مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»

سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۱۶۳-۱۴۳

یک طرح احراز هویت امن سه عامله برای شبکه‌های حسگر بی‌سیم سلامت الکترونیک مبتنی بر خم بیضوی

محمدحسن کاظمی‌پوران[۱]، مجید بیات*[۲]، سید مرتضی پورنقی[۳]، زهرا هاتفی[۴]، نگین حامیان[۴]

۱- دانشجوی کارشناسی ارشد رایانش امن، و ۲- استادیار، گروه کامپیوتر، دانشگاه شاهد، تهران، ایران، ۳- دکتری فناوری اطلاعات،گروه کامپیوتر، دانشگاه قم، ایران، ۴- کارشناس ارشد مخابرات امن و رمزنگاری، گروه مخابرات، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران، ایران

(دریافت: ۹۷/۰۶/۱۹، پذیرش: ۹۸/۰۳/۲۸)

چکیده

شبکه‌های بی‌سیم بدن شامل بسیاری گره کوچک است که در بدن بیمار یا اطراف آن کاشته می‌شود. این گره‌های حسگر می‌توانند داده‌های پزشکی را از بیمار جمع‌آوری کرده و این اطلاعات ارزشمند را به یک نمایشگر داده یا یک دستیار دیجیتال شخصی انتقال دهند. سپس، ارائه‌دهندگان خدمات سلامت می‌توانند از طریق مجوز به این اطلاعات دسترسی پیدا کنند. داده‌های پزشکی اغلب شخصی و خصوصی است و محرمانه بودن اطلاعات و حفظ حریم خصوصی کاربران از نگرانی‌های اصلی این سامانه‌ها است. بنابراین افزایش تأمین امنیت داده‌های خدمات سلامت از اهمیت حیاتی برخوردار است. یکی از عوامل مهم ایجاد امنیت در شبکه‌های سلامت الکترونیک، پروتکل‌های احراز هویت می‌باشند که به طرفین ارتباطات این امکان را می‌دهد تا از هویت یکدیگر اطمینان پیدا کنند و بتوانند خود را به‌طرف دیگر بشناسانند. اخیراً دراین‌ارتباط، چالا و همکارانش [۱] یک پروتکل احراز هویت و توافق کلید سه عامله مبتنی بر خم بیضوی را برای شبکه‌های حسگر بی‌سیم سلامت ارائه داده‌اند. در این مقاله، ما چند ضعف امنیتی مانند حمله دسترسی مجاز داخلی و عدم امنیت پیشرو و قابل‌ردیابی بودن کاربر را در طرح چالا بیان می‌کنیم و سپس یک طرح امن احراز هویت سه عامله برای شبکه‌های حسگر بی‌سیم سلامت پیشنهاد می‌کنیم. در ادامه ویژگی‌های امنیتی طرح خود را بررسی و با کمک ابزار پروووریف امنیت آن را به‌طور صوری بررسی می‌کنیم. تحلیل امنیتی ارائه‌شده و مقایسه‌های امنیتی و کارایی بیان‌شده با طرح‌های مرتبط، بیان می‌کنند که طرح پیشنهادی یک طرح احراز هویت امن کارا برای شبکه‌های حسگر بی‌سیم سلامت است.

کلیدواژه‌ها: احراز هویت، سلامت الکترونیک، توافق کلید، امنیت، حریم خصوصی، پروووریف

علائم و اختصارات

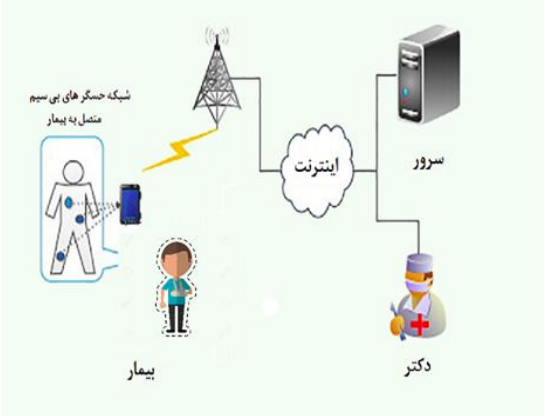
SC_i	کارت هوشمند	$h(.)$	تابع درهم‌ساز یک‌طرفه مقاوم در برابر تصادم
ID_i، PW_i، Bio_i	به ترتیب شناسه کاربر i، کلمه عبور و مدل زیست‌سنجی کاربر i	s_0	کلید اصلی ۱۶۰ بیتی که مختص TA است
$Gen(.), Rep(.)$	روش‌های تولید نسبی و قطعی احتمالی زیست‌سنجی در استخراج فازی	$P(x_P, y_P), \mathbf{k}.P$	به ترتیب نقطه‌ای از منحنی بیضوی (ECC)روی خم E_p (a,b) و ضرب نقطه‌ای روی خم، E_p (a,b)
t	آستانه خطا استفاده‌شده توسط استخراج فازی	ΔT	حداکثر تأخیر انتقال
σi , τ_i	به ترتیب کلید مخفی زیست‌سنجی و پارامتر عمومی تکثیر	T_s , T_i	به ترتیب مهر زمانی کاربر و حسگر
		SK	کلید جلسه بین کاربر و حسگر
		$\|\|, \oplus$	به ترتیب XOR بیتی و عملیات پیوند

*رایانامه نویسنده پاسخگو: mbayat@shahed.ac.ir

۱. مقدمه

سلامت الکترونیک و شبکه‌های حسگر بی‌سیم[1] به دلیل گسترش اینترنت، تلفن‌های هوشمند و برنامه‌های کاربردی سلامت در سال‌های اخیر موردتوجه بسیاری قرارگرفته است یک جنبه در حال ظهور از سلامت الکترونیک یا مراقبت‌های الکترونیکی پزشکی از راه دور شبکه‌های حسگر بی‌سیم بدنی است که هر بیماری که وارد شبکه می‌شود به‌وسیله حس‌گرهای متصل به بدنش وضعیت سلامت خود را ازجمله فشارخون، ضربان قلب و غیره را در اختیار سامانه سلامت الکترونیک از راه دور قرار می‌دهد و سپس این حسگرهای کوچک پس از دریافت و دسته‌بندی اطلاعات آن‌ها را به‌وسیله شبکه‌های بلوتوث، وای فای یا اینترنت عمومی در اختیار موبایل یا ساعت هوشمند و ... قرار می‌دهد. دستگاه هوشمند اطلاعات را به‌وسیله اینترنت به سرور سلامت منتقل می‌کند و دکتر می‌تواند با مشاهده وضعیت بیمار و همچنین سوابق پزشکی تجویز لازم را ارسال نمایند.

همه این‌ها کمک می‌کنند که بتوان وضعیت بیمار را از راه دور کنترل کرد. این فناوری همچنین به پزشکان این اجازه را می‌دهد که در هر مکانی اطلاعات پزشکی خودشان را ارائه دهند و نیاز مراجعه حضوری در همه موارد پزشکی کمتر بشود. با افزایش نیازمندی و کاربردهای سلامت الکترونیک پروتکل‌های سلامت الکترونیک باید به‌گونه‌ای کارآمد و بهینه باشد تا پزشکان، مراکز درمانی و پرستاران را به‌وسیله شبکه‌ای واحد به هم متصل و ارتباط آن‌ها را مدیریت کند. معماری اولیه سامانه سلامت الکترونیک از راه دور در شکل (۱)توضیح داده شده است.



شکل (۱): معماری معمول سامانه پایش سلامت الکترونیک [۱].

توسعه و گسترش فزاینده شبکه دستگاه‌های ارتباطی بی‌سیم، دسترسی و کاربردهای فراوانی را مهیا کرده است و کاربران در هر زمان و مکانی به شبکه دسترسی دارند. به‌طور طبیعی کاربران قبل از دریافت خدمات در شبکه باید احراز هویت شوند. احراز هویت کاربران معمولاً با کمک شناسه کاربر مجاز، کلمه عبور او، کارت هوشمند و اطلاعات منحصربه‌فرد زیست‌سنجی کاربر انجام می‌شود. چالش‌های متعددی برای احراز هویت در سامانه سلامت الکترونیک از راه دور وجود دارد ازجمله می‌توان به ظرفیت حافظه محدود، توان محدود گره‌های حسگر، حفظ حریم خصوصی کاربران و... اشاره کرد. تاکنون طرح‌های زیادی برای احراز هویت در سامانه سلامت الکترونیک ارائه‌شده است که در ادامه به آن‌ها اشاره می‌کنیم. در سال ۲۰۱۶، لی liu و همکاران [۲] یک پروتکل احراز هویت مبتنی بر زوج سازی دوخطی که قابلیت اطمینان در احراز هویت کاربر و همچنین ارتباط امن بین کاربر و گره‌های حسگر را فراهم می‌کند ارائه دادند. سپس چالا[2] و همکارانش [۱] نشان دادند پروتکل لی و همکاران [۲] در برابر برخی حملات، ازجمله، حمله کارت هوشمند به سرقت رفته[3]، حمله حدس زدن کلمه عبور[4]، حمله دسترسی مجاز داخلی[5] و حمله جعل هویت کاربر[6] مقاوم نیست. چالا و همکارانش نشان دادند علاوه بر حملات ذکرشده پروتکل لی و همکاران در ارائه اعتبار سنجی متقابل[7] مناسب ناموفق است.

برای رفع نواقص موجود در پروتکل لی، چالا و همکارانش [۱] در سال ۲۰۱۸ یک پروتکل سه عامله احراز هویت و توافق کلید مناسب برای شبکه‌های حسگر بی‌سیم مراقبت‌های سلامت مبتنی بر منحنی بیضوی ارائه دادند.

در این مقاله، ما چند ضعف امنیتی مانند حمله دسترسی مجاز داخلی و عدم امنیت پیشرو[8] و قابل‌ردیابی بودن[9] کاربر را در طرح چالا بیان می‌کنیم و سپس یک طرح امن احراز هویت سه عامله برای شبکه‌های حسگر بی‌سیم سلامت پیشنهاد می‌کنیم.

۱-۱. کارهای مرتبط

به‌طورکلی، یک روش تائید اعتبار از یک یا ترکیبی از سه عامل برای احراز هویت استفاده می‌کند. چیزی که کاربران می‌دانند (مثل کلمه عبور) چیزی که کاربران دارند (مثل کارت هوشمند)

1- Wireless Body Area Networks
2- Challa

3- Stolen Smart Card Attack
4- Password Guessing Attack
5- Privileged Insider Attack
6- User Impersonation Attack
7- Proper Mutual Authentication
8- Forward Secrecy
9- Untraceability

و چیزی که کاربران هستند (مثل ویژگی‌های زیست‌سنجی [۳]. کلمه عبور رایج‌ترین عامل احراز هویت در شبکه‌های مختلف (خدمات ایمیل، شبکه‌های اجتماعی) است.

لمپارت[1] اولین طرح اعتبار سنجی مبتنی بر کلمه عبور را که بتواند هویت کاربران را از طریق یک کانال ناامن تائید کند در سال ۱۹۸۱پیشنهاد کرد [۴]. بااین‌حال، این نوع از برنامه‌های تائید اعتبار به ذات آسیب‌پذیر است، لذا با توجه به امنیت پایین پروتکل‌های احراز هویت تک عامله و حملات صورت گرفته ازجمله حمله حدس زدن برون‌خط کلمه عبور [2]، فیشینگ[3] و ... پروتکل نیازمند راه‌حل مؤثری برای مسائل فوق است بنابراین محققان این‌گونه پیشنهاد کرده‌اند که یک عامل دیگر نیز در احراز هویت دخیل باشد، برای همین مهم پروتکل‌های احراز هویت دو عامله که کلمه عبور و کارت هوشمند ادغام می‌شوند ارائه شدند. با این‌حال کارت‌های هوشمند ممکن است ازدست‌رفته یا دزدیده‌شده و سپس اطلاعات ذخیره‌شده در کارت‌های هوشمند می‌تواند استخراج شود. برای پاسخگویی به چنین نگرانی، پروتکل‌های احراز هویت سه عامله پیشنهادشده است [۵] که در آن، کاربر کارت هوشمند خود را به یک کارت‌خوان وارد می‌کند، نام کاربری و کلمه عبور را ارائه می‌دهد و همچنین اطلاعات زیست‌سنجی[4] را در مرحله ورود وارد می‌کند. سرور تنها اگر کلمه عبور، کارت هوشمند و اطلاعات زیست‌سنجی معتبر باشند، می‌تواند کاربر را تائید کرده و اجازه ورود به سامانه را برای او صادر کند.

لی[5] و همکاران [۵] یک پروتکل احراز هویت سه عامله مبتنی بر اثرانگشت ارائه داده‌اند بااین‌حال، لین[6] و همکاران [۶] مشخص کردند که طرح لی و همکاران نسبت به حمله جعل هویت آسیب‌پذیر است. سپس، یک طرح بهینه بدون جداول تائید را پیشنهاد کردند، که اجازه می‌دهد تا کاربران کلمه عبور خود را آزادانه انتخاب و به‌روزرسانی کنند. کو[7] و همکاران [۷] نیز بر روی طرح لی و همکاران [۵] حمله جعل را پیاده‌سازی کردند، که در آن مهاجم می‌تواند هر کاربر قانونی را جعل کند. خان[8] و همکاران [۸] نشان دادند که طرح احراز هویت Lin و همکاران [۶] نمی‌تواند در مقابل حملات سرور دروغین[9] مقاومت کند. همچنین خان و همکاران طرح لین و همکاران را برای دست‌یابی به احراز هویت متقابل بهبود دادند. هی[10] و همکاران [۹] نشان دادند که پروتکل احراز هویت خان و همکاران نسبت به حمله جعل هویت آسیب‌پذیر است.

کیم[11] و همکاران [۱۰] ساختار پروتکل‌های احراز هویت سه عامله با استفاده از کلمه عبور، کارت هوشمند و اثرانگشت را پیشنهاد دادند. با این‌حال، اسکات[12] ثابت کرد طرح کیم و همکاران در معرض حمله جعلی هویت کاربر است [۱۱].

چن[13] و همکاران [۱۲] یک پروتکل احراز هویت سه عامله جدید برای دستگاه‌های تلفن همراه ارائه دادند. خان و همکاران [۱۳] نشان دادند که پروتکل چن و همکاران نسبت به حمله حدس برون‌خط کلمه عبور آسیب‌پذیر است. یون[14] و همکاران [۱۴] یک پروتکل احراز هویت سه عامله مبتنی بر رمزنگاری منحنی بیضوی ارائه دادند.

فن[15] و همکاران [۱۵] یک پروتکل احراز هویت سه عامله که حریم خصوصی را حفظ کند پیشنهاد کردند. ایده اصلی برای رسیدن به حفظ حریم خصوصی در این الگوریتم، انتخاب یک‌رشته تصادفی و ترکیب آن با داده‌های زیست‌سنجی است.

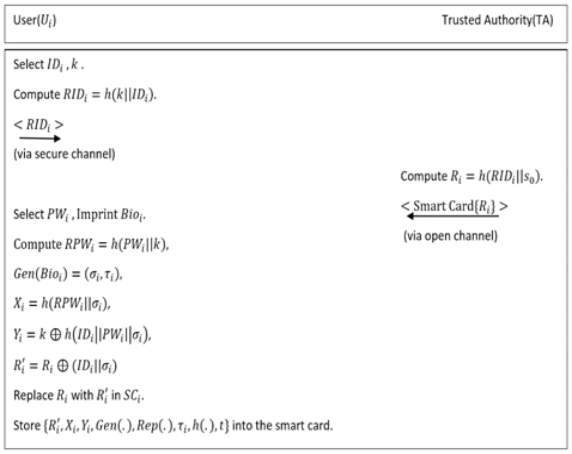
جیانگ[16] و همکاران [۳] پس از شناسایی حمله جعل هویت در طرح وُو[17] و همکاران [۱۶] پروتکل احراز هویت مبتنی بر ابر[18] برای سلامت الکترونیک که از رمزنگاری سبک‌وزن خم بیضی استفاده می‌کند ارائه دادند. ایرشاد[19] و همکارانش [۱۷]، ضعفی در پروتکل جیانگ یافتند که منجر به حمله منع سرویس[20] می‌شود. ایرشاد و همکارانش با اضافه کردن یک گام اضافی در مرحله اعتبارسنجی متقابل به پروتکل جیانگ برای غلبه بر حمله منع سرویس، همان پروتکل را باکمی تغییر پیشنهاد کردند. در سال ۲۰۱۷، لی و همکاران [۲] یک پروتکل احراز هویت مبتنی بر زوج سازی دوخطی که قابلیت اطمینان در احراز هویت کاربر و همچنین ارتباط امن بین کاربر و گره‌های حسگر را فراهم می‌کند ارائه دادند. سپس چالا و همکاران [۱] نشان دادند پروتکل لی و همکاران در برابر برخی حملات، ازجمله حمله کارت هوشمند به سرقت رفته، حمله حدس زدن کلمه عبور، حمله دسترسی مجاز داخلی و حمله جعل هویت کاربر مقاوم نیست. چالا و همکارانش

1- Lamport
2- Offline Password Guessing Attack
3- Phishing
4-Biometric
5- Lee
6- Lin
7- Ku
8- Khan
9 Server Spoofing Attack
10- Rhee
11- Kim
12 Scott
13- Chen
14- Yoon
15- Fan
16- Jiang
17- Wu
18- Cloud
19- Irshad
20- Denial-of-service attack

نشان دادند علاوه بر حملات ذکرشده پروتکل لی و همکاران در ارائه اعتبارسنجی متقابل مناسب ناموفق است. برای رفع نواقص موجود در پروتکل لی و همکاران، چالا و همکاران [۱] در سال ۲۰۱۸ یک پروتکل سه عامله احراز هویت و توافق کلید مناسب برای شبکه‌های حسگر بی‌سیم مراقبت‌های سلامت مبتنی بر منحنی بیضوی ارائه دادند.

۱-۲. نوآوری مقاله

در این مقاله طرح چالا و همکاران [۱] را بررسی می‌کنیم و نشان می‌دهیم در برابر حمله دسترسی مجاز داخلی آسیب‌پذیر است و همچنین این طرح امنیت پیشرو و غیر قابل‌ردیابی بودن کاربر را تضمین نمی‌کند. سپس یک طرح احراز هویت ارتقا یافته امن برای شبکه سلامت الکترونیک ارائه می‌دهیم که ویژگی‌های امنیتی لازم برای شبکه‌های حسگر بی‌سیم را دارا باشد. همچنین امنیت طرح را به‌صورت صوری و با کمک ابزار پرووریف[1] ارائه می‌دهیم.



شکل (۲): مرحله ثبت نام طرح چالا [۱]

۱-۳. ساختار مقاله

در فصل ۲، مباحث مقدماتی موردنیاز مقاله ارائه می‌شود. در فصل ۳ طرح چالا و آسیب‌پذیرهای آن را بیان می‌کنیم. طرح پیشنهادی در فصل ۴ مطرح می‌شود و در فصل ۵ تحلیل‌های امنیتی و کارایی طرح پیشنهادی ارائه می‌گردد. درنهایت در فصل ۶ نتیجه‌گیری مقاله آورده می‌شود.

۲. مباحث مقدماتی

در این بخش مباحث مقدماتی، اصطلاحات و تعاریف مرتبط با این مقاله مطرح می‌گردد

.

1-ProVerif

۲-۱. منحنی بیضوی

رمزنگاری منحنی بیضوی[2] (ECC) یک رمزنگاری به روش کلید عمومی است که بر اساس ساختاری جبری از منحنی‌های بیضوی بر روی میدان‌های متناهی طراحی‌شده است. استفاده از منحنی‌های بیضوی در رمزنگاری به‌طور جداگانه توسط کوبلیتز[3] و میلر[4] در سال ۱۹۸۵ پیشنهاد شد [۴].

اوایل، سامانه‌های رمزنگاری مبتنی بر کلید عمومی با این فرض که پیدا کردن دو یا بیشتر از دو عامل اول بزرگ برای یک عدد صحیح بزرگ مشکل است امن تلقی می‌شدند. برای پروتکل‌های مبتنی بر منحنی بیضوی، فرض بر این است که پیدا کردن لگاریتم گسسته از یک عنصر تصادفی منحنی بیضوی با توجه به یک نقطه پایه عمومی شناخته‌شده غیرعملی است. اندازه منحنی بیضوی تعیین‌کننده سختی مسئله است. مزیت اصلی که توسط ECC وعده داده می‌شد یک کلید با اندازه کوچک‌تر بود، که این موضوع به معنی کاهش ذخیره‌سازی و انتقال [۱۸] موردنیاز است، به این معنی که، یک سامانه منحنی بیضوی می‌تواند همان سطح از امنیت را که یک سامانه مبتنی بر RSA با طول کلید بیشتر فراهم می‌کند را ایجاد کند، به‌عنوان‌مثال، یک کلید عمومی ۲۵۶ بیتی مبتنی بر ECC می‌بایست امنیت قابل‌مقایسه‌ای با یک کلید عمومی ۳۰۷۲ بیتی مبتنی بر RSA داشته باشد. آن‌گاه، یک منحنی بیضوی $E_p(a,b)$ به‌صورت ذیل تعریف می‌شود:

با فرض $p > 3$ یک عدد اول بر روی منحنی بیضوی $E_p(a,b)$ حول میدان متناهی $Z_p = \{0,1,\dots,p-1\}$ داریم رابطه:

$E: y^2 = x^3 + ax + b (modp)$ که a, b ∈ Z_p مقادیر ثابت منحنی بیضوی و x , y متغیرهای مقدارپذیر $4a^3 + 27b^2 \neq 0$ منحنی بیضوی هستند.یک منحنی بیضوی حول میدان متناهی Z_p عبارت است از نقطه‌ای در بی‌نهایت که به‌صورت O نمایش داده می‌شود، به‌علاوه مجموعه‌ای از جواب‌های $S(x,y) \in Z_p \times Z_p$ که در رابطه فوق صدق کند [۱۹].

۲-۲. استخراج فازی[5]

پروتکل چالا برای احراز هویت زیست‌سنجی، از استخراج فازی استفاده می‌کند به‌گونه‌ای که تابع تولید اعداد تصادفی Gen(.) اطلاعات زیست‌سنجی Bio_i را از ورودی دریافت کرده و یک کلید زیست‌سنجی با طول l بیت به نام $\sigma_i \in \{0,1\}^l$ و پارامتر عمومی

2- Elliptic Curve Cryptography
3- Kobleitz
4- Miller
5- Fuzzy extractor

τ_i را به‌عنوان خروجی برمی‌گرداند. تابع دیگر استخراج فازی Rep(.) در مرحله احراز هویت استفاده می‌شود. این تابع اطلاعات زیست‌سنجی Bio_i' و τ_i که توسط کاربر وارد می‌شود را به‌عنوان ورودی دریافت می‌کند. این تابع فاصله $d(Bio_i', Bio_i) \leq t$ را بررسی می‌کند که t مقدار آستانه تحمل خطا است. خروجی این تابع، کلید زیست‌سنجی σ_i است که $\sigma_i = \text{Rep}(Bio_i', \tau_i)$ [۱].

۲-۳. زوج سازی دوخطی[1]:

زوج‌سازی یک نگاشت دوسویه است که به‌صورت زیر تعریف می‌شود:

$e: G_1 \times G_2 \rightarrow G_T$

که در آن، G_1 و G_2 زیرگروه‌هایی دوری از منحنی بیضوی روی میدان متناهی هستند و G_T زیرگروهی از یک گروه ضربی روی میدان متناهی است. زوج‌سازی‌های دوخطی ویژگی‌های زیر را دارا می‌باشند.

- دوخطی بودن[2]: به ازای تمامی

$\forall a, b \in Z \quad و \quad P \in G_1, Q \in G_2$

داریم $e(aP, bQ) = e(P, Q)^{ab}$

- زوال‌ناپذیری[3]:

$\forall P \in G_1, P \neq O \quad \exists Q \in G_2 : e(P, Q) \neq 1$

$\forall Q \in G_2, Q \neq O \quad \exists P \in G_1 : e(P, Q) \neq 1$

- محاسبه‌پذیری[4]: به ازای همه $(P, Q) \in G_1 \times G_2$، $e(P, Q)$ قابل محاسبه است.

۲-۴. ملزومات امنیتی پروتکل‌های احراز هویت سلامت الکترونیک مبتنی بر کلمه عبور

یک طرح احراز هویت باید ویژگی‌های امنیتی زیر را تضمین کند.

۲-۴-۱. گمنامی[5]

این ویژگی بیان می‌کند که هویت کاربر از دید مهاجم مخفی باشد و مهاجم نتواند با کمک پیام‌های تبادل شده به شناسه کاربر دسترسی پیدا کند [۲۱-۲۰].

۲-۴-۲. غیر قابل‌ردیابی

این ویژگی تضمین می‌کند که سرور یا مهاجم نمی‌تواند کاربر را ردیابی کند و مقدمه این ویژگی گمنامی کاربر است [۱].

۲-۴-۳. امنیت پیشرو

این ویژگی یک پروتکل ارتباطی امن است که تضمین می‌کند، افشای کلیدهای بلندمدت[6] کاربران، امنیت کلیدهای جلسه گذشته آن‌ها را به خطر نمی‌اندازد.

۲-۴-۴. مقاوم در برابر حمله حدس کلمه عبور

این حملات به دو نوع برخط و برون‌خط تقسیم می‌شوند. حملات برون‌خط زمانی ممکن است که مهاجم کپی کلمه عبور رمزگذاری شده را از کانال ارتباطی یا از کارت هوشمند دریافت کند. در این حمله، مهاجم هزاران کلمه عبور را در هر ثانیه حدس می‌زند و با آن‌ها منطبق می‌دهد

تا زمانی که عملیات حدس زدن موفق شود [۱۴]. مهاجم همچنین می‌تواند واژه‌نامه‌های کلمه عبور از پیش تعیین‌شده را برای بهبود قابل‌توجه این روند استفاده کند [۲۲]. در حملات برخط[7] مهاجم به‌عنوان یک کاربر مجاز حدس‌های ممکن برای کلمه عبور را امتحان می‌کند تا موفق به ورود شود. حدس زدن کلمه عبور برخط دامنه محدودی دارد، زیرا برنامه‌های کاربردی تلاش‌های بی‌پایان را اجازه نمی‌دهد و کاربر را پس از چند تلاش ناموفق مسدود می‌کند، درحالی‌که در حدس زدن کلمه عبور برون‌خط چنین محدودیتی وجود ندارد [۲۳].

۲-۴-۵. مقاوم در برابر حمله تکرار[8]

در یک حمله تکرار، مهاجم، کانال ارتباطی را شنود و پیام های احراز هویت را کپی می‌کند. پیام‌های احراز هویت، که حاوی پاسخ کاربر در برابر چالش سرور هستند، در ارتباطات بعدی دوباره توسط مهاجم ارسال می‌شوند تا امکان دسترسی و سوءاستفاده از سامانه را داشته باشند. حملات تکرار نیز می توانند بر روی دسترسی به سامانه تأثیر بگذارند، زیرا مهاجم می تواند پیام‌های تکراری را به‌صورت متوالی و در یک‌زمان ارسال کند. سامانه هدف هر پیام را پردازش می‌کند تا بتواند احراز هویت کند، ازاین‌رو، سامانه مشغول شده و نمی‌تواند پاسخگوی دیگر کاربران باشد.

۲-۴-۶. مقاوم در برابر حمله دسترسی مجاز داخلی

این حمله توسط فردی که دارای دسترسی مجاز به سامانه است انجام می شود [۱]. یک فرد می تواند اطلاعات حساس از سامانه سلامت الکترونیک کاربر را سرقت و افشا کند، ازاین‌رو حریم خصوصی و گمنامی کاربر به‌راحتی توسط مهاجم به مخاطره می‌افتد. یک فرد مجاز داخلی دارای دسترسی ویژه به سامانه نیز

1- Bilinear pairing
2- Bilinearity
3- Non-degeneracy
4- Computability
5- Anonymity
6- Long term key
7- Online
8- Replay attack

می‌تواند بر یکپارچگی اطلاعات تأثیر گذاشته و پیام‌های مبادله‌ای را تغییر دهد.

۲-۴-۷. مقاوم در برابر حمله مسدود کردن سرویس

در این حمله، مهاجم تعداد زیادی از پیام‌های احراز هویت را به سرور می فرستد تا آن را مشغول کند و از ارائه خدمات به کاربران قانونی مختل کند. همان‌گونه که سرور هر بسته (قانونی یا غیرقانونی) را پردازش می کند حافظه، قدرت پردازش و پهنای باند مصرف می‌شود. تحت چنین حمله‌ای، ارسال پیام‌های دروغی تمام منابع سرور را به ظرفیت کامل خود می رساند و بنابراین، سرور نمی‌تواند درخواست‌های بیشتری را پردازش کند [۱].

۲-۴-۸. مقاوم در برابر حمله جعل هویت

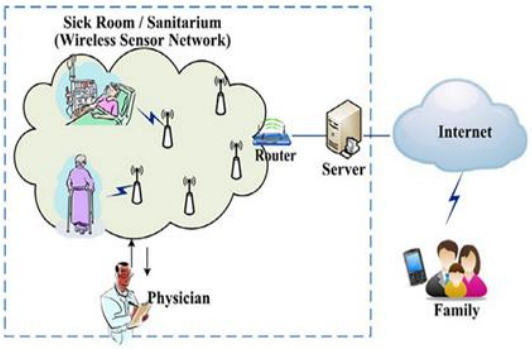
در یک حمله جعل هویت، حمله کننده، هویت یکی از اعضای مشروع (در اینجا سرور و کاربران) را برای دسترسی به سامانه سلامت الکترونیک می‌رباید. در حمله جعل هویت سرور، مهاجم هویت سرور را جعل کرده تا اطلاعات یک کاربر قانونی را با ترفندهایی به دست آورده و به سامانه دسترسی پیدا کند. در حمله جعل هویت کاربر، مهاجم هویت کاربر مشروع را برای سوءاستفاده از خدمات ارائه‌شده توسط سامانه جعل می‌کند [۱].

۲-۴-۹. مقاوم در برابر حمله کارت هوشمند به سرقت رفته

در این حمله مهاجم با سرقت کارت هوشمند کاربر مجاز سعی می‌کند با کمک تحلیل توان یا زمان اجرای الگوریتم، اطلاعات خصوصی کاربر را از کارت هوشمند به دست آورد و از این طریق به اهداف خود در طرح احراز هویت برسد.

۳. مروری بر طرح چالا

در این بخش، طرح اخیر پیشنهادشده توسط چالا و ارزیابی امنیتی آن را بیان می‌کنیم. سه موجودیت اصلی در این پروتکل شامل مرجع مورد اعتماد[1](TA)، گره‌های حسگر[2] و بیمار است. معماری سامانه در شکل (۳) نشان داده شده است. در این سناریو، بیماران در بیمارستان یا مراکز بهداشتی مجهز به دستگاه‌های پایش بی‌سیم هستند که گره‌های حسگر به‌طور مداوم موارد حیاتی بیمار را ثبت می‌کنند. ایستگاه مبنا داده‌های فیزیولوژیکی حسگرهای متصل به بیماران را به‌صورت دوره‌ای به‌هنگام‌رسانی می‌کند. این داده‌ها در سرورهای مرکز مراقبت بارگذاری می‌شوند تا توسط متخصصین پزشکی تحلیل شوند.



شکل (۳): معماری معمول سامانه مراقبت سلامت الکترونیکی در بیمارستان [۱]

برای اطمینان از دسترسی مجاز به داده‌ها و تضمین ارتباط امن، هر کاربر (کارکنان پزشکی و بیماران) باید در سامانه ثبت‌نام کند و هویتش توسط TA احراز شود. این طرح متشکل از چهار مرحله است که هر یک از آن‌ها در بخش‌های زیر آمده است.

۳-۱. مرحله راه‌اندازی سامانه

مرجع مورد اعتماد TA سامانه را با اجرای مراحل پیش رو راه‌اندازی می‌کند. گام اول: TA منحنی بیضوی $E_p(a,b)$ را بر روی یک میدان متناهی Z_p^* (که p یک عدد اول بزرگ است) انتخاب می‌کند. که در آن P یک مولد از مرتبه n روی $E_p(a,b)$ است، $s \in Z_p^*$ کلید اصلی مخفی است و همچنین داریم: $O = \mathrm{n.P}$ و $4\mathrm{a}^3 + 27\mathrm{b}^2 \neq 0 \pmod{\mathrm{p}}$

گام دوم: پس‌ازآن کلید عمومی $\mathrm{P_{pub}} = \mathrm{s_0.P}$ توسط TA محاسبه و یک تابع رمزنگاری درهم‌سازی یک‌طرفه h(.) نیز توسط TA انتخاب می‌شود.گام سوم: پروتکل چالا برای احراز هویت زیست‌سنجی از استخراج فازی بخش ۲-۳ استفاده می‌کند. گام چهارم: درنهایت پارامترهای (۱) به‌عنوان پارامترهای عمومی سامانه منتشر و $\mathrm{s_0}$ به‌صورت مخفی توسط TA نگه‌داری می‌شود.

$$\{E_p(a,b), \mathrm{p}, \mathrm{P}, \mathrm{h}(.), \mathrm{P_{pub}}, \mathrm{Gen}(.), \mathrm{Rep}(.), \mathrm{t}\} \qquad (1)$$

۳-۲. مرحله ثبت گره حسگر قبل از استقرار

همراه با راه‌اندازی سامانه ذکرشده، تمام گره‌های حسگر موردنیاز نیز در حالت برون‌خط توسط TA ثبت می‌شوند.در ادامه:گام اول. برای هر گره حسگر SN_j، یک ID منحصربه‌فرد ID_j و یک کلید خصوصی اصلی منحصربه‌فرد $mk_j \in Z_p^*$ توسط TA انتخاب می‌شود. سپس TA کلید خصوصی $S_j = \mathrm{h}(ID_j \,||\, mk_j)$ را محاسبه می‌کند. گام دوم، سپس ID_j و S_j در حافظه SN_j قبل از استقرار آن در میدان هدف ذخیره می‌شوند. TA همچنین $\{ID_j \,،\, S_j\}$را در پایگاه داده خودش، متناظر با آن گره حسگر ذخیره می‌کند.

1- Trusted Authority
2- Sensor nodes

۳-۳. مرحله ثبت کاربر

یک کاربر U_i (برای مثال، یک بیمار) پس از حضور فیزیکی در مرکز درمانی خود را به سامانه معرفی می‌کند. پس از تائید موسسه مربوطه و کسب مجوز از مدیر سامانه، در پایان این مرحله، به کاربر U_i یک کارت هوشمند امن تعلق می‌گیرد. مراحل ارائه کارت هوشمند به شرح زیر است: گام اول: U_i یک شناسه هویت ID_i و عدد تصادفی $k \in Z_p^*$ را انتخاب می‌کند. سپس $RID_i = \mathrm{h}(k \| ID_i)$ را محاسبه کرده و درخواست ثبت‌نام RID_i را از طریق یک کانال امن به TA ارسال می‌کند. گام دوم: TA به‌محض دریافت درخواست ثبت، $R_i = \mathrm{h}(RID_i \| s_0)$ را محاسبه می‌کند و آن را بر روی یک کارت هوشمند SC_i ذخیره می‌کند و سپس SC_i را از طریق یک کانال امن به U_i ارسال می‌کند.

گام سوم: کاربر پس از دریافت کارت هوشمند، کلمه عبور را انتخاب و اطلاعات زیست‌سنجی خود (در اینجا اثرانگشت) را در حسگر ترمینالی خاص اصطلاحاً پرینت می‌کند. سپس مقادیر شماره ۲ سمت کاربر محاسبه می‌شود.

$$\begin{aligned} &\mathrm{Gen}\,(Bio_i) = (\sigma_i, \tau_i)\\ &\mathrm{RPW}_i = \mathrm{h}(\mathrm{PW}_i \| \mathrm{K})\\ &\mathrm{X}_i = \mathrm{h}\,(\mathrm{RPW}_i \| \sigma_i)\\ &\mathrm{Y}_i = \mathrm{K} \oplus \mathrm{h}\,(ID_i \| \mathrm{PW}_i \| \sigma_i)\\ &R_i' = R_i \oplus \mathrm{h}\,(ID_i \| \sigma_i) \end{aligned} \quad (۲)$$

گام چهارم: کاربر U_i اطلاعات شماره ۳ را در کارت هوشمند

$$\{X_i, Y_i, Gen(.), Rep(.), \tau_i, h(.), t\} \quad (۳)$$

SC_i ذخیره و مقدار R_i را با R_i' تعویض می‌کند. درنهایت کارت هوشمند حاوی مقادیر

$\{ R_i', \mathrm{X}_i, \mathrm{Y}_i, \mathrm{Gen}\,(.), \mathrm{Rep}\,(.), \tau_i, \mathrm{h}(.), \mathrm{t} \}$ است.

۴-۳. مرحله ورود

کاربر U_i برای ورود باید مراحل زیر را طی کند. گام اول: کاربر کارت هوشمند، شناسه و کلمه عبور خود را وارد می‌کند سپس اطلاعات زیست‌سنجی خود را در ترمینال زیست‌سنجی پرینت می‌کند. گام دوم: کارت هوشمند مقادیر شماره (۴) را محاسبه کرده و بررسی می‌کند آیا تساوی $X_i' = X_i$ برقرار است.

$$\begin{aligned} &\sigma'_i = \mathrm{Rep}\,(\mathrm{Bio}_i', \tau_i\ )\\ &k' = \mathrm{Y}_i \oplus \mathrm{h}(\mathrm{ID}_i' \| \mathrm{PW}_i' \| \sigma'_i)\\ &RPW_i' = \mathrm{h}(\ \mathrm{PW}_i' \| k'\ )\\ &X_i' = \mathrm{h}(RPW_i' \| \sigma'_i) \end{aligned} \quad (۴)$$

گام سوم: اگر تصدیق موفق بود، کاربر عدد تصادفی $m \in Z_p^*$ و مهر زمانی T_i را تولید و پس از محاسبه مقادیر شماره (۵)، پیام درخواست ورود $\{ DID_i, DID_j, M_i, T_i, V_i \}$ را کامل می‌کند. درنهایت کاربر U_i پیام درخواست ورود را از طریق کانال عمومی به TA ارسال می‌کند.

$$\begin{aligned} &M_i = m.P = (M_i^x, M_i^y)\\ &N_i = m.P_{pub} = (N_i^x, N_i^y)\\ &RID_i' = \mathrm{h}\,(k' \| ID_i')\\ &DID_i = RID_i' \oplus N_i^y\\ &DID_j = ID_j \oplus N_i^y\\ &R_i^* = R_i \oplus \mathrm{h}(ID_i' \| \sigma'_i)\\ &V_i = \mathrm{h}\,(DID_i \| DID_j \| T_i \| M_i \| R_i^*) \end{aligned} \quad (۵)$$

که ID_j شناسه گره حسگر SN_j است که کاربر U_i می‌خواهد به آن دسترسی داشته باشد و (M_i^x, M_i^y) به مؤلفه محور x و مؤلفه محور y نقطه M_i از منحنی بیضوی اشاره می‌کند.

۵-۳. مرحله احراز هویت و توافق کلید

در این مرحله، TA هویت یک کاربر قانونی را تائید می‌کند و به ایجاد کلید جلسه بین یک گره حس‌گر SN_j و کاربر U_i از طریق مراحل زیر کمک می‌کند. گام اول: TA پس از دریافت پیام درخواست ورود $\{DID_i, DID_j, M_i, T_i, V_i\}$ از کاربر در زمان T_i' ابتدا صحت مهر زمانی T_i' را با شرط $T_i' - T_i \le \Delta T$ چک می‌کند، اگر برقرار بود آنگاه مقادیر (۶) را محاسبه می‌کند. TA بررسی می‌کند آیا تساوی $V_i^* = V_i$ برقرار است همچنین بررسی می‌کند ID_j^* در پایگاه داده ثبت‌نام‌شده باشد. اگر یکی از این چک‌ها به شکست منجر شود، جلسه بلافاصله منقطع می‌شود.

$$\begin{aligned} &N_{\mathrm{TA}} = \mathrm{s}_0.M_i = (N_{TA}^x, N_{TA}^y)\\ &RID_i = DID_i \oplus N_{TA}^y\\ &ID_j = DID_j \oplus N_{TA}^y\\ &\mathrm{R}_i = \mathrm{h}\,(RID_i \| \mathrm{s}_0)\\ &V_i^* = \mathrm{h}(DID_i \| DID_j \| \mathrm{T}_i \| \mathrm{M}_i \| \mathrm{R}_i) \end{aligned} \quad (۶)$$

گام دوم: TA مهر زمانی فعلی T_{TA} و مقدار شماره (۷) را محاسبه می‌کند و پیام $W_{TA}, T_{TA}, \mathrm{T}_i$ را از طریق کانال عمومی به گره حسگر SN_j ارسال می‌کند.

$$W_{TA} = h(R_i) \oplus \mathrm{h}(S_j \| T_{TA} \| \mathrm{T}_i) \quad (۷)$$

گام سوم: به‌محض دریافت پیام و بررسی صحت زمانی پیام، گره حسگر مهر زمانی فعلی T_j و مقادیر (۸) را تولید می‌کند. سپس پاسخ پیام احراز هویت را به‌وسیله کانال عمومی به کاربر ارسال می‌کند.

$$\begin{aligned} &h(R_i) = W_{TA} \oplus \mathrm{h}(S_j \| T_{TA} \| \mathrm{T}_i)\\ &SK_{ij}' = \mathrm{h}\,(ID_j \| h(R_i) \| \mathrm{h}\,(\mathrm{S}_j) \| T_i \| T_j)\\ &V_{\mathrm{SN}_j} = \mathrm{h}(SK_{ij}' \| ID_j \| T_j\ )\\ &W_j = \mathrm{h}(ID_j \| h(R_i)) \oplus \mathrm{h}(S_j) \end{aligned} \quad (۸)$$

گام چهارم: کاربر به‌محض دریافت پیام پاسخ $< W_j, V_{\mathrm{SN}_j}, T_j >$ در زمان T_j' ابتدا صحت مهر زمانی T_j' را با شرط $T_j' - T_j \le \Delta T$ چک می‌کند، اگر برقرار بود آنگاه مقادیر شماره (۹) را محاسبه می‌کند. U_i سپس بررسی می‌کند

آیا تساوی $V^*_{SN_j} = V_{SN_j}$ برقرار است یا خیر، اگر برقرار بود، کاربر ارتباطی امن را با گره حسگر SN_j به‌وسیله کلید جلسه SK'_{ij} آغاز می‌کند (شکل ۴).

$$h(S_j) = W_j \oplus h(ID_j || h(R^*_j)) \quad (۹)$$

$$SK'_{ij} = h(ID_j || h(R^*_i) || h(S_j) || T_i || T_j)$$

$$V^*_{SN_j} = h(SK'_{ij} || ID_j || T_j)$$

شکل (۴): مرحله ورود و احراز هویت طرح چالا [۱]

۳-۶. مرحله تغییر و به‌روزرسانی کلمه عبور و زیست‌سنجی

این مرحله تنها سمت کاربر اجرا می‌شود تا بار محاسباتی و ارتباط سرور بالا نرود. ابتدا کاربر نام کاربری، کلمه عبور و اطلاعات زیست‌سنجی قبلی خود را در اختیار سامانه قرار می‌دهد و سامانه با چک کردن اطلاعات احراز هویت او طبق روابط شماره (۱۰)، وضعیت کاربر مجاز را مشخص می‌کند اگر کاربری غیرمجاز بود ارتباط قطع می‌شود و در غیر این صورت کارت هوشمند کلمه عبور و اطلاعات جدید زیست‌سنجی کاربر را دریافت می‌کند و پس از محاسبات شماره (۱۱) مقادیر جدید شماره (۱۲) را در کارت هوشمند جایگزین می‌شوند.

$$\sigma_i^{old} = Rep(\mathrm{Bio}_i^{old}, \tau_i)$$
$$K' = Y_i \oplus h(ID_i \,||PW_i^{old}||\sigma_i^{old})$$
$$RPW_i^{old} = h(PW_i^{old} \,||\, K')$$
$$X_i^{old} = h(PW_i^{old} \,||\, \sigma_i^{old})$$
$$\text{Check if } X_i^{old} = X_i \text{ ?} \qquad (۱۰)$$

$$\mathrm{Gen}(\mathrm{Bio}_i^{new}) = (\sigma_i^{new}), \tau_i^{new})$$
$$PW_i^{new} = \mathrm{h}(PW_i^{new} \,||\, K')$$
$$X_i^{new} = \mathrm{h}(RPW_i^{new} || \,\sigma_i^{new})$$
$$Y_i^{new} = K' \oplus \mathrm{h}(\mathrm{ID}_i||PW_i^{new}|| \,\sigma_i^{new})$$
$$R_i^{new} = (R_i' \oplus \mathrm{h}(\mathrm{ID}_i \,||\, \sigma_i^{old})) \oplus$$
$$\mathrm{h}(\mathrm{ID}_i|| \,\sigma_i^{new}) = R_i \oplus \mathrm{h}((\mathrm{ID}_i|| \,\sigma_i^{new}) \qquad (۱۱)$$

$$\{R_i', X_i^{new}, Y_i^{new},$$
$$\mathrm{Gen}(.), \mathrm{Rep}(.), \tau_i, \mathrm{h}(.), \mathrm{t}\} \qquad (۱۲)$$

۳-۷. مرحله اضافه شدن برخط گره حسگر جدید

گاهی نیاز است به یک شبکه از پیش استقراریافته گره حسگر جدیدی اضافه کنیم، زیرا ممکن است تعدادی از گره‌های حسگر مشکل توان باتری پیدا کنند و یا توسط مهاجم دزدیده شوند. برای افزودن گره حسگر SN_j^{new} به شبکه مراحل زیر سپری می‌شود.

گام اول: برای گره حسگر SN_j^{new} یک ID منحصربه‌فرد ID_j^{new} و یک کلید سری اصلی منحصربه‌فرد $mk_j^{new} \in Z_p^*$ توسط TA انتخاب می‌شود. سپس TA کلید خصوصی

$S_j^{new} = \mathrm{h}(ID_j^{new}|| \,mk_j^{new})$ را محاسبه می‌کند.

گام دوم: سپس ID_j^{new} و S_j^{new} در حافظه SN_j^{new} قبل از استقرار آن در میدان هدف ذخیره می‌شوند. TA همچنین ID_j^{new} و S_j^{new} را در پایگاه داده خودش، متناظر با آن گره حسگر ذخیره می‌کند.

گام سوم: TA در پیامی ID_i^{new} را پخش[1] می‌کند و همه کاربران را از وجود گره حسگر جدید مطلع می‌کند تا بتوانند به گره حسگر جدید دسترسی داشته باشند.

۳-۸- مرحله اضافه شدن کاربر جدید

در شبکه‌های حسگر بی‌سیم سلامت، ممکن است کاربر ثبت‌شده در یک بازه زمانی به سامانه وارد نشده و حال بخواهد از سامانه استفاده کند و یا یک کاربر جدید بخواهد وارد سامانه شود. در این مرحله تمامی مراحل ثبت کاربر باید اجرا شود و اگر کاربر قبلاً ثبت‌شده باشد اطلاعات جدید او در سمت سرور و کارت هوشمند جایگزین شود.

۳-۹. تحلیل ضعف‌های امنیتی طرح چالا

در این بخش ما برخی از ایرادات امنیتی طرح چالا را مطرح خواهیم کرد.

۳-۹-۱. حمله دسترسی مجاز داخلی

پیش‌فرض طرح‌های احراز هویت TA یا ابر را یک موجودیت کنجکاو و البته صادق در نظر می‌گیرند [۲۵-۲۴] که تنها وظیفه کمک به کاربران سامانه برای ارتباط امن را دارد، بنابراین پروتکل باید به‌گونه‌ای طراحی شود که TA مقادیر کلیدهای جلسه در ارتباطات را نتواند به دست آورد. می‌توان نشان داد که در پروتکل چالا مرجع مورد اعتماد TA توانایی تولید کلید جلسه بین کاربر و گره حسگر SK_{ij}' را دارا است.

$$SK_{ij}' = \mathrm{h}\,(ID_j||\mathrm{h}(R_i)||\,\mathrm{h}(\mathrm{S}_j)||T_i\,||T_j)$$

الف - همان‌طور که در مرحله ۳-۲ مطرح شد TA $\{ID_j, S_j\}$ را در پایگاه داده خودش، متناظر با آن گره حسگر ذخیره می‌کند، پس دو مؤلفه ID_j و $\mathrm{h}(S_j)$ از کلید جلسه را دارد.

ب – TA، $R_i = h(RID_i|| \,s_0)$ را در مرحله ۳-۳ می‌سازد. T_i و T_j نیز در شبکه موجود است . پس TA توانایی ساخت کلید جلسه بین کاربر و گره حسگر را دارا است که باعث دسترسی‌های غیرمجاز داخلی می‌شود.

۳-۹-۲. قابل‌ردیابی

مهاجم A با شنود کانال پیام کاربر به TA در مرحله ۳-۴ را دریافت می‌کند. که شامل مقادیر DID_i, DID_j است. حال مهاجم A با عملیات (۱۳) به مقادیری دست پیدا می‌کند که در تمام ارتباطات برای کاربری خاص ثابت هستند، لذا همین مسئله باعث ردیابی کاربر و ارتباطات او می‌شود.

$$DID_i \oplus DID_j = RID_i' \oplus ID_j$$

از مرحله ۳-۴ داشتیم.

$$DID_i = RID_i' \oplus N^y{}_i \qquad (۱۳)$$
$$DID_j = ID_j \oplus N^y{}_i$$

$RID_i' \oplus \mathrm{ID}_j$ در همه مراحل مقدار ثابتی است.

۳-۹-۳. امنیت پیشرو

الف - فرض می‌کنیم مهاجم A کلیدهای بلندمدت سمت سرور TA را سرقت کرده است . حال مهاجم با شنود کانال پیام T_i, T_j را دریافت می‌کند. سپس مهاجم A با محاسبات شماره (۱۲) توانایی ساخت کلید جلسه را دارد.

در امنیت پیشرو فرض بر این است که مهاجم نتواند با ترکیب کلیدهای بلندمدت و اطلاعات شنود شده از کانال عمومی، کلیدهای جلسه گذشته را بسازد. در محاسبات شماره ۱۴ نشان می‌دهیم که مهاجم چگونه کلیدهای جلسه گذشته SK_{ij}' بین کاربر U_i و گره حسگر SN_j را می‌سازد.

1- Broadcast

$$
\begin{aligned}
&N_{TA} = S_0 \,.\, M_i \\
&N_{TA} = (N_{TA}^x, N_{TA}^y) \\
&RID_i = DID_i \oplus N_{TA}^y \\
&R_i = h\,(RID_i \,||\, s_0\,) \\
&ID_j = DID_j \oplus N_{TA}^y \\
&N_{TA}^y = \mathrm{h}\,(ID_j||\mathrm{h}(R_i)||\,\mathrm{h}(S_j)||T_i\,||T_j)
\end{aligned}
\qquad (۱۴)
$$

۳-۹-۴. عدم احراز هویت TA توسط حسگر

پروتکل چالا احراز هویت TA توسط گره حسگر SN_j را پشتیبانی نمی‌کند. در پروتکل چالا هیچ‌گونه بررسی از سمت گره حسگر برای تشخیص صحت پیام‌های ارسالی از طرف TA وجود ندارد. TA پیام $< W_{TA}, T_{TA}, T_i >$ را به گره حسگر SN_j می‌فرستد و حسگر بدون هیچ بررسی‌ای، محاسبات خود را انجام داده و به کاربر ارسال می‌کند.

۴. طرح پیشنهادی

ما در این مقاله با ارائه راه‌حل‌هایی برای رفع ضعف‌های امنیتی عنوان‌شده در بخش ۳-۹ روی پروتکل چالا، این طرح را بهبود داده و پروتکلی امن و قابل‌اثبات ارائه می‌دهیم. پروتکل چالا می‌تواند با تغییر یک گام در مرحله ورود ۳-۴ و تغییر مرحله احراز هویت ۳-۵ در مقابل حملات ذکرشده مقاوم شود.

همچنین در طرح چالا، TA در مرحله ثبت گره حسگر به ازای هر حسگر یک کلید تصادفی mk_j انتخاب می‌کند و کلید اصلی TA هیچ نقشی در تولید کلیدهای خصوصی حسگرها ندارد. لذا این مرحله از طرح چالا کاملاً ناکارآمد است.

بنابراین مراحل ۳-۱، ۳-۳، ۳-۶، ۳-۷ و ۳-۸ مشابه پروتکل چالا بدون تغییر باقی می‌مانند و بخش‌های ۳-۲، ۳-۴ و ۳-۵ تغییر می‌کنند.

۴-۱. ارائه طرح پیشنهادی

۴-۱-۱. مرحله ثبت گره حسگر قبل از استقرار

تمام گره‌های حسگر موردنیاز نیز در حالت برون‌خط توسط TA ثبت می‌شوند. بدین منظور دو گام توسط TA انجام می‌شود. گام اول : برای هر گره حسگر SN_j، یک ID منحصربه‌فرد ID_j توسط TA انتخاب می‌شود. سپس TA کلید خصوصی $S_j = \mathrm{h}(ID_j \,||\, s_0\,)$ را محاسبه می‌کند. گام دوم : سپس ID_j و S_j در حافظه SN_j قبل از استقرار آن در میدان هدف ذخیره می‌شوند. TA همچنین $\{ID_j\}$را در پایگاه داده خودش، متناظر با آن گره حسگر ذخیره می‌کند.

۴-۱-۲. مرحله ورود جدید

تمامی مراحل مشابه مرحله ورود قدیم ۳-۴ اجرا می‌شود به‌غیراز ساخت DID_j که به‌صورت مقابل تغییر می‌یابد.

$$DID_j = ID_j \oplus N_i^x$$

کافی است مؤلفه M_i^y را جایگزین مؤلفه M_i^x کنیم تا مهاجم نتواند به‌وسیله عملیات XOR بیتی به مقداری ثابت برسد و این‌گونه پروتکل ویژگی غیر قابل‌ردیابی بودن را ارضا می‌کند.

۴-۱-۳. مرحله احراز هویت و توافق کلید جدید

گام اول: در این مرحله مشابه مرحله ۳-۵ پس از بررسی صحت مهر زمانی، TA بررسی می‌کند آیا تساوی $V_i^* = V_i$ برقرار است یا خیر. با این تفاوت که برای ساخت ID_j از رابطه زیر کمک می‌گیرد.

$$\mathrm{ID}_j = \mathrm{DID}_j \oplus N_{TA}^x$$

گام دوم: در این گام نیز مشابه گام دوم مرحله ۳-۵ TA مهر زمانی فعلی T_{TA} و مقادیر شماره (۱۵) را محاسبه می‌کند سپس پیام $W_{TA}, H_{TA}, M_i, T_{TA}, \mathrm{T}_i$ را از طریق کانال عمومی به گره حسگر SN_j ارسال می‌کند.

$$W_{TA} = h(R_i) \oplus h(S_j \,||M_i^x||\, M_i^y||\, T_{TA}||T_i)\,. \qquad (۱۵)$$

$$H_{TA} = h(W_{TA}||S_j||\, T_{TA}||T_i)$$

ما برای مقابله با حمله شخص مجاز داخلی مؤلفه‌های (M_i^x, M_i^y) را در ساخت W_{TA} گنجاندیم و همچنین M_i را همراه با پیام منتقل می‌کنیم.

در پروتکل جدید یک مرحله جدید نیز برای احراز هویت TA توسط SN_j اضافه کردیم. TA مقدار H_{TA} را می‌سازد و به همراه پیام به SN_j منتقل می‌کند تا با بررسی این مقدار TA را احراز هویت کند.

گام سوم : به‌محض دریافت پیام توسط SN_j و بررسی صحت زمانی پیام، SN_j با محاسبات شماره (۱۶) H_{TA}^* را محاسبه کرده سپس بررسی می‌کند آیا تساوی $H_{TA}^* = H_{TA}$ برقرار است یا خیر، اگر برقرار بود SN_j مهر زمانی فعلی T_j و مقادیر شماره (۱۷) را محاسبه می‌کند. کلید جلسه sk_{ij} را ذخیره می‌کند، سپس پاسخ پیام احراز هویت $< W_j, V_{SNj}, B_j, T_j >$ را از طریق کانال عمومی به کاربر ارسال می‌کند.

$$H_{TA}^* = h(W_{TA}||S_j||\, T_{TA}||T_i) \qquad (۱۶)$$

$$h(R_i) = W_{TA} \oplus h(S_j \,||M_i^x||\, M_i^y||\, T_{TA}||T_i)\,, \qquad (۱۷)$$

$$\text{Choose } b_j \in Z_p^*.$$

$$b_j.p = B_j = (B^x{}_j, B^y{}_j)$$

$$sk_{ij} = \mathrm{h}(b_j.M_i||ID_j|\ h(R_i)\ ||h(S_j)||T_i||T_j)$$

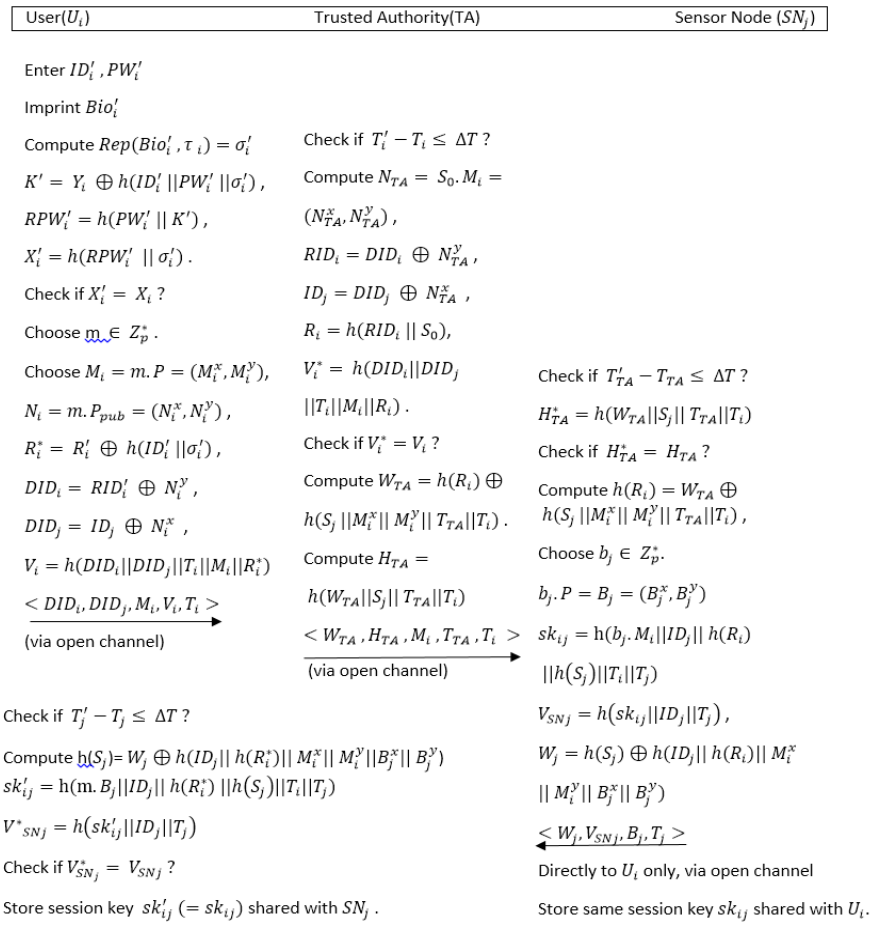
$$V_{SNj} = h(sk_{ij}||ID_j||T_j)\,,$$

$$W_j = h(S_j) \oplus h(ID_j||h(R_i)$$

$M_i^x||M_i^y \,||\, B^x{}_j||\, B^y{}_j)$

گام چهارم : کاربر به‌محض دریافت پیام پاسخ

$< W_j, V_{SN_j}, B_j, T_j >$ در زمان T_j' ابتدا صحت مهر زمانی T_j' را با شرط $T_j' - T_j \leq \Delta T$ چک می‌کند، اگر برقرار بود آن‌گاه مقادیر شماره (۱۸) را محاسبه می‌کند.کلید جلسه را ذخیره می‌کند U_i سپس بررسی می‌کند آیا تساوی $V_{SN}^* = V_{SN}$ برقرار است یا خیر، اگر برقرار بود، کاربر ارتباطی امن را با گره حسگر SN_j به‌وسیله کلید جلسه SK_{ij}' آغاز می‌کند (شکل ۵).



شکل (۵): مرحله ورود و احراز هویت طرح پیشنهاد

$$h(S_j) = W_j \oplus h(ID_j|| h(R_i{}^*)|| M_i^x||M_i^y||B_j^x||B_j^y)$$

$$SK_{ij}' = h(m.B_j||ID_j|| h(R_i^*) ||h(S_j)||T_i||T_j) \qquad (۱۸)$$

$$V_{SN_j}^* = h(SK_{ij}'|| ID_j|| T_j)$$

۵. تحلیل امنیت و کارآمدی

در بخش ۵-۱ نشان خواهیم داد که پروتکل پیشنهادی در مقابل حملات ذکرشده و دیگر حملات مقاوم است. در ۵-۲ مقایسه عملکرد پروتکل پیشنهادی با دیگر پروتکل‌ها آورده شده است. در ۵-۳ نیز تحلیل طرح پیشنهادی با کمک ابزار پروویریف ارائه‌شده است.

۵-۱. بررسی ویژگی‌های امنیتی

در این قسمت نشان خواهیم داد که پروتکل پیشنهادی ویژگی‌های امنیتی ذکرشده در بخش ۲-۵ را دار است.

۵-۱-۱. مقاوم در برابر حمله دسترسی مجاز داخلی

مهاجم که یک کاربر مجاز در سمت TA است به اطلاعات TA ازجمله کلید خصوصی TA، اطلاعات احراز هویت کاربر U_i و اطلاعات ثبت گره حسگر S_j $\{s_0, RID_i, ID_j, S_j\}$ دسترسی دارد. TA توانایی ساخت، $R_i = h(RID_i|| s_0)$ را در مرحله ۳-۳ دارد.

بااین‌حال مهاجم توانایی ساخت کلید جلسه بین کاربر و گره حسگر را به دلیل وجود مؤلفه $b_j.M_i$ که تنها توسط گره حسگر و کاربر ساخته می‌شود را ندارد.

$$sk_{ij} = \mathrm{h}(b_j.M_i||ID_j||\, h(R_i)\, ||h(S_j)||T_i||T_j)$$

با فرض این‌که کارت هوشمند کاربر پس از احراز هویت دزدیده شود، مهاجم توانایی دریافت اطلاعات ذخیره‌شده $\{R'_i, X_i, Y_i, \tau_i\}$ در کارت هوشمند SC_i را دارد، بااین‌حال توانایی ساخت PW_i یا ID_i کاربر را ندارد، زیرا حدس ID_i نیازمند دانستن کلید مخفی k است که با اطلاعات موجود ساخته نمی‌شود و در کارت هوشمند هم ذخیره نشده است. همچنین حدس PW_i نیازمند مقادیر $\mathrm{K}, \sigma_i, ID_i$ است که با توجه به عملیات درهمسازی یک‌طرفه $H(.)$ امکان‌پذیر نیست.

۵-۱-۲. مقاوم در برابر حمله جعل هویت

فرض کنیم مهاجمی که قصد جعل هویت کاربر را دارد با شنود کانال به پیام ورود کاربر $< DID_i, DID_j, M_i, V_i, T_i >$ دست‌یافته و تلاش می‌کند با ساخت پیام ورود خود را کاربری مجاز معرفی کند. مهاجم برای ساخت M_i, DID_i, DID_j باید یک عدد تصادفی $\mathrm{m}' \in Z_p^*$ انتخاب کند که این دانش تنها مختص کاربر U_i است. پس مهاجم قادر به جعل کاربر نیست.

مهاجمی که قصد جعل هویت گره حسگر SN_j را دارد کانال پیام $< W_j, V_{SNj}, B_j, T_j >$ را شنود و سعی دارد با ساخت پیام پاسخ، خود را گره مجاز معرفی کند. مهاجم برای ساخت W_j, V_{SN_j}, B_j باید یک عدد تصادفی $b_j \in Z_p^*$ انتخاب کند که این دانش تنها مختص گره حسگر SN_j است، پس مهاجم قادر به جعل گره حسگر نیست.

مهاجمی که قصد جعل هویت مرجع مورد اعتماد TA را دارد پیام $< W_{TA}, H_{TA}, M_i, T_{TA}, T_i >$ را شنود کرده و سعی در ساخت پیام جعلی دارد. مهاجم برای ساخت پیام جعلی نیازمند مقادیر $h(R_i)$ و $R_i = h(RID_i \,||\, s_0)$ است که این دانش به دلیل مخفی بودن s_0 قابل کسب نیست، پس مهاجم قادر به جعل هویت سرور نیست. بنابراین پروتکل در برابر حمله دسترسی مجاز داخلی مقاوم است.

۵-۱-۳. مقاوم در برابر حمله حدس کلمه عبور برون‌خط

با فرض دست‌یابی مهاجم به اطلاعات ذخیره‌شده کاربر در کارت هوشمند $\{R'_i, X_i, Y_i, Gen(.), Rep(.), \tau_i, h(.), t\}$ از نظر محاسباتی دست‌یابی به نام کاربری و کلمه عبور و دیگر مقادیر به دلیل یک‌طرفه بودن h(.) امکان‌پذیر نیست. به‌عبارت‌دیگر مهاجم با در اختیار داشتن مقادیر X_i, Y_i و R'_i که:

$\mathrm{X}_i = \mathrm{h}\,(\mathrm{RPW}_i \,||\sigma_i)$

$\mathrm{Y}_i = \mathrm{K} \oplus \mathrm{h}\,(ID_i||\,\mathrm{PW}_i \,||\,\sigma_i\,)$

$R'_i = R_i \oplus \mathrm{h}\,(ID_i||\,\sigma_i)$

هستند، به علت امن بودن تابع درهم‌ساز و نداشتن مقدار خصوصی K توانایی محاسبه کلمه عبور کاربر را ندارد.

۵-۱-۴. مقاوم در برابر حمله کارت هوشمند به سرقت رفته

فرض کنید کاربر کارت هوشمند خود را گم‌کرده است یا مهاجم آن را از کاربر سرقت کرده است، مهاجم در صورت دستیابی به کارت هوشمند، اطلاعات ذخیره‌شده در آن $\{R'_i, X_i, Y_i, Gen(.), Rep(.), \tau_i, h(.)\}$ را استخراج می‌کند اما به دلیل یک‌طرفه بودن h(.) دستیابی به مقادیر PW_i, ID_i و K امکان‌ناپذیر نیست. بنابراین مهاجم با به دست آوردن اطلاعات ذخیره‌شده در کارت هوشمند نه به کلمه عبور و نه به شناسه کاربر دست میابد.

۵-۱-۵. مقاوم در برابر حمله مسدود کردن سرویس

واردکردن نام کاربری، کلمه عبور و اطلاعات زیست‌سنجی نادرست به‌دفعات زیاد در یک بازه زمانی خاص توسط کاربر مجاز می‌تواند کیفیت پاسخگویی سامانه را کاهش دهد. برای مقاومت در برابر این حمله از مهر زمانی استفاده‌شده است. همچنین برای جلوگیری از این حمله کارت هوشمند کاربر در این پروتکل با بررسی تساوی $X'_i = ?\ X_i$ در سمت کاربر از ارسال اطلاعات نادرست به سرور جلوگیری می‌کند. به‌عبارت‌دیگر مقدار $\mathrm{X}_i = \mathrm{h}\,(\mathrm{RPW}_i \,||\sigma_i)$ در حافظه کارت هوشمند کاربر ذخیره می‌شود و به ازای هر درخواست کاربر برای ورود و اتصال به شبکه پس از واردکردن نام کاربری، کلمه عبور و اطلاعات زیست‌سنجی، کارت هوشمند کاربر مقدار X'_i را می‌سازد و با X_i مقایسه می‌کند. اگر تساوی نادرست بود ارتباط قطع می‌شود، بنابراین مهاجم نمی‌تواند با واردکردن چندین پیام احراز هویت نادرست بار محاسباتی سرور را تحت شعاع قرار دهید لذا این پروتکل در برابر این حمله مقاوم است.

۵-۱-۶. مقاوم در برابر حمله تکرار

مهاجم نمی‌تواند پیام‌های شنود شده از کانال را باز ارسال کند زیرا در تمام پیام‌ها زمان T قیدشده است و به‌محض دریافت پیام توسط طرف مقابل ارتباط ابتدا اختلاف‌زمانی بررسی می‌شود. بنابراین این پروتکل در برابر این حمله مقاوم است.

۵-۱-۷. احراز هویت دوطرفه

کاربر U_i و گره حسگر SN_j همدیگر را به کمک TA و با استفاده از $V_i = h(DID_i||DID_j||T_i||M_i||R_i^*)$ و $V_{SN_j} = h(sk_{ij}||ID_j||T_j)$ احراز هویت می‌کنند.

همچنین برای احراز هویت بین TA و SN_j سرور مقدار $H_{TA} = h(W_{TA}||S_j||\, T_{TA}||T_i)$ را می‌سازد و به همراه پیام به SN_j

منتقل می‌کند تا SN_j با بررسی این مقدارTA را احراز هویت کند.

۵-۱-۸. گمنامی

شناسه کاربری ID_i در تمامی ارتباطات مخفی است و در هیچ پیامی به‌صورت مستقیم استفاده‌نشده است. علاوه بر این $DID_i = RID_i' \oplus N_i^y$ در هر مرحله یکتا است، زیرا $m \in Z_p^*$عددی تصادفی است که در هر مرحله توسط کاربر برای ساخت N_i^y استفاده می‌شود پس DID_i قابل‌ردیابی نیز نیست.

بنابراین گمنامی کاربر در این پروتکل تضمین می‌شود.

۵-۲. مقایسه عملکرد

مقایسه الزامات امنیتی و مقاومت در برابر حملات مذکور با پروتکل‌های دیگر در جدول ۲ ذکرشده است و همچنین مقایسه بار محاسبات پروتکل پیشنهادی با پروتکل‌های دیگر در جدول ۳ ذکرشده است.

جدول (۲): مقایسه ویژگی‌های امنیتی

	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}	I_{13}	I_{14}	I_{15}
لی [۲]	×	×	×	×	√	×	×	×	√	×	×	×	√	×	×
وُو [۱۶]	√	√	√	√	×	√	×	√	√	×	√	×	×	×	×
ارشد [۲۳]	√	√	√	√	√	√	√	√	√	√	√	×	√	√	×
چالا [۱]	×	×	√	√	√	×	√	√	√	×	√	√	√	√	√
پروتکل ما	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

جدول (۳): زمان تقریبی موردنیاز برای توابع مختلف [۶]

نماد	توضیح	زمان تقریبی محاسبه (ثانیه)
T_h	تابع درهم‌ساز	0.00032
T_{ecm}	منحنی بیضوی	0.0171
T_{sym}	رمزنگاری و رمزگشایی متقارن	0.0056
T_{inv}	معکوس پیمانه‌ای	0.00004275
T_m	ضرب پیمانه‌ای	0.00001425
T_{bp}	زوج سازی دوخطی	0.0045
T_{fe}	عملیات استخراج فازی	0.0171

۵-۲-۱. مقایسه امنیتی

مقایسه الزامات امنیتی و مقاومت در برابر حملات محتمل بین پروتکل پیشنهادی و تعدادی از پروتکل‌های ارائه‌شده اخیر مثل پروتکل لی [۲]، پروتکل وُو [۱۶]، پروتکل ارشد[1] [۲۳] و پروتکل چالا [۱] در جدول (۲) ذکرشده است. این مقایسه نشان می‌دهد که پروتکل پیشنهادی ما نسبت به طرح‌های مشابه ویژگی‌های امنیتی بیشتری را برآورده می‌کند.

۵-۲-۲. مقایسه بار محاسبات

در این بخش ما مقایسه‌ای بین پروتکل خود و تعدادی از پروتکل‌های ارائه‌شده اخیر مانند پروتکل لی [۲]، پروتکل وُو [۱۶]، ارشد [۲۳]، جیانگ [۳] و پروتکل چالا [۱] انجام می‌دهیم. زمان تقریبی موردنیاز برای اجرای توابع مختلف و نمادهای آن‌ها در جدول (۳) شرح داده شده است. زمان محاسبه توابع خم بیضوی، استخراج فازی و توابع دیگر ذکرشده برای تعدادی از پروتکل‌های اخیر در جدول (۴) به استناد محاسبات مقاله چالا آورده شده است. ما پروتکل پیشنهادی را با مقالات مشابه در مراحل ورود و احراز هویت مقایسه کردیم. جدول (۴) به‌وضوح نشان می‌دهد که پروتکل ما به توجه به‌اضافه شدن مرحله احراز هویت دوطرفه و وجود بار محاسباتی گره حسگر، افزایش زمان چشمگیری نسبت به طرح چالا ندارد و اندک زمان اضافه‌شده با توجه به ارتقای امنیت قابل‌قبول است.

1- Arshad

I_1: گمنامی کاربر؛ I_2: حمله دسترسی مجاز داخلی؛ I_3: حمله حدس کلمه عبور برون‌خط؛ I_4: حمله کارت هوشمند به سرقت رفته؛ I_5: حمله منع سرویس؛ I_6: امنیت پیشرو؛ I_7: حمله جعل هویت؛ I_8: حمله مهاجم میانی (شنود)؛ I_9: حمله تکرار؛ I_{10}: احراز هویت دوطرفه؛ I_{11}: توافق کلید جلسه؛ I_{12}: گم‌شدن یا دزدیدن کارت هوشمند لغو شده؛ I_{13}: مرحله تغییر کلمه عبور مستقل از TA؛ I_{14}: پشتیبانی از به‌روزرسانی زیست‌سنجی؛ I_{15}: پشتیبانی از مرحله اضافه شدن گره حسگر پویا

جدول (۴): مقایسه بار محاسباتی هنگام اجرای مرحله ورود و احراز هویت

پروتکل	سمت کاربر	سمت سرور(TA)	سمت گره حسگر	بار محاسباتی کلی
لی [۲]	$2T_{ecm} + 3T_h + 1T_{bp}$	$1T_h + 2T_{bp}$	$3T_h + 1T_{bp}$	$2T_{ecm} + 7T_h + 4T_{bp} \approx 0.54444\ s$
جیانگ [۳]	$6T_h + 1T_{ecm} + 1T_{fe}$	$2T_{ecm}+5T_h + 2T_{sym}$	-	$3T_{ecm} + 1T_{fe} + 11T_h + 2T_{sym} \approx 0.08312s$
وُو [۱۶]	$2T_{ecm} + 2T_{sym} + 5T_h + 1T_{fe}$	$2T_{ecm} + 2T_{sym} + 6T_h$	-	$4T_{ecm} + 11T_h + 1T_{fe} + 4T_{sym} \approx 0.10022\ s$
ارشد [۲۳]	$2T_{ecm} + 8T_h + 1T_m$	$2T_{ecm} + 7T_h + 1T_m + 1T_{inv}$	-	$4T_{ecm} + 15T_h + 2T_m + 1T_{inv} \approx 0.07327\ s$
چالا [۱]	$2T_{ecm} + 10T_h + 1T_{fe}$	$1T_{ecm} + 4T_h$	$5T_h$	$3T_{ecm} + 19T_h + 1T_{fe} \approx 0.07448\ s$
پروتکل ما	$2T_{ecm} + 10T_h + 1T_{fe}$	$1T_{ecm} + 5T_h$	$6T_h + 1T_{ecm}$	$4T_{ecm} + 21T_h + 1T_{fe} \approx 0.09222\ s$

۵-۳. نرم‌افزار پروورِیف

پروورِیف یک ابزار برای تجزیه و تحلیل خودکار پروتکل های رمزنگاری است[۲۷-۲۶]. این نرم افزار از سیستم های رمزنگاری شامل: رمزگذاری متقارن و نامتقارن، امضاهای دیجیتال، توابع چکیده‌ساز و اثبات دانایی صفر پشتیبانی می‌کند. پروورِیف قادر به اثبات ویژگی‌های دستیابی، ادعاهای متقابل و همبستگی مشاهداتی می‌باشد. این قابلیت ها به ویژه برای امنیت کامپیوتر مفید هستند، زیرا آنها اجازه تجزیه و تحلیل خصوصیات پنهان کاری و احراز هویت را می دهند. علاوه بر این، خواص در حال ظهور مانند حفظ حریم خصوصی، قابلیت ردیابی و قابل اطمینان بودن نیز می تواند مورد توجه قرار گیرد. علاوه بر این، این ابزار قادر به بازسازی حمله می باشد: هنگامی که یک ویژگی را نمی توان ثابت کرد، پروورِیف تلاش می‌کند تا یک ردیابی اجرایی که ویژگی مورد نظر را جعل می کند، بازسازی کند.

پروورِیف نرم‌افزاری برای اثبات محرمانه بودن شرایط در یک پروتکل است. همچنین این نرم‌افزار قادر به ارائه ردیابی حمله است. به‌عنوان مثال یک ردیابی بسیار کوتاه به‌صورت زیر نشان داده می‌شود:

out(c, ˜M) with ˜M = RSA at {1}

که نشان می‌دهد که در مکان $\{1\}$ علت اصلی دسترسی مهاجم رخ داده است.

شرح شبیه‌سازی و خروجی طرح پیشنهادی با نرم‌افزار پروورِیف در ضمیمه الف آورده شده است.

۵-۴. مقایسه هزینه مخابراتی

در این بخش سربار مخابراتی طرح پیشنهادی را با طرح‌های مشابه مقایسه می‌کنیم. فرض کنید شناسه کاربر، شناسه گره حسگر، اعداد تصادفی، مهر زمانی، تابع درهم‌ساز (مثلاً SHA-1) و نقاط روی خم بیضوی به ترتیب ۱۲۸ بیت، ۱۶ بیت، ۱۲۸ بیت، ۳۲ بیت، ۱۶۰ بیت و ۱۶۰ بیت است [۱]. در جدول ۵ هزینه مخابراتی طرح پیشنهادی را با طرح چالا مقایسه شده است. تعداد بیت‌های جدول (۷)، از مجموع طول بیت‌های پیام‌های تبادل شده در پروتکل محاسبه شده‌اند. در طرح پیشنهادی، این پیام‌ها عبارتند از $\{DID_i, DID_j, M_i, T_i, V_i\}$، $\{W_{TA}, H_{TA}, M_i, T_{TA}, T_i\}$ و $\{W_j, V_{SNj}, B_j, T_j\}$ که مجموع طول بیت آن‌ها ۱۵۸۴ بیت می‌شود. همان‌طور که در جدول (۷) مشخص است هزینه مخابراتی طرح پیشنهادی از طرح چالا کمی بیشتر است که به دلیل ارتقای ویژگی‌های امنیتی قابل‌قبول است.

جدول (۵): مقایسه هزینه مخابراتی

پروتکل	تعداد پیام‌ها	تعداد بیت‌ها
لی [۲]	۴	۱۴۰۸
وُو [۱۶]	۲	۱۷۱۲
ارشد [۲۳]	۳	۱۷۹۲
چالا [۱]	۳	۱۲۶۸
پروتکل ما	۳	۱۵۸۴

۵-۴. شبیه‌سازی طرح پیشنهادی با OPNET

در این بخش به منظور بررسی کارآیی طرح پیشنهادی شبیه‌سازی مرحله ورود و احراز هویت طرح پیشنهادی را به کمک نرم‌افزار OPNET ارائه می‌کنیم. نرم‌افزار OPNET بستر مناسبی برای مدل‌سازی، شبیه‌سازی، ارزیابی کارایی شبکه‌ها و بررسی ترافیک و زمان پاسخ‌دهی شبکه به درخواست‌ها را ارائه می‌کند. نرم‌افزار OPNET از چندین ویرایشگر مجزا تشکیل شده است که تمامی آن‌ها توسط یک ویرایشگر مرکزی به‌صورت سلسله مراتبی کنترل می‌شوند. ویرایشگر گره برای پیکربندی عملکرد و رفتار گره‌ها، ویرایشگر فرمت بسته‌ها برای تعیین نوع و چگونگی انتشار بسته‌ها در شبکه و ویرایشگر فرآیند که رفتار کلی شبکه را پیکربندی می‌کند از جمله ویرایشگرهای مهم این نرم‌افزار محسوب می‌شوند [۳۰-۲۸].

نتایج شبیه‌سازی طرح پیشنهادی با نرم‌افزار OPNET در ضمیمه ب آورده شده است.

۶. نتیجه‌گیری

در این مقاله یک طرح احراز هویت برای شبکه‌های حسگر بی‌سیم سلامت الکترونیک را بررسی و ضعف‌های امنیتی آن ارائه گردید. سپس یک طرح ارتقا یافته معرفی کردیم که ویژگی‌های امنیتی لازم برای طرح‌های احراز هویت در شبکه سلامت الکترونیک را دار است. در طرح جدید گمنامی و عدم ردیابی کاربر حفظ می‌شود، کلید جلسه تنها توسط طرفین رابطه قابل ساخت است و همچنین احراز هویت دوطرفه بین اجزای سامانه برقرار شد. همچنین با استفاده از ابزار پروورِیف امنیت طرح پیشنهادی را به‌طور صوری بررسی کردیم. درنهایت با شبیه‌سازی طرح خود با کمک OPNET عملیاتی بودن طرح پیشنهادی را نشان دادیم.

۷. مراجع

[1] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 69, pp. 534-554, 2018.

[2] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 59, pp. 250-261, 2017.

[3] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," The Journal of Supercomputing, vol. 72, no. 10, pp. 3826-3849, 2016.

[4] M. U. Aslam, A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, and B. Aslam, "A survey of authentication schemes in telecare medicine information systems," Journal of medical systems, vol. 41, no. 1, p. 14, 2017.

[5] J. Lee, S. Ryu, and K. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electronics Letters, vol. 38, no. 12, pp. 554-555, 2002.

[6] C.-H. Lin and Y.-Y. Lai, "A flexible biometrics remote user authentication scheme," Computer Standards & Interfaces, vol. 27, no. 1, pp. 19-23, 2004.

[7] W. Ku, S. Chang, and M. Chiang, "Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards," Electronics Letters, vol. 41, no. 5, pp. 240-241, 2005.

[8] M. K. Khan, and J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme," Computer Standards & Interfaces, vol. 29, no. 1, pp. 82-85, 2007.

[9] H. S. Rhee, J. O. Kwon, and D. H. Lee, "A remote user authentication scheme without using smart cards," Computer Standards & Interfaces, vol. 31, no. 1, pp. 6-13, 2009.

[10] H.-S. Kim, S.-W. Lee, and K-.Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," ACM SIGOPS Operating Systems Review, vol. 37, no. 4, pp. 32-41, 2003.

[11] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," ACM SIGOPS Operating Systems Review, vol. 38, no. 2, pp. 73-75, 2004.

[12] C. L. Chen, C. C. Lee, and C. Y. Hsu, "Mobile device integration of a fingerprint biometric remote authentication scheme," International Journal of Communication Systems, vol. 25, no. 5, pp. 585-597, 2012.

[13] M. K. Khan, S. Kumari, and M. K. Gupta, "More efficient key-hash based fingerprint remote authentication scheme using mobile device," Computing, vol. 96, no. 9, pp. 793-816, 2014.

[14] E.-J. Yoon, and K.-Y. Yoo, “Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” The Journal of supercomputing, vol. 63, no. 1, pp. 235-255, 2013.

[15] C.-I. Fan, and Y.-H. Lin, “Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics,” IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 933-945, 2009.

[16] F. Wu, L. Xu, S. Kumari, and X. Li, “A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks,” Computers & Electrical Engineering, vol. 45, pp. 274-285, 2015.

[17] A. Irshad, and S. A. Chaudhry, “Comments on “A privacy preserving three-factor authentication protocol for e-health clouds”,” The Journal of Supercomputing, vol. 73, no. 4, pp. 1504-1508, 2017.

[18] Z. Liu, H. Seo, J. Großschädl, and H. Kim, “Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1385-1397, 2016.

[19] M. Abdorasoul, R. Saed, and R. Alireza, “A New Elliptic Curve Based Electronic Voting Protocol,” Journal Of Electronical & Cyber Defence, vol. 5, no. 2, pp. 67-74, 2017(In Persian)

[20] M. Kompara, S. H. Islam, and M. Hölbl, “A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs,” Computer Networks, vol. 148, pp. 196-213, 2019.

[21] A. Gupta, M. Tripathi, T. J. Shaikh, and A .Sharma, “A lightweight anonymous user authentication and key establishment scheme for wearable devices,” Computer Networks, vol. 149, pp. 29-42, 2019.

[22] T.-Y. Chen, C.-C. Lee, M.-S. Hwang, and J.-K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi-server environments,” The Journal of Supercomputing, vol. 66, no. 2, pp. 1008-1032, 2013.

[23] H. Arshad, and M. Nikooghadam, “Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems,” Journal of medical systems, vol. 38, no. 12, pp. 136, 2014.

[24] H. Xiong, and Z. Qin, “Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks,” IEEE transactions on information forensics and security, vol. 10, no. 7, pp. 1442-1455, 2015.

[25] S. Ji, Z. Gui, T. Zhou, H. Yan, and J. Shen, “An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services,” IEEE Access, vol. 6, pp. 69603-69611, 2018.

[26] B. Blanchet, B. Smyth, and V. Cheval, “ProVerif 1.93: Automatic cryptographic protocol verifier, user manual and tutorial,” Internet][cited June 2016], Available from: https://www. bensmyth. com/publications/20-١٠ProVerif-manualversion-1.93, 2016.

[27] B. Blanchet, "Automatic verification of security protocols in the symbolic model: The verifier proverif," Foundations of Security Analysis and Design VII, pp. 54-87: Springer, 2014.

[28] C. Cao, Y. Zuo, and F. Zhang, "Research on comprehensive performance simulation of communication IP network based on OPNET." pp. 195-197.

[29] C. Zhu, O. W. Yang, J. Aweya, M. Ouellette, and D. Y. Montuno, “A comparison of active queue management algorithms using the OPNET Modeler,” IEEE Communications Magazine, vol. 40, no. 6, pp. 158-167, 2002.

[30] K. Salah, P. Calyam, and M. Buhari, “Assessing readiness of IP networks to support desktop videoconferencing using OPNET,” Journal of Network and Computer Applications, vol. 31, no .4 , pp. 921-943, 2008.

ضمیمه الف

۱-الف. مرحله راه اندازی سامانه

در این مرحله توابع، کانال‌های مورد نیاز و متغیرهای مورد نیاز تعریف می‌شوند. مطابق شکل (۱-الف) ، در خطوط ۱ و۲، دو کانال معرفی شده است که یکی امن و دیگر عمومی می‌باشد. همچنین در ادامه عملگر XOR، توابع Gen(.) و Rep(.)، خم بیضوی و توابع چکیده‌ساز برای انواع و تعداد مختلف ورودی‌ها تعریف شده‌اند.

۲-الف. زیرفرآیند TA

در پروویریف دستورات به صورت رفت و برگشتی می‌باشند. در این بخش به توضیح فعالیت‌هایی که TA در طول اجرای پروتکل باید انجام دهد، می‌پردازیم. همانطور که اشاره شد، سرور TA در سه مرحله فعالیت می‌کند. در شکل (۲-الف) دستورات آورده شده‌اند.

ابتدا در مرحله ثبت گره حسگر، TA باید یک شناسه منحصربه‌فرد برای هر گره تولید کند، که این کار با دستور new انجام می‌شود و مشخص شده‌است که از نوع رشته‌بیت می‌باشد و همچنین مقدار S_j را محاسبه می‌کند و آن را با استفاده از دستور out از طریق کانال امن s برای گره حسگر ارسال می‌کند.

سپس در مرحله ثبت کاربر، ابتدا TA مقدار RID_i را از طریق کانال امن و با استفاده از دستور in دریافت می‌کند و سپس محاسبات لازمه را انجام می‌دهد و مقدار R_i را از طریق کانال امن ارسال می‌کند.

در مرحله ورود جدید، TA اطلاعات لازم را از طریق کانال عمومی دریافت می‌کند.

در نهایت در مرحله احراز هویت و توافق کلید، محاسبات لازمه را با استفاده از دستور let انجام می‌دهد، مهر زمانی جدید را با استفاده از دستور new تولید می‌کند و سپس اطلاعات را از طریق کانال امن ارسال می‌کند.

```
1  free c: channel.
2  free s: channel [private].
3
4
5  type biometric.
6  fun Xor(bitstring, bitstring): bitstring.
7
8  type nonce.
9  type timestamp.
10
11 fun Rep(biometric, bitstring): bitstring.
12 fun Gen(biometric): bitstring.
13
14 fun ECC(bitstring, bitstring): bitstring.
15 fun ECC1(bitstring, bitstring): bitstring.
16
17 fun L(bitstring): bitstring.
18 fun h(bitstring, bitstring): bitstring.
19 fun F(bitstring, bitstring, timestamp): bitstring.
20 fun e(bitstring, bitstring, bitstring): bitstring.
21 fun E(bitstring, bitstring, bitstring, bitstring): bitstring.
22 fun f(bitstring, bitstring, timestamp, bitstring, bitstring): bitstring.
23 fun G(bitstring, bitstring, bitstring, bitstring, bitstring, bitstring): bitstring.
24 fun l(bitstring, bitstring, bitstring, bitstring, bitstring, timestamp): bitstring.
25 fun g(bitstring, bitstring, timestamp, bitstring): bitstring.
26 fun Q(bitstring, bitstring, bitstring, timestamp, bitstring): bitstring.
27
28 free s0: bitstring [private].
29 type host.
30 free skij: bitstring [private].
```

شکل (۱-الف). دستورات مربوط به مرحله راه اندازی سامانه

```
let TA(s0: bitstring, ppub: bitstring, P: bitstring) =
      (*Sensor node registration phase*)

       new IDj: bitstring;
       let sj = h(IDj, s0) in
       out (s, (IDj, sj));
      (*user registration phase*)
       in(s, RIDi: bitstring);
       let Ri = h(RIDi, s0) in
       out (s, Ri);
       (*New login phase*)
       in (c, (DIDi: bitstring, DIDj: bitstring, Mxi: bitstring, Myi: bitstring, Ti: bitstring, vi: bitstring));
(*Authentication and key agreement phase*)
       let (NTAx: bitstring, NTAy: bitstring) = ECC1(s0,(Mxi, Myi)) in
       let RIDi = Xor(DIDi, NTAy) in
       let IDj = Xor(DIDj, NTAx) in
       let Ri = h(RIDi, s0) in
          let v1i = G(DIDi, DIDj, Ti, Mxi, Myi, Ri) in

       new TTA: timestamp;
       let WTA = Xor(L(Ri), g(sj, (Mxi, Myi), TTA, Ti)) in
       let HTA = g(WTA, sj, TTA, Ti) in
       out (s, (WTA, HTA, (Mxi, Myi), TTA,Ti)).
```

شکل (۲-الف). دستورات مربوط به زیرفرآیند TA

۳-الف. زیر فرآیند حسگر

گره‌های حسگر در دو مرحله‌ی ثبت گره حسگر قبل از استقرار و مرحله احراز هویت و توافق کلید فعالیت می‌کند. همانطور که در شکل (۳-الف) نشان داده شده‌است، در مرحله ثبت گره، اطلاعات لازم از طریق کانال امن دریافت می‌شوند. در مرحله‌ی احراز هویت و توافق کلید، اطلاعات را از طریق کانال امن و از طرف TA دریافت می‌کنند. سپس محاسبات را انجام می‌دهند و احراز هویت را انجام می‌دهد (خطوط ۸۶-۸۵)، و سپس محاسبات انجام شده را از طریق کانال عمومی ارسال می‌کند.

۴-الف. زیرفرآیند کاربر

کاربر در سه مرحله‌ی ثبت کاربر، احراز هویت و توافق کلید و تغییر و به‌روزرسانی کلمه عبور و بیومتریک نقش دارد. مانند زیرفرآیندهای قبل نیز در این قسمت نیز مانند پروتکل پیشنهادی در هر مرحله اطلاعات را دریافت می‌کند و محاسبات لازمه را انجام می‌دهد و اطلاعات مورد نیاز را ارسال می‌کند. دستورات این بخش در شکل (۴-الف) آورده شده‌است.

```
let SNj(P: bitstring, ppub: bitstring) =
       (*Sensor node registration phase*)
       in(s, (IDj: bitstring, sj: bitstring));
(*Authentication and key agreement phase*)

       in (s, (WTA: bitstring, HTA: bitstring, Mxi: bitstring, Myi: bitstring, TTA: bitstring, Ti: bitstring));
          let HTA1 = E(WTA, sj, TTA, Ti) in
          if HTA1 = HTA then
         event userauthenticated(skij);
       new Tj: timestamp;
       let Ri = Xor(WTA, E(sj, (Mxi, Myi), TTA, Ti)) in
       new bj: bitstring;
       let (Bxj: bitstring, Byj: bitstring) = ECC(bj,P) in
       let (bxj: bitstring, byj: bitstring) = ECC1(bj,(Mxi, Myi)) in
       let skij = l((bxj, byj), IDj, L(Ri), L(sj), Ti, Tj) in
       let vsnj = F(skij, IDj, Tj) in
       let wj = Xor(L(sj), E(IDj, L(Ri), (Mxi, Myi), (Bxj, Byj))) in
       out (c, (wj, vsnj, (Bxj, Byj), Tj)).

```

شکل (۳-الف). دستورات مربوط به زیرفرآیند حسگر

```
let SNj(P: bitstring, ppub: bitstring) =
      (*Sensor node registration phase*)
      in(s, (IDj: bitstring, sj: bitstring));
(*Authentication and key agreement phase*)

      in (s, (WTA: bitstring, HTA: bitstring, Mxi: bitstring, Myi: bitstring, TTA: bitstring, Ti: bitstring));
         let HTA1 = E(WTA, sj, TTA, Ti) in
         if HTA1 = HTA then
        event userauthenticated(skij);
      new Tj: timestamp;
      let Ri = Xor(WTA, E(sj, (Mxi, Myi), TTA, Ti)) in
      new bj: bitstring;
      let (Bxj: bitstring, Byj: bitstring) = ECC(bj,P) in
      let (bxj: bitstring, byj: bitstring) = ECC1(bj,(Mxi, Myi)) in
      let skij = l((bxj, byj), IDj, L(Ri), L(sj), Ti, Tj) in
      let vsnj = F(skij, IDj, Tj) in
      let wj = Xor(L(sj), E(IDj, L(Ri), (Mxi, Myi), (Bxj, Byj))) in
      out (c, (wj, vsnj, (Bxj, Byj), Tj)).
```

شکل (۴-الف). دستورات مربوط به زیرفرآیند کاربر

۵-الف. زیرفرآیند کارت هوشمند

در این بخش کارت هوشمند تنها در مرحله ورود جدید فعالیت انجام می‌دهد و همچنین احراز هویت سنسور را انجام می‌دهد (خطوط ۱۴۸-۱۴۹). محاسبات طبق دستورات موجود در شکل (۵-الف) انجام می‌شود.

```
let sci(Ri: bitstring, P: bitstring, ppub: bitstring, Bio1i: biometric, ID1i: bitstring, pw1i: bitstring, q1i: bitstring) =
(*New login phase*)
     in (s, (R1i: bitstring, Xi: bitstring, Yi: bitstring, zi: bitstring, IDj: bitstring));
     let q1i = Rep(Bio1i, zi) in
     let k1 = Xor(Yi, e(ID1i, pw1i, q1i)) in
     let PRW1i = h(pw1i, k1) in
        let x1i: bitstring = h(PRW1i,q1i) in

     new Ti: timestamp;
     new m: bitstring;
     let (Mxi: bitstring, Myi: bitstring) = ECC(m,P) in
     let (Nxi: bitstring, Nyi: bitstring) = ECC(m,ppub) in
     let RID1i: bitstring = h(k1, ID1i) in
     let DIDi: bitstring = Xor(RID1i, Nyi) in
     let DIDj: bitstring = Xor(IDj, Nxi) in
     let R2i = Xor(Ri, h(ID1i,q1i)) in
     let vi = f(DIDi, DIDj, Ti, (Mxi, Myi), R2i) in

     out (c, (DIDi, DIDj, (Mxi, Myi), Ti, vi));
      in (c, (wj: bitstring, vsnj: bitstring, Bxj: bitstring, Byj: bitstring, Tj: bitstring));
      let Lsj = Xor(wj, G(IDj, L(R1i), Bxj, Byj, Mxi, Myi)) in

        let sk1ij = Q(IDj, L(R1i), Lsj, Ti, Tj)in
        let v1snj = e(sk1ij, IDj, Tj) in
        if v1snj = vsnj then
        event sensorauthenticated(skij);
     in (s, (R1i: bitstring, Xinew: bitstring, Yinew: bitstring, zinew: bitstring)).
```

شکل (۵- الف). دستورات مربوط به زیرفرآیند کارت هوشمند

۶-الف. شروع پروسه

این مرحله، آخرین قسمت دستورات می‌باشد. در این قسمت فرآیند پردازش و اجرای پروتکل آغاز می‌شود. در شکل (۶- الف) کدهای مربوط به مرحله‌ی آخر نشان داده شده است

در این قسمت ابتدا اطلاعات مورد نیاز هر کاربر تولید می‌شوند و در خط آخر، هر هویت و اطلاعات اولیه مربوطه مشخص شده‌است.

```
process
new s0: bitstring;
new ppub: bitstring;
new q1i: bitstring;
 new pw1i: bitstring;
 new ID1i: bitstring;
 new Bio1i: biometric;
 new ppub: bitstring;
 new P: bitstring;
 new Ri: bitstring;
 new Bioi: biometric;
 new pwi: bitstring;
 new k: bitstring;
new PRW1i: bitstring;
new IDi: bitstring;


  ((!TA(s0, ppub, P)) | (!SNj(P, ppub)) | (!user(k, pwi, Bioi, ppub, P, IDi)) | (!sci(Ri, P, ppub, Bio1i, ID1i, PRW1i, q1i)))
```

شکل (۶-الف). دستورات مربوط به شروع پروسه

۷-الف. ادعاها

محرمانگی کلید نشست بدان معناست که مهاجم نباید قادر به دانستن مقدار کلید نشست باشد. برای سنجش محرمانگی کلید نشست از دستور خط ۳۷ در شکل (۷-الف) استفاده شده‌است. همچنین جهت بررسی احراز هویت کاربر به حسگر از رویدادهای تعریف شده در خط ۳۴ و ادعای تعریف شده در خط ۴۱ موجود در شکل (۷-الف) استفاده شده‌است. علاوه‌براین، دستورات موجود در خطوط ۳۵ و ۴۲ موجود در شکل (۷-الف) مربوط به احراز هویت حسگر برای کاربر می‌باشد.

```
(*Query*)

event userauthenticated(bitstring).
event sensorauthenticated(bitstring).

query attacker (skij).

free SKij: bitstring.

query event(userauthenticated(skij)) ==> inj-event(userauthenticated(SKij)).
query event(sensorauthenticated(skij)) ==> inj-event(sensorauthenticated(SKij)).
```

شکل (۷-الف). دستورات مربوط به ادعاهای موجود برای پروتکل پیشنهادی

۸-الف. خروجی نرم‌افزار

پس از اجرای دستورات خروجی نرم‌افزار به صورت شکل (۸-الف) می‌باشد. نرم‌افزار پرووریف می‌تواند سه نوع نتیجه زیر را نمایش بدهد:

۱. RESULT[Query] is true : ادعا انجام شده است و هیچ حمله‌ای وجود ندارد. در این مورد پرووریف هیچگونه استخراج حمله و ردیابی حمله‌ای نشان نمی‌دهد.
۲. RESULT[Query] is false : ادعا نادرست است و پرووریف یک حمله علیه ویژگی امنیتی دلخواه را کشف کرده است. ردیابی حمله به درستی قبل از نتیجه نمایش داده می‌شود. (استخراج حمله نیز نمایش داده می‌شود، اما باید بر روی ردیابی حمله تمرکز کنیم، زیرا آن نشان دهنده حمله واقعی است.)
۳. RESULT[Query] cannot be proved : در این حالت پرووریف نمی‌تواند ثابت کند که ادعا درست است و همچنین نمی‌تواند یک حمله پیدا کند که نشان دهنده‌ی نادرست بودن درخواست باشد.

همانطور که در شکل ۱۲ نشان داده شده‌است، تمام ادعاها انجام شده‌است و هیچ حمله‌ای وجود ندارد. بنابراین در پروتکل پیشنهادی محرمانگی کلید نشست حفظ می‌شود و همچنین احراز هویت متقابل بین کاربر و حسگر به درستی انجام می‌شود.

```
-- Query not attacker(skij[])
nounif mess(s[],RIDi_436)/-5000
Completing...
Starting query not attacker(skij[])
RESULT not attacker(skij[]) is true.
-- Query inj-event(userauthenticated(skij[])) ==> inj-event(userauthenticated(SKi
j[]))
nounif mess(s[],RIDi_1088)/-5000
Completing...
Starting query inj-event(userauthenticated(skij[])) ==> inj-event(userauthenticat
ed(SKij[]))
RESULT inj-event(userauthenticated(skij[])) ==> inj-event(userauthenticated(SKij[
])) is true.
-- Query inj-event(sensorauthenticated(skij[])) ==> inj-event(sensorauthenticated
(SKij[]))
nounif mess(s[],RIDi_1847)/-5000
Completing...
Starting query inj-event(sensorauthenticated(skij[])) ==> inj-event(sensorauthent
icated(SKij[]))
RESULT inj-event(sensorauthenticated(skij[])) ==> inj-event(sensorauthenticated(S
Kij[])) is true.
```

شکل (۸-الف). خروجی نرم‌افزار

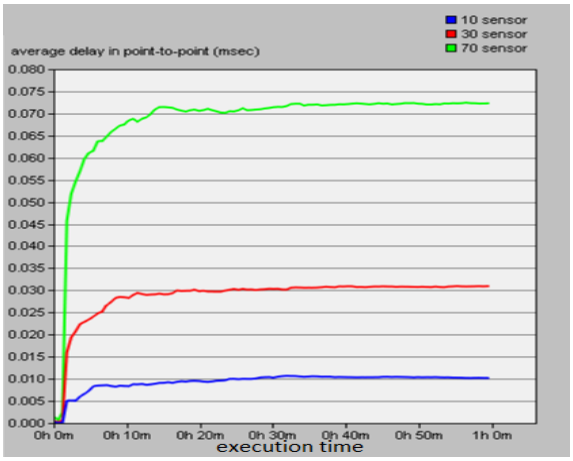
ضمیمه ب:

۱-ب. سناریوی شبیه‌سازی:

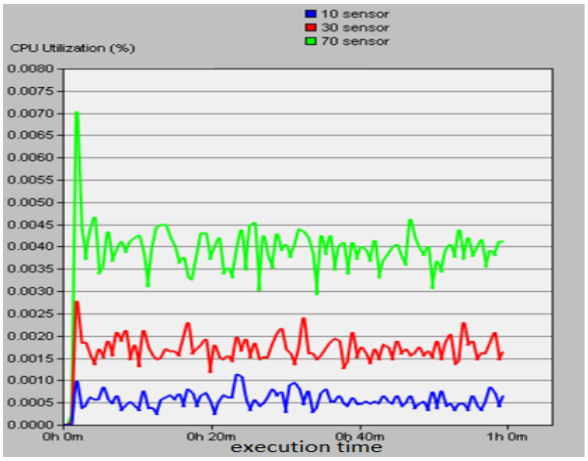
از آنجایی که نرم‌افزار OPNET فاقد شبیه‌سازی ماژول‌های رمزنگاری است لذا ما این ماژول‌ها را به صورت جداگانه بر روی گره‌هایی با مشخصات استفاده شده در شبیه‌ساز OPNET شبیه‌سازی کرده و تاثیر آن را در ویرایشگر گره‌ی OPNET اعمال کرده‌ایم زمان اجرای هر یک از این ماژول‌ها در جدول ۳ آمده است. ما طرح پیشنهادی خود را در یک محدوده ۱۰۰ متر مربعی با تعداد ۱۰، ۳۰ و ۷۰ حسگر به مدت ۳۶۰۰ ثانیه شبیه‌سازی کرده‌ایم. بنابراین میانگین فاصله حسگرها از TA در حدود ۱۰۰ متر فرض شده است.

۲-ب. نتایج شبیه‌سازی:

متوسط زمان اجرای فرآیند احراز هویت طرح پیشنهادی برای تعداد ۱۰، ۳۰ و ۷۰ حسگر بر حسب میلی ثانیه در شکل (۱-ب) نشان داده شده‌است. همان‌طور که مشخص است با افزایش تعداد حسگرها در شبکه زمان احراز هویت نیز افزایش می‌یابد. همچنین متوسط میزان بار پردازشی TA برای شبکه‌ای با ۱۰، ۳۰ و ۷۰ حسگر بر حسب درصد در شکل (۲-ب) نشان داده شده است. کامپیوتر شبیه سازی دارای CPU، Intel Core i5 (2nd Gen) 2520M/2.5 GHz، RAM 4GB است. همانطور که مشاهده می‌شود در ابتدای راه‌اندازی شبکه که تمامی حسگرها یکباره وارد شبکه می‌شوند میزان پردازش سرور TA زیاد اما پس از چند ثانیه این مقدار تقریباً همگرا می‌شود همچنین با افزایش تعداد حسگرها میزان بار پردازشی سرور TA نیز افزایش می‌یابد. اما حتی با وجود ۷۰ حسگر در شبکه حداکثر بار پردازشی TA در حدود ۴۰ ٪ باقی می‌ماند بنابراین نگرانی از عدم امکان پاسخگویی سرور TA در طرح پیشنهادی ما وجود ندارد.



شکل (۱-ب). متوسط زمان اجرای فرآیند احراز هویت طرح پیشنهادی



شکل (۲-ب). متوسط بار پردازشی سرور TA در طرح پیشنهادی

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

A Secure Three Factor Authentication Scheme for Wireless Healthcare Sensor Networks Based on Elliptic Curve

M. H. Kazemi Pooran, M. Bayat*, S. M. Pournaghi, Z. Hatefi, N. Hamian

*Department of Computer Engineering, Shahed University, Tehran, Iran

(Received: 10/09/2018, Accepted: 18/06/2019)

ABSTRACT

Wireless body area networks (WBANs) include many tiny sensor nodes which are planted in or around a patient's body. These sensor nodes can collect biomedical data from the patient and transmit these valuable data to a data sink or a personal digital assistant. Later, health care service providers can get access to these data through authorization. The biomedical data are usually personal and private. Consequently, data confidentiality and user privacy are of primary concerns for WBAN. One of the most important factors for providing security in e-healthcare networks, is authentication protocols which allow both parties to authenticate each other. Recently, regarding this issue, Challa et al.[1] presented an efficient elliptic curve based provably secure three-factor key agreement and authentication protocol for wireless healthcare sensor networks. In this paper, firstly we identify some security flaws of the Challa et al.'s scheme such as privileged-insider attacks, lack of forward secrecy and user traceability. Then, we present a three-factor authentication scheme for (WBANs) and evaluate the security properties of our scheme formally via "ProVerif". Presented security analysis and comparisons show that the proposed scheme is an efficient secure authentication scheme for WBANs.

Keywords: Authentication, E-Health, Key Agreement, Security, Privacy, ProVerif

* Corresponding Author Email: mbayat@shahed.ac.ir