یک طرح احراز اصالت امن برای سیستم‌های ارتباطات ماهواره‌ای متحرک

سیده فاطمه افتخاری[1]، کیان کیقباد[2]، علی پاینده[3]

۱. کارشناس ارشد مخابرات رمز، دانشگاه صنعتی مالک‌اشتر

۲. استادیار دانشکده فناوری اطلاعات، دانشگاه صنعتی مالک‌اشتر keyghobad.kiyan@gmail.com

۳. استادیار دانشکده فناوری اطلاعات، دانشگاه صنعتی مالک‌اشتر

تاریخ دریافت: ۹۲/۸/۲۶ تاریخ پذیرش: ۹۳/۴/۳۰

چکیده

احراز اصالت از جمله پارامترهای مهمی است که یک شبکه ماهواره‌ای برای تامین امنیت خود به آن نیاز دارد. در همین راستا، در سال‌های اخیر مقالات متعددی برای تامین این نیاز ارائه شده‌اند. در این مقاله یک طرح احراز اصالت امن و کارآمد برای سیستم‌های ارتباطات ماهواره‌ای متحرک ارائه شده است که علاوه بر تامین امنیت‌های مدنظر در مقالات، دربرابر حمله ممانعت از سرویس نیز امن است؛ به این معنی که در مرحله به‌روزرسانی هویت موقتی کاربر، اگر ارتباط بین کاربر با شبکه مرکزی به دلایلی قطع شود امکان برقراری مجدد نشست احراز اصالت وجود دارد.دراین طرح از محاسبات بسیار پیچیده مانند رمزنگاری کلید عمومی یا رمزنگاری کلید خصوصی استفاده نشده استو طرح تنها مبتنی بر تابع چکیده‌ساز و عملیات XOR است و در مقایسه با طرح‌های دیگر از هزینه محاسباتی کمتری برخوردار است. علاوه بر این، این طرح در برابر حملاتی مانند جعل هویت، الحاق، تکرار، سرقت جدول NCC و دزدیدن کارت هوشمند امن است.

کلید واژه

ارتباطات ماهواره‌ای متحرک،احراز اصالت، حمله ممانعت از سرویس، تابع چکیده‌ساز.

مقدمه

امروزه شبکه‌های ارتباطات ماهواره‌ای متحرک[1] با پیشرفت تکنولوژی ارتباطات بسیار مورد توجه قرارگرفته‌اند. این شبکه‌ها امکان اتصال بین شبکه‌های زمینی دور، سرویس‌های اینترنت، کاربردهای چندرسانه‌ای متقابل و انتقال نرخ بالای داده را فراهم می‌کنند. این شبکه‌ها ترکیبی از ماهواره، گذرگاه‌ها[2]، کاربران متحرک و مرکز کنترل شبکه[3](NCC) هستند. ماهواره قسمت فضایی این شبکه است که اتصال بین کاربران متحرک و گذرگاه‌ها را فراهم می‌کند. گذرگاه‌ها قسمتی از شبکه هستند که روی زمین مستقر شده و دسترسی به بخش فضایی را فراهم می‌کنند و نیز رابطی بین شبکه‌های زمینی هستند. کاربران متحرک از طریق ماهواره به گذرگاه‌ها متصل می‌شوند. NCC برای هماهنگ‌کردن دسترسی به منابع ماهواره‌ای و انجام عملیات منطقی برای مدیریت و کنترل، به سیستم مدیریت اطلاعات کاربر متصل می‌شود[۱].

در شکل (۱)، شبکه ارتباطات ماهواره‌ای متحرک نشان داده شده است.

شبکه‌های ارتباطات ماهواره‌ای متحرک در کنار کاربردهای فراوان، چالش‌های امنیتی نیز دارند. به علت ماهیت پخش بی‌سیم در ماهواره‌ها، استراق سمع برای مهاجمان در این شبکه‌ها خیلی راحت‌تر از شبکه‌های متحرک یا ثابت زمینی است[۱]. به دلیل آنکه توانایی ذخیره‌سازی و پردازش در ماهواره محدود است، منابع محاسباتی در شبکه ماهواره‌ای باید به صورت بهینه مورد استفاده قرارگیرند[۲] و نیز به دلیل متحرک بودن ماهواره و کاربر در شبکه‌های ماهواره‌ای متحرک، مدت زمانی که کاربر در دید ماهواره قرار دارد و می‌تواند با آن ارتباط برقرار کند محدود بوده و در نتیجه، طرح‌های امنیتی که برای این شبکه‌ها ارائه می‌شوند باید از نظر هزینه محاسباتی و ارتباطی بهینه باشند.

1.Mobile Satellite Communication Systems
2.Gateway
3.Network Control Centre (NCC)

احراز اصالت در شبکه‌های ماهواره‌ای می‌تواند با استفاده از پروتکل‌های احراز اصالت مبتنی بر رمزنگاری متقارن یا نامتقارن انجام شود که هردو یک کلید نشست را برپا و مبادله می‌کنند. برای شبکه‌های ماهواره‌ای پروتکل‌های امنیتی نقطه-به-نقطه[۴] زیادی پیشنهاد شده است که اطلاعات محرمانه را به منظور احراز اصالت تسهیم می‌کنند. این اطلاعات محرمانه برای اثبات هویت در یک نشست پروتکل استفاده می‌شوند[۳].

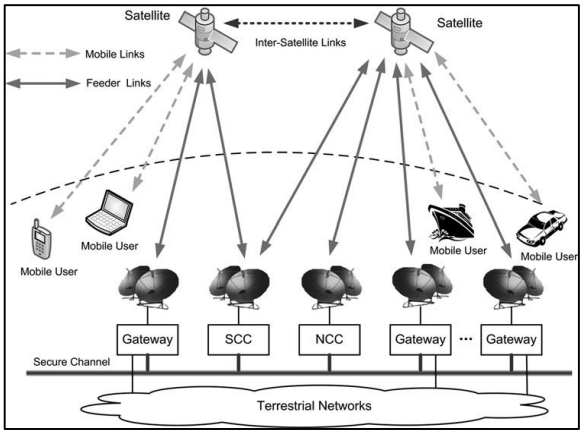
یک پروتکل احرازاصالت مناسب برای شبکه‌های ماهواره‌ای متحرک باید ویژگی‌های زیر را داشته باشد:

احراز اصالت دو طرفه[۵] : منظور این است که هر یک از شرکت‌کنندگان در سیستم ارتباطات ماهواره‌ای بتوانند یکدیگر را قبل از توافق در مورد کلید نشست مشترک احراز اصالت کنند[۴].

گمنامی[۶] : برای حفظ حریم و امنیت کاربر، هویت اصلی کاربران باید مخفی بماند تا در صورتی که مهاجم خود را به جای NCC قرار داد، نتواند کاربران را از هم تشخیص دهد.

محرمانگی[۷] : در ارتباطات محرمانه، پیام‌های ردوبدل شده بین دو طرف ارتباط به وسیله یک کلید محرمانه رمز می‌شود تا مهاجم نتواند به محتوای پیام‌ها پی ببرد.

نشست مستقل[۸] : در صورتی که نشست‌ها از هم مستقل نباشند، با شنود و حمله به یک نشست توسط مهاجم، بقیه نشست‌ها هم ناامن می‌شوند، بنابراین باید کلید نشست استفاده شده در پروتکل در هر نشست به‌روز شود و مستقل از کلید نشست قبلی باشد.



شکل ۱. شبکه ارتباطات ماهواره‌ای متحرک[۱]

هزینه محاسباتی پایین: یک پروتکل برای آنکه قابل پیاده‌سازی در شبکه‌های ماهواره‌ای باشد باید تا حد امکان امن و دارای هزینه محاسباتی پایین باشد.

4. Peer-To-Peer
5. Mutual Authentication
6. Anonymity
7. Confidentiality
8. Session Independence

کارهای انجام شده

در سال ۲۰۰۳، آقای هوآنگ و همکارانش[۵] یک پروتکل احراز اصالت مبتنی بر رمزنگاری کلید سرّی[۹] برای سیستم‌های ارتباطات ماهواره‌ای متحرک ارائه دادند. پروتکل آنها با وجود کاهش پیچیدگی محاسباتی با استفاده از رمزنگاری کلید سرّی به جای رمزنگاری کلید عمومی، دارای ضعف‌هایی نیز بود:

۱- در این پروتکل به دلیل آنکه کلید نشست بعدی به وسیله کلید نشست جاری حفاظت می‌شود، حمله کلید معلوم[۱۰] امکان‌پذیر است به طوری که اگر یک بار کلید نشست به دلایلی به خطر بیفتد، کلیدهای بعدی می‌توانند به دست آیند و دیگر ارتباطات امن نخواهد بود. ۲- در این پروتکل به دلیل آنکه کلیدهای سرّی که اطلاعات حساسی هستند، با هر کاربر متحرک به اشتراک گذاشته و در جدول بررسی سرور ذخیره می‌شوند، در صورت مورد حمله قرار گرفتن سرور، این پروتکل دیگر امن نخواهد بود. بنابراین پروتکل در برابر حمله تصدیق‌کننده مسروقه[۱۱] آسیب‌پذیر است. در نتیجه، مدیریت کلید سرّی در این پروتکل یک وظیفه حساس و مهم است که باالطبع هزینه سنگینی را به سیستم وارد می‌کند.

در سال ۲۰۰۵ آقای چانگ و همکارانش[۶] یک طرح احراز اصالت دو طرفه برای سیستم‌های ارتباطات ماهواره‌ای متحرک پیشنهاد کردند. در طرح پیشنهادی آنها، از عملیات محاسباتی XOR و تابع چکیده‌ساز استفاده می‌شود و NCC نیاز به انتخاب یک کلید سرّی جدید و یک هویت موقتی برای کاربر در هر نشست احراز اصالت ندارد. در این طرح با استفاده از مبادله کلید دیفی-هلمن برای تولید یک کلید دور جدید، می‌توان به امنیت پیشرو کامل[۱۲] دست پیدا کرد.در هر حال، این پروتکل دارای ضعف‌هایی است: ۱- اگر یک شنودکننده مقدار چکیده‌شده را با به خطر انداختن NCC به دست آورد، می‌تواند با قطع پیام درخواست ارسالی از طرف کاربر متحرک، از احراز اصالت استفاده شده در نشست جاری بهره‌برداری کند. در چنین روشی، یک شنودکننده می‌تواند هویت کاربر یا NCC را جعل کند. ۲- اگر مقدار چکیده شده زنجیره تماما استفاده شود، یک مرحله به‌روزرسانی کلید اضافی با محاسبات نمایی زمان‌بر نیاز است. در نتیجه، پروتکل به حجم زیادی از پهنای باند ارتباطی و منابع محاسباتی نیاز دارد. ۳- به دلیل آنکه در طرح آنها هویت موقتی کاربر در هر نشست به‌روز نمی‌شود، موقعیت کاربر به راحتی قابل ردیابی خواهد بود.

در سال ۲۰۰۹ آقای چن و همکارانش [۷] یک سازوکار احراز اصالت برای سیستم‌های ارتباطات ماهواره‌ای متحرک پیشنهاد کردند. از این پس، آن را با عنوان پروتکل CLC ارجاع

9. Secret Key Cryptography (SKC)
10. Known Key Attack
11. Stolen-Verifier Attack
12. Perfect Forward Security

می‌دهیم. هدف آنها فراهم کردن احراز اصالت بین کاربر متحرک و NCC درون یک سیستم مخابرات ماهواره‌ای LEO مانند گلوبال استار[13] و ایریدیوم[14] بود.

در پروتکل CLC، NCC یک رمزنگاری مبتنی بر لگاریتم گسسته را آغاز می‌کند و جفت کلید عمومی و خصوصی خود را در مرحله مقدماتی می‌سازد. در این پروتکل، اطلاعات مورد نیاز کاربر توسط NCC در کارت هوشمند ذخیره و برای کاربر ارسال می‌شود. پروتکل CLC دارای ضعف‌هایی است: ۱- این پروتکل در برابر حمله جعل در صورت دزدیده شدن کارت هوشمند امن نیست؛ به دلیل آنکه در مرحله احراز اصالت، وقتی کاربر کارت هوشمند خود را به دستگاه کارتخوان وارد می‌کند، دستگاه به طور خودکار کلید نشست سرّی و پیام احراز اصالت را بدون نیاز به داده‌های ورودی از طرف کاربر محاسبه می‌کند، در نتیجه مهاجم تنها با داشتن کارت هوشمند کاربر قانونی می‌تواند به شبکه دسترسی پیدا کند. ۲- اگر مهاجم به طریقی بتواند پارامترهای ذخیره شده در جدول NCC را به دست آورد، می‌تواند به وسیله الگوریتم اقلیدسی استفاده شده در پروتکل، به کلید سرّی کاربر و کلید خصوصی NCC دست‌یابد. ۳- این طرح در برابر حمله ممانعت از سرویس[15] آسیب‌پذیر است به طوری که اگر هنگام به‌روزرسانی هویت موقتی توسط NCC، ارتباط بین NCC و کاربر قطع شود و کاربر هویت موقتی خود را به روز نکند دیگر به عنوان یک کاربر معتبر شناخته نخواهد شد نمی‌تواند با شبکه ارتباط برقرار کند.

در سال ۲۰۱۱ آقای یون و همکارانش [8] برای برطرف کردن ضعف‌های طرح CLC، یک طرح احراز اصالت برای شبکه‌های متحرک ماهواره‌ای ارائه دادند. طرح آنها مبتنی بر تابع چکیده‌ساز است که خود منجر به کاهش پیچیدگی محاسباتی در شبکه می‌شود. در این طرح به دلیل آنکه اطلاعات حساسی در جدول بررسی NCC ذخیره نمی‌شود و هویت کاربر در آن به صورت رمزشده ذخیره می‌شود، در مقابل حمله تصدیق‌کننده مسروقه و حمله الحاق[16] امن است. این طرح در برابر حمله ممانعت از سرویس آسیب‌پذیر است.

در سال ۲۰۱۱ آقای لی و همکارانش[9] برای برطرف کردن برخی ضعف‌های پروتکل CLC یک پروتکل احراز اصالت را مبتنی بر تابع چکیده‌ساز و XOR برای شبکه‌های متحرک ماهواره‌ای ارائه کردند. طرح آنها در کنار ویژگی‌های مثبت داری ضعف‌هایی است: ۱- در برابر حمله ممانعت از سرویس آسیب‌پذیر است. ۲- مهاجم در صورت دسترسی به هویت موقتی کاربر، به راحتی می‌تواند به وسیله حمله تکرار هویت کاربر را جعل و به شبکه دسترسی پیدا کند.

در سال ۲۰۱۲ آقای چانگ و همکارانش [4] یک پروتکل احراز اصالت و توافق کلید برای شبکه‌های ماهواره‌ای متحرک ارائه کردند. این طرح در جهت رفع ضعف‌های طرح CLC، از جمله آسیب‌پذیری در برابر دزدیده شدن کارت هوشمند، ارائه شد. در این طرح، هویت دائمی کاربر و نیز کلمه عبور او برای ورود به سیستم نیاز است.

این طرح دارای سه مرحله مقداردهی اولیه، ثبت نام و احراز اصالت است. در مرحله مقداردهی اولیه، ابتدا NCC یک عدد اول بزرگ p، یک مولد g گروه ضربی z_p^* با مرتبه q و یک کلید خصوصی طویل x در z_p^* را انتخاب و کلید عمومی $(r=g^x \bmod pr)$ محاسبه می‌کند.

در مرحله ثبت نام، کاربر درخواست ثبت شدن در NCC را می‌دهد تا برای احراز اصالت در مواقع مورد نیاز به عنوان یک کاربر قانونی شناخته شده و اجازه ورود به شبکه را پیدا کند. در این مرحله، کاربر هویت دائمی (U_{ID}) و کلمه عبور (PW) خود را از طریق یک کانال امن برای NCC ارسال می‌کند. NCC پس از دریافت آنها، یک هویت موقت (T_{ID}) برای کاربر تولید می‌کند و با انتخاب عدد تصادفی k، $1 \le k < q$، محاسبات زیر را انجام می‌دهد:

$$S = h(U_{ID})x + kr^{-1} \bmod q \quad (۱)$$

$$L = h(U_{ID}, k) \oplus PW \quad (۲)$$

که در آنها، h(.) تابع چکیده‌ساز و $\oplus$ عملیات XOR است. NCC سپس T_{ID} و L را در کارت هوشمند کاربر ذخیره و آن را از طریق یک کانال امن برای کاربر ارسال می‌کند و T_{ID}، U_{ID}، S و r را در جدول بررسی خود ذخیره می‌کند.

در مرحله احراز اصالت کاربر برای آنکه تصدیق شود، a و b را به صورت زیر محاسبه و آنها را به همراه T_{ID} برای NCC ارسال می‌کند:

$$a = h(L \oplus PW, T_{ID}) \quad (۳)$$

$$b = L \oplus PW \oplus T_{IDNew} \quad (۴)$$

T_{IDNew} هویت موقتی به‌روز شده‌ای است که کاربر برای خود انتخاب می‌کند. NCC پس از دریافت اطلاعات کاربر، با توجه به T_{ID} دریافتی، r، S و U_{ID} متناظر کاربر را از جدول بررسی خود پیدا می‌کند و از معادله (۱)، k را به دست می‌آورد. سپس به کمک اطلاعات استخراج شده، a' را به صورت زیر محاسبه می‌کند.

$$a' = h(h(U_{ID}, k), T_{ID}) \quad (۵)$$

اگر a' با a دریافتی برابر باشد، کاربر تصدیق و در غیر این صورت، نشست توسط NCC قطع می‌شود. پس از آنکه NCC کاربر

13.Globarstar
14. Iridium
15. Denial Of Service Attack
16. Insertion Attack

را به عنوان یک کاربر قانونی شناخت، هویت موقتی جدید (T_{IDNew}) را به صورت زیر به دست می‌آورد.

$$T_{IDNew}' = b' \oplus h(U_{ID}, k) \quad (۶)$$

سپس T_{IDNew} جدید را جایگزین T_{ID} می‌کند. برای آنکه این احراز اصالت دوطرفه باشد و NCC هم توسط کاربر تصدیق شود، NCC به محاسبه c، به صورت زیر پرداخته و آن را برای کاربر ارسال می‌کند. کلید نشستی (sk) که NCC برای رمز کردن پیام‌هایش از آن استفاده می‌کند نیز در زیر آمده است:

$$c = h(h(U_{ID}, k), T_{IDNew}) \quad (۷)$$

$$sk = h(h(U_{ID}, k), T_{ID}, T_{IDNew}) \quad (۸)$$

کاربر پس از دریافت اطلاعات ارسالی از طرف NCC، به محاسبه c' به صورت زیر می‌پردازد و در صورتی که c' با c ارسالی برابر باشد NCC را تصدیق می‌کند. کلید نشستی که کاربر برای رمز کردن پیام‌هایش از آن استفاده می‌کند (sk') نیز در زیر آمده است:

$$c' = h(L \oplus PW, T_{IDNew}) \quad (۹)$$

$$sk' = h(L \oplus PW, T_{ID}, T_{IDNew}) \quad (۱۰)$$

اما با این وجود، این طرح دارای ضعف‌هایی نیز هست. در این طرح، در جدول NCC هویت دائمی کاربر بدون هیچ رمزشدنی ذخیره می‌شود. در مرحله احراز اصالت، به دلیل آنکه کلید با هویت موقتی XOR می‌شود و از آنجا که b نیز برای NCC ارسال می‌شود و نیز قابل شنود است، مهاجم با یکبار شنود و ذخیره b و شنود دوباره در مرحله بعدی نشست و به دست آوردن هویت موقتی کاربر، به راحتی می‌تواند کلید را به دست آورد و حمله جعل هویت را انجام دهد. علاوه بر این، در این پروتکل و پروتکل‌های [۵،۶،۷،۸،۹] سازوکار به‌روزکردن به صورت یک عمل خودکار در نظر گرفته شده و در آن‌ها احتمال تداخل یا از دست رفتن پیام در نظر گرفته نمی‌شود. به طوری که اگر هر حادثه ناخواسته‌ای اتفاق بیفتد و فرآیند احراز اصالت را قطع کند، پروتکل به یک حالت تعریف نشده می‌رسد و کاربر و NCC روی T_{ID} ناهمزمان می‌شوند.

در این مقاله علاوه بر برطرف‌کردن ضعف‌های موجود در روش [۴]، روند به‌روزرسانی به گونه‌ای طراحی شده است که برخلاف طرح‌های گذشته، پروتکل در برابر حمله ممانعت از سرویس و قطع ارتباط مقاوم باشد.

روش پیشنهادی

در این قسمت یک طرح احراز اصالت امن و کارآمد برای شبکه‌های ماهواره‌ای متحرک ارائه می‌شود. سه شرکت‌کننده در این طرح در نظر گرفته شده‌اند: کاربر متحرک، ماهواره و NCC. این طرح شامل دو مرحله: ثبت نام و احراز اصالت است.

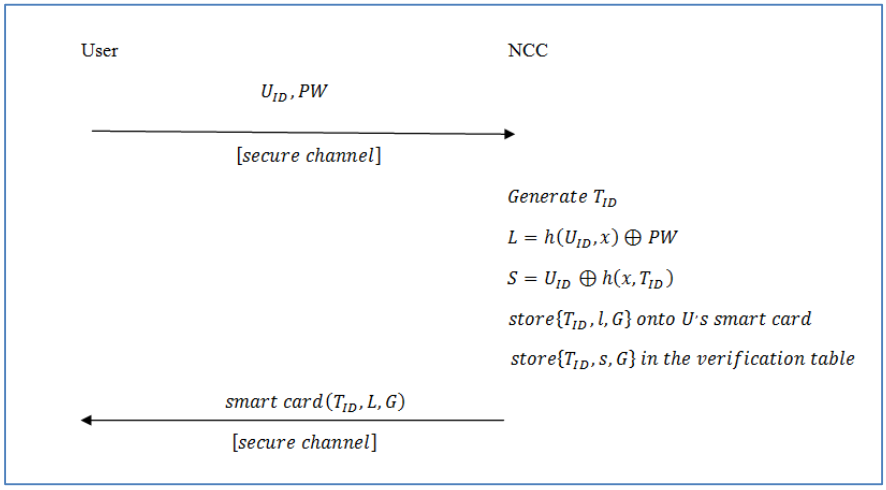
مرحله ثبت نام

در مرحله ثبت نام، کاربرانی که می‌خواهند به NCC متصل شوند باید ابتدا به عنوان یک کاربر قانونی ثبت شوند تا برای اتصال به شبکه در نشست‌های بعدی احراز اصالت شوند. در مرحله ثبت نام در این طرح، ابتدا کاربر هویت دائمی (U_{ID}) و کلمه عبور (PW) خود را از طریق یک کانال امن، برای NCC ارسال می‌کند. NCC پس از دریافت آنها، یک هویت موقتی (T_{ID}) را برای کاربر تعیین می‌کند و سپس به محاسبه L ,S به صورت زیر می‌پردازد:

$$L = h(U_{ID}, x) \oplus PW \quad (۱۱)$$

$$S = U_{ID} \oplus h(x, T_{ID}) \quad (۱۲)$$

x، کلید خصوصی NCC است. سپس NCC، T_{ID}، S را به همراه G که یک عدد است، در جدول خود و T_{ID}، L و G را در کارت هوشمند کاربر ذخیره و آن را برای کاربر ارسال می‌کند. مرحله ثبت نام این طرح در شکل (۲) نشان داده شده است.



شکل ۲.مرحله ثبت نام طرح پیشنهادی

مرحله احراز اصالت

کاربر برای هر بار اتصال به شبکه یا ارتباط با بقیه کاربران ابتدا باید احراز اصالت شود. در نتیجه برای این منظور، کارت هوشمند خود را به دستگاه کارتخوان وارد و هویت دائمی و کلمه عبور خود را به عنوان اطلاعات ورودی و سرّی وارد می‌کند تا دستگاه محاسبات زیر را انجام دهد:

$$a = h(L \oplus PW) \oplus r \quad (۱۳)$$

$$b = h(U_{ID}, T_{ID}, r) \quad (۱۴)$$

r یک عدد تصادفی است که دستگاه خود آن را انتخاب می‌کند. کاربر a، b و T_{ID} را برای ماهواره می‌فرستد. ماهواره نیز داده‌های دریافتی را به همراه هویت خود (LEO_{ID}) به سمت NCC ارسال می‌کند. NCC پس از دریافت اطلاعات، ابتدا هویت ماهواره را مورد بررسی قرار می‌دهد. پس از تایید هویت ماهواره، NCC به کمک T_{ID} دریافتی از جدول خود S مربوط به کاربر مورد نظر را پیدا می‌کند و با انجام محاسبات زیر، به U'_{ID} دست می‌یابد.

$$U'_{ID} = S \oplus h(x, T_{ID}) \quad (۱۵)$$

NCC پس از به دست آوردن U'_{ID}، برای بررسی اعتبار کاربر محاسبات زیر را انجام می‌دهد:

$$r' = a \oplus h(hU'_{ID}, x) \quad (۱۶)$$

$$b' = h(U'_{ID}, T_{ID}, r') \quad (۱۷)$$

سپس اگر b ارسالی با 'b برابر بود، کاربر را تصدیق و در غیر این صورت، نشست را قطع می‌کند.پس از تصدیق کاربر، برای آنکه NCC نیز تصدیق شود، NCC، هویت موقتی کاربر را به‌روز می‌کند. (T_{IDNew}) و C و d را به صورت زیر محاسبه و آنها را برای کاربر از طریق ماهواره ارسال می‌کند. برای امنیت در برابر قطع ارتباط، NCC علاوه بر ذخیره هویت موقتی جدید در جدول خود، T_{ID}را تا برقراری نشست بعدی پاک نمی‌کند.

$$C = h(T_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew} \quad (۱۸)$$

$$d = h(T_{IDNew}) \quad (۱۹)$$

ماهواره پس از دریافت این اطلاعات از NCC، آنها را به همراه LEO_{ID} به سمت کاربر ارسال می‌کند. کاربر پس از دریافت اطلاعات و بررسی صحت هویت ماهواره، محاسبات زیر را برای بررسی اعتبار NCC انجام می‌دهد:

$$C = h(T_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew} \quad (۲۰)$$

$$d' = h(T'_{IDNew}) \quad (۲۱)$$

سپس، در صورتی که d ارسالی با 'd برابر نباشد، نشست را قطع و در غیر این صورت، هویت NCC را تصدیق و در کارت خود، T'_{IDNew} را جایگزین T_{ID} می‌کند.

اگر به هر دلیلی اطلاعات ارسالی NCC به کاربر نرسد، کاربر از هویت موقتی به‌روز شده اطلاع پیدا نکرده و برای برقراری ارتباطات بعدی از T_{ID} استفاده می‌کند. در این حالت NCC با دریافت T_{ID} متوجه می‌شود که کاربر T_{IDNew} را دریافت نکرده و مجددا C و D را به کمک ماهواره برای کاربر ارسال می‌کند:

$$D = h(T_{IDNew}) \oplus G \quad (۲۲)$$

$$C = h(T_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew} \quad (۲۳)$$

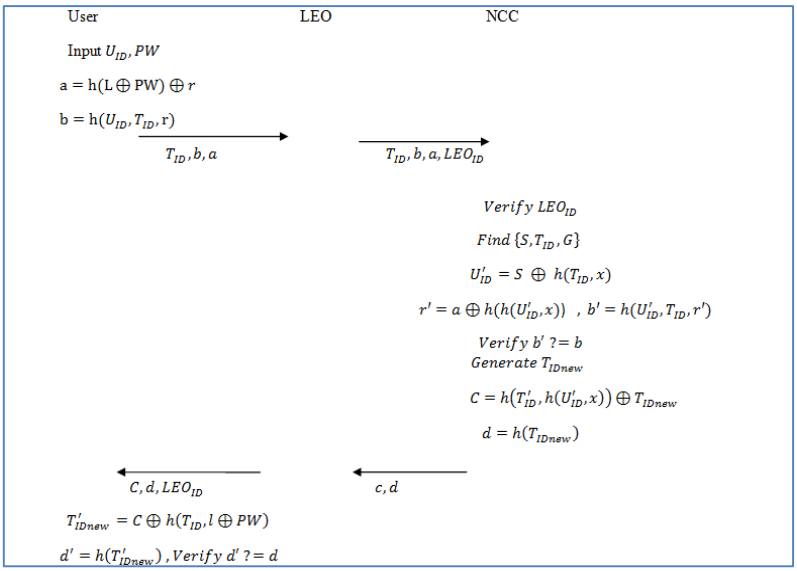
کاربر با دریافت C و به دست آوردن T_{IDNew} به محاسبه D پرداخته و G را از آن به دست می‌آورد، کاربر با دریافت G متوجه می‌شود که باید هویت موقتی خود را به‌روز و مرحله احراز اصالت را مجددا انجام دهد. این روند موجب می‌شود که پروتکل در برابر حمله ممانعت از سرویس امن باشد.

در این طرح، NCC و کاربر برای حفظ محرمانگی پیام‌های خود از یک کلید نشست استفاده می‌کنند که آنها را به ترتیب به صورت زیر محاسبه می‌کنند:

$$key = h(h(U_{ID}, x), r) \quad (۲۴)$$

$$key = h(L \oplus PW, r) \quad (۲۵)$$

شکل (۳)، مرحله احراز اصالت طرح پیشنهادی را نشان می‌دهد.



شکل ۳. مرحله احراز اصالت طرح پیشنهادی

بررسی روش پیشنهادی

بررسی ویژگی‌های مورد نیاز

احراز اصالت دوطرفه: در این طرح هر دو طرف ارتباط یعنی کاربر و NCC یکدیگر را احراز اصالت می‌کنند. کاربر برای آنکه تصدیق شود، $a = h(L \oplus PW) \oplus r$ و $b = h(U_{ID}, T_{ID}, r)$ را برای NCC ارسال و NCC با بررسی اطلاعات دریافتی از کاربر، اصالت او را بررسی می‌کند و درصورت تایید اصالت کاربر، یک هویت موقتی جدید برای او تولید و $C = h(T'_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew}$ و $d = h(T_{IDNew})$ را برای کاربر ارسال می‌کند، کاربر با داشتن $T_{IDNew}, L \oplus PW$ را از عبارت C به دست می‌آورد و به محاسبه می‌پردازد. سپس 'd را با d ارسالی از طرف NCC مقایسه می‌کند، اگر با هم برابر باشند NCC تصدیق می‌شود.

گمنامی: در طرح پیشنهادی، گمنامی کاربر تامین شده است زیرا هویت اصلی کاربر در کارت هوشمند او و جدول NCC ذخیره نمی‌شود و نیز برای برقراری نشست و احراز اصالت به ارسال هویت اصلی کاربر نیازی نیست و از هویت موقتی برای این امر استفاده می‌شود که آن هم در هر نشست به‌روز می‌شود. در نتیجه مهاجم با شنود داده‌های ارسالی بین کاربر و NCC نمی‌تواند به هویت دائمی کاربر پی ببرد.

محرمانگی: در این طرح، کلید نشست $h(h(U_{ID}, X), r) = h(L \oplus PW, r)$ برای رمزکردن پیام‌های بین کاربر و NCC ارائه شده است که در هر نشست به‌روز می‌شود.

نشست مستقل: در این طرح به دلیل آنکه a و b در طرف کاربر و C در طرف NCC در هر نشست به‌روز می‌شوند، هر نشست احراز اصالت مستقل از نشست قبلی است و نیز در این طرح کلید نشست هر بار به‌روز می‌شود.

محاسبات سبک: در این طرح تنها از تابع چکیده‌ساز و عملیات XOR در طی احراز اصالت استفاده می‌شود که چون عملیات سبکی هستند بار محاسباتی زیادی را به سیستم تحمیل نمی‌کنند. در جدول ۱، عملکرد روش پیشنهادی با روش‌های دیگر مقایسه شده است.

جدول ۱. مقایسه ویژگی‌های روش پیشنهادی با سایر روش‌ها

پروتکل‌های موجود	ویژگی‌های مورد نیاز پروتکل احراز اصالت				
	احراز اصالت متقابل	گمنامی	محرمانگی	نشست مستقل	محاسبات سبک
روش پیشنهادی	+	+	+	+	+
Chang [۴]	+	+	+	+	+
Yoon [۸]	+	+	+	+	+
Lee [۹]	+	+	+	+	+
Chen [۷]	+	+	+	+	-
Chang [6]	+	+	-	+	-
Hwang [۵]	+	+	-	-	-

تحلیل امنیتی

* **حمله تصدیق‌کننده مسروقه:** در گروهی از طرح‌های احراز اصالت، شبکه دارای جدولی به نام جدول کلمه عبور است که حاوی داده‌های درستی‌یاب[17] مربوط به کاربران است(معمولا تابعی از کلمه عبور است). اگر اطلاعات حساس و مهم بدون رمزشدن در این جدول ذخیره شوند، مهاجم در صورت دسترسی به این جدول به راحتی می‌تواند به این اطلاعات مهم دست پیدا کرده و امنیت پروتکل و در نتیجه سیستم را به خطر بیندازد. برای مقابله با این نوع حمله، باید اطلاعات مهم و حساس در جدول رمز شوند تا به راحتی قابل دسترسی نباشند.

در طرح پیشنهادی، NCC در جدول خود $\{S = U_{ID} \oplus h(x, T_{ID}), T_{ID}, G\}$ را ذخیره می‌کند. اگر مهاجم به طریقی بتواند به این جدول دسترسی پیدا کند، نمی‌تواند اطلاعات مهمی راجع به کاربر به دست آورد و حداکثر اطلاعاتی که می‌تواند کسب کند: ۱- به دست آوردن G است که یک عدد بوده و در پیام احراز اصالت کاربر، $\{a = h(L \oplus PW) \oplus r, T_{ID}, b = h(U_{ID}, T_{ID}, r)\}$ نقشی ندارد تا به کمک آن بتوان هویت کاربر را جعل کرد. ۲- به دست آوردن T_{ID} هم کمکی به مهاجم نخواهد کرد زیرا T_{ID} یک پیام آشکار برای همگان است که کاربر آن را بدون پوشش امنیتی برای NCC ارسال می‌کند و برای جعل هویت کاربر به دانستن L و PW و U_{ID} نیاز است. ۳- بدست آوردن $S = U_{ID} \oplus h(x, T_{ID})$ از این جهت کمکی به مهاجم نخواهد کرد که مهاجم تنها با دانستن S و T_{ID} نمی‌تواند هویت دائمی کاربر یا کلید x را از آن به دست آورد، بنابراین طرح پیشنهادی در مقابل حمله تصدیق‌کننده مسروقه امن است.

* **حمله الحاق:** در حمله الحاق مهاجم با دسترسی به جدول شبکه و اضافه‌کردن اطلاعات یک کاربر جعلی به جدول، خود را به عنوان یک کاربر قانونی ثبت و در نتیجه به شبکه وصل می‌شود. برای جلوگیری از این حمله باید اطلاعات مهم در جدول به وسیله رمزکردن محافظت شوند.

در طرح پیشنهادی، بر فرض اگر یک مهاجم بتواند به جدول NCC دست پیدا کند و بخواهد با واردکردن اطلاعات یک کاربر جعلی به شبکه وصل شود، باید بتواند عبارت $S = U_{ID} \oplus h(x, T_{ID})$ را بسازد که این امر نیازمند دانستن کلید سرّی NCC یعنی است. در نتیجه این طرح در برابر حمله الحاق مقاوم است.

* **حمله جعل هویت**[18] : در حمله جعل هویت کاربر، مهاجم با جعل یک پیام احراز اصالت قانونی، خود را به عنوان کاربر قانونی به شبکه معرفی کرده و سعی می‌کند از این طریق به شبکه دسترسی پیدا کند. در حمله جعل هویت شبکه، مهاجم با جعل یک پیام احراز اصالت شبکه خود را به عنوان شبکه برای کاربر جا می‌زند و به این طریق سعی در برقراری ارتباط با کاربر می‌کند.

برای حمله جعل هویت کاربر در این طرح، مهاجم باید بتواند با جعل یک درخواست احراز اصالت $\{a = h(L \oplus PW) \oplus r, T_{ID}, b = h(U_{ID}, T_{ID}, r)\}$ یک کاربر قانونی را جعل کند اما این کار امکان‌پذیر نیست زیرا برای جعل $a = h(L \oplus PW) \oplus r$ باید از L و PW مطلع باشد و برای جعل $b = h(U_{ID}, T_{ID}, r)$

17. Verifier

18. Impersonation Attack

نیز نیاز به دانستن هویت دائمی کاربر (U_{ID}) دارد و به دلیل آنکه از PW و هویت کاربر(U_{ID}) تنها خود او مطلع است، در نتیجه مهاجم قادر به جعل پیام‌های b و a نخواهد بود. از طرفی برای جعل NCC نیز، مهاجم باید بتواند $C = h(T'_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew}$ را محاسبه کند که محاسبه این عبارت نیاز به دانستن هویت دائمی کاربر U_{ID} و کلید سرّی NCC یعنی x دارد و چون از x تنها خود NCC مطلع است در نتیجه مهاجم قادر به جعل پیام احراز اصالت NCC نخواهد بود. در نتیجه این طرح در مقابل حمله جعل هویت کاربر و NCC مقاوم است.

* **حمله تکرار**[19]: در حمله تکرار، مهاجم ابتدا با استراق سمع خطوط ارتباطی، پیام‌های مربوط به یک یا چند نشست احراز اصالت را جمع‌آوری کرده و سپس با ترکیب و استفاده مجدد آنها (معمولا بدون دسترسی به کلید محرمانه مشترک کاربر و شبکه و بی‌نیاز از ایجاد تغییرات گسترده در پیام‌های ذخیره شده) تلاش در ساخت یک تقاضای احراز اصالت جعلی می‌کند و با ارسال آن به سمت شبکه، به جای کاربر اصلی وارد سیستم می‌شود.

در این طرح، NCC پس از هر نشست موفق هویت موقتی کاربر (T_{ID}) را به‌روز می‌کند. این امر موجب می‌شود که:

۱- $b = h(U_{ID}, T_{ID}, r)$ که از پیام‌های احراز اصالت کاربر است در هر نشست به‌روز شده در نتیجه امکان حمله از طریق شنود و تکرار درخواست وجود ندارد.

۲- $C = h(T'_{ID}, h(U'_{ID}, x)) \oplus T_{IDNew}$ که پیام احراز اصالت NCC است، با به روز شدن T_{ID} به‌روز شده و مهاجم با شنود و تکرار آن برای کاربر، قادر به تصدیق هویت توسط او نخواهد بود. در نتیجه طرح پیشنهادی نسبت به حمله تکرار امن است.

* **حمله ممانعت از سرویس:** در حمله ممانعت از سرویس، مهاجم می‌تواند به وسیله قطع یا مسدودکردن پیام انتقالی بین کاربران یا کاربر و شبکه، همزمانی و همگامی بین آنها را مختل کند. به عنوان مثال، ممکن است که شبکه داده‌های مشترک را به‌روز رسانی کند در حالی که این کار در کاربر مورد نظر انجام نگیرد و در نتیجه آنها نمی‌توانند یکدیگر را برای مدت طولانی احراز اصالت کنند. برای رفع تاثیرات این حمله، طرفین نشست می‌توانند با داشتن یک رونوشت از اطلاعات مربوط به نشست قبلی، این حمله را تشخیص داده و داده‌های مشترک‌شان را دوباره همگام کنند.

این طرح در برابر حمله ممانعت از سرویس امن است زیرا NCC پس از به روز کردن هویت موقتی کاربر (T_{IDNew})، هویت موقتی قبلی(T_{ID}) را تا قبل از برقراری نشست دوباره و اطمینان از دریافت هویت به روز شده توسط کاربر، از جدول خود پاک نمی‌کند. این امر موجب می‌شود که حتی در صورت قطع ارتباط به طور عمد یا غیر عمد، کاربر بتواند دوباره توسط NCC تصدیق شود.

* **دزدیدن کارت هوشمند:** در برخی از پروتکل‌ها، کاربر اطلاعات لازم برای احراز اصالت خود را در کارت هوشمند ذخیره می‌کند. اگر پروتکل به گونه‌ای طراحی شود که تنها با واردکردن کارت به دستگاه کارتخوان محاسبات مد نظر پروتکل انجام شود و دیگر نیازی به واردکردن اطلاعاتی از طرف کاربر نباشد، مهاجم با دزدیدن کارت هوشمند کاربر به راحتی می‌تواند به شبکه وصل شود. برای مقابله با این حمله، پروتکل باید طوری طراحی شود که هنگام وارد کردن کارت به دستگاه، دستگاه اطلاعات محرمانه‌ای را که مختص به خود کاربر است از او بخواهد.

طرح پیشنهادی از این جهت نسبت به دزدیدن کارت هوشمند امن است که کاربر با وارد کردن کارت خود به دستگاه کارتخوان باید هویت دائمی (U_{ID}) و کلمه عبور (PW) خود را نیز به عنوان اطلاعات وردی وارد کند تا دستگاه بتواند به وسیله آنها و اطلاعات ذخیره شده در کارت پیام احراز اصالت کاربر را محاسبه کند. در نتیجه در این طرح، مهاجم تنها با داشتن کارت هوشمند کاربر قادر به دسترسی به شبکه نخواهد بود.

در جدول ۲، ویژگی‌های امنیتی روش پیشنهادی در مقابل دیگر روش‌ها مورد بررسی قرار داده شده است.

تحلیل کارآیی روش پیشنهادی

براساس تخمین انجام شده توسط آقای Potlapally و همکارانش[۱۰]، محاسبه یک تابع چکیده‌ساز یکطرفه مانند SHA-1 حدودا به $0.76\mu j$ انرژی، محاسبه یک تابع چکیده‌ساز کلیددار به حدودا $1.16\mu j$ انرژی نیاز دارد و محاسبه یک رمزنگاری متقارن مانند AES به حدودا $9.08\mu j$ انرژی نیاز دارد. از عملیات XOR به دلیل آنکه انرژی کمی مصرف می‌کند، می‌توان صرف نظر کرد. بر همین اساس، به عنوان نمونه هزینه محاسباتی طرح پیشنهادی آقای Chen و همکارانش برابر می‌شود با

$$2S + 4H + 2HM = (2\times 9.08) + (4\times 0.76) + (2\times 1.16) = 23.52\mu J$$

هزینه محاسباتی طرح پیشنهادی آقای Chang و همکارانش برابر می‌شود با $5H = 5\times 0.76 = 3.9\mu j$ و هزینه محاسباتی طرح پیشنهادی ما برابر می‌شود با $9H = 9\times 0.76 = 6.84\mu j$.

در جدول ۳، مقایسه‌ای بین روش‌های ارائه شده و روش پیشنهادی از نظر مصرف انرژی و در نتیجه هزینه محاسباتی در مرحله احراز اصالت انجام شده است. با توجه به این جدول، به غیر از روش [۴] که از امنیت بالایی برخوردار نیست، میزان توان مصرفی روش ارائه شده از دیگر روش‌ها کمتر است بنابراین روش ارائه شده علاوه بر برخورداری از امنیت بیشتر نسبت به سایر روش‌ها از هزینه محاسباتی کمتری نیز برخوردار است.

19. Replay Attack

جدول۲.مقایسه ویژگی‌های امنیتی روش پیشنهادی با سایر روش‌ها

پروتکل‌های موجود	انواع حمله‌ها					
	حمله تصدیق کننده مسروقه	حمله الحاق	حمله جعل هویت	حمله تکرار	امنیت در برابر دزدیده شدن کارت	حمله ممانعت از سرویس
روش پیشنهادی	+	+	+	+	+	+
Chang [۴]	+	+	-	-	+	-
Yoon [۸]	+	+	+	+	+	-
Lee[۹]	+	-	+	–	+	-
Chen [۷]	+	+	+	+	-	-
Chang [6]	-	-	-	+	-	-
Hwang [۵]	-	-	-	+	-	-

جدول۳.مقایسه هزینه محاسباتی روش پیشنهادی با سایر روش‌ها

پروتکل‌های موجود	توابع رمزنگاری				انرژی مصرفی (E_i)
	رمزنگاری متقارن	تابع چکیده‌ساز (Hash)	تابع چکیده‌ساز کلیددار (MAC)	عملیات XOR	انرژی برحسب E_i
روش پیشنهادی		۹		۷	۶/۸۴
Chang [۴]		۵		۴	۳/۹
Yoon [۸]		۶	۴	۳	۹/۲
Lee [۹]		۱۰		۸	۷/۶
Chen [۷]	۲	۴	۲		۲۳/۵۲
Chang [6]		$6+N-(j-1)^*$			
Hwang [۵]	۴				۳۶/۳۲

* j : منظور j-مین احراز اصالت و N : تعداد دفعات اتصال به NCC

بررسی پروتکل پیشنهادی با ابزار درستی‌یابی AVISPA

ابزار درستی‌یاب AVISPA برای ارزیابی پروتکل‌ها از نظر ویژگی‌های امنیتی مورد استفاده قرار می‌گیرد. این ابزار یکی از کامل‌ترین ابزارهای خاص تحلیل پروتکل محسوب می‌شود که در آن تحلیل یک پروتکل کاملا به صورت خودکار انجام می‌گیرد. این ابزار با دریافت یک توصیف سطح بالا از پروتکل و اهداف مورد نظر، ماشین حالت پروتکل را با توجه به حضور و دانش مهاجمان از پروتکل ترسیم کرده و با بررسی ماشین حالت، برآورده شدن یا نشدن اهداف امنیتی را گزارش می‌دهد و در صورت شکست پروتکل الگوی حمله را ترسیم می‌کند. پروتکل‌هایی که توسط ابزار AVISPA مورد مطالعه قرار می‌گیرند باید به زبان HLPSL توصیف شوند. زبان HLPSL یک زبان مدل‌سازی ساده و مبتنی بر نقش است که امکان توصیف و مدل‌سازی پروتکل و مشخص کردن اهداف امنیتی مورد نظر را فراهم می‌کند و تمامی ساختارهای کنترلی، داده‌ای، نیازمندی‌های امنیتی و انواع توابع رمزنگاری در این زبان قابل توصیف است.

علاوه بر مسائل بالا، ابزار درستی‌یاب AVISPA به این دلایل برای بررسی امنیت پروتکل انتخاب می‌شوند: ۱- توصیف پروتکل در این ابزار با استفاده از منطق HLPSL [۲۰] ساده بوده و از واسط گرافیکی مناسبی برخوردار است. ۲- با استفاده از چهار ابزار قوی که مبتنی بر منطق‌های مختلفی هستند ابزاری با قدرت و مناسب برای

20. High Level Protocols Specification Language

ارزیابی پروتکل‌های احراز اصالت به شمار می‌رود. ۳- امکان ارزیابی پروتکل را بر مبنای اهداف مختلفی که توسط کاربر تعیین می‌شود فراهم می‌کند. ۴- تمام فرآیند درستی‌یابی و کشف الگوی حمله در این ابزار به صورت خودکار انجام می‌شود.

در این مقاله از ابزار درستی‌یاب AVISPA برای اثبات امنیت پروتکل ارائه شده استفاده می‌شود. در ادامه بخش کد HLPSL مربوط به درستی‌یابی پروتکل پیشنهادی، همراه با خروجی حاصل از ارزیابی پروتکل با استفاده از ابزار درستی‌یاب AVISPA ارائه می‌شود. عامل‌های شرکت‌کننده در این پروتکل، NCC و کاربر متحرک هستند.

نقش کاربر در پروتکل پیشنهادی به صورت زیر تعریف می‌شود:

```
role
role_U(U:agent,K:text,R:text,T:text,SND,RCV:channel(dy)
)
played_by U
def=
        local

        State:nat,Tn:text,Hash:function,Xor:function
        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|> State':=1 /\
SND(T.Xor(Hash(K).R).Hash(U.T.R))
                2. State=1 /\
RCV(Xor(Hash(T.K).Tn').Hash(Tn')) =|> State':=2
end role
```

SND وRCV کانال‌های ارتباطی نقش با دنیای خارج هستند که از نوع DY تعریف شده‌اند. در این نوع کانال مهاجم قابلیت کنترل کانال را دارد. H از نوع تابع چکیده‌ساز است. با دستور played_by ایفاکننده نقش از میان عامل‌ها مشخص می‌شود. در بخش local متغیرهای محلی مورد نیاز نقش تعریف خواهند شد که شامل اعداد نانس و state که شماره‌ای است که حالت فعلی عامل را در ماشین حالت بیان می‌کند.

در بخش transition نحوه تعامل این نقش با سایر نقش‌ها در قالب دستورهای انتقالی بیان می‌شود.

- نقش NCC:

```
role
role_S(S:agent,U:agent,T:text,Tn:text,K:text,SND,RCV:cha
nnel(dy))
played_by S
def=
        local

        State:nat,R:text,Hash:function,Xor:function
        init
                State := 0
        transition
                1. State=0 /\
RCV(T.Xor(Hash(K).R').Hash(U.T.R')) =|> State':=1 /\
SND(Xor(Hash(T.K).Tn).Hash(Tn))
end role
```

- در این بخش نشست تعریف می‌شود که در آن از هر یک از نقش‌های تعریف شده برای عوامل شرکت‌کننده در پروتکل نمونه‌هایی گرفته و تعامل آنها در قالب نشست مشخص می‌شود:

```
role session1(R:text,S:agent,U:agent,T:text,Tn:text,K:text)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_S(S,U,T,Tn,K,SND2,RCV2) /\
role_U(U,K,R,T,SND1,RCV1)
end role
```

در این بخش محیط مربوط به درستی‌یاب که شامل چندین نشست است، تعریف می‌شود. همچنین دانشی که مهاجم از کل پروتکل دارد توصیف می‌شود که شامل نام عوامل درگیر و تابع چیکده‌ساز است:

```
role environment()
def=
        const

        hash_0:function,uaer:agent,const_1:text,server:ag
ent,key:text,auth_1:protocol_id,auth_2:protocol_id
        intruder_knowledge = {}
        composition

        session1(const_1,server,uaer,const_1,const_1,key)
end role
```

- در ادامه، اهداف امنیتی که ابزار AVISPA باید صحت آنها را در مورد پروتکل توصیف شده بررسی کند، مشخص شده‌اند:

```
goal
        authentication_on auth_1
        authentication_on auth_2
end goal

environment()
```

- خروجی حاصل از درستی‌یابی پروتکل پیشنهادی با استفاده از AVISPA به صورت زیر است:

```
%OFMC

%Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
C:\progra~1\SPAN\testsuite\results\hlpslGenFile.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.01s
searchTime: 0.04s
visitedNodes: 6 nodes
depth: 3 plies
```

همان‌طور که خروجی ابزار درستی‌یابی AVISPA نشان می‌دهد پروتکل احراز اصالت پیشنهادی امن است.

نتیجه‌گیری

در این مقاله یک طرح احراز اصالت امن و کارآمد برای شبکه‌های ماهواره‌ای متحرک ارائه شد. این طرح مبتنی بر تابع چکیده‌ساز و عملیات XOR است که موجب کاهش هزینه‌های محاسباتی سیستم می‌شود. تعداد توابع چکیده‌ساز به کار رفته در این طرح به گونه‌ای است که این طرح را نسبت به روش‌های گذشته از نظر هزینه محاسباتی سبک‌ترکرده‌است. احراز اصالت دوطرفه، محرمانگی، مدیریت کلید ساده، نشست مستقل، پوشیدگی و گمنامی کاربر از جمله ویژگی‌های دیگر این طرح است. این طرح در برابر حمله تکرار، حمله الحاق، حمله تصدیق‌کننده مسروقه، حمله جعل هویت، حمله دزدیدن کارت هوشمند کاربر و حمله ممانعت از سرویس امن است. در کارهای گذشته، به دلیل آنکه NCC پس از نشست موفق، هویت موقتی کاربر را به‌روز و هویت قبلی را از جدول خود پاک می‌کند، در صورت قطع ارتباط و عدم دریافت هویت موقتی توسط کاربر، امکان برقراری نشست دوباره بین NCC و کاربر وجود ندارد. مقاوم بودن این طرح در برابر حمله ممانعت از سرویس، امکان برقراری نشست دوباره را در صورت قطع ارتباط بین کاربر و NCC، به شبکه می‌دهد.

مرجع‌ها

[1] G. Zheng, H. T. Ma, C. Cheng and Y. C.Tu, “Design and logical analysis on the access authentication scheme for satellite mobile communication networks,” IET Inf. Secur,2012, Vol. 6, Iss.1, pp. 6–13.
[2] L. Qi, and L. Zhi, “Authentication and Access Control in Satellite Network,” 3rd International Symposium on Electronic Commerce and Securit- y, 2010.
[3] L. Lasc, R. Dojenand T. Coffey, “A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications,” International Journal of Information Security and Privacy, January-March 2011, 5(1), 33-49.
[4] C. C. Chang, T. F. Cheng and H. L. Wu, “An authentication and key agreement protocol for satellite communications,” Int. J. Commun. Syst, Published online in Wiley Online Library, sept 2012.
[5] M. S. Hwang, C. C. Yang and C. Y. Shiu, “An authentication scheme for mobile satellite communication systems,” ACM SIGOPS Operati- ng Systems Review, October 2003, 37(4):42–47.
[6] Y. F. Chang and C. C. Chang, “An efficient authentication protocol for mobile satellite communication systems,” ACM SIGOPS Oper, Syst, Rev,2005, 39(1), pp. 70–84.
[7] T. H. Chen, W. B. Lee and H. B. Chen, “A self-verification authentication mechanism for mobile satellite communication systems,” Computers & Electrical Engineering January, 2009, 35(1):41–48.
[8] E. J. Yoon, K. Y. Yoo, J. W. Hong, S. Y. Yoon, D. I. Park and M. J. Choi, “An efficient and secure anymous authentication scheme for mobile satellite communication systems,” EURASIP Journal on Wireless Communicati- ons and Networking, 2011.
[9] C. C. Lee, C. T. Li and R. X. Chang, “A simple and efficient authentication scheme for mobile satellite communication systems,”Int- ernationalJournal of SatelliteCommunicatio- ns and Networking, January/February 2012.
[10] N. R. Potlapally, S. Ravi, A. Raghunathan andN. K. Jha,“A study of the energy consumption characteristics of cryptographic algorithms and security protocols”. IEEE Tra-ns Mob Comput,2006, 5(2):128-143.