان کرده و سپس حملات انجام‌شده را با جزییات بیشتری ارائه می‌کنیم.

- **مدل اوفی- فان جهت ارزیابی قابلیت عدم ردیابی**

مدل اوفی- فان که برای ارزیابی حمله‌های عدم ردیابی و عدم ردیابی پسرو مورد استفاده قرار می‌گیرد، به شرح زیر است [۱۸]:

در این مدل، یک شریک[1] می‌تواند شامل برچسب و یا کارت‌خوان باشد. هر یک از شرکا می‌توانند فعالانه در اجرای پروتکل مشارکت کنند و پروتکل را تا پایان ادامه دهند. طرفین درگیر در پروتکل بر روی یک کانال بی‌سیم و ناامن با یکدیگر تعامل دارند که این کانال به‌طور کامل در کنترل یک مهاجم قدرتمند قرار دارد. به این مهاجم توانایی‌ها و قدرت عمل بسیاری داده می‌شود که این توانایی‌ها به‌طور رسمی در قالب پرسمان‌های زیر مدل می‌شوند:

- **Execute (R ,T ,i) query**

توسط این پرسمان، به مهاجم قابلیت شنود و استراق سمع نشست‌های برگزارشده بین طرفین داده می‌شود. به بیان رسمی، هنگامی‌که مهاجم اقدام به ارسال Execute (R, T, i) query می‌کند، قادر می‌شود تا iمین نشست برگزارشده بین برچسب T وکارت‌خوان R را به‌طور کامل شنود کرده و اطلاعات ردوبدل شده در آن نشست را به دست بیاورد. در واقع با این پرسمان، مهاجم قادر است یک حمله غیرفعال[2] انجام دهد.

1. Party
2. Passive Attack

- **Send (U1 ,U2 ,I ,m)query**

توسط این پرسمان به مهاجم قابلیت انجام حملات فعال داده می‌شود. به بیان رسمی، با ارسال پرسمان Send (U1,U2,I,m)query توسط مهاجم، به او اجازه داده می‌شود تا با جعل هویت یک کارت‌خوان $U_1 \in \text{Readers}$ (و یا برچسب $U_1 \in \text{Tags}$)، بتواند به انتخاب خودش پیام m را در نشست iم از پروتکل، به برچسب نمونه $U_2 \in \text{Tags}$ (و یا کارت‌خوان $U_2 \in \text{Readers}$) ارسال کند و پاسخ او را بر طبق پروتکل دریافت کند. به‌علاوه توسط این پرسمان، مهاجم این قدرت را دارد تا پاسخ‌های دریافتی از طرف مقابل خود را تغییر داده و حاصل را برای طرف دیگر ارسال کند و او نیز بر طبق پروتکل به او پاسخ دهد.

- **Corrupt (T ,K) query**

مهاجم با ارسال این پرسمان دارای این توانایی می‌شود تا برچسب را به مخاطره[1] بیندازد و به همه مقادیر مخفی و محرمانه‌ای که بر روی آن ذخیره شده است دسترسی پیدا کند. به بیان رسمی، هنگامی‌که مهاجم پرسمان Corrupt (T, K) query را ارسال می‌کند، در مقابل، همه اطلاعات ذخیره‌شده روی برچسب $T \in \text{Tags}$ به اوداده می‌شود که پارامتر K معرف تمام مقادیر مخفی ذخیره‌شده روی برچسب T است که این مقادیر شامل کلیدها، شناسه و سایر پارامترهای امنیتی برچسب T است.

- **تعریف حریم خصوصی غیرقابل ردیابی[2](UPriv)**

مفهوم حریم خصوصی غیرقابل ردیابی (UPriv) با استفاده از بازی g تعریف می‌شود که این بازی بین مهاجم A و مجموعه‌ای از کارت‌خوان و برچسب‌های نمونه انجام می‌شود و دارای سه مرحله است. مهاجم A بازی g را به شرح زیر انجام می‌دهد.

- **مرحله یادگیری[3]**

در این مرحله، ابتدا مهاجم به انتخاب خود، دو برچسب T_0 و T_1 را انتخاب می‌کند تا با آن‌ها وارد تعامل شود. او می‌تواند در این مرحله هر نوع پرسمان Send و Execute را ارسال کند. به‌علاوه، هنگامی‌که انجام بازی g مربوط به ارزیابی مفاهیم عدم ردیابی پیشرو و پسرو باشد، مهاجم می‌تواند علاوه بر پرسمان‌های Send و Execute اقدام به ارسال Corrupt query نیز نماید.

- **مرحله چالش[4]**

پس از مرحله یادگیری، مهاجم برچسب‌های انتخابی خود در مرحله یادگیری، یعنی T_0 و T_1 را به‌عنوان برچسب‌های منتخب خود به چالشگر معرفی می‌کند. سپس چالشگر برچسب $\tau_b \in \{\tau_0, \tau_1\}$ را به‌صورت تصادفی انتخاب و در اختیار مهاجم می‌گذارد. با در اختیار گذاشتن T_b، مهاجم بازهم مجاز است تا پرسمان‌های Send و Execute را به تعداد قابل قبولی ارسال کند که این تعداد بستگی به نوع پروتکل مورد آزمایش دارد.

- **مرحله حدس[5]**

در نهایت مهاجم A، بازی را خاتمه داده و بیت $b' \in \{0,1\}$ را به‌عنوان حدس خود اعلام می‌کند. در واقع او باید اعلام کند که در مرحله چالش با کدام برچسب در ارتباط بوده است. هرچقدر که بیت b' اعلام‌شده از طرف مهاجم با احتمال بیشتری با بیت b یکسان باشد، میزان موفقیت مهاجم بیشتر می‌شود.

میزان موفقیت مهاجم A در این بازی توسط یک تابع مزیت[6] و به‌صورت زیر تعریف می‌شود:

$$\text{Adv}_A^{\text{upriv}}(K) = \left|\text{pr}(b' = b) - \text{pr}(\text{random coin flip})\right|$$

$$= \left| \text{pr}(b' = b) - \frac{1}{2} \right| \quad \text{where} \quad 0 \le \text{Adv}_A^{\text{upriv}}(K) \le \frac{1}{2} \qquad (۲)$$

که pr(random coin flip) نشانگر احتمال آن است که مهاجم بیت b' را به‌صورت تصادفی انتخاب کند و به دلیل توزیع یکنواخت، این احتمال برابر با ۱/۲ است. هر اندازه مزیت به دست آمده برای مهاجم به ۱/۲ نزدیک‌تر باشد، نشان‌دهنده قدرت مهاجم در تمایز قائل شدن بین T_0 و T_1 است و در نتیجه، قابلیت عدم ردیابی پروتکل ضعیف‌تر خواهد بود.

۱.۳. حمله جعل برچسب

در این بخش بدون نیاز به مقدارهای مخفی ID_k و S_j می‌توان برچسب مورد نظر را جعل کرد که مبنای این حمله‌بر اساس فرض $a<b$ می‌باشد که:

$$a \bmod b \equiv a \qquad (۳)$$

پس به همین صورت به ازای $R_i<S_j$ خواهیم داشت:

1. Compromise
2. Untraceable Privacy
3. Learning Phase
4. Challenge Phase
5. Guess Phase
6. Advantage Function

$$RID_i = \left(R_t - R_t mod\ s_j + 1\right)_{(0:47)} \parallel \left(R_t + s_j - R_t mod\ s_j\right)_{(48:95)}$$
$$= (1)_{(0:47)} \parallel (s_j)_{(48:95)} \quad (۴)$$

توجه داریم که با برقراری شرط $R_t<S_j$ در معادله (۴)، مقدار $R_t \bmod S_j$ برابر R_t می‌شود، لذا می‌توان نوشت

$$\left(R_t - R_t mod\ s_j + 1\right)_{(0:47)} = (1)_{(0:47)}$$

از آنجایی‌که R_t مستقل است، می‌توان از این مشاهده برای حمله جعل برچسب استفاده کرد که مراحل انجام این حمله به‌صورت زیر می‌باشد:

۱) مهاجم یک دور از اجرای پروتکل را شنود کرده و مقادیر $R_t \oplus \beta,\ \alpha,\ R_r$ را به دست می‌آورد که در اینجا فرض شده است که $R_t<S_j$؛ پس خواهیم داشت:

$$RID_i = (1)_{(0:47)} \parallel (s_j)_{(48:95)} \quad (۵)$$

۲) در دور بعدی پروتکل، زمانی که کارت‌خوان R'_r و پیام "درخواست" را ارسال می‌کند، مهاجم خود را به‌جای برچسب جا می‌زند و زوج $(R't, \alpha)$ را به کارت‌خوان می‌فرستد، که:

$R'_t = R_t \oplus \beta \oplus R_r \oplus R'_r$ می‌باشد. کارت‌خوان نیز پیام دریافتی را به سرویس‌دهنده نهایی ارسال می‌کند.

۳) سرویس‌دهنده به‌ازای هر زوج (ID_k, S_j) مربوط به برچسب، یک β تولید می‌کند و سپس مقدار $R't$ و RID'_i را از پیام دریافتی به‌صورت زیر به‌دست می‌آورد:

$$R'_t = R_t \oplus \beta \oplus R_r \oplus R'_r \oplus \beta$$
$$RID'_i = \left(R'_t - R'_t mod\ s_j + 1\right)_{(0:47)} \parallel \left(R'_t + s_j - R'_t mod\ s_j\right)_{(48:95)} \quad (۶)$$

۴) سپس سرویس‌دهنده با استفاده از $R't$ و RID'_i محاسبه‌شده از قسمت قبل، و همچنین مقدار α از پیام دریافتی، برقراری رابطه زیر را بررسی می‌کند:

$$\alpha \stackrel{?}{=} h\left(ID_k \oplus R'_t \oplus R'_r \oplus RID'_i\right) \quad (۷)$$

اگر $R'_t<S_j$ پس خواهیم داشت:

$$RID'_i = (1)_{(0:47)} \parallel (s_j)_{(48:95)} = RID_i \quad (۸)$$
$$= h(ID_k \oplus R_t \oplus R_r \oplus RID_i)$$
$$= h\left(ID_k \oplus R_t \oplus R_r \oplus RID_i\right)$$
$$= \alpha \quad (۹)$$

رابطه فوق برقرار می‌باشد. بنابراین، سرویس‌دهنده مهاجم را به عنوان یک برچسب مجاز تایید هویت می‌کند.

توجه داریم که این حمله با دو شرط $R_t<S_j$ و $R'_t<S_j$ انجام شده است، که احتمال برقرار بودن شرط‌ها برابر ۱/۲ است و لذا احتمال انجام حمله برابر ۱/۴ است. به بیان ریاضی می‌توان نوشت:

$$P(\text{موفقیت}) = P\left(R_t < s_j\right) \times P\left(R_t < s_j\right)$$
$$= \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

که تابع P(A)، احتمال رخداد A را نشان می‌دهد.

۲.۳. حمله ردیابی

در این حمله، اشاره‌ای به یکی دیگر از ضعف‌های پروتکل MAPS تحت عنوان حمله ردیابی می‌شود. در ادامه نشان می‌دهیم که مهاجم می‌تواند با استفاده از ضعف‌های موجود در پروتکل، آن را ردیابی می‌کند. بیان ریاضی مسئله به‌صورت زیر قابل بیان است:

مرحله یادگیری: در این مرحله مهاجم جهت شنود، یک برچسب T_0 را انتخاب می‌کند. در ادامه، مهاجم پرسمان Execute (R, T_0, j) را ایجاد می‌کند و پیام‌های $M_1 = (R_{t,j}^{T_0} \oplus \beta_j^{T_0})$ و $M_2 = (R_{t,j}^{T_0} \oplus S_{j+1}^{T_0})$ را که بین برچسب T_0 و سرویس‌دهنده نهایی مبادله شده است را به دست می‌آورد. نماد $X_i^{T_X}$ مقدار X مرتبط با برچسب T_X در اجرای iم را نشان می‌دهد.

مرحله چالش: در این مرحله، مهاجم دو برچسب (T_0, T_1) را انتخاب کرده و جهت تست، پرسمان $Test(T_0, T_1, j+1)$ را به آنها ارسال می‌کند. در ادامه، مهاجم بسته به بیت تصادفی انتخاب‌شده از مجموعه $b \in \{0,1\}$، برچسب T_b را از مجموعه $\{T_0, T_1\}$ انتخاب می‌کند. در ادامه، مهاجم پرسمان Execute(R, T_b, j+1) را ایجاد کرده و پیام‌های $M_3 = (R_{t,j+1}^{T_b} \oplus \beta_{j+1}^{T_b})$ و $M_4 = (R_{t,j+1}^{T_b} \oplus S_{j+2}^{T_b})$ را ازداده‌های مبادله‌شده بین T_b و سرویس‌دهنده نهایی به دست می‌آورد.

مرحله حدس: در نهایت، مهاجم بازی g را متوقف کرده و بیت $b' \in \{0,1\}$ را به عنوان حدسی از b اعلام می‌کند. در عمل، مهاجم روابط زیر را دنبال می‌کند:

$$b' = \begin{cases} 0 & if \ \ [M_1 \oplus M_2]_{[95]} = [M_3 \oplus M_4]_{[95]} \\ 1 & otherwise \end{cases} \quad (۱۰)$$

که $[X]_{95}$ نمایانگر LSB بیت X است. بنابر این:

$$\begin{aligned} \mathrm{Adv}_{\mathrm{A}}^{\mathrm{upriv}}(\mathrm{K}) &= \left|\mathrm{pr}(\mathrm{b}'=\mathrm{b}) - \mathrm{pr}(\text{random coin flip})\right| \\ &= \left|pr(b'=b) - \frac{1}{2}\right| = \left|\frac{3}{4} - \frac{1}{2}\right| = \frac{1}{4} >> \varepsilon \end{aligned} \quad (۱۱)$$

اثبات: مهاجم بعد از به دست آوردن پیام‌های M_1، M_2، M_3، و M_4 با استفاده از شنود، مراحل زیر را دنبال می‌کند:

$$\begin{aligned} M_1 \oplus M_2 &= \left(R_{t,j}^{T_0} \oplus \beta_j^{T_0}\right) \oplus \left(R_{t,j}^{T_0} \oplus S_{j+1}^{T_0}\right) \\ &= \beta_j^{T_0} \oplus S_{j+1}^{T_0} \\ &= \left(S_{j[0:47]}^{T_0} \parallel ID_{[48:95]}^{T_0}\right) \oplus \left(S_{j+1[0:47]}^{T_0} \parallel S_{j+1[48:95]}^{T_0}\right) \end{aligned}$$

$$\Longrightarrow [M_1 \oplus M_2]_{[95]} = ID_{[95]}^{T_0} \oplus S_{j+1[95]}^{T_0} \quad (۱۲)$$

$$\begin{aligned} M_3 \oplus M_4 &= \left(R_{t,j+1}^{T_b} \oplus \beta_{j+1}^{T_b}\right) \oplus \left(R_{t,j+1}^{T_b} \oplus S_{j+2}^{T_b}\right) \\ &= \beta_{j+1}^{T_b} \oplus S_{j+2}^{T_b} \\ &= \left(S_{j+1[0:47]}^{T_b} \parallel ID_{[48:95]}^{T_b}\right) \oplus \left(S_{j+2[0:47]}^{T_0} \parallel S_{j+2[48:95]}^{T_0}\right) \end{aligned}$$

$$\Longrightarrow [M_3 \oplus M_4]_{[95]} = ID_{[95]}^{T_b} \oplus S_{j+2[95]}^{T_b} \quad (۱۳)$$

در [۱۶] نشان داده شده است که کلید S_j مضربی از ۲ نمی‌باشد، لذا شنودگر می‌داند که:

$$S_{j+1[95]}^{T_0} = S_{j+2[95]}^{T_b} = 1 \begin{cases} [M_1 \oplus M_2]_{[95]} = \overline{ID_{[95]}^{T_0}} \\ [M_3 \oplus M_4]_{[95]} = \overline{ID_{[95]}^{T_0}} \end{cases} \quad (۱۴)$$

حال، اگر فرض کنیم دنباله بیت ID^{TX} دارای تابع توزیع احتمال یکنواخت باشد، می‌توان نوشت:

$$\begin{aligned} \mathrm{pr}(\mathrm{b}'=\mathrm{b}) &= \frac{1}{2} \times \mathrm{pr}(\mathrm{b}'=0|\mathrm{b}=0) + \frac{1}{2} \times \mathrm{pr}(\mathrm{b}'=1|\mathrm{b}=1) \\ &= \frac{1}{2} \times \mathrm{pr}\left(\mathrm{ID}_{[95]}^{\mathrm{T_b}} = \mathrm{ID}_{[95]}^{\mathrm{T_0}} | \mathrm{T_b} = \mathrm{T_0}\right) + \frac{1}{2} \times \mathrm{pr}\left(\mathrm{ID}_{[95]}^{\mathrm{T_b}} \neq \mathrm{ID}_{[95]}^{\mathrm{T_0}} | \mathrm{T_b} = \mathrm{T_1}\right) \\ &= \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \end{aligned} \quad (۱۵)$$

۳.۳. حمله ردیابی پسرو

در این بخش، به بررسی ضعف دیگری از پروتکل مورد نظر تحت عنوان حمله ردیابی پسرو پرداخته می‌شود. چونکه مقدار ID در طول اجرای کل پروتکل ثابت است، لذا مهاجم می‌تواند برچسب موردنظر را با احتمال بالا ردیابی کند.

مرحله یادگیری: در این مرحله، مهاجم یک پرسمان $\mathrm{Corrupt}(T_0,K)$ را در دور j از پروتکل ایجاد می‌کند. سپس پارامترهای امنیتی برچسب T_0 یعنی $\left(ID^{T_0}, S_j^{T_0}\right)$ را به دست می‌آورد.

مرحله چالش: در این مرحله، مهاجم یک پرسمان Test $(T_0,T_1,j\text{-}1)$ ارسال کرده و برچسب $T_b \in \{T_0, T_1\}$ را به‌دست می‌آورد. مهاجم یک پرسمان Execute $(R, T_b, j\text{-}1)$ را برای دریافت اطلاعات مبادله شده بین T_0 و کارت‌خوان در دور $(j\text{-}1)$ ارسال می‌کند و مهاجم پیام‌های $M_2' = (R_{t,j-1}^{T_b} \oplus S_j^{T_b})$ و $M_1' = (R_{t,j-1}^{T_b} \oplus \beta_{j-1}^{T_b})$ را به‌دست می‌آورد.

مرحله حدس: در نهایت، مهاجم بازی g را خاتمه می‌دهد و یک $b' \in \{0,1\}$ بیت را به‌عنوان یک حدس نتیجه می‌دهد که به‌صورت زیر می‌باشد:

$$b' = \begin{cases} 0 & if \ \ [M_1' \oplus M_2']_{[48:95]} = [ID^{T_0} \oplus S_j^{T_0}]_{[48:95]} \\ 1 & otherwise \end{cases}$$

$$Adv_A^{uprive}(K) = \left|pr(b'=b) - \frac{1}{2}\right|$$

$$= \left|\left(1 - 2^{-49}\right) - \frac{1}{2}\right| = \frac{1}{2} - 2^{-49} >> \epsilon \quad (۱۶)$$

اثبات:

$$M_1' \oplus M_2' = \left(R_{t,j-1}^{T_b} \oplus \beta_{j-1}^{T_b}\right) \oplus \left(R_{t,j-1}^{T_b} \oplus S_j^{T_b}\right) = \beta_{j-1}^{T_b} \oplus S_j^{T_b}$$

$$= \left(S_{j-1[0:47]}^{T_b} \parallel ID_{[48:95]}^{T_b}\right) \oplus \left(S_{j[0:47]}^{T_b} \parallel S_{j[48:95]}^{T_b}\right)$$

$$[M_1' \oplus M_2']_{([48:95])} = ID_{([48:95])}^{(T_b)} \otimes S_{j[48:95]}^{T_b}$$

$$\mathrm{pr}(\mathrm{b}'=\mathrm{b}) = \frac{1}{2} \times \mathrm{pr}(\mathrm{b}'=0|\mathrm{b}=0) + \frac{1}{2} \times \mathrm{pr}(\mathrm{b}'=1|\mathrm{b}=1)$$

$$= \frac{1}{2} \times \mathrm{pr}\left(\left[\mathrm{ID}^{\mathrm{T_b}} \oplus \mathrm{S}_{\mathrm{j}}^{\mathrm{T_b}}\right]_{[48:95]} = \left[\mathrm{ID}^{\mathrm{T_0}} \oplus \mathrm{S}_{\mathrm{j}}^{\mathrm{T_0}}\right]_{[48:95]} | \mathrm{T_b} = \mathrm{T_0}\right)$$

$$= \frac{1}{2} \times \mathrm{pr}\left(\left[\mathrm{ID}^{\mathrm{T_b}} \oplus \mathrm{S}_{\mathrm{j}}^{\mathrm{T_b}}\right]_{[48:95]} \neq \left[\mathrm{ID}^{\mathrm{T_0}} \oplus \mathrm{S}_{\mathrm{j}}^{\mathrm{T_0}}\right]_{[48:95]} | \mathrm{T_b} = \mathrm{T_1}\right)$$

$$= \frac{1}{2} \times 1 + \frac{1}{2} \times \left(1 - 2^{-48}\right) = 1 - 2^{-49} \quad (۱۷)$$

۴. پروتکل بهبودیافته

همان‌طور که مشاهده شد، از مهم‌ترین نقاط ضعف پروتکل MAPS می‌توان به شیوه به‌روزرسانی کلید S_j اشاره کرد که در یک کانال ناامن فرستاده می‌شود، که همین عامل به دشمن اجازه دسترسی به کلید و یا تغییر آن را می‌دهد. از دیگر نقاط ضعف پروتکل موردنظر می‌توان به وجود پارامتر ثابتی مانند ID و همچنین به ساختار β اشاره کرد که وجود این نقاط ضعف به مهاجم امکان انجام حمله‌های ردیابی و ردیابی پسرو را خواهد داد. در ادامه ما به

بهبود این پروتکل و رفع این نواقص خواهیم پرداخت.

برای جلوگیری از حمله ردیابی، در پروتکل بهبودیافته مقادیر مخفی S_j جدید و مرحله قبل ذخیره می‌شود و همچنین برای جلوگیری از ردیابی پسرو، در پروتکل MAPS پارامتر ID در هر مرحله به‌روزرسانی می‌شود.

پروتکل بهبودیافته نیز دارای دو مرحله: مرحله مقداردهی اولیه و مرحله احراز هویت می‌باشد.

مرحله مقداردهی اولیه: در این مرحله، در سرویس‌دهنده نهایی به ازای هر برچسب پارامترهای (ID_{old} ,ID_{new} ,S_{j-1} ,S_j) ذخیره می‌شود و در هر برچسب نیز پارامترهای (ID_{old} ,S_{j-1}) نیز ذخیره می‌شود. توجه شود که مقادیر (ID_{old} ,S_{j-1}) مربوط به مقادیر مرحله قبل می‌باشند.

مرحله احراز هویت: این مرحله، از فازهای زیر تشکیل شده است.

۱. روند این مرحله مشابه پروتکل MAPS می‌باشد.
۲. روند این مرحله مشابه پروتکل MAPS می‌باشد.
۳. روند این مرحله مشابه پروتکل MAPS می‌باشد.
۴. بعد از دریافت پیام از کارت‌خوان، سرویس‌دهنده نهایی به ازای هر ID_k و S_k پارامتر β را محاسبه کرده و سپس مقدار R_t را از پیام $R_t \oplus \beta$ به‌دست می‌آورد.
۵. سپس مقدار $h(ID_k \oplus R_t \oplus R_r \oplus RID_i)$ را محاسبه کرده و با α دریافتی مقایسه می‌کند و در صورت برابری، احراز هویت برچسب با موفقیت انجام می‌شود و سرویس‌دهنده نهایی پیام $h(\beta \oplus RID_i)$ را محاسبه کرده و به برچسب ارسال می‌کند.
۶. سرویس‌دهنده نهایی بعد از احراز هویت برچسب، مقادیر مخفی خود را به‌صورت زیر به‌روزرسانی می‌کند:

- اگر $ID=ID_{new}$

$$S_{j-1} \leftarrow S_j$$
$$S_j \leftarrow h(S_j || RID_i)$$
$$ID_{old} \leftarrow ID$$
$$ID_{new} \leftarrow h(ID || S_j)$$

- و اگر $ID=ID_{old}$

$$S_j \leftarrow h(S_j || RID_i)$$
$$ID_{new} \leftarrow h(ID || S_j)$$

۷. برچسب نیز بعد از دریافت پیام، $h(\beta \oplus RID_i)$ را محاسبه و با پیام دریافتی مقایسه می‌کند و در صورت برابری، هویت سرویس‌دهنده نهایی تأیید می‌شود و مقادیر مخفی خود را به صورت زیر به‌روزرسانی می‌کند.

$$S_j \leftarrow h(S_j || RID_i)$$
$$ID \leftarrow h(ID || S_j) \qquad (۱۸)$$

۵.تحلیل امنیتی پروتکل بهبودیافته

در پروتکل بهبودیافته، نقاط ضعف ذکرشده برطرف شده است و در ادامه به چگونگی امن بودن این پروتکل بهبودیافته در مقابل حمله‌های جعل برچسب، ردیابی و ردیابی پسرو پرداخته می‌شود.

حمله جعل برچسب: از آنجایی که در پروتکل بهبودیافته، در هر مرحله مقدار S_j و ID تغییر می‌کند بنابراین ساختار RID_i و β نیز تغییر می‌کند. در نتیجه، مهاجم نمی‌تواند حمله جعل برچسب را با موفقیت انجام دهد.

حمله جعل کارت‌خوان: در این حمله، مهاجم سعی می‌کند با استفاده از پیام‌های شنودشده و تغییر آنها، خود را به عنوان یک کارت‌خوان مجاز به برچسب معرفی کند. ولی از آنجایی‌که در پروتکل بهبودیافته، اطلاعات مبادله‌شده توسط تابع یک‌طرفه چکیده‌ساز محافظت می‌شوند و همچنین در هر مرحله از اجرای پروتکل، مقادیر مخفی S_j و ID به‌روزرسانی می‌شوند، بنابراین ساختار RID_i و β نیز تغییر می‌کند. در نتیجه، مهاجم نمی‌تواند کارت‌خوان را جعل کند.

حمله ردیابی: از آنجایی‌که اعمال حمله ردیابی در پروتکل MAPS از ساختار β و پیام $R_t \oplus S_{j+1}$ ناشی می‌شد، لذا در پروتکل بهبودیافته با اعمال تغییراتی در ساختار پیام ارسالی از سرویس‌دهنده به برچسب و همچنین عملیات به‌روزرسانی ID در هر دور از پروتکل مانع از انجام حمله ردیابی خواهد شد.

حمله ردیابی پسرو: در پروتکل بهبودیافته با اعمال عملیات به‌روزرسانی S_j و ID_k و همچنین تغییر در روش به‌روزرسانی مقادیر مخفی، دشمن حتی با در اختیار داشتن ID_k و S_j قادر به انجام حمله ردیابی پسرو نمی‌باشد؛ زیرا در هر دور این مقادیر به‌روزرسانی می‌شوند.

در جدول ۱، تحلیل امنیتی برخی از پروتکل‌های احراز هویت متقابل که در سال‌های اخیر پیشنهاد شده است با پروتکل بهبود یافته پیشنهادشده، مورد مقایسه واقع شده است. مشاهده می‌شود که بر خلاف پروتکل‌های مشابه، پروتکل پیشنهادشده، امنیت و محرمانگی کاربران را تامین می‌کند و در مقابل تهدیدهای متفاوت امن است.

حمله ناهمزمانی: برای انجام حمله ناهمزمانی، مهاجم سعی می‌کند با متوقف کردن روند اجرای پروتکل از به‌روزرسانی کلید در برچسب جلوگیری کند و باعث ناهمزمانی برچسب و سرویس‌دهنده نهایی شود. ولی در پروتکل بهبود یافته، از آنجایی‌که سرویس‌دهنده نهایی به‌ازای هر برچسب، پارامترهای $(ID_{old}, ID_{new}, S_{j-1}, S_j)$ را در خود ذخیره می‌کند، لذا اگر مهاجم حتی روند اجرای پروتکل را متوقف کند و جلوی به‌روزرسانی کلید برچسب را بگیرد، همچنان سرویس‌دهنده نهایی کلید قدیمی برچسب را دارد و لذا ناهمزمان نمی‌شوند.

جدول ۱. تحلیل امنیتی پروتکل‌ها

پروتکل‌ها / حمله‌ها	پروتکل تیان و همکاران [۹]	پروتکل لیو و همکاران [۱۰]	پروتکل کیم [۱۷]	پروتکل بهبود داده شده
حمله جعل	×	✓	×	✓
حمله جعل کارت‌خوان	×	×	✓	✓
حمله ردیابی	×	×	×	✓
حمله ردیابی پسرو	✓	×	×	✓
حمله ناهمزمانی	✓	✓	✓	✓

x: ناامن ✓امن

۶. نتیجه

در این مقاله، به تحلیل امنیت و محرمانگی یک پروتکل احراز هویت متقابل در سامانه‌های RFID پرداخته شد. این پروتکل در سال ۲۰۱۳ توسط کیم ارایه شده است. نشان داده شد که برخلاف ادعای طراح پروتکل، این پروتکل در مقابل حمله‌هایی نظیر جعل برچسب، ردیابی و ردیابی پسرو ضعف دارد، و لذا این پروتکل نمی‌تواند امنیت و محرمانگی کاربر را فراهم کند. در این مقاله، حمله‌های ردیابی و ردیابی پسرو در قالب مدل اوفی- فان انجام شد. در ادامه، جهت رفع ضعف‌های پروتکل کیم، یک پروتکل احراز هویت دوسویه که در واقع نسخه بهبودیافته از پروتکل کیم است، ارایه شد. در نهایت، تحلیل امنیتی پروتکل پیشنهادشده با برخی از پروتکل‌های احراز هویت دوسویه که در سال‌های اخیر پیشنهاد شده است مورد مقایسه قرار گرفت و مشاهده شد که پروتکل پیشنهادشده، در مقایسه با سایر پروتکل‌ها از امنیت و محرمانگی خوبی برخوردار است.

۷. مراجع

[1] R. Weinstein, "RFID: a technical overview and its application to the enterprise," *IT Professionals,* vol. 7, pp. 27-33, 2005.

[2] E.-C. Australia,, "Access control, sensor control, and transponders," Available on: http://www.rfid.com.au/rfid uhf.htm, 2008.

[3] U.S. DoD, "Beginning to see RFID playback," [Online]. Available: www.defenseinddustrydaily.com/logistic/. [Accessed 24 may 2006].

[4] T. Chothia, and V. Smirnov, "A traceability attack against E-passports," in *R. Sion (Ed.): FC 2010, LNCS 6052, pp. 20-34*, 2010.

[5] D. Henrici, "RFID Security and privacy: concepts, protocols and architectures," *Lecture Notes Electrical Engineering, Springer-Verlag Berlin Heidelberg,* vol. 17, 2008.

[6] F. Xiao, Y. Zhou, J. Zhou, H. Zhu, and X. Niu, "Security protocol for RFID system conforming to EPC-C1G2 standard," *Journal of Computers,* vol. 8, no. 3, pp. 605-612, 2013.

[7] M. H. Habibi, M. Gardeshi, and M. Alagheband, "Cryptanalysis of two mutual authentication protocols for low-cost RFID," *International Journal of Distributed and Parallel Systems (IJDPS),* vol. 2, no. 1, pp. 103-114, 2011.

[8] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Recursive linear and differential cryptanalysis of ultralightweight authentication protocols," *IEEE Transactions on Information Forensics and Security,,* vol. 8, no. 7, pp. 1140 - 1151, July 2013.

[9] Y. Tian-tian, and F. Quan-yuan, "A security RFID authentication protocol based on hash function," in *International Symposium on Information Engineering and Electronic Commerce (IEEE)*, 2009.

[10] L. A. Liu, X. Z. Lai, D. S. Yan, Z. Q. Chen, and L. Yang, "Mutual authentication protocol based on hash function of RFID systems," in *International Conference on Machine Learning and Cybernetics, (IEEE)* , 2011.

[11] M. Nouri, Z. Zeinolabedini, B. Abdolmaleki, N. Farhangian, "Analysis of a novel audio hash function based upon stationary wavelet transform," in *Application of Information and Communication Technologies (AICT), 2012 6th International Conference*, 2012 .

[12] M. Nouri, N. Farhangian, K. Baghery, and Z. Zeinolabedini, "Conceptual discrete wavelet transformation speech hashing for content authentication," in *Application of Information and Communication Technologies (AICT), 2012 6th International Conference on*, Tbilisi , 2012.

[13] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic approach to privacy-friendly tag," in *RFID Privacy Workshop 2003*, 2003.

[14] G. Tsudik, "YA-TRAP: Yet another trivial RFID authentication protocol," in *International Conference on Pervasive Computing and Communications*, 2006 .

[15] G. Tsudik, "A family of dunces: trivial RFID identification and authentication protocols," in *Symposium on Privacy-Enhancing Technologies*, 2007.

[16] J.-S.Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Computer Communication,* vol. 34, pp. 391-397, 2011.

[17] H. Kim, "RFID mutual authentication protocol based on synchronized secret," *International Journal of Security and Its Applications,* vol. 7, no. 4, pp. 37-50, 2013.

[18] K. Ouafi, and R.C.-W. Phan, "Traceable privacy of recent provably-secure RFID protocols," in *ACNS 2008, LNCS 5037, pp. 479–489.*, 2008.