

ارائه پروتکلی جامع و سبک وزن برای احراز هویت دو طرفه دستگاه‌های VoIP مبتنی بر کارت هوشمند

مهدی نیکوقدم^۱، هاله امین طوسی^۲

^۱ دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری، دانشگاه فردوسی مشهد

آمستادیار دانشکده مهندسی، دانشگاه فردوسی مشهد، amintoosi@um.ac.ir

چکیده

همزمان با فراگیری استفاده از فناوری صوت بر روی IP (VoIP) برای انتقال داده‌های چند رسانه‌ای نظیر صوت و تصویر، پروتکل برقراری نشست (SIP)، در مرکز توجه بسیاری از تحقیقات قرار گرفته است. برای برقراری یک کانال ارتباطی امن بین دو طرف ارتباط با استفاده از SIP، احراز هویت طرفین از اهمیت بالایی برخوردار است. در سال‌های اخیر، پژوهش‌های زیادی در زمینه پروتکل‌های احراز هویت انجام شده است که از جمله می‌توان طرحی سبک وزن برای احراز هویت در VoIP را که توسط ژنگ و همکاران ارائه شده نام برد. در این مقاله ابتدا اثبات خواهیم کرد طرح ژنگ در برابر حملات افشای پارامترهای تصادفی و منع سرویس مقام نیست و نیاز امنیتی محرمانگی رو به جلو را تامین نمی‌کند. در ادامه، پروتکلی سبک وزن و کارآمد ارائه کرده‌ایم و نشان داده‌ایم که پروتکل پیشنهادی در مقابل حملات مختلف مقاوم است و قادر به تامین نیازمندی‌های امنیتی اساسی همانند محرمانگی رویه جلو و گمنامی کاربر می‌باشد. همچنین عملکرد پروتکل پیشنهادی را به لحاظ پیچیدگی محاسباتی مورد بررسی قرار داده و نشان داده ایم که روش پیشنهادی در مقایسه با اغلب روشهای مشابه، دارای پیچیدگی محاسباتی کمتری می‌باشد. در نهایت، صحت پروتکل پیشنهادی را با ابزارهای رسمی Scyther و Proverif اثبات نموده ایم.

کلیدواژه

احراز هویت، SIP، VoIP، Scyther، Proverif

مقدمه

مرحله ثبت نام، برقراری تماس، تبادل داده و خاتمه تماس می‌باشد [۲].

در مرحله ثبت نام، قبل از شروع جلسه، هر کدام از طرفین ارتباط پیغام REGISTER را برای سرویس دهنده ثبت نام ارسال نموده و مشخصات مکان کنونی خود را ثبت می‌کنند. سپس در مرحله برقراری تماس برای شروع مکالمه، کاربری که قصد تماس گرفتن را دارد یک پیغام INVITE برای سرویس دهنده‌ای که در آن ثبت نام کرده ارسال می‌کند و اعلام می‌کند که می‌خواهد با این شماره تماس بگیرد. سپس خدمات دهنده، مکان کاربر طرف مقابل یعنی مقصد تماس را پیدا کرده و پیام INVITE را برای او ارسال می‌کند. وقتی که پیام INVITE به کاربر مقصد می‌رسد، پیام‌های RINGING، TRYING و OK مبادله شده و در نهایت،

سازمان Internet Engineering Task Force در سال ۱۹۹۹ پروتکلی برای برقراری جلسه که مبتنی بر استاندارد RFC2543 بود را ارائه داد [۱] که از آن، برای ارتباطات صوت بر روی IP یا VoIP^۱ نیز استفاده می‌شود. پروتکل برقراری جلسه یا SIP^۲ یکی از محبوب‌ترین پروتکل‌های علامت‌دهی است که برای برقراری مدیریت و خاتمه ارتباط بین طرفین به کار می‌رود. این پروتکل، یک پروتکل لایه کاربرد بوده و با توجه به وظیفه آن، که برقراری و مدیریت جلسه است در لایه پایین تر، از TCP که پروتکلی اتصال‌گرا و قابل اعتماد است استفاده می‌کند. از رقبای SIP می‌توان به پروتکل‌های H.323، MGCP و Megaco اشاره کرد. به طور خلاصه، عملکرد پروتکل SIP در سیستم VoIP شامل ۴

^۲ Session Initiation Protocol

^۱ Voice over Internet Protocol

مقصد ارتباط، پیام ACK را برای کاربر شروع کننده ارتباط می فرستد.

در مرحله تبادل داده ها، نوبت به پروتکل RTP^۳ خواهد رسید و داده ها به صورت انتها به انتها بین مبدا و مقصد مبادله می شوند. در نهایت در مرحله خاتمه تماس، بعد از مبادله اطلاعات، هر یک از طرفین می توانند پیام BYE را به عنوان درخواست خاتمه تماس برای طرف مقابل ارسال کنند و در جواب آن زمانی که پیام OK را دریافت کنند ارتباط خاتمه می یابد.

مهم ترین بحث امنیتی در مورد پروتکل SIP، بحث احراز هویت است که در تمامی مراحل ذکر شده در بالا دارای اهمیت بسزایی است. در مرحله ثبت نام، در زمان برقراری تماس، باید با استفاده از مکانیزم های احراز هویت، از ثبت نام کاربران غیر مجاز جلوگیری شود. همچنین، در زمان برقراری تماس باید با پیام INVITE، هر یک از طرفین، ارتباط هویت واقعی طرف مقابل را شناسایی کند. در نهایت در مرحله خاتمه تماس، در زمان اتمام یک جلسه با پیام BYE یا CANCEL، باز هم باید هویت کاربر فرستنده این چنین پیامی برای طرف مقابل تأیید شود.

از طرفی در بحث برقراری تماس از طریق شبکه VoIP، یکی از مسائلی که اهمیت بسزایی دارد بحث کم شدن تاخیر در تماس می باشد. به همین دلیل، ایجاد کلید نشست در ابتدای کار به طوری که طرفین بتوانند در ادامه ارتباط از طریق این کلید نشست، با هم ارتباط داشته باشند اهمیت به سزایی دارد. با توجه به مطالبی که در بالا گفته شد، فرایند تصدیق هویت و توافق کلید در پروتکل SIP از نظر امنیتی از اهمیت بالایی برخوردار است. به همین دلیل، تحقیقات و پژوهش های زیادی در احراز هویت و توافق کلید در شبکه های VoIP انجام شده است [۸-۶] [۵] [۴] [۳].

در این مقاله، ابتدا به بررسی و تحلیل طرح احراز هویت و تبادل کلید ژنگ و همکاران [۹] می پردازیم و نشان می دهیم که این طرح در برابر حمله افشای پارامترهای تصادفی [۱۳-۱۰] و حمله منع سرویس مقاوم نیست و نیاز امنیتی محرمانگی رو به جلو [۱۰] را تأمین نمی کند. در ادامه، پروتکلی امن و کارا برای احراز هویت و تبادل کلید در VoIP ارائه خواهیم نمود و با استفاده از تحلیل رسمی و غیررسمی نشان خواهیم داد که پروتکل پیشنهادی در مقابل حملات مختلف، مقاوم است. همچنین نشان خواهیم داد که پروتکل پیشنهادی به لحاظ پیچیدگی زمانی، عملکرد بهتری نسبت به پروتکل های مشابه دارد.

ساختار مقاله به شرح زیر است: در ابتدا در بخش کارهای پیشین به بررسی کارهای گذشته می پردازیم. سپس در بخش بررسی و تحلیل طرح ژنگ و همکاران، طرح ژنگ و همکاران [۹] را مورد بررسی و تحلیل قرار می دهیم. در ادامه در بخش پروتکل پیشنهادی، پروتکلی بهبود یافته و امن برای احراز هویت و تبادل کلید ارائه خواهیم داد که در برابر حملات مختلف مقاوم است. در ادامه ابتدا در بخش تحلیل امنیتی پروتکل پیشنهادی به تحلیل امنیتی غیررسمی پروتکل پیشنهادی خواهیم پرداخت و در بخش اثبات رسمی امنیت پروتکل پیشنهادی با استفاده از ابزارهای Scyther و Proverif، پروتکل پیشنهادی خود را با ابزارهای رسمی Scyther [۱۴] و Proverif [۱۵] مورد تحلیل و بررسی قرار خواهیم داد. همچنین در تحلیل و مقایسه پیچیدگی زمانی و سخت افزاری طرح پیشنهادی و دیگر طرح های مشابه، پروتکل پیشنهادی را از نظر پیچیدگی زمانی با دیگر پروتکل های مشابه مقایسه خواهیم کرد. در نهایت، به نتیجه گیری و کارهای آینده می پردازیم.

کارهای پیشین

در سال ۲۰۰۵ دورلانیک و همکاران [۱۶] یک رویکرد جدید برای احراز هویت امن SIP با استفاده از رمزنگاری منحنی بیضوی ارائه نمودند. یون و همکاران [۱۷] در سال ۲۰۱۰ نشان دادند که طرح احراز هویت دورلانیک و همکاران در برابر حمله حدس رمز عبور^۴ و حمله Denning-Sacco و حمله دزدیده شدن تأیید کننده ها^۵ مقاوم نیست. آن ها همچنین یک طرح احراز هویت امن و مناسب برای شبکه های VoIP ارائه دادند.

در سال ۲۰۱۴ ژنگ و همکاران [۱۸] طرحی برای احراز هویت و توافق کلید در SIP مبتنی بر رمز عبور و کارت هوشمند ارائه دادند که نیاز به ذخیره سازی رمز عبور کاربران در خدمات دهنده ندارد. همچنین در سال ۲۰۱۴، فراش [۱۹] روشی امن برای احراز هویت و توافق کلید در SIP ارائه کرد و ادعا کرد که در برابر اکثر حملات مقاوم است. اما در سال ۲۰۱۵ کوماری و همکاران [۲۰] طرحی دو فاکتوره ارائه دادند که بر پایه مسئله سخت منحنی بیضوی^۶ استوار بود. همچنین آن ها اثبات کردند که طرح فراش [۱۹] گمنامی و حریم خصوصی کاربر را فراهم نمی کند و در برابر حمله لو رفتن پارامترهای تصادفی یک جلسه و حمله حدس رمز عبور، آسیب پذیر است.

پس از مدتی ژنگ و همکاران [۲۱] نشان دادند که روش ارائه شده قبلی آنها [۱۸] در برابر حمله جعل هویت مقاوم نیست و

^۶ elliptic curve discrete logarithm problem

^۳ Real-time Transport Protocol
^۴ off-line password guessing attacks
^۵ stolen-verifier attacks

همکاران [۳۲] در سال ۲۰۱۸ طرحی در مورد تامین نیاز امنیتی محرمانگی رو به جلو در پروتکل های SIP ارائه دادند که ژنگ و همکاران [۹] در سال ۲۰۱۹ ضمن بررسی ایرادات امنیتی طرح کیو و همکاران [۳۲]، طرح بهبود یافته ای ارائه دادند. در این مقاله اثبات خواهیم کرد که طرح ژنگ و همکاران [۹]، در برابر حمله افشای پارامترهای تصادفی^۷ و حمله منع سرویس، مقاوم نیست و نیاز امنیتی محرمانگی رو به جلو^۸ را تامین نمی کند.

بررسی و تحلیل طرح ژنگ و همکاران

در این بخش، روش ارائه شده توسط ژنگ و همکاران [۹] بطور خلاصه ارائه شده و ضعف های امنیتی آن بیان می گردد. جدول ۱ نمادهای بکار رفته در پروتکل ارائه شده در طرح ژنگ و همکاران [۹] را نشان می دهد. جدول ۱. نمادهای به کار رفته در طرح [۹]

نماد	توضیحات
U	کاربر
S	خدمات دهنده
ID	شناسه کاربر
PW	رمز عبور انتخابی کاربر
S_p	کلید محرمانه خدمات دهنده
sk	کلید نشست ایجاد شده بین طرفین
\oplus	عملگر XOR
	عملگر الحاق دو رشته

در طرح ژنگ و همکاران [۹]، کاربر ابتدا شناسه ID و رمز عبور PW و عدد r را برای خود انتخاب می کند و پارامترهای VPw و Hid را بر طبق روابط (1) و (2) محاسبه نموده و پارامترهای VPw و Hid بر روی کانال امن برای خدمات دهنده ارسال می کند.

$$VPw = h(PW || ID || r) \quad (1)$$

$$Hid = h(ID \oplus r) \quad (2)$$

خدمات دهنده با دریافت پارامترهای VPw و Hid، پارامترهای N و R را طبق روابط (۳) و (۴) می سازد سپس پارامترهای N و Hid را درون حافظه خود و پارامتر R را درون کارت هوشمند ذخیره می کند و در نهایت کارت هوشمند را برای کاربر بر روی کانال امن ارسال می کند.

$$N = VPw \oplus h(S_p || Hid) \quad (3)$$

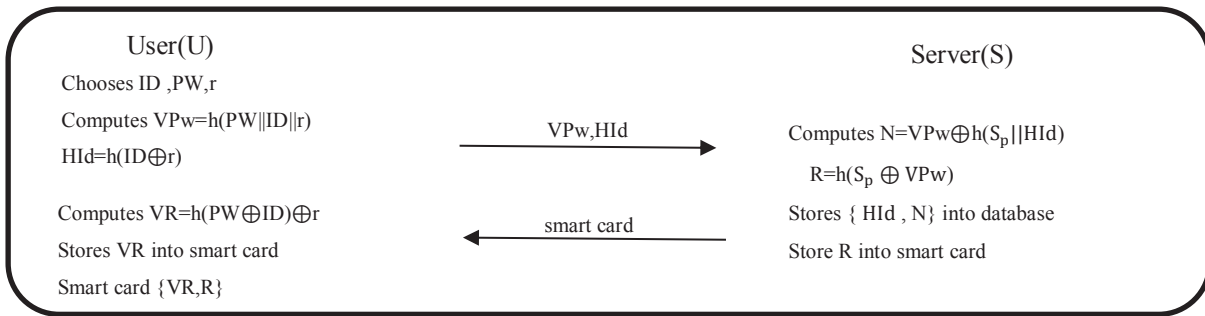
$$R = h(S_p \oplus VPw) \quad (4)$$

کاربر به محض دریافت کارت هوشمند، پارامتر VR را از رابطه (۵) محاسبه می کند و درون کارت هوشمند قرار می دهد. در نهایت در مرحله ثبت نام، پارامترهای VR و R درون کارت

پروتکل توسعه یافته ای با استفاده از کارت هوشمند ارائه دادند. در سال ۲۰۱۵ ژیانگ و همکاران [۲۲] نشان دادند که طرح [۱۸] در برابر حمله داخلی آسیب پذیر است و برای حل این مشکل طرح جدیدی را ارائه نمودند.

در سال ۲۰۱۵ تو و همکاران [۲۳] نشان دادند که طرح ژنگ و همکاران [۱۸] در برابر حمله جعل هویت مقاوم نیست و یک طرح بهبود یافته ارائه دادند و ادعا کردند که هزینه محاسباتی طرح آن ها حدود ۷۵ درصد هزینه محاسباتی طرح ژنگ و همکاران است. در سال ۲۰۱۶، فراش و همکاران [۲۴] ادعا کردند که طرح تو و همکاران هنوز هم در برابر حمله جعل هویت مقاوم نیست و همچنین در برابر حمله تغییر رمز عبور آسیب پذیر است و طرح بهبود یافته ای ارائه دادند. در سال ۲۰۱۷ چادری و همکاران [۲۵] ثابت کردند که طرح [۲۳] در برابر حملات جعل هویت خدمات دهنده و حمله تکرار و همچنین حمله منع سرویس مقاوم نیست و نیاز امنیتی گمنامی کاربر را تامین نمی کند. آنها همچنین ادعا کردند که طرح فراش و همکاران [۲۴] گمنامی کاربر را تامین نمی کند و مستعد حمله تکرار است. همچنین می شرا و همکاران [۲۶] طرح تو و همکاران [۲۳] را مورد بررسی قرار داده و ضعف امنیتی آن را در برابر حمله مرد میانی نشان دادند. همچنین برای رفع این ضعف امنیتی، پروتکلی ارائه کرده و آن را از نظر سر بار محاسباتی با طرح تو و همکاران [۲۳] مقایسه نمودند. در سال ۲۰۱۶، فراش و عطاری [۲۷] طرحی برای احراز هویت SIP ارائه دادند که در سال ۲۰۱۷ توسط لو و همکاران [۲۸] مورد بررسی قرار گرفت و نشان داده شد که طرح فراش و عطاری [۲۷] در برابر حمله حدس رمز عبور مقاوم نیست. نویسندگان سپس یک طرح بر اساس رمزنگاری منحنی بیضوی ارائه دادند و ادعا کردند که در برابر حملات مختلف مقاوم است. همچنین در سال ۲۰۱۶، لو و همکاران [۲۹] طرحی برای احراز هویت SIP ارائه دادند که در سال ۲۰۱۸ توسط سورش کومار و همکاران [۳۰] مورد تحلیل قرار گرفت و نشان داده شد که قادر به تامین گمنامی کاربر نیست و در برابر حملات جعل هویت کاربر و جعل هویت خدمات دهنده آسیب پذیر است. لذا آن ها طرحی بهبود یافته برای احراز هویت و توافق کلید ارائه دادند. سپس در سال ۲۰۱۹، سوراو و همکاران [۴] محدودیت های طرح سورش کومار و همکاران [۳۰] را نشان دادند و طرحی بهبود یافته بدون افزایش هزینه محاسباتی ارائه نمودند. همچنین در سال ۲۰۱۶ ژنگ و همکاران [۳۱] طرحی برای احراز هویت sip ارائه دادند که روانبخش و همکاران [۱۰] اثبات کردند که ژنگ و همکاران نیاز امنیتی محرمانگی رو به جلو را تامین نمی کنند. کیو و

Known-session-specific Temporary Information Attack^۷
perfect forward secrecy^۸



شکل ۲. مرحله ثبت نام طرح ژنگ و همکاران [9]

حال خدمات دهنده عدد تصادفی r_b را انتخاب می کند و کلید نشست را طبق رابطه (۱۴) می سازد. در انتها پارامترهای D و $Auth_s$ را برای کارت هوشمند ارسال می کند. سپس روابط (۱۵) و (۱۶) را محاسبه می کند. و در انتها پارامترهای D و $Auth_s$ را برای کارت هوشمند ارسال می کند.

$$VPw'' = N \oplus h(S_p || Hid') \quad (11)$$

$$R' = h(S_p \oplus VPw'') \quad (12)$$

$$r'_a = h(R' \oplus VPw'') \oplus C \quad (13)$$

$$sk_s = h(r'_a || r_b || Hid') \quad (14)$$

$$D = h(R' || VPw'') \oplus r_b \quad (15)$$

$$Auth_s = h(sk_s || D) \quad (16)$$

کارت هوشمند به محض دریافت پارامترهای D و $Auth_s$ ابتدا پارامتر r'_b را از رابطه (۱۷) محاسبه نموده و سپس کلید نشست را از رابطه (۱۸) محاسبه می کند و سپس با مقایسه $Auth_s = h(sk_u || D)$ خدمات دهنده را احراز هویت می نماید.

$$r'_b = h(R || VPw') \oplus D \quad (17)$$

$$sk_u = h(r'_a || r'_b || Hid') \quad (18)$$

شمای کلی مرحله احراز هویت طرح ژنگ و همکاران در شکل ۲ قابل مشاهده است.

هوشمند قرار دارند. مراحل گفته شده در شکل ۱ نشان داده شده اند.

$$VR = h(PW \oplus ID) \oplus r \quad (5)$$

در مرحله احراز هویت، ابتدا کاربر، شناسه و رمز عبور خود را وارد می کند و سپس پارامتر r' از رابطه (۶) و همچنین پارامترهای Hid' و VPw' از روابط (۷) و (۸) توسط کارت هوشمند محاسبه می شود.

$$r' = VR \oplus h(PW \oplus ID) \quad (6)$$

$$Hid' = h(ID \oplus r') \quad (7)$$

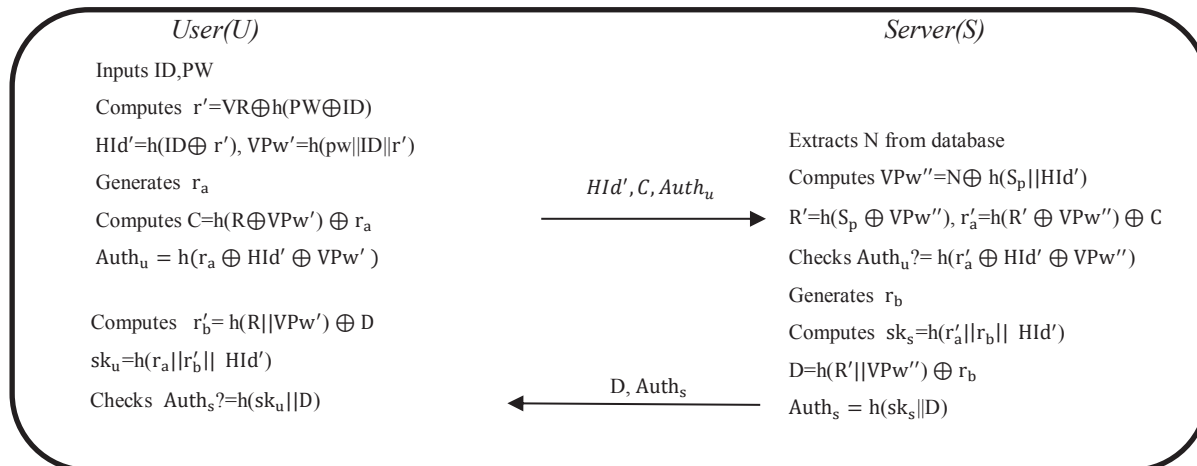
$$VPw' = h(pw || ID || r') \quad (8)$$

در ادامه، عدد تصادفی r_a را انتخاب و روابط (۹) و (۱۰) را محاسبه می کند و در نهایت پارامترهای $Auth_u$ و C و Hid' را برای خدمات دهنده ارسال می نماید.

$$C = h(R \oplus VPw') \oplus r_a \quad (9)$$

$$Auth_u = h(r_a \oplus Hid' \oplus VPw') \quad (10)$$

حال خدمات دهنده، ابتدا پارامتر N را از کارت هوشمند استخراج می کند و سپس VPw'' و R' و r'_a را طبق روابط (۱۱)، (۱۲) و (۱۳) محاسبه می کند. سپس با مقایسه $Auth_u = h(r'_a \oplus VPw'' \oplus Hid' \oplus VPw'')$ هویت کارت هوشمند و کاربر برای خدمات دهنده احراز می شود.



شکل ۲. مرحله احراز هویت طرح ژنگ و همکاران [۹]

حملات وارده به طرح ژنگ و همکاران [۹]

مراحل ۱ تا ۴ و همچنین رابطه $r'_b = h(R||VPw') \oplus D$ می‌تواند تمامی پارامترهای کلید نشست یعنی $sk_u = h(r'_a || r'_b || Hid')$ را به دست آورده و آن را بسازد.

حمله منع سرویس: از آنجایی که در پروتکل هیچ مهر زمانی استفاده نشده است، در زمانی که پیغام $Auth_u$ و Hid' فرستاده می‌شود، خدمات دهنده، اطلاعاتی را در پایگاه داده جستجو می‌کند در نتیجه مهاجم میتواند با تکرار این پیغام، باعث این شود که خدمات دهنده مشغول شده و اصطلاحاً حمله منع سرویس اتفاق بیفتد.

پروتکل پیشنهادی

در این بخش، به معرفی پروتکل پیشنهادی خواهیم پرداخت. پروتکل پیشنهادی، شامل سه مرحله ثبت نام، احراز هویت و تغییر رمز عبور است که در ادامه هر یک را به تفصیل توضیح خواهیم داد. جدول ۲ نمادهای به کار رفته در پروتکل پیشنهادی را نمایش می‌دهد.

جدول ۲. نمادهای به کار رفته در طرح پیشنهادی

نماد	توضیحات
U	کاربر
S	خدمات دهنده
ID_i	شناسه کاربر
PW_i	رمز عبور انتخابی کاربر
x	کلید محرمانه خدمات دهنده
SK	کلید نشست ایجاد شده بین طرفین
\oplus	عملگر XOR
h(.)	تابع درهم ساز یک طرفه
$E(.) / D(.)$	رمزنگاری و رمزگشایی
	عملگر الحاق دو رشته

مرحله ثبت نام

در ابتدا کاربر، شناسه ID ، رمز عبور PW_i و عدد تصادفی a_i را انتخاب می‌کند. سپس پارامتر MPW_i را از رابطه (۱۹) محاسبه می‌کند. در نهایت پارامترهای a_i ، MPW_i ، ID_i را بر روی کانال امن، برای خدمات دهنده ارسال می‌کند.

$$MPW_i = h(ID_i || h(PW_i \oplus a_i)) \oplus PW_i \quad (19)$$

خدمات دهنده به محض دریافت پارامترهای a_i ، MPW_i و ID_i ، ابتدا عدد تصادفی b_i را تولید می‌کند. سپس روابط (۲۰) تا (۲۴) را محاسبه نموده و در ادامه، پارامترهای Hid' و b_i را با H_i طبق رابطه (۲۴) با کلید محرمانه خودش رمز می‌کند. در انتها،

حمله افشای پارامترهای تصادفی^۹: بر طبق مقالات [۱۰-۱۳] حمله ای وجود دارد که بر طبق آن، اگر اعداد تصادفی پروتکل لو بروند و به دست مهاجم بیفتند، مهاجم نباید قادر باشد به کلید نشست برسد. در پروتکل ژنگ و همکاران [۹]، اگر فرض بر این باشد که اعداد موقتی یا تصادفی r_a و r_b به دست مهاجم بیفتند، از آنجایی که Hid' بر روی کانال عمومی رد و بدل میشود، مهاجم می‌تواند به کلید نشست $sk_s = h(r'_a || r'_b || Hid')$ برسد چرا که به تمامی پارامترهای آن دسترسی دارد.

عدم تامین نیاز امنیتی محرمانگی رو به جلو: در حمله محرمانگی رو به جلو فرض بر آن است که اگر پارامترهای طولانی مدت مانند کلید خصوصی خدمات دهنده لو برود و دست مهاجم بیفتد، مهاجم نتواند به کلید نشست برسد [۱۰]. در ادامه، اثبات خواهیم کرد که اگر کلید محرمانه خدمات دهنده لو برود مهاجم می‌تواند به کلید نشست برسد.

مرحله ۱: فرض کنید کلید محرمانه خدمات دهنده یعنی S_p لو برود. از آنجایی که Hid' بر روی کانال عمومی رد و بدل می‌شود مهاجم می‌تواند با استفاده از آن در پایگاه داده جستجو کند و N معادل آن را به دست بیاورد.

مرحله ۲: طبق فرض مهاجم S_p را دارد و همچنین Hid' که بر روی کانال عمومی قرار دارد، از طرفی طبق مرحله ۱ مهاجم پارامتر N را دارد. حال از آنجایی که در رابطه $VPw'' = N \oplus h(S_p || Hid')$ تمامی پارامترها را دارد، می‌تواند VPw'' را محاسبه کند.

مرحله ۳: طبق فرض، مهاجم کلید محرمانه یعنی S_p را دارد، همچنین پارامتر VPw'' را طبق مراحل ۱ و ۲ به دست آورده، در نتیجه در رابطه $R' = h(S_p \oplus VPw'')$ می‌تواند پارامتر R' را محاسبه کند.

مرحله ۴: از آنجایی که پارامتر C بر روی کانال عمومی رد و بدل می‌شود و همچنین طبق مراحل ۱ و ۲ و ۳ مهاجم از رابطه $r'_a = h(R' \oplus VPw'') \oplus C$ می‌تواند به r'_a که برابر با r_a هست دست پیدا کند.

مرحله ۵: از آنجایی که $R' = R$ و $VPw'' = VPw'$ ، همچنین به علت اینکه پارامتر D بر روی کانال عمومی ارسال می‌شود طبق

^۹ Known-session-specific Temporary Information Attack

$$c_i = b_i + a_i \quad (25)$$

$$M_2 = b_i \oplus c_i \quad (26)$$

مرحله احراز هویت:

در مرحله احراز هویت، کاربر، کارت هوشمند خود را وارد دستگاه کارت خوان نموده، شناسه و رمز عبور ID_i^* و PW_i^* خود را وارد می کند. سپس کارت هوشمند، روابط (27) تا (30) را محاسبه و با مقایسه $D_i^* = D_i$ مشخص می شود که کارت به سرقت نرفته است و در اختیار صاحب اصلی آن است. سپس، روابط (31) تا (33) محاسبه شده و در نهایت، کارت هوشمند، پارامترهای b_i, q_i, G_i و M_1 را برای خدمات دهنده بر روی کانال عمومی ارسال می کند

پارامترهای b_i و D_i و q_i و H_i را درون کارت هوشمند ذخیره نموده و کارت هوشمند را بر روی کانال امن برای کاربر ارسال می نماید.

$$C_i = h(b_i || ID_i) \quad (20)$$

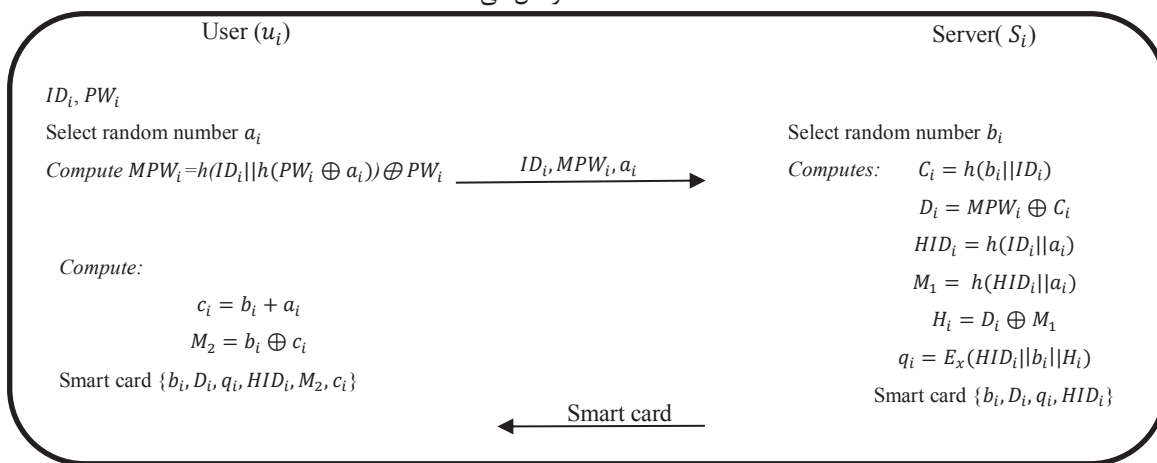
$$D_i = MPW_i \oplus C_i \quad (21)$$

$$HID_i = h(ID_i || a_i) \quad (22)$$

$$H_i = D_i \oplus M_1 \quad (23)$$

$$q_i = E_x(HID_i || b_i || H_i) \quad (24)$$

کاربر به محض دریافت کارت هوشمند، روابط (25) و (26) را محاسبه نموده و پارامترهای C_i و M_2 را درون کارت هوشمند ذخیره می کند. به این ترتیب، همانطور که در شکل 3 مشاهده می شود، مرحله ثبت نام به پایان می رسد.



شکل 3. مرحله ثبت نام طرح پیشنهادی

تایید خواهد شد. کارت هوشمند به محض دریافت پیام، ابتدا تازگی پیغام را بررسی می کند و سپس روابط (40) و (41) را محاسبه می کند و در صوتی که M_5 ارسالی با M_5 محاسبه شده برابر باشد در این صورت، اصالت پیغام ارسالی محرز می شود و هویت خدمات دهنده تایید خواهد شد.

$$N_1 = D_i \oplus M_4 \quad (41)$$

$$M'_5 = h(N_1 || D_i) \quad (42)$$

حال، کارت هوشمند، عدد تصادفی N_2 را انتخاب و روابط (43) تا (46) را محاسبه می کند. سپس عدد تصادفی N_3 را انتخاب و رابطه (47) محاسبه می شود. پس از آن، بر طبق رابطه (48)، کلید نشست در سمت کارت هوشمند/کاربر ساخته می شود. در نهایت، پارامترهای M_8, M_{10}, M_9 را کارت هوشمند از طریق کانال عمومی و ناامن برای خدمات دهنده ارسال می کند.

$$M_6 = h(N_2 || M_4) \quad (43)$$

$$M_7 = N_1 \oplus N_2 \quad (44)$$

$$M_8 = M_7 \oplus N_1 \quad (45)$$

$$M_9 = h(N_2 || M_5) \quad (46)$$

$$M_{10} = N_2 \oplus N_3 \quad (47)$$

$$SK = h(M_6 || N_2 || HID_i || N_3) \quad (48)$$

$$a_i = c_i - b_i \quad (27)$$

$$MPW_i^* = h(ID_i^* || h(PW_i^* \oplus a_i)) \oplus PW_i^* \quad (28)$$

$$C_i^* = h(b_i || ID_i^*) \quad (29)$$

$$D_i^* = MPW_i^* \oplus C_i^* \quad (30)$$

$$HID_i = h(ID_i || a_i) \quad (31)$$

$$G_i = HID_i \oplus c_i \quad (32)$$

$$M_1 = h(HID_i || a_i) \quad (33)$$

خدمات دهنده به محض دریافت پیام، ابتدا تازگی پیام را مورد بررسی قرار می دهد سپس پارامتر q_i را از آنجایی که با کلید خدمات دهنده، سپس، عدد تصادفی N_1 را انتخاب نموده، سپس روابط (37) و (38) و (39) و (40) را محاسبه می کند و در نهایت پارامترهای M_4 و M_5 را برای کارت هوشمند ارسال می کند.

$$M_3 = h(N_1 || M_1) \quad (37)$$

$$D_i = H_i \oplus M_1 \quad (38)$$

$$M_4 = D_i \oplus N_1 \quad (39)$$

$$M_5 = h(N_1 || D_i) \quad (40)$$

کارت هوشمند به محض دریافت پیام، ابتدا تازگی پیغام را بررسی می کند و سپس روابط (40) و (41) را محاسبه می کند و در صوتی که M_5 ارسالی با M_5 محاسبه شده برابر باشد در این صورت، اصالت پیغام ارسالی محرز می شود و هویت خدمات دهنده

محرمانه خدمات دهنده می‌توان به آن رسید. در نتیجه امکان چنین حمله‌ای وجود ندارد.

حمله جعل هویت خدمات دهنده: فرض کنید مهاجم در پیام دوم M_4^* و M_5^* را با هدف جعل هویت خدمات‌دهنده جایگزین M_4 و M_5 کند. از آنجایی که پیام دریافت شده، M_4 و M_5 از طریق $M_5^* = ? M_5$ احراز هویت می‌شود، از آنجایی که M_5^* از D_1 ساخته می‌شود که خود کاربر آن را می‌سازد در نتیجه امکان جعل هویت خدمات‌دهنده وجود ندارد.

حمله داخلی: در حمله داخلی فرض بر این است که مهاجم، خود، یکی از افراد داخلی سیستم خدمات دهنده است و سعی در رسیدن به رمزعبور خدمات‌دهنده دارد. از آنجایی که کاربر شناسه و رمزعبور خود را به طور مستقیم به سمت خدمات دهنده ارسال نمی‌کند و آن را در پوشش $MPW_i = h(ID_i || h(PW_i \oplus a_i)) \oplus PW_i$ برای خدمات دهنده ارسال می‌کند، در نتیجه امکان چنین حمله‌ای وجود ندارد.

حمله جعل هویت کاربر: از آنجایی که در دو مرحله، پیام‌های رسیده شده از طریق کاربر به خدمات‌دهنده از طریق مقایسه $M_1^* = ? M_1$ و $M_9^* = ? M_9$ احراز هویت می‌شود، اگر فرض شود که در پیام اول، مهاجم q_1 را در بین راه جایگزین q_i کند، چون امکان باز شدن q_1 جعلی با کلید محرمانه خدمات‌دهنده وجود ندارد در نتیجه در همین مرحله ارتباط قطع می‌شود. به شکل مشابه، اگر مهاجم پارامترهای جعلی M_{10}^* و M_8^* را جایگزین M_{10} و M_8 کند، از آنجایی که در ساخت پارامتر M_9 از پارامتر M_5 استفاده می‌شود، که خدمات‌دهنده از پارامتر M_5 که خود آن را می‌سازد در ساخت M_9 استفاده می‌کند، در نتیجه امکان جعل هویت کاربر وجود نخواهد داشت.

حمله تکرار: در این حمله، مهاجم پیام‌های انتقالی بین دو موجودیت را به دست آورده و آن‌ها را در زمان دیگری ارسال می‌کند. طرفین ارتباط، متوجه تازگی پیام‌ها نشده و با این پیام، به مانند یک پیام جدید رفتار می‌شود و مراحل توافق کلید جلسه طی می‌شود. در پروتکل پیشنهادی، به علت وجود مهرهای زمانی و بررسی آن‌ها در ابتدای هر گام و همچنین به علت وجود اعداد تصادفی امکان حمله تکرار وجود نخواهد داشت.

تامین نیاز امنیتی گمنامی و حریم خصوصی کاربر [۳۳]: از آنجایی که در مرحله ثبت نام، خدمات‌دهنده برای کاربر، شناسه موقت $HID_i = h(ID_i || a_i)$ را ساخته و در اختیار او قرار می‌دهد و در ادامه کار، در تمامی مراحل، از شناسه موقت استفاده می‌شود، لذا امکان رسیدن به شناسه اصلی از روی کانال عمومی نیست و در نتیجه، گمنامی کاربر تامین می‌شود.

خدمات‌دهنده به محض دریافت پیام، ابتدا تازگی پیام را بررسی نموده و سپس روابط (۴۹) و (۵۰) و (۵۱) را محاسبه می‌کند. در صورتی که M_9 ارسال شده با M_9 ساخته شده برابر باشد در این صورت صحت پیام ارسال شده تایید، و کارت هوشمند/کاربر احراز هویت می‌شود.

$$M_7 = M_8 \oplus N_1 \quad (49)$$

$$N_2 = N_1 \oplus M_7 \quad (50)$$

$$M_9^* = h(N_2 || M_5) \quad (51)$$

خدمات‌دهنده، روابط (۵۲) و (۵۳) را محاسبه می‌کند و در نهایت همانطور که در شکل ۴ مشاهده می‌شود، کلید نشست را از رابطه (۵۴) محاسبه خواهد کرد.

$$N_3 = N_2 \oplus M_{10} \quad (52)$$

$$M_6 = h(N_2 || M_4) \quad (53)$$

$$SK = h(M_6 || N_2 || HID_i || N_3) \quad (54)$$

مرحله تغییر رمز عبور:

در این مرحله، ابتدا کاربر شناسه و رمز عبور قدیمی خود را وارد می‌کند. کارت هوشمند، روابط (۲۷) تا (۳۰) را محاسبه می‌کند و در صورتی که $D_i^* = D_i$ برقرار باشند، مشخص می‌شود که کارت هوشمند به سرقت نرفته است. حال کاربر، درخواست تغییر رمزعبور را داده، رمزعبور جدید را وارد می‌کند و روابط (۵۵) تا (۵۸) محاسبه خواهد شد. در نهایت، D_i^{**} جایگزین D_i درون کارت هوشمند می‌شود.

$$a_i = c_i - b_i \quad (55)$$

$$MPW_i^{**} = h(ID_i^{**} || h(PW_i^{**} \oplus a_i)) \oplus PW_i^{**} \quad (56)$$

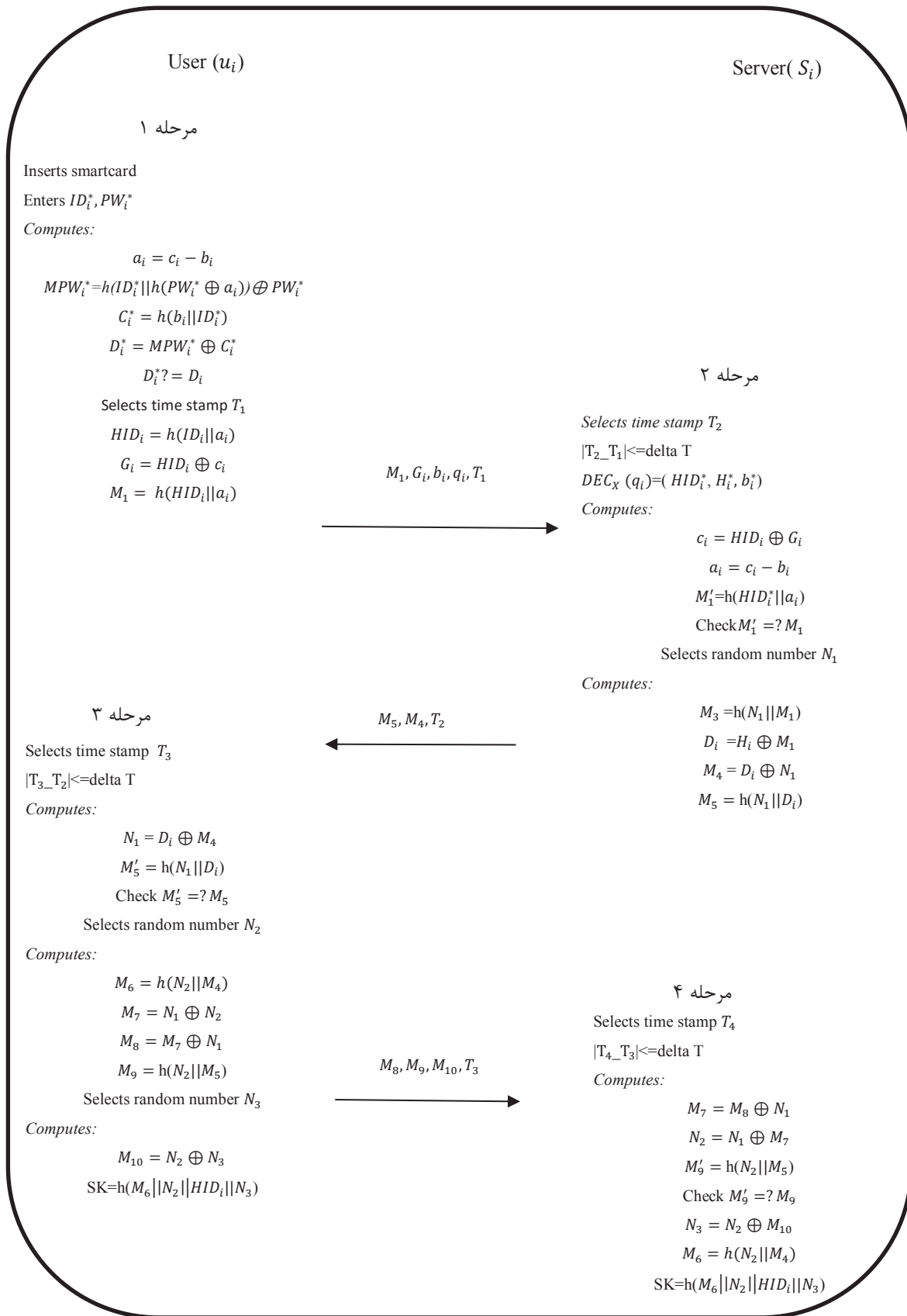
$$C_i^* = h(b_i || ID_i^*) \quad (57)$$

$$D_i^{**} = MPW_i^{**} \oplus C_i^* \quad (58)$$

تحلیل امنیتی غیر رسمی پروتکل پیشنهادی:

تامین نیاز امنیتی محرمانگی رو به جلو: در این نیاز امنیتی، فرض بر این است که اگر پارامترهای طولانی مدت مانند کلید محرمانه خدمات دهنده لو برود، باز هم مهاجم نباید قادر باشد به کلید نشست دست پیدا کند. از آنجایی که درون کلید نشست، پارامترهای N_2 و N_3 وجود دارد که حتی با لو رفتن کلید محرمانه خدمات دهنده، امکان رسیدن به آن‌ها وجود ندارد در نتیجه نیاز امنیتی محرمانگی رو به جلو تامین می‌شود.

حمله افشای پارامترهای تصادفی: در این حمله، فرض بر این است که اگر مهاجم بتواند به پارامترهای تصادفی دست پیدا کند، نباید این امکان وجود داشته باشد که به کلید نشست دست پیدا کند. حال اگر پارامترهای تصادفی N_1 و N_2 و N_3 لو بروند، مهاجم امکان رسیدن به کلید نشست را ندارد چراکه در کلید نشست، پارامتر HID_i وجود دارد که تنها در صورت لو رفتن کلید



شکل ۴. مرحله احراز هویت طرح پیشنهادی

ProVerif ابزاری قدرتمند برای تحلیل پروتکل‌های امنیتی است که از ابتکاراتی مانند رمزنگاری/رمزگشایی و درهم سازی یک طرفه و ساخت تابع‌های مختلف پشتیبانی می‌کند. همچنین حملات مختلف وارده به یک پروتکل امنیتی را بررسی می‌نماید. شکل ۶ نتیجه بررسی پروتکل پیشنهادی را نمایش می‌دهد که حاکی از امن بودن پروتکل پیشنهادی و کلید نشست است. همچنین شکل ۸ کدهای نوشته شده برای ابزار ProVerif می‌باشد.

Claim	Status	Comments
MAHDI user MAHDI,user1 Alive	Ok	No attacks within bounds.
MAHDI,user2 Nisynch	Ok	No attacks within bounds.
MAHDI,user3 Niagree	Ok	No attacks within bounds.
MAHDI,user4 Weakagree	Ok	No attacks within bounds.
MAHDI,user5 Secret H1(H1(N2,m4),N2,H1(IDi,ai),N3)	Ok	No attacks within bounds.
server MAHDI,server1 Alive	Ok	No attacks within bounds.
MAHDI,server2 Nisynch	Ok	No attacks within bounds.
MAHDI,server3 Niagree	Ok	No attacks within bounds.
MAHDI,server4 Weakagree	Ok	No attacks within bounds.
MAHDI,server5 Secret H1(H1(XOR(XOR(XOR(XOR(H1(IDi,H1(XOR(pvi,ai),N2),N3),N2),N3),N2),N3),N2),N3)	Ok	No attacks within bounds.

شکل ۵. خروجی تحلیل پروتکل با استفاده از ابزار Scyther

```
RESULT inj-event( AuthServerSj(IDi)) ==> injevent)
beginServerSj(IDi) is true.
RESULT inj-event( AuthUserUi(ID_۱۸۹۰)) ==> injevent)
beginUserUi(ID_۱۸۹۰) is true.
RESULT not attacker(SK[]) is true.
```

شکل ۶. خروجی ابزار ProVerif

با توجه به مطالب گفته شده، جدول سه نشان‌دهنده مقایسه امنیتی پروتکل پیشنهادی با دیگر طرح‌های مشابه را نشان می‌دهد. طرح پیشنهادی نسبت به طرح‌های مشابه، از نظر امنیتی قوی‌تر می‌باشد و در مقابل حملات مختلف مقاوم است و نیازهای امنیتی مختلف را تامین می‌کند.

حمله منع سرویس: در حمله منع سرویس، مهاجم سعی می‌کند با ارسال پیام‌های متوالی و بی ارزش، خدمات دهنده را مشغول کند به طوری که خدمات‌دهنده، امکان سرویس‌دهی به کاربر را نداشته باشد. در پروتکل پیشنهادی، به علت وجود اعداد تصادفی و همچنین وجود مهرهای زمانی و بررسی تازگی پیام در ابتدای هر گام، امکان وجود چنین حمله‌ای وجود ندارد. همچنین به علت اینکه پروتکل پیشنهادی سبک وزن است و هیچ جستجویی در پایگاه داده خدمات‌دهنده و یا محاسبه پیچیده‌ای در سمت خدمات‌دهنده وجود ندارد، در نتیجه امکان حمله منع سرویس وجود ندارد.

اثبات رسمی امنیت پروتکل پیشنهادی با استفاده از ابزارهای Proverif و Scyther

Scyther [۱۴] و Proverif [۱۵] ابزارهایی قدرتمند و مؤثر به منظور تجزیه و تحلیل، شناسایی حمله‌های احتمالی و آسیب‌پذیری‌های پروتکل‌های امنیتی هستند. این دو ابزار رسمی، پروتکل را به طور خودکار تحلیل نموده و رفتار آن را در مقابل اکثر حمله‌های ممکن، مورد بررسی دقیق قرار می‌دهند. در شکل ۷ کدهای نوشته‌شده برای ابزار scyther را مشاهده می‌نمایید.

شکل ۵، خروجی بررسی پروتکل پیشنهادی توسط scyther را نمایش می‌دهد. ویژگی Niagree تضمین می‌کند که طرفین ارتباط مطمئن هستند که پیام‌ها به طور امن و با ترتیبی درست بین آن‌ها رد و بدل شده است. ویژگی Nisynch تضمین می‌کند که پیام‌های رد و بدل شده بین طرفین قابل رمزگشایی و ارسال دوباره نباشد. ویژگی Alive تضمین می‌کند که ترتیب مراحل پروتکل به وسیله طرفین ارتباط، تایید شده است. ویژگی Weakagree تضمین می‌کند که در پروتکل، امکان جعل هویت وجود نداشته باشد. ویژگی secret نیز تضمین خواهد کرد که پارامتر مربوطه امن خواهد ماند. همانگونه که در شکل ۵ نشان داده شده است پروتکل احراز هویت معرفی شده در مقاله، قادر است تمامی ویژگی‌های فوق را تامین نماید.

<pre> usertype TimeStamp; const P; secret x, Y; secret IDi, pwi, ai, bi, Ci, x, m4; macro mpwi=XOR(H1(IDi, H1(XOR(pwi, ai))), pwi); macro Ci = H1(bi, IDi); macro Di= XOR(mpwi, Ci); macro HIDi= H1(IDi, ai); macro m1=H1(HIDi, ai); hashfunction H1; secret XOR: Function; macro Hi=XOR(Di, m1); macro qi={HIDi, bi, Hi}x; macro ci=add(bi, ai); macro m2=XOR(bi, ci); secret add: Function; secret sub: Function; protocol MAHDI(user, server) { role user { var N1, m5, m4; macro ai=add(bi, ci); macro Ai= H1(b1, Pi); macro mpwi1=XOR(H1(IDi, H1(XOR(pwi, ai))), pwi); macro Ci1 = H1(bi, IDi1); macro Di1= XOR(mpwi1, Ci); match(Di1, Di); macro HIDi1= H1(IDi, ai); macro Gi=XOR(HIDi1, ci); macro m^=H^(HIDi1, ai); send_1(user, server, (m1, Gi, bi, qi)); recv_2(server, user, (m5, m4)); macro N1=XOR(Di, m4); macro m55=H1(N1, Di); match(m5, m55); fresh N2; macro m6=H1(N2, m4); macro m7= XOR(N1, N2); macro m8=XOR(N1, m7); macro m9=H^(N2, m55); fresh N3; macro m10=XOR(N2, N3); macro sk=H1(m6, N2, HIDi, N3); send_3(user, server, (m8, m9, m10)); claim (user, Alive); claim (user, Nisynch); claim(user, Niagree); claim(user, Weakagree); claim(user, Secret, sk); }; </pre>	<pre> role server { var N2, N3; recv_1(user, server, m1, Gi, bi, qi); macro ai=sub(bi, ci); macro m12=H1(HIDi1, ai); match(m12, m1); fresh N1; macro m3=H1(N1, m12); macro Di=XOR(Hi, m^); macro m4=XOR(Di, N1); macro m5=H1(N1, Di); send_2(server, user, (m5, m4)); recv_3(user, server, (m8, m9, m10)); macro m7=XOR(m8, N1); macro N2=XOR(N1, m7); macro m99=H1(N2, m5); match(m99, m9); macro N3= XOR(N2, m10); macro m6=H1(N2, m4); macro sk=H1(m6, N2, HIDi, N3); claim (server, Alive); claim (server, Nisynch); claim(server, Niagree); claim(server, Weakagree); claim(server, Secret, sk); }; }; </pre>
---	--

شکل ۷. کدهای شبیه سازی پروتکل پیشنهادی با ابزار Scyther

<pre> (*Channels *) free SCh: channel [private]. (*Confidential Channel*) free PCh: channel. (*Open/insecure Channel*) (***) Constants and Variables (***) free IDi : bitstring. free SIDj : bitstring. free x : bitstring [private] . free BIOi : bitstring [private] . free PWi : bitstring [private] . (***) Constructor (***) fun h(bitstring) :bitstring. fun H(bitstring) :bitstring. fun XOR(bitstring, bitstring): bitstring. fun ENC(bitstring, bitstring): bitstring. fun DEC(bitstring, bitstring): bitstring. fun CONCAT(bitstring ,bitstring):bitstring. fun add(bitstring,bitstring):bitstring. fun sub(bitstring,bitstring):bitstring. (** Destructors & related Equations **) equation forall u: bitstring, v: bitstring; XOR (XOR(u,v) ,v)=u. reduc forall w: bitstring, key: bitstring; DEC (ENC (w, Pub) , Prs)=w. event beginUserUi (bitstring) . event AuthUserUi (bitstring) . event beginServerSj (bitstring) . event AuthServerSj (bitstring) . (*****p r o c e s s e s***** **** User Ui ****) let UserUi= (***** Registration ****) new ai:bitstring; let MPWi=XOR(h(CONCAT(IDi,h(XOR(PWi,ai))))),PWi) in out (SCh , (IDi , MPWi , ai)) ; in (SCh , (xbi:bitstring,xDi:bitstring,xqi:bitstring,xHIDi:bitstring)); let ci=add(xbi,ai)in let M2=XOR(xbi,ci) in (***) Login and Authentication (***) event beginUserUi (IDi) ; let ai=add(xbi,ci)in let MPWi=XOR(h(CONCAT(IDi,h(XOR(PWi,ai))))),PWi) in let Ci=h(CONCAT(xbi,IDi))in let Di=XOR(MPW, Ci)in if (xDi=Di) then let HIDi=h(CONCAT(IDi,ai))in let Gi=XOR(HIDi,ci)in let M1=h(CONCAT(HIDi,ai))in out(PCh,(M1,Gi,xbi,xqi)); in(PCh,(xM5:bitstring,xM4:bitstring)); let N1=XOR(Di,xM4) in let M5=h(CONCAT(N1,Di))in if (M5=xM5)then new N2:bitstring; </pre>	<pre> let M6=h(CONCAT(N2,M4)) in let M7=XOR(N1,N2)in let M8=XOR(M7,N1) in let M9=h(CONCAT(N2,M5)) in new N3:bitstring; let M10=XOR(N2,N3)in let sk=h(CONCAT(CONCAT(CONCAT(M6,N2),HIDi),N3))in out(PCh,(M8,M9,M10)); (****Server (Sj) ****) (** Server Sj **) let ServerSj= (***** Registration *****) event beginServerSj (SIDj); new bi:bitstring; let Ci=h(CONCAT(IDi,bi)) in let Di=XOR(xMPWi,Ci)in let HIDi=h(CONCAT(IDi,xai))in let M1=h(CONCAT(HIDi,xai))in let Hi=XOR(Di,M1)in let qi=ENC(CONCAT(HIDi,CONCAT(bi,Hi)),x)in out (SCh,(bi,Di,qi,HIDi)); in(PCh,(xM1:bitstring,xGi:bitstring,xbi:bitstring,xqi:bitstring)); let ci=XOR(HIDi,Gi) in let ai=sub(bi,ci)in let M1=h(CONCAT(HIDi,ai))in if (xM1=M1) then new N1:bitstring; let M3=h(CONCAT(N1,M1))in let Di=XOR(Hi,M1)in let M4=XOR(Di,N1)in let M5=h(CONCAT(N1,Di))in out(PCh,(M5,M4)); in(PCh,(xM8:bitstring ,xM9:bitstring ,xM10:bitstring)) let M7=XOR(M8,N1) in let N2=XOR(N1,M7) in let M9=h(CONCAT(N2,M5)) in if (xM9=M9)then let N3=XOR(N2,xM10) in let M6=h(CONCAT(N2 M4))in let sk=h(CONCAT(CONCAT(CONCAT(M6,N2),HIDi),N3))in else 0. process ((! UserUi) (!ServerSj)) (** Queries **) free sk: bitstring [private]. query attacker (SK). query IDi: bitstring ; inj event (AuthUserUi (IDi)) ==> inj event (beginUserUi (IDi)). query id : bitstring ; inj event (endServerSj (IDi)) ==> inj event (beginServerSj (IDi)). </pre>
--	---

شکل ۸. کدهای شبیه سازی پروتکل پیشنهادی با ابزار proverif

نیازهای امنیتی مختلف را تامین می کند. این امر نشان از برتری روش پیشنهادی نسبت به روش های مشابه دارد.

با توجه به مطالب گفته شده، جدول سه نشان دهنده مقایسه امنیتی پروتکل پیشنهادی با دیگر طرح های مشابه را نشان می دهد. طرح پیشنهادی نسبت به طرح های مشابه، از نظر امنیتی قوی تر می باشد و در مقابل حملات مختلف مقاوم است و

جدول ۳. مقایسه امنیتی روش پیشنهادی با طرح های مشابه

نیازمندی امنیتی	[۲۳]	[۲۶]	[۲۹]	[۹]	طرح پیشنهادی
محرماتگی رو به جلو	بله	بله	بله	خیر	بله
گمنامی کاربر	خیر	خیر	خیر	بله	بله
مقاومت در برابر حمله تکرار	خیر	خیر	بله	بله	بله
مقاومت در برابر حمله جعل هویت خدمات دهنده	خیر	بله	خیر	بله	بله
مقاومت در برابر حمله جعل هویت کاربر	خیر	بله	خیر	بله	بله
مقاومت در برابر حمله افشای پارامترهای تصادفی	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	خیر	بله
مقاومت در برابر منع سرویس	خیر	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	در مقاله اصلی بررسی نشده	بله

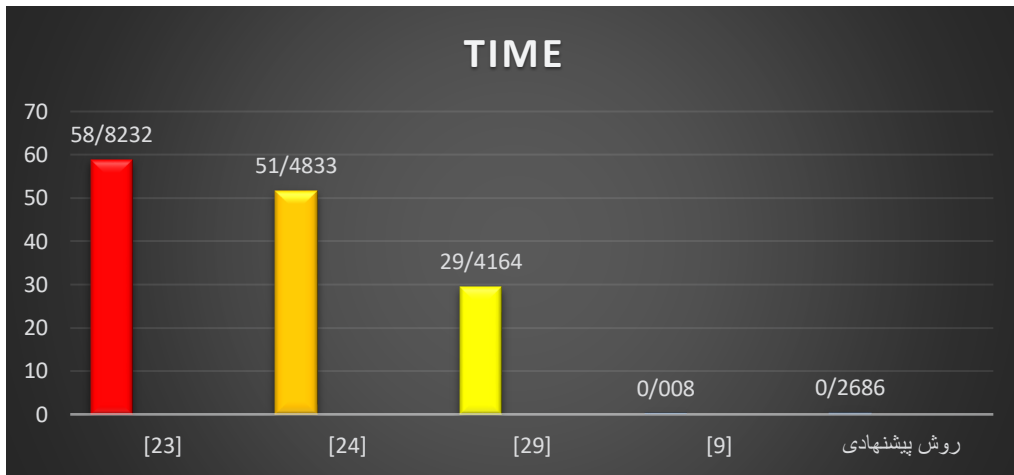
پیشنهادی و طرح های مشابه است. همانطور که شکل ۹ نشان می دهد، طرح پیشنهادی از نظر سربار زمانی، بهتر و یا نزدیک به طرح های مشابه عمل می کند. اهمیت این مساله زمانی مشخص می شود که برتری روش پیشنهادی را در زمینه مقاومت در برابر حملات شناخته شده در برابر سایر روش های مورد مقایسه، در نظر بگیریم. به عبارت دیگر، طرح پیشنهادی قادر است با پیچیدگی زمانی کمتر از اغلب روش های مشابه، نیازمندیهای امنیتی را به طور کامل تامین نماید.

تحلیل و مقایسه پیچیدگی زمانی و سخت افزاری طرح پیشنهادی و دیگر طرح های مشابه

بر طبق مقالات [۳۴] و [۳۵]، پیچیدگی زمانی هر ضرب نقطه ای روی منحنی بیضوی، $7,3529$ میلی ثانیه و هر درهم ساز یک طرفه $0,0004$ میلی ثانیه است. همچنین پیچیدگی زمانی هر جمع نقطه ای روی منحنی بیضوی، $0,009$ میلی ثانیه و مدت زمان هر رمزنگاری/رمزگشایی $0,1303$ میلی ثانیه می باشد. اگر h و mu و ad و en/d را به ترتیب نمادهای درهم ساز یکطرفه و ضرب نقطه ای روی منحنی بیضوی و جمع نقطه ای روی منحنی بیضوی و همچنین رمزنگاری/رمزگشایی در نظر بگیریم، جدول ۴ نشان دهنده مقایسه پیچیدگی زمانی طرح

جدول ۴. مقایسه پیچیدگی زمانی

طرح پیشنهادی	[۹]	[۲۹]	[۲۶]	[۲۳]
زمان مرحله ثبت نام	$5h$	$3h$	$4mu+1ad+5h$	$4mu+6h$
زمان مرحله احراز هویت	$15h+1en/d$	$4mu+9h$	$3mu+5h$	$4mu+7h$
زمان کل	$20h+2en/d$	$4mu+12h$	$7mu+1ad+10h$	$8mu+13h$
زمان (میلی ثانیه)	0.2686	29.4164	51.4833	58.8232



شکل ۹. نمودار مقایسه پیچیدگی زمانی طرح پیشنهادی و طرح‌های مشابه

نتیجه‌گیری و کارهای آینده

در این مقاله، پروتکلی کارآمد و سبک‌وزن برای ارتباط امن دستگاه‌های VoIP مبتنی بر کارت هوشمند ارائه گردید. تحلیل‌های امنیتی پروتکل نشان داد که طرح ارائه شده در برابر حملات مختلف مقاوم است و نیازهای امنیتی گوناگون را تأمین می‌کند همچنین صحت امنیتی پروتکل با کمک ابزار Scyther و نیز Proverif بررسی و تایید گردید. همچنین در آینده می‌توان طرحی ارائه گردد که فقط مبتنی بر رمز عبور باشد، یعنی نیازی به کارت هوشمند احساس نشود، همچنین می‌توان پروتکل پیشنهادی را از نظر زمانی بهبود بخشید.

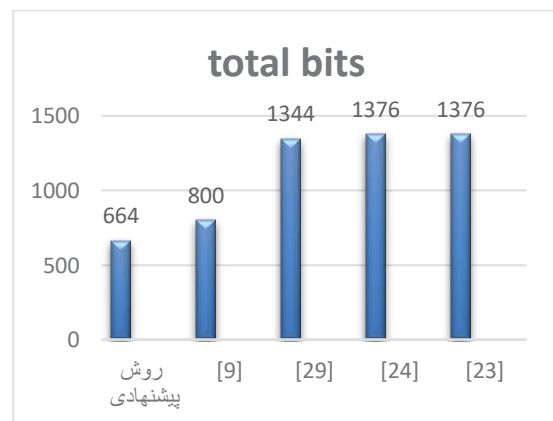
مراجع

- [1] Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L. Http authentication: Basic and digest access authentication. In: IETF RFC2617, 1999.
- [2] Yeh H., Chen T., Shih W., Robust smart card secured authentication scheme on SIP using Elliptic Curve Cryptography. Computer Standards & Interfaces; 2014, vol. 36, no.2, pp: 397-402.
- [3] Zhang L, Tang S, Zhu S, An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks, J Netw Comput Appl, 2016, vol. 59, pp. 126-133.

برای مقایسه طرح‌های مختلف میتوان تعداد بیت‌های موجود در پیام‌های مبادله شده در مرحله احراز هویت را نیز در نظر گرفت. بر اساس مقالات [۱۰] [۳۶] [۳۷] هر تابع درهم ساز یک طرفه ۱۶۰ بیت، ضرب اسکالر ۳۲۰ بیت، پارامتر رمزنگاری شده ۱۲۰ بیت، شناسه ۱۶۰ بیت و مهر زمانی ۳۲ بیت نیاز دارد. با مراجعه به جدول مقایسه‌ای ۵ و شکل ۱۰، مشاهده می‌شود که پروتکل پیشنهادی حاوی کمترین تعداد بیت رد و بدل شده بر روی کانال در مرحله احراز هویت است.

جدول ۵. مقایسه سخت افزاری

طرح	تعداد پیام‌های رد و بدل شده	تعداد بیت‌های رد و بدل شده
پیشنهادی	۳	۶۶۴
[۹]	۳	۸۰۰
[۲۶]	۳	۱۳۴۴
[۲۶]	۳	۱۳۷۶
[۲۳]	۳	۱۳۷۶



شکل ۱۰. نمودار مقایسه تعداد بیت‌های رد و بدل شده

- [12] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, 2019, vol. 43, p. 10.
- [13] Ostad-Sharif, A, Abbasinezhad-Mood, D, Nikooghadam, M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. *Int J Commun Syst.* 2019, vol. 32, no. 5.
- [14] Cremers, C, Scyther - Semantics and Verification of Security Protocols. Ph.D. dissertation, Eindhoven University of Technology, 2006.
- [15] Blanchet B, Cheval V, Allamigeon X, Smyth B. ProVerif: Cryptographic protocol verifier in the formal model. (Available at: <http://prosecco.gforge.inria.fr/personal/bblanche/proverif/>).
- [16] A. Durlanik, I. Sogukpinar. SIP authentication scheme using ECDH. *World Enformatika Society Transaction on Engineering Computing and Technology*, 2005, vol. 8, pp.350-353.
- [17] EJ Yoon, KY Yoo, et al..A secure and efficient SIP authentication scheme for converged VoIP networks. *Computer Communications*, 2010, vol. 33, pp.1674-1681.
- [18] Zhang L., Tang S., Cai Z.. Efficient and flexible password authenticated key agreement for Voice over Internet Protocol Session Initiation Protocol using smart card. *International Journal of Communication Systems* 2014.
- [19] Farash MS. Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. *Peer-to-Peer Networking and Applications*. 2016, vol. 9, no. 1, pp: 82–91.
- [20] Kumari S, Chaudhry S, Wu F, Li X, Farash M, Khan M. An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Applications*. 2015, vol. 10. no. 1, pp. 92-105.
- [4] Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for sip. *Peer-to-Peer Networking and Applications*, 2017, vol. 10, no. 1, pp. 1-15.
- [5] Sourav S., Odelu V., Prasath R., Enhanced Session Initiation Protocols for Emergency Healthcare Applications. In: Thampi S., Madria S., Wang G., Rawat D., Alcaraz Calero J. (eds) *Security in Computing and Communications (SSCC), Communications in Computer and Information Science*, 2018, vol 969, pp 278-289.
- [6] Arshad H, Nikooghadam M. An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. *Multimedia Tools and Applications* 2016, vol. 75, no.1, pp.181-197.
- [7] H. Arshad and M. Nikooghadam, "Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol," *J. Supercomput.*, 2015, vol. 71, no. 8, pp. 3163–3180.
- [8] Dhillon, P.K.; Kalra, S. Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. *Multimed.ToolsAppl.* 2019, vo. 78, no. 16, pp.22199-22222.
- [9] Zhang Y, Xie K, Ruan O An improved and efficient mutual authentication scheme for session initiation protocol. *PLoS ONE*, , 2019, vol.14, vo.3.
- [10] Ravanbakhsh, N., Mohammadi, M. Nikooghadam, Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme, *M. Multimed Tools Appl*, 2019, vol. 78, no. 9, pp. 11129-11153.
- [11] Amin R, Islam S, Biswas G, Giri D, Khan MK, Kumar N. A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments. *Secur Commun Netw.* 2016, vol. 9, no.17, pp.4650-4666.

- [29] Lu Y, Li L, Peng H, Yang Y, A secure and efficient mutual authentication scheme for session initiation protocol. *Peer-to-Peer Netw Appl*, 2016, vol. 9, no. 2, pp. 449-459.
- [30] V. Sureshkumar, R. Amin, and R. Anitha, A robust mutual authentication scheme for session initiation protocol with key establishment, *Peer-to-Peer Netw. Appl.*, 2018, vol. 11, no. 5, pp. 900-91.
- [31] Zhang L, Tang S, Zhu S, An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. *J Netw Comput Appl*, 2016, vol.59, pp.126-133.
- [32] Qiu S, Xu G, Ahmad H. An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy. *PLOS ONE*, 2018, vol. 13, no, 3.
- [33] M. Nikooghadam, R. Jahantigh, and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools Appl.*, 2017, vol.76, no.11, pp. 13401-13423.
- [34] Xu, L., Wu, F., Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. *Journal of medical systems*, 2015, vol. 39, no. 10.
- [35] Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Obaidat, M. S., Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. *Journal of medical systems*, 2015, vol. 39, no.11, pp. 137.
- [36] Xu L, Wu F Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. *J Med Syst*, 2015, vol. 39, no. 2, pp: 1-9.
- [37] Kumari S, Karupiah M, Das AK, Li X, Wu F, Gupta V. Design of a secure anonymity preserving authentication scheme for session initiation protocol using elliptic curve cryptography. *J Ambient Intell Human Comput.*, 2018, vol. 9, no.3, pp 643-653.
- [21] Zhang L, Tang S, Cai Z. Cryptanalysis and improvement of password-authenticated key agreement for session initiation protocol using smart cards. *Security and Communication Networks.*, 2014, vol. 7, no. 12, pp.2405-2411.
- [22] Jiang Q, Ma J, Tian Y, Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al. *Int J Commun Syst*, 2015, vol.28, no. 7, pp:1340-1351.
- [23] Tu, H., Kumar, N., Chilamkurti, N., Rho, S., An improved authentication protocol for session initiation protocol using smart card. *Peer-to-Peer Networking and Applications*, 2015, vol. 8, no. 5, pp. 903-910.
- [24] Farash MS. Security analysis and enhancements of an improved authentication protocol for session initiation protocol with provable security. *Peer-to-Peer Networking and Applications*, 2016, vo. 9, no. 1, pp: 91-102.
- [25] Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for sip. *Peer-to-Peer Networking and Applications*, 2017, vol. 10, no. 1, pp. 10-1.
- [26] Mishra D, Das AK, Mukhopadhyay S, A secure and efficient ECC-based user anonymity preserving session initiation authentication protocol using smart card. *Peer-to-peer Netw Appl*, 2016, vol. 9, no. 1, pp. 171, 172.
- [27] Farash MS, Attari MA. An anonymous and untraceable password-based authentication scheme for session initiation protocol using smart cards. *International Journal of Communication Systems*, 2016, vol. 29. no. 13, pp. 1956-1967.
- [28] Lu Y, Li L, Peng H, Yang Y, An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. *Multimedia Tools and Applications*, 2017, vol. 76, no. 2, pp. 1801-1815.

