تحلیل امنیتی پروتکل احراز اصالت سبک‌وزن گوتام و اصلاح آن

رضا سمیاری *[1]، رحیم اصغری[2]
۱- دانشجوی کارشناسی ارشد مخابرات امن، دانشگاه صنعتی مالک اشتر تهران
۲- استادیار دانشگاه صنعتی مالک اشتر تهران

چکیده

اخیراً گوتام پیشنهاد یک طرح احراز هویت کاربر سبک‌وزن مبتنی بر شناسه با مرحله توافق کلید با استفاده از رمزنگاری منحنی بیضوی ارائه نمود که برای محیط سرویس‌دهنده/گیرنده مناسب می‌باشد. بااین‌حال، مابعد از بررسی‌هایی که انجام دادیم دریافتیم که این طرح دارای ضعف‌های امنیتی متعددی است، ازجمله ضعف در برابر حملاتی از قبیل محرمانگی روبه‌جلو , انسداد سرویس، ردیابی، دزدیدن کارت هوشمند و غیره. در این مقاله، جهت اصلاح طرح گوتام و برطرف کردن ضعف‌های آن، نسخه جدیدی از طرح احراز هویت ناشناس به همراه توافق کلید مورداستفاده برای محیط سرویس‌دهنده/گیرنده را پیشنهاد نمودیم. در طرح احراز هویت پیشنهادی، سعی شده است که علاوه بر استفاده از مزایای طرح احراز هویت گوتام از یک روش ترکیبی مبتنی بر رمزهای کلید همگانی و رمزهای کلیدمتفارن برای ایجاد اصلاحات لازم بکارگیری شود. در انتها، تحلیل‌های امنیتی لازم برای اثبات درستی اصلاحات انجام‌شده ارائه گردیده است.

کلمات کلیدی: رمزنگاری، پروتکل احراز هویت، گمنامی، پروتکل احراز هویت گوتام، اینترنت اشیا

۱. مقدمه

اصطلاح اینترنت اشیا تکامل مستمر اینترنت را به شبکه‌ای از اشیاء هوشمند توصیف می‌کند. این اشیاء قابلیت اتصال به اینترنت رادارند و می‌توانند باهم و با منابع مرکزی ارتباط برقرار کنند. اینترنت اشیا از فناوری‌های متعددی مانند شبکه‌های حسگر بی‌سیم، شهرهای هوشمند، خانه‌های هوشمند و سامانه‌های تلفن همراه استفاده می‌کند. این سناریوها نیاز به راه‌حل‌های امن برای جلوگیری از نشت اطلاعات خصوصی و فعالیت‌های مخرب دارند. بااین‌وجود، ساختارهای اینترنت اشیا مبتنی بر آی پی، با محدودیت دستگاه‌های اینترنت اشیا مانند مصرف انرژی، منابع محاسباتی، محدوده ارتباطات، حافظه به‌طور کامل طراحی نشده است. به‌عنوان یک نتیجه، به‌کارگیری راه‌حل‌های امنیتی بسیار سبک، برای اطمینان از امنیت دستگاه‌های منابع محدود اینترنت اشیا مناسب است[1, 2].

همانند شبکه‌های آی پی موجود، در سناریوهای مختلف اینترنت اشیا ، اصول اولیه رمزنگاری در اینترنت اشیا برای رعایت اهداف امنیتی که یکی از مهم‌ترین این اصول مسئله احراز هویت است، استفاده می‌شود که در این مقاله موردبحث قرارمی گیرد[3,4, 5]. در اینترنت اشیا، احراز هویت شامل فرآیند شناسایی کاربران، دستگاه‌ها، برنامه‌ها و محدود کردن دسترسی فقط برای کاربران مجاز می‌باشد. اگر اینترنت اشیا را یک محیط سرویس‌دهنده/گیرنده در نظر بگیریم، آن سرویس دهنده می‌تواند با کمک پروتکل‌های احراز هویت دستگاه قانونی یا ثبت‌شده اینترنت اشیا را شناسایی و از پذیرفتن دستگاه‌های غیرقانونی یا جعلی امتناع نماید. سپس سرویس دهنده و دستگاه، کلیدی برای برقراری ارتباط امن فراهم می‌کند که شامل انتقال داده‌های حساس، فرمان و به‌روزرسانی اطلاعات دستگاه و غیره می‌باشد. بنابراین احراز هویت نقش مهمی را در

* Corresponding author: رضا سمیاری
Email: REZA.SEMYARI@GMAIL.COM

رعایت الزامات امنیتی برای دستگاه‌های اینترنت اشیا ایفا می‌کند. طی سال‌های متمادی، پروتکل‌های احراز هویت بسیاری برای دستگاه‌های تعبیه‌شده که از رمزنگاری متقارن یا رمزنگاری کلید عمومی استفاده می‌کنند پیشنهادشده است [2,5, 6].

در این مقاله، ما یک طرح ترکیبی به‌صورت استفاده هم‌زمان از رمزهای کلید همگانی که یکی از بهترین‌های آن رمزهای مبتنی بر خم بیضوی است که مناسب برای دستگاه‌های محدود اینترنت اشیاست و رمزهای کلید خصوصی ارائه می‌کنیم.
در این طرح پیشنهادی، از رمزهای کلید همگانی صرفا برای توافق کلید بین سرویس‌گیرنده و سرویس دهنده استفاده می شود و در بقیه مراحل از رمزهای متقارن که شامل کلمه عبور است، استفاده می شود.
ساختار این مقاله به این گونه است که در بخش دوم مروری بر طرح احراز هویت گوتام شده است. در بخش سوم نقاط ضعف این پروتکل را بررسی می‌کنیم. در بخش چهارم طرح پیشنهادی جهت اصلاح ضعف ها را بیان کرده و در بخش پایانی تحلیل امنیتی طرح احراز هویت پیشنهادی به همراه مقایسه ها ارائه شده است.

۲. مروری بر طرح گوتام

گوتام یک طرح احراز هویت متقابل با توافق کلید جلسه بین کاربر U و یک سرویس دهنده S از راه دور را ارائه می‌دهد. سرویس دهنده ابتدا پارامترهای سیستم را تنظیم نموده و در زمان ثبت‌نام یک کلید مخفی برای هر کاربر توزیع می‌کند. طرح پیشنهادی گوتام در پنج فاز انجام می‌شودکه شامل فاز اولیه سیستم، مقادیر حداکثر و حداقل، USN، مرحله ثبت‌نام کاربر، احراز هویت متقابل با مرحله توافق کلید و مرحله به‌روزرسانی هویت است. در ادامه به تشریح فاز های مختلف این طرح می پردازیم[7, 8].

۲-۱. فاز راه‌اندازی سیستم

سرویس دهندهS، در پنج گام پارامترهای زیر را برای راه‌اندازی سیستم تولید می‌کند[7, 8].
گام ۱: سرویس دهنده S ، یک معادله منحنی بیضوی به همراه درجه n انتخاب می‌کند.
گام ۲ : سرویس دهندهS ، یک نقطه پایه P را بر روی E انتخاب می‌کند.
گام ۳ : سرویس دهندهS ، کلید خصوصی خود با نام q_s را انتخاب کرده، سپس کلید عمومی را به‌صورت معادله زیر محاسبه می‌کند.

$$Q_S = q_s * P \quad (1)$$

گام ۴: سرویس دهنده S ، چهار تابع چکیده ساز یک‌طرفه با نام های H1 (.)، H2 (.)، H3 (.)،H4 (.) و کد تأیید پیام MAC_k () را تولید می‌کند.
گام ۵ : سرویس دهندهS ، کلید خصوصی q_s را ذخیره و پیام زیر را منتشر می‌کند.

$$\{E, P, QS, H1(.), H2(.), H3(.), H4(.), MAC_k()\} \quad (2)$$

۲-۲. مقادیر حداکثر و حداقل و USN

مقادیر حداکثر و حداقل اختصاص داده‌شده به هر کاربر در مرحله ثبت‌نام صورت می پذیرد. اندازه مقدار حداکثر، حداقل باید سه برابر مقدار حداقل باشد. و یک شماره توالی منحصربه‌فرد به نامUSN نیز برای هر کاربر همراه با مقادیر حداکثر و حداقل اختصاص داده می‌شود.

۲-۳. فاز ثبت‌نام کاربر

فاز ثبت‌نام زمانی رخ می‌دهد که کاربر U بخواهد از راه دور با سرویس دهنده S ارتباط برقرار نماید. تمام گام های این فاز در یک کانال امن قرار می‌گیرد[7, 8].

گام ۱: کاربر با آی دی خود وارد سرویس دهنده می‌شود.

گام ۲: سرویس دهنده S مقدار IDU را ذخیره کرده و مقدار Hu=H1(IDU) را محاسبه می‌کند.

گام ۳: سرویس دهنده S مقدار حداکثر و حداقل را همراه با شماره توالی کاربر (USN) تعیین می‌کند.

گام ۴: سرویس دهنده S کلید مخفی کاربر را به روش زیر محاسبه می‌نماید:

$$xU= (1/ (qS.hU)) P) \quad (3)$$

گام ۵: مقادیر xU ، حداکثر، حداقل، USN را در یک کارت هوشمند چاپ می‌کند و آن را به کاربر U می‌دهد.

۲-۴. تأیید هویت مشترک با مرحله توافق کلید

در این مرحله، کاربر U درخواستی را به سرویس دهنده از راه دور برای دسترسی به تعدادی از منابع S می‌فرستد. سپس سرویس دهنده S درخواست را با تائید کاربر U در نظر می‌گیرد و جلسه بین U و S با یک کلید جلسه انجام می‌شود. کاربر U از طریق ارسال یک شناسه ناشناس به سرویس دهنده S به روش زیر، احراز هویت ناشناس می‌شود.

۲-۴-۱. تأیید هویت کاربر U توسط سرویس دهنده S

مرحله ۱ : U کارت هوشمند خود را به دستگاه کارت‌خوان C وارد می‌کند و هویت IDU را وارد می‌کند.

مرحله ۲: دستگاه کارت خوان C، شناسه ناشناس AIDU را با استفاده از Rand، Max، Min و TU زمان فعلی را به صورت زیر محاسبه می‌کند.

مرحله ۲-۱: محاسبه UR با در نظر گرفتن یک عدد تصادفی :Rand که در زیر ذکرشده:

$$UR = (Rand \%(Max - Min + 1)) + Max; \quad (4)$$

به طوری که

$$Rand>Max>Min$$

مرحله ۲-۲: تولید شناسه شناسایی AID_U با استفاده از مقدار محاسبه‌شده:

$$AIDU=IDU \oplus H_2 (U_R ||T_U) \quad (5)$$

مرحله ۳: دستگاه کارت خوان C ، یک شماره تصادفی r_U را انتخاب نموده و مقادیر را به صورت زیر محاسبه می‌کند.

$$R = r_u. P \quad , \quad R^1 = r_u. x_u \quad (6)$$
$$k = H_3(IDU, T_U, R, R^1), \quad MAC_k (IDU, T_U, R)$$

درنهایت کاربر U یک پیام درخواستی

$$M_1 = [AID_U, T_U, R, USN, Rand, MAC_k (IDU, T_U, R)] \quad (7)$$

را به سرویس دهنده S ارسال می‌کند.

مرحله ۴: پس از دریافت پیام M_1، سرویس دهنده S اعتبار بازه زمانی را با انجام رابطه زیر می‌سنجد.

$$\Delta T \leq TS1 - T_U \quad (8)$$

مرحله ۵: سرویس دهنده S مقدار UR را از دریافت Rand محاسبه می‌کند و سپس IDU را از AIDU. رمزگشایی می کند. اگر هرکدام از مقادیر IDU یا ΔT نامعتبر باشد، سرویس دهنده S سیستم تأیید هویت را قطع می‌کند.

$$UR = (Rand \% (Max Min + 1)) + Max \quad (9)$$
$$IDU = AIDU \oplus H_2 (UR ||T_U)$$

اگر IDU و ΔT معتبر باشند، سرویس دهنده S محاسبه روابط زیر را انجام می‌دهد.

$k = H_3 (IDU, T_U, R, R^1)$ و

$h_U = H_1(ID_U)$ $R^1 = (1/(q_s . h_u)) . R$ (10)

و سپس یکپارچگی $MAC_k(IDU, T_U, R)$ را با کلید k می‌سنجد. اگر خروجی منفی تولید کند، سیستم از جلسه خارج در غیر این صورت کاربر U توسط سرویس دهنده S تأیید می‌شود.

۲-۴-۲: احراز هویت سرویس دهنده S توسط کاربر U

مرحله ۷ : سرویس دهنده S به‌طور تصادفی عدد r_s را انتخاب و محاسبه مقادیر زیر را انجام می دهد[7, 8, 9].

$L = r_S . P, L_S = r_S . R, MAC_k (ID_U, T_{S2}, L)$

$S_k = H_4(IDU, T_U, TS2, L, L_S, UR)$ (11)

و سپ پیام زیر را می‌فرستد.

$M_2 = [AID_U, TS2, L, MAC_k(ID_U, TS2, L)]$ (12)

که در آن s_k یک کلید جلسه است و TS2 نشانگر زمان سرویس دهنده است که زمان فعلی را در هنگام ارسال پیام نشان می‌دهد.

مرحله ۸: پس از دریافت M2، کاربر U یکپارچگی $MAC_k(ID_U, T_{S2}, L)$ با کلید k تائید می‌کند. اگر آن را نگه ندارد، سیستم قطع خواهد شد در غیر این صورت، کاربر U محاسبه مقادیر زیر را انجام می‌دهد.

$L_U = r_U . L, s_k = H_4(IDU, T_U, TS2, L, L_U, U_R)$ (13)

مرحله۹ : اگر مقدار کلید نشست دریافت شده و مقدار محاسبه‌شده، برابر با مقدار S باشد، توسط کاربر U تائید می‌شود.

۲-۵. فاز به‌روزرسانی هویت

زمانی که یک کاربر بخواهد به جهت جلوگیری از حملات مخرب، شناسه هویت خود را تغییر دهد، از این فاز استفاده می شود. کاربرU تولید مقدار AIDU را با کمک IDU کنونی انجام می‌دهد و نشان می‌دهد که در مرحله احراز هویت متقابل است، سپس مقادیر زیر را با انتخاب عدد تصادفی r_u محاسبه می‌کند.

$k = H_3(IDU, TU, R, R1)$

$R = r_u . P, R^1 = r_u . x_u$ (14)

را محاسبه می‌کند. در حال حاضر، U یک هویت IDU # را دوباره انتخاب می‌کند و مقدار

$AIDU\# = IDU \oplus \#IDU$ (15)

را محاسبه می‌کند .و یک پیام به‌روزرسانی شده را می‌فرستد:

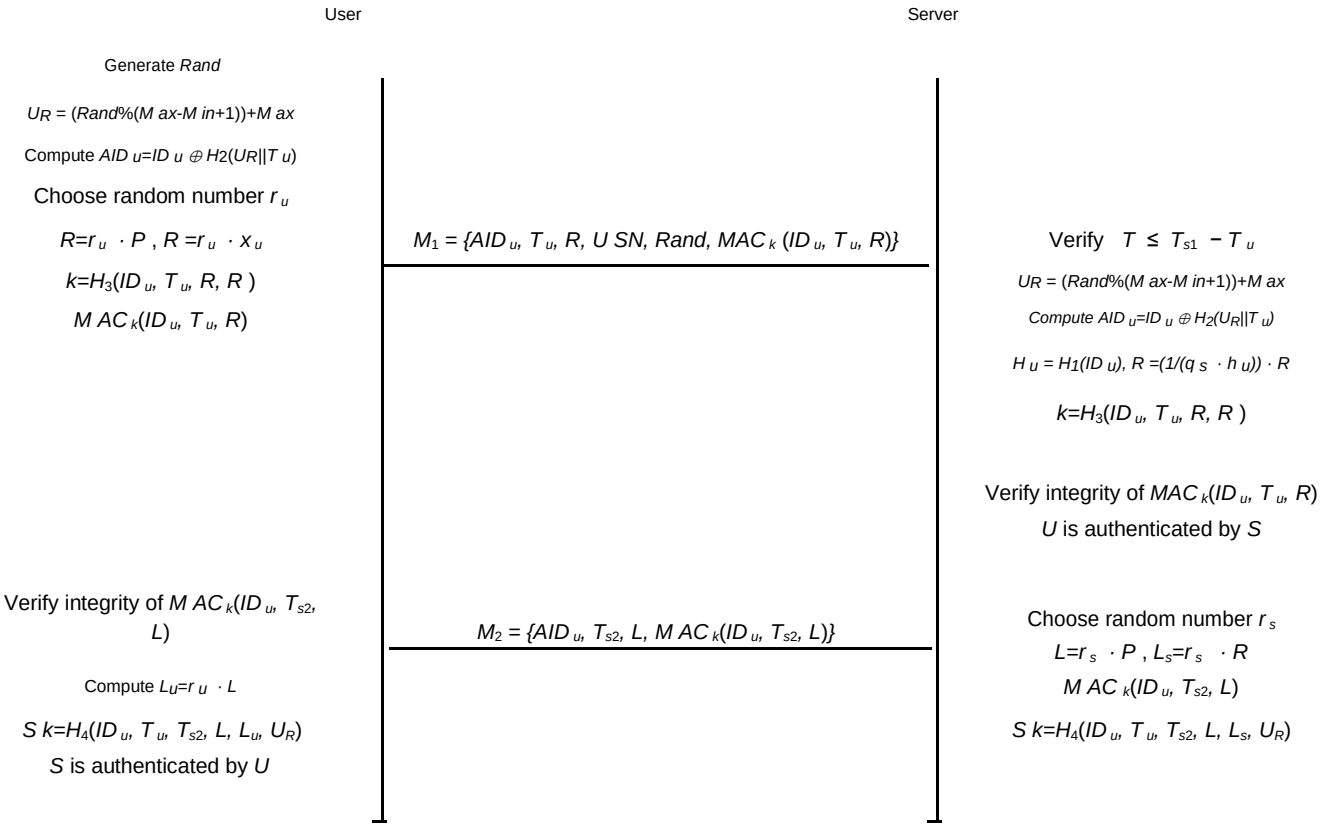
$M = [AID_U, AIDU\#, USN, Rand, T_U, MAC_k(ID_U, IDU\#)]$ (16)

پس از دریافت پیام از کاربرU سرویس دهنده S، مقدار IDU فعلی را همان‌طور که در مرحله احراز هویت توضیح داده‌شده است از AIDU رمزگشایی خواهد کرد، و دوباره IDU # از AIDU # بدست می آید که به شرح زیر است:

$\#IDU = IDU \oplus AIDU\#$ (17)

اکنون کاربر S به‌روزرسانی IDU را با کمک مقدار IDU # و محاسبه نمودن $h_U\# = H_1(ID_U\#)$ و بکارگیری کلید مخفی کاربر P.$(1 / (q_S . h_U))$ $x_U\# = (1 / (q_S . h_U)).P$ انجام می‌دهد. کاربرS چاپ کردن مقادیر x_u #، مقدارحداکثر، مقدارحداقل و مقدار USN در یک کارت هوشمند را انجام داده و آن را در یک کانال امن به کاربر U ارائه می‌دهد.

مراحل انجام پروتکل احراز هویت گوتام در شکل ۱ آمده است.



شکل۱: مروری بر طرح احراز هویت گوتام

۳. نقاط ضعف طرح گوتام

طرح گوتام که برای احراز هویت دوطرفه و توافق کلید مطرح‌شده است، برخی از نقص‌ها را با خود به همراه دارد. در این بخش، ضعف های موجود در طرح گوتام را بیان می نماییم.

۳-۱. ضعف اول: ضعف درمحرمانگی روبه‌جلو

سرویس‌گیرنده Ci هویت اصلی خود را از طریق رابطه زیر به‌روزرسانی می‌کند.

$$AIDU\# = IDU \oplus \#IDU \quad (18)$$

مهاجم اگر ارزش اولیه هویت سابق را بداند، می‌تواند هویت اصلی جدید را محاسبه کند. هم چنین هویت اولیه نیز می تواند به همان شیوه محاسبه شود. درعین حال انتخاب ارزش هویت توسط سرویس‌گیرنده ، ممکن است باعث ایجاد تصادم با سایر سرویس‌گیرندگان هم بشود. همچنین این پروتکل هیچ گونه اشاره‌ای به نحوه برخورد با این وضعیت ندارد.

۳-۲. ضعف دوم: ضعف قابل‌ردیابی بودن

طرح گوتام از طریق محاسبه UR از غیرقابل ردیابی بودن سرویس‌گیرنده محافظت می‌کند و سپس در پیام M1 در زمان احراز هویت متقابل با مرحله توافق کلید، مقدار USN و Rand را ارسال می‌کند. ازآنجاکه USN ارزش منحصربه‌فردی دارد، سرویس دهنده S می‌تواند با استفاده از جستجوی USN مقدار حداکثر و حداقل را برای

سرویس‌گیرنده و سپس شناسه او محاسبه کند. این بدین معنی است که این طرح هرچند که شناسه سرویس‌گیرنده را پنهان می‌کند، اما یک هویت دیگری به نام USN اضافه می‌کند. مهاجم USN سرویس‌گیرنده را به رسمیت می‌شناسد، زیرا این مقدار تغییر نمی‌کند.

از طرفی اضافه کردن استفاده از تابع Rand در M1 نیز هزینه‌های ارتباطی را افزایش می‌دهد، که ممکن است به دلیل کمبودهای موجود در منابع محاسباتی و توان پردازشی بر عملکرد پروتکل ارائه‌شده در محیط بی‌سیم تأثیر بگذارد.

۳-۳. ضعف سوم: ضعف درمقابل حمله کارت هوشمند به سرقت رفته

حمله کارت هوشمند به این معنی است که یک مهاجم حملات حدس رمز عبور آفلاین را با دست‌کاری پیام‌های تحت نظارت پروتکل و اطلاعات ذخیره‌شده در کارت هوشمند راه‌اندازی می‌کند. البته خود گوتام در مقاله اش در رابطه با ضعف پروتکل پیشنهادی اش نسبت به این نوع حمله بحث و به وجود آن اذعان نموده است.

۴. طرح احراز هویت سبک‌وزن پیشنهادی

طرح احراز هویت پیشنهادی ما چهار فاز دارد که عبارت‌اند از :

- فاز مقداردهی اولیه
- فاز ثبت‌نام کاربر
- فاز احراز هویت متقابل به همراه توافق کلید
- فاز به‌روزرسانی اطلاعات شخصی کاربر مانند کلمه عبور

۴-۱. فاز اول: مقداردهی اولیه سیستم

سرویس دهنده S یک معادله خم بیضوی E و نقطه p روی آن معادله را انتخاب می‌کند. همچنین سرویس دهنده S باید کلید عمومی را به‌صورت زیر به دست آورد:

$$Q_S = q_u * P \quad (19)$$

جایی که q_s کلید خصوصی‌اش است. درنهایت مقادیر $\{E , P , Q_S\}$ را به‌صورت عمومی منتشر می‌کند.

۴-۲. فاز دوم: ثبت‌نام کاربر

در این مرحله یک کاربر U هویت خود (IDU) را از طریق یک کانال امن به سرویس دهنده S ثبت می‌کند. سرویس دهنده S مقدار IDU را می‌بیند و کلید خصوصی کاربر را به‌صورت زیر محاسبه می‌کند.

$$D_U = [t_{ss}/q_s . h(IDU)] . P \quad (20)$$

را تولید کرده جایی که t_{ss} یک عدد تصادفی است. سپس یک مجموعه از هویت‌های سایه به‌صورت $ID_{sh} = \{id_{sh1}, id_{sh2}, \dots\}$ ایجاد می‌کند که برای هر هویت می‌تواند در رابطه زیر برقرار باشد.

$$id_{shi} = h(IDU \,||\, R \,||\, D_U) \quad (21)$$

جایی که $R = r_{s1} . P$ می‌باشد. هم چنین سرویس دهنده S مجموعه $K_m = \{k_{m1} , \dots\}$ را تولید می‌کند لذا برای هر id_{shi} یک k_{mi} داریم که برای محاسبه آن می‌توان از رابطه زیر استفاده نمود:

$$k_{mi} = h(IDU \,||\, id_{shi} \,||\, R^1) \quad (22)$$

که $R^1 = r_{s2} . P$ است.

همچنین سرویس دهنده S یک شماره دنباله USN که بر اساس تعداد درخواست‌های کنترل‌شده می‌باشد که توسط خودش محاسبه می‌شود. جایی که برای هر درخواست یک کاربر یک واحد به آن اضافه می‌شود و در سیستم مقدار جدید ذخیره می‌شود.البته یک نسخه از آن را نیز به کاربر می‌دهد.

در گام بعدی از این فاز S یک کارت هوشمند را که حاوی $\{D_U, (ID_{sh}, K_m), USN, h()\}$ را از طریق یک کانال امن برای کاربر می‌فرستد.

در گام بعدی سرویس دهنده S می‌خواهد که از کلید خصوصی خودش استفاده کند تا مقادیر $\{IDU, D_U, K_m\}$را به‌روزرسانی نماید. به‌این‌ترتیب خواهیم داشت:

$$IDU\#=IDU \oplus h(q_s \| USN)$$
$$D_U\#=D_U \oplus h(IDU \| q_s)$$
$$K_m\#=K_m \oplus h(IDU \| q_s) \quad (23)$$

یک کپی از مقادیر فوق در پایگاه داده خود ذخیره می شود.

در گام بعدی این فاز پس از دریافت کارت هوشمند ,کاربر U کلید خصوصی خود را دارد و می‌تواند مقادیر زیر را به دست آورد.

$$D_U^* = D_U \oplus h(h(IDU) \oplus h(P_U))$$
$$K_m^* = K_m \oplus h(h(IDU) \oplus h(P_U))$$
$$ID_{sh}^* = ID_{sh} \oplus h(h(IDU) \oplus h(P_U)) \quad (24)$$

جایی که P_U چیزی مانند یک کلمه عبور است که فقط کاربر U می‌داند.

کارت هوشمند می‌تواند یک تابعی از کلید خصوصی و کلمه عبور و هویت ایجاد کرده و به همراه مقادیر بالا به‌جای مقادیر قبلی‌شان آن را در کارت هوشمند ذخیره کند. تابع می‌تواند به‌صورت زیر باشد:

$$A^*=h(h(D_U) \oplus h(P_U) \oplus h(IDU)) \quad (25)$$

این مرحله در شکل۲ به‌صورت خلاصه توضیح داده‌شده است.

۴-۳. فاز سوم: احراز هویت چندمرحله‌ای به همراه توافق کلید

در این مرحله کاربر U به سرویس دهنده S باید یک پیام احراز هویت را بفرستد. در ابتدا کاربر از طریق پایانه کارت هوشمند خوان ID و کلمه عبورش را وارد می کند. پایانه هم مقادیر زیر را حساب خواهد نمود:

$$D_U=D_U^* \oplus [h(h(IDU) \oplus h(P_U))]$$
$$A=h(h(D_U) \oplus h(P_U) \oplus h(IDU)) \quad (26)$$

اگر بعد از به دست آوردن مقدار A از رابطه بالا و مقایسه آن با A^* این دو رابطه یکی شدند می‌توان نتیجه گرفت که پایانه کارت هوشمند کاربر Uرا به رسمیت شناخته است. سپس کارت هوشمند یک عدد تصادفی r_{sc} را تولید کرده و هویت مستعار AIDU و دو عدد تصادفی را تشکیل می‌دهد. به‌این‌ترتیب:

$$AIDU=h(IDU \| r_{sc} \| USN \| D_U) \quad (27)$$

$N_{U2}=D_U+N_{U1}$ و $N_{U1}=r_{sc} . P$

سپس کلید K را تشکیل می دهد :

$$K= h(IDU \| N_{U1} \| N_{U2} \| USN)$$

$$M1= \{AIDU , N_{U1} , USN , MAC_K(AIDU , N_{U2} , USN)\} \quad (28)$$

در گام بعدی کاربر پیام M1 را به سرویس دهنده S می‌فرستد.

سرویس دهنده پس از دریافت پیام ابتدا USN را بررسی و معتبر بودن آن را احراز می نماید . ازآنجاکه سرویس دهنده بیشترین شماره توالی انتقال اخیر را برای هر کاربر نگه می‌دارد، می‌تواند مقدار USNرا در پایگاه داده خود پیدا کند. سپس سرویس دهنده از کلید خصوصی خودش برای محاسبه IDU استفاده می‌کند. البته سرویس دهنده می‌تواند مقادیر N_{U1}, N_{U2}و K را نیز محاسبه کند تا یکپارچگی پیام M1 نیز بررسی گردد. همچنین سرویس دهنده می‌تواند معتبر بودن AIDU را نیز بررسی نماید.

در طی گام های بالا سرویس دهنده هویت کاربر U را احراز خواهد کرد. اگر سرویس دهنده نتواند USNرا پیدا کرده یا نتواند از معتبر بودن AIDU اطمینان حاصل نماید، ارتباط را فوراً خاتمه خواهد داد در غیر این صورت سرویس دهنده S پیام M2 را تشکیل و برای کاربر U ارسال می کند. پیام M2 شامل موارد زیر است:

ابتدا سرویس دهنده یک کلید نشست S_K را به‌صورت

$$S_K=h(IDU \| T_{SU} \| N_{U1}) \quad (29)$$

تشکیل می‌دهد و عبارت زیر را به دست می‌آورد.

$$S_K^*=h(N_{U2}) \oplus S_K \quad (30)$$

را به دست می‌آورد. در گام بعدی $MAC_K(r_{sc}, T_{SU}, S_K^*, N_{U2})$ را تشکیل می‌دهد . جایی که T_{SU}برابر عبارت زیر است:

$$T_{SU}=h(D_U \| IDU \| r_{sc}) \oplus USN_{NEW} \quad (31)$$

مقدار USN ای که در عبارت بالا می‌بینیم از گام قبلی است. زمانی که سرویس دهنده S می خواهد پیام $MAC_K()$ را بررسی‌کند، اگر شرایط برقرار بود یک واحد به USN اضافه می شود.

در گام بعد سرویس دهنده باید پیام M2 را که طبق محاسبات زیر بدست می آید به کاربر ارسال کند.

$$M2=\{S_K^*, T_{SU}, MAC_K(IDU, T_{SU}, L1, S_K^*, N_{U2})\} \quad (32)$$

بعد از دریافت پیام، پایانه کارت هوشمند مقدار $MAC_K()$ را مانند همان چیزی که در پیام M2 منتقل‌شده، محاسبه و یکپارچگی پیام را بررسی می‌کند. اگر شرایط برقرار بود هویت سرویس دهنده برای کاربر احراز می‌شود.

کارت هوشمند مقادیر USNو DU جدید را به دست می‌آورد وبه‌جای مقادیر قبلی ذخیره می‌کند:

$$USN_{NEW}=h(DU \| IDU \| r_{sc}) \oplus T_{SU}$$
$$DU_{NEW}=h(DU \| IDU \| USN_{NEW}) \quad (33)$$

اگر شرایط برقرار نبود کاربر نیاز دارد تا با یک زوج (Id_{sh}, k_m) که استفاده‌نشده‌اند، یک درخواست جدید ایجاد کند.

اگر یک حالت خاصی پیش بیاید که سرویس دهنده هیچ USN ای را در پیام M1 پیدا نکرد، ابتدا AIDU را معتبر خواهد کرد. (جایی که تلاش می‌کند id_{shi} را در AIDU با مقایسه ورودی‌های پایگاه داده تشخیص دهد.) اگر سرویس دهنده بتواند id_{shi} را در پایگاه داده پیدا کند می‌تواند k_{mi} متناظرش را بیابد و پارامترهای دیگر MAC_K را در M1 نیز پیدا کند. سپس یک کلید خصوصی جدید تولید کرده، همانند روشی که در فاز دوم مطرح شد یک عدد تصادفی دیگر مانند t_{ss} را انتخاب کرده و طبق رابطه داده‌شده در این مرحله مقدار کلید خصوصی را به دست می‌آورد. مقدار Z هم می تواند بیا کمک رابطه زیر به دست آید:

$$Z=DU_{NEW} \oplus h(IDU \| k_{mj}): \quad (34)$$

که این مقدار را به کاربر می‌فرستد.

پیام MAC_K را نیز می تواند به‌صورت زیر به دست آورد :

$$h(S_K^*, r_{sc}, T_{SU}, Z) \oplus k_{mi} \quad (35)$$

اگر سرویس دهنده نتواند id_{shi} را در AIDU پیدا کند به ارتباط پایان داده و از کاربر می‌خواهد که یک (id_{dhi}, k_{mi}) استفاده‌نشده را بفرستد. این مرحله در شکل۳ نشان داده‌شده است.

۴-۴. فاز چهارم

کاربر می‌تواند اطلاعات شخصی‌اش را که در این طرح برای آن از کلمه عبور استفاده کردیم، خودش به‌روز کند. برای انجام این کار، شخص باید مقادیر کلمه عبور قدیمی و جدید به همراه هویت اصلی خود را وارد کارت کند که درنهایت داریم:

$$D_U{**}=DU \oplus h(h(IDU)\oplus h(P_U{*}))$$
$$ID_{sh}{**}=ID_{sh}\oplus h(h(IDU)\oplus h(P_U{*}))$$
$$K_m{**}=K_m \oplus h(h(IDU)\oplus h(P_U{*})) \quad (36)$$

سپس این مقادیر به‌جای مقادیر قبلی در کارت هوشمند ذخیره می‌شوند.

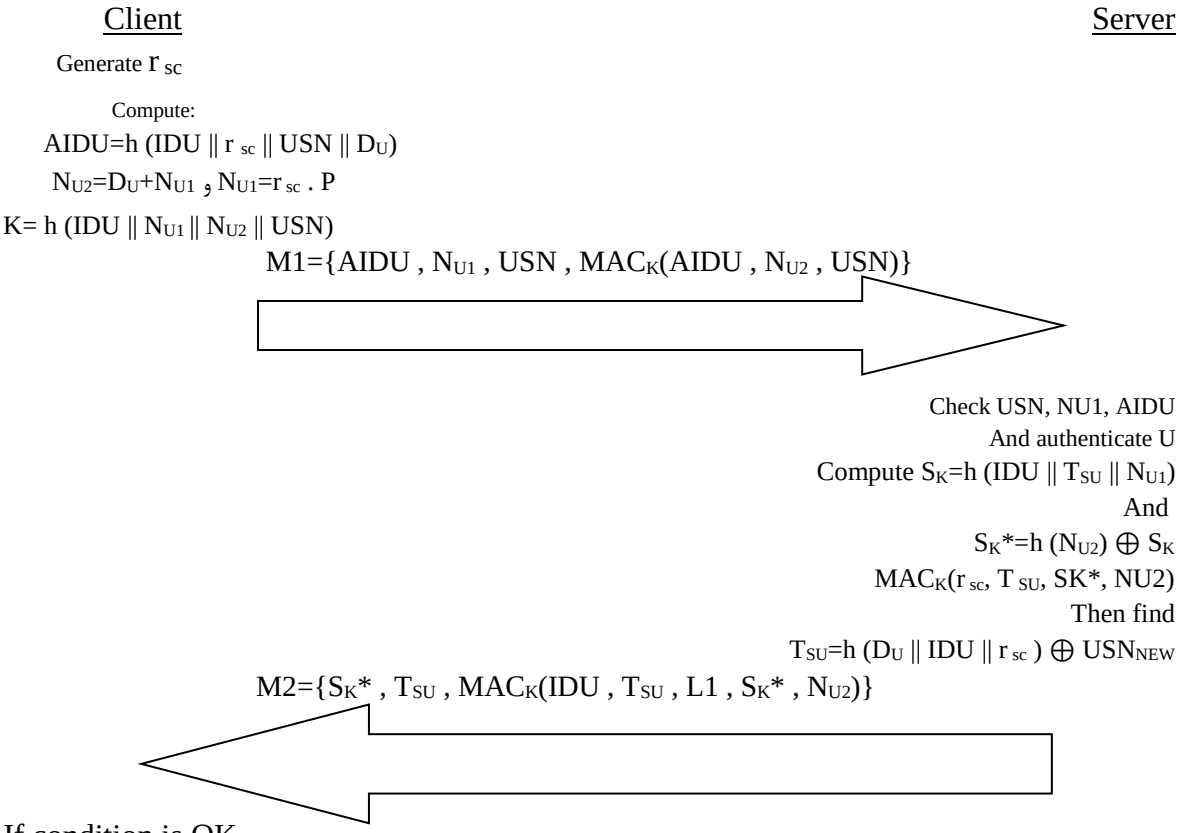
Client	Server
	Compute client's private key: $D_U= [t_s/q_s . h(IDU)]. P$
	Generate: $ID_{sh}= \{id_{sh1}, id_{sh2}, \ldots\}$ و $K_m= \{ k_{m1}, \ldots \}$
Secure channel	
	$\{D_U, (ID_{sh}, K_m), USN, h()\}$
Compute these :	Update these values: $\{IDU, D_U, K_m\}$

$$D_U{*} = D_U \oplus h(h(IDU) \oplus h(P_U))$$
$$K_m{*} = K_m \oplus h(h(IDU) \oplus h(P_U))$$
$$ID_{sh}{*} = ID_{sh} \oplus h(h(IDU) \oplus h(P_U))$$

And:

$$A{*}=h(h(D_U) \oplus h(P_U) \oplus h(IDU))$$

شکل ۲. فاز ثبت‌نام کاربر



شکل ۳. احراز هویت به همراه توافق کلید

۵. تحلیل امنیت پروتکل پیشنهادی

در این بخش به تحلیل امنیت پروتکل پیشنهادی که احراز هویت متقابل بین سرویس‌گیرنده/ دهنده را فراهم می‌کند می پردازیم. نتایج این مقایسه در جدول شماره یک آمده است.

۵-۱. احراز هویت دوطرفه

هر دو طرف باید یکدیگر را در یک مدل سرویس‌گیرنده/ دهنده احراز هویت کنند. در مرحله احراز هویت با مرحله توافق کلید، پیام $MAC_K(AIDU , N_{U2} , USN)$ درواقع کار احراز هویت سرویس گیرنده را انجام می‌دهد.
برای احراز هویت سرویس دهنده هم پیام $MAC_K(IDU , T_{SU} , L1 , S_K^* , N_{U2})$ این مهم را تحقق می‌بخشد.

۵-۲. مقاومت در برابر حمله تکرار

یک مهاجم می‌تواند پیام احراز هویت را ضبط کند و سپس آن را برای سرویس دهنده پخش کند، که به‌راحتی در محیط بی‌سیم برای برنامه اینترنت اشیا این کار قابل انجام است. بنابراین لازم است که دسترسی به پیام را بررسی کنید. در این طرح ما از یک شمارنده توالی استفاده کردیم که درواقع این‌طور می‌توان بیان کرد که مفهوم شماره توالی به‌طور عمده برای سرعت بخشیدن به فرآیند احراز هویت و همچنین جلوگیری از هر تلاشی برای انجام حمله بازپخش یا تکرار می‌باشد. سرویس دهنده با دیدن USN و مقایسه با مقدار ذخیره‌شده سرویس دهنده می‌تواند بفهمد که کدام یک فردکاربر است و اگر این دو مقدار باهم مطابقت نداشته باشند سرویس دهنده سریعاً ارتباط را خاتمه می‌دهد. اگر این مورد اتفاق بیفتد از کاربر درخواست می‌شود که یک زوج (id_{shi} , k_{mi}) استفاده‌نشده را بفرستد. البته بعد از استفاده، این لیست باید به‌روز شده و هر دو طرف باید این زوج هویت سایه و کلید را حذف کنند[10, 11].

۵-۳. گمنامی

در این طرح ما از هویت‌های سایه و موقت و کلیدهای موقتی استفاده کرده‌ایم که این موضوع گمنامی را برای ما به دست می‌آورد. از طرفی هویت موقت AIDU از عدد تصادفی هم استفاده کرده که گمنامی و قابل‌ردیابی بودن طرح را کامل می‌کند.

۵-۴. به‌روزرسانی کلید خصوصی

چون از یک عدد تصادفی در ساخت کلید خصوصی استفاده کرده‌ایم مهاجم نمی‌تواند کلید خصوصی را ردیابی کند و همان‌طور که توضیح دادیم در هر مرحله، اگر سرویس دهنده USN کاربر مربوطه را نتواند پیدا کند این امکان وجود دارد که عدد تصادفی دیگری را انتخاب و یک کلید خصوصی تولید کرده و برای کاربر ارسال کند.

۵-۵. مقاومت در برابر عدم دست‌کاری پیام

مهاجم به علت وجود کد احراز هویت پیام یا MAC نمی‌تواند تغییری در پیام به وجود آورد زیرا کلید K را در اختیار ندارد.

۵-۶. مقاومت در برابر حمله دزدیده شدن کارت هوشمند

اگر کارت هوشمند دزدیده شود مهاجم می‌تواند به پارامترهای ذخیره‌شده در آن برسد. ولی در طرح ما فرض می شود که مهاجم کارت هوشمند را دزدیده است که بازهم نمی‌تواند به کلمه عبور برسد. از طرفی چون در این طرح هر کاربر برای خودش یک مجموعه اعتبارات مختص به خودش را دارد اگر آن موارد گم یا دزدیده شوند این اتفاق نمی‌تواند روی امنیت کل سیستم تأثیر بگذارد.

۵-۷. امنیت پیشرو و پس‌رو

یک پروتکل را دارای امنیت پیشرو گوییم اگر کلید نشست این مرحله روی مراحل بعدی تأثیر نگذارد. در این طرح بعد از اتمام هر مرحله هم کاربر و هم سرویس دهنده باید کلید مشترک خودش را و هم کاربر کلید خصوصی خودش را به‌روزرسانی کند. چون از تابع چکیده ساز یک‌طرفه استفاده نمودیم، مهاجم نمی‌تواند از DU_{NEW} به DU برسد.

۵-۸. مقاومت در برابر جعل هویت

برای ایجاد پروتکل مقاوم در برابر حمله جعل هویت، ما فرض می‌کنیم که مهاجم هویت اصلی و موقت مشتری را می‌تواند تولید کند. ولی چون نمی‌تواند پیام $MAC_K(AIDU , N_{U2} , USN)$ را تولید کند چون کلید خصوصی کاربر را ندارد می گوییم پروتکل ما در برابر این حمله مقاوم است.

۵-۹. مقاومت در برابر حمله کلید نشست لو رفته

حمله کلید نشست لو رفته را این‌طور می‌توان بیان کرد که یک مهاجم، کلید جلسه قبلی را دریافت کند ولی نتواند به کلید جلسه فعلی دسترسی پیدا نماید. در طرح پیشنهادی ما، جلسه توافق شده مبتنی بر مسائل سخت و یک تابع چکیده ساز یک‌طرفه بوده و کلید جلسه به صورت کلید کوتاه‌مدت است. بنابراین طرح ما در برابر این حمله نیز موفق خواهد بود.

۵-۱۰. مقاومت در برابر حمله انسداد سرویس(DOS)

بسیاری از پروتکل‌ها در برابر حملات انسداد سرویس آسیب‌پذیر هستند که به علت عدم هم‌زمان‌سازی بین شرکت‌کنندگان رخ می‌دهد[11, 12]. درنتیجه، یک پروتکل احراز هویت ناشناس ممکن است نیاز به سازگاری با برخی از ویژگی‌های امنیتی ضروری مانند قابلیت غیر مرتبط بودن داشته باشد. بعضی از پروتکل‌های احراز هویت موجود مبتنی بر چکیده ساز، باید پس از هر فرایند تأیید هویت، به‌روزرسانی کلید را انجام دهند. در این حالت، هنگامی‌که فرآیند تأیید هویت پایان می‌یابد، هم کاربر و هم سرویس دهنده باید کلید مشترک خود را با استفاده از تابع چکیده ساز یک‌طرفه به‌روز کنند. بااین‌حال، استفاده‌ی تنها از این روش می‌تواند منجر به حملات انسداد سرویس گردد که در بسیاری از پروتکل‌های موجود به‌ویژه هنگامی‌که سرویس دهنده پایگاه داده خود را با کلید مخفی مشترک جدید به‌روزرسانی می‌کند، اما کاربر نمی‌تواند این کار را انجام دهد، رخ می دهد. ازاین‌رو استدلال می‌شود که مشکل حملات انسداد سرویس در طراحی پروتکل تائید هویت سبک‌وزن گوتام وجود دارد. در این طرح چون ما از مجموعه‌ای از هویت‌های غیر مرتبط به هم و کلیدهای متناظرشان استفاده کردیم توانستیم این ضعف را نیز مرتفع کنیم.

جدول ۱: مقایسه ویژگی‌های امنیتی طرح احراز هویت پیشنهادی با طرح گوتام

طرح احراز هویت پیشنهادی	طرح احراز هویت گوتام	ویژگی‌های امنیتی
✓	✓	احراز هویت دوطرفه
✓	✓	مقاوم در برابر حمله تکرار
✓	✓	گمنامی
✓	✓	مقاوم در برابر جعل هویت
✓	✓	مقاوم در برابر عدم دست‌کاری پیام
✓	✓	مقاوم در برابر حمله کلید نشست لو رفته
✓		مقاوم در برابر حمله دزدیده شدن کارت هوشمند
✓		به‌روزرسانی کلید خصوصی
✓		امنیت پیشرو و پس‌رو
✓		مقاومت در برابر حمله انسداد سرویس

۶. نتیجه‌گیری

در این مقاله، ابتدا طرح احراز هویت گوتام را بررسی و ضعف های آن را بیان نمودیم. سپس با ارائه یک اصلاحیه جدید باکمک پروتکل توافق کلیدی که بر اساس استفاده ترکیبی از رمزهای خم بیضوی و کلمه عبور بوده است، طرح جدیدی پیشنهاد نمودیم، که برای دستگاه‌های با منابع محدود یا سایر دستگاه‌های کم توان دراینترنت اشیا مناسب است.
این طرح نه‌تنها مزایای طرح قبلی را به همراه دارد، بلکه امنیت بیشتری را فراهم می‌کند و مصرف زمان و قدرت را کاهش می‌دهد که در دستگاه‌های با توان پردازشی کمتر ارزشمند است.

۷. مراجع

1. J-S Cho, Y-S Jeong, and S. Park, “Consideration on the Brute-force Attack Cost and Retrieval Cost: a Hash-based radio-frequency identification (RFID) Tag Mutual Authentication Protocol Computers,” & Mathematics with Applications(۲۰۱۲)

2. *P. Gope, and T. Hwang,“A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-time Application Data Access in Wireless Sensor Networks,” IEEE Transactions on Industrial Electronics, DOI:10.1109/TIE.2016.2585081, 2016*

3. *P. Gope, T. Hwang, “Lightweight and Energy Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks,” IEEE Systems Journal, DOI: 10.1109/JSYST.2015.2416396, November 2015*

4. *M.L. Das, “Two-factor user authentication in wireless sensor networks,” IEEE Transaction on Wireless Communications. vol. 8 no. 3, pp. 1086– 1090, March 2009*

5. *H. Debiao, C. Jianhua, and H. Jin, “An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security,” Information Fusion, vol. 13, no. 3, pp. 223–230, 2012*

6. *N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of computation, vol. 48, no. 177, pp. 203–209, 1987*

7. *R. A. Goutham, G.-J. Lee, and K.-Y. Yoo, “An anonymous id-based remote mutual authentication with key agreement protocol on ecc using smart cards,” in Proceedings of the 30th Annual ACM Symposium on Applied Computing. ACM, 2015, pp. 169–174*

8. *Wei Zhang, Dongdai Lin," A Lightweight Anonymous Mutual Authentication with Key Agreement Protocol on ECC", 2017 IEEE Trustcom/BigDataSE/ICESS*

9. *. Griffin, "Biometric-based cybersecurity techniques." In Advances in Human Factors in Cybersecurity, pp. 43-53. Springer International Publishing, 2016*

10. A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,2017

11. .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

12. Prosanta Gope, Jemin Lee, Member, " Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks", IEEE, and Tony Q. S. Quek, Senior Member, IEEE,2016