طرحی امن و کارا برای احراز هویت کاربران در شبکه‌های حسگر بی‌سیمِ مبتنی بر مفهوم اینترنت اشیاء

حمیدرضا یزدان پناه [۱،۱]، محمدرضا حسنی آهنگر[۲]، مهدی عزیزی[۳]، آرش غفوری

۱- دانشجوی کارشناسی ارشد شبکه‌های کامپیوتری، ۲- دانشیار گروه مهندسی کامپیوتر،۳- استادیار گروه مهندسی برق

دانشگاه جامع امام حسین(ع)، دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات

چکیده

اینترنت اشیاء اصطلاحی است برای توصیف دنیایی که در آن اشیا قادر خواهند بود بااتصال به اینترنت یا به کمک ابزارهای ارتباطی، با سایر اشیا تعامل داشته باشند و اطلاعات خود را باهم و یا با انسان‌ها به اشتراک بگذارند و کلاس جدیدی از قابلیت‌ها، برنامه‌های کاربردی و سرویس‌ها را ارائه دهند. دنیایی که در آن تمامی اشیا و دستگاه‌های نامتجانس قابلیت آدرس‌دهی و درنتیجه قابلیت کنترل‌پذیری دارند. شبکه‌های حسگر بی‌سیم در یک چنین محیطی نقش مهمی را بازی می‌کند چراکه حسگرها جزء کلیدی اینترنت اشیاء محسوب شده و شامل یک میدان گسترده از این کاربردهاست. محققان در تلاش‌اند که چگونه می‌توانند شبکه‌های حسگر بی‌سیم را به‌صورت بهتری در محیط اینترنت اشیا یکپارچه کنند. یکی از جنبه‌های این یکپارچگی دیدگاه امنیت است. اخیراً محمد سبزی نژاد و ترکانویچ طرح کارآمدی برای احراز هویت کاربران و توافق کلید در شبکه‌های حسگر بی‌سیم نامتجانس مبتنی بر مفهوم اینترنت اشیا ارائه دادند. اگرچه طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ کارآمد است، اما با تحلیل و بررسی‌های صورت گرفته مشخص شد که این طرح ناامن بوده و در مقابل برخی حملات رمزنگاری آسیب‌پذیر است. در این مقاله ضعف‌های امنیتی طرح سبزی نژاد و ترکانویچ نشان داده شده و سپس طرحی امن و کارا برای احراز هویت کاربران ارائه می‌شود.

کلمات کلیدی: اینترنت اشیاء، شبکه‌های حسگر بی‌سیم، احراز هویت، توافق کلید.

۱. مقدمه

ورود غیرمجاز به یک سیستم، همواره موردتوجه مهاجمین و نفوذ گران بوده است. نفوذ به این سیستم‌ها درعین‌حال که منافع بسیاری برای مهاجمان به ارمغان می‌آورد، ممکن است خسارات جبران‌ناپذیری را به سازمان‌ها و اشخاص تحمیل کند. یکی از مهم‌ترین راهکارها برای مقابله با این‌گونه تهدیدات و برای افزایش ایمنی شبکه‌ها استفاده از پروتکل‌های احراز هویت است. احراز هویت، یکی از مهم‌ترین و اساسی‌ترین گام‌ها در برقراری امنیت است که هدف اصلی آن حصول اطمینان از اعتبار و

[1] **Corresponding author: حمیدرضا یزدان پناه**
Email: hryazdanpanah@ihu.ac.ir

اصالت یک ارتباط است[۱]. به‌عنوان‌مثال در حالتی که اصالت یک پیام مدنظر است، سرویس احراز هویت باید به دریافت‌کننده این اطمینان را بدهد که این پیام از منبعی که مدعی ارسال آن بوده، صادر شده است و این کار با ارسال و دریافت چند پیام بین آن دو انجام می‌شود. به عبارتی مکانیزم‌های احراز هویت روش‌هایی برای کنترل ورود کاربران از طریق یک شبکه ارتباطی ناامن به یک کارگزار هستند. بنابراین استفاده از یک پروتکل کارا و مستحکم بدین منظور، می‌تواند از بسیاری از حمله‌های مهاجمان جلوگیری کند. اگر امنیت کافی به هنگام احراز هویت برآورده نگردد، یک مهاجم که به خطوط ارتباطی دسترسی دارد، می‌تواند با انجام حمله‌هایی همچون حمله جعل، حمله تکرار، حمله نشست‌های موازی، حمله واژه‌نامه، حمله حدس پسورد و غیره به‌صورت غیرمجاز وارد سیستم گردد و از خدمات آن سوءاستفاده کند. درنتیجه مکانیزم احراز هویت باید توانایی مقابله با چنین حمله‌هایی را داشته باشد. همچنین یکی از مهم‌ترین ملاحظات در طراحی پروتکل‌های احراز هویت، توجه به محیطی است که این پروتکل‌ها مورد کاربرد قرار خواهند گرفت. محیط‌های مختلف دارای محدودیت‌های مختلفی هستند. مانند محدودیت پردازشی، محدودیت فضای پیاده‌سازی، محدودیت توان مصرفی و محدودیت هزینه پیاده‌سازی[۲]. هر سیستم یا هر محیطی دارای خصوصیات و اقتضائات خاصی است که بایستی توسط طراحان مکانیزم‌های احراز هویت موردتوجه قرار گیرد. علاوه بر این برآورده کردن پاره‌ای از ویژگی‌های امنیتی همچون گمنامی کاربر، امنیت پیشرو، اصلاح‌پذیری، عدم تمییز پیام و محرمانگی، افزایش سطح ایمنی طرح و رضایت کاربران خود را در پی دارد که در بسیاری از مکانیزم‌ها در نظر گرفته نمی‌شود[۳]. روش‌های احراز هویت مبتنی بر کلمه عبور به دلیل سادگی و هزینه کم، رایج‌ترین مکانیزم احراز هویت در محیط‌های هوشمند به شمار می‌روند، ولی میزان اطمینان از عملکرد این طرح‌ها تنها به میزان محرمانگی کلمه عبور بستگی دارد و بافاش شدن کلمه عبور امنیت طرح به‌کلی از بین می‌رود[۴]. برای رفع این کاستی اخیراً مکانیزم‌های احراز هویت مبتنی بر دو یا چند فاکتور امنیتی موردتوجه قرار گرفته است. یکی از این مکانیزم‌ها، استفاده از کارت هوشمند به همراه کلمه عبور است. مزایای بالقوه کارت هوشمند، کاربرد آن را در طرح‌های احراز هویت توجیه می‌کند[۵]. این مزایا عبارت‌اند از :

- کارت هوشمند قابل‌حمل است.
- حافظه قابل‌خواندن و نوشتن دارد، بنابراین می‌تواند داده‌های محرمانه‌ای همچون کلیدهای رمزنگاری و تعدادی از پارامترهای دیگر که در حین فرایند احراز اصالت به آن نیاز است را در خود ذخیره کند.
- محاسبات رمزنگاری را از طریق پردازشگر داخلی خود انجام می‌دهد.

در کنار این مزایا، موانعی نیز در استفاده از آن وجود دارد.این موانع عبارت‌اند از:

- کاربرد کارت هوشمند محدود به محیط‌هایی است که در آن‌ها امکاناتی برای مبادله اطلاعات با کارت هوشمند وجود داشته باشد(دستگاه کارت خان).
- توان محاسباتی کارت هوشمند محدود است و برای پیاده‌سازی الگوریتم‌هایی که هزینه محاسباتی زیادی دارند (همچون رمزنگاری نامتقارن) مناسب نیست.
- امکان گم‌شدن یا دزدیده شدن و درنتیجه سوءاستفاده از آن‌ها وجود دارد.

اخیراً سبزی نژاد و ترکانویچ [۶] مکانیزمی سبک و کارا برای توافق کلید و احراز هویت دوطرفه کاربران در WSN[1] نامتجانس مبتنی بر مفهوم اینترنت اشیاء[2] ارائه دادند که در آن کاربران از راه دور می‌توانند بدون ارتباط اولیه با GWN[3] با گره موردنظر ارتباط برقرار کنند. ما این طرح را جهت سهولت UAKAS[4] می‌نامیم. در این طرح از گره GWN به‌عنوان یک جزء سوم برای کمک در فرایند احراز هویت استفاده می‌شود. این در حالی است که در اکثر طرح‌های ارائه شده اصل براین قرار است که

[1] Wireless Sensor Networks
[2] Internet of Things
[3] Gateway node
[4] User Authentication and Key Agreement Scheme

کاربر برای دسترسی به یک گره دلخواه در ابتدا به گره GWN متصل شود. روش ارائه‌شده توسط سبزی نژاد و ترکانویچ احراز هویت دوطرفه مابین کاربر، گره انتهایی و GWN را تضمین می‌کند. همچنین طرح ارائه‌شده توسط سبزی نژاد و همکارانش به دلیل اینکه تنها از محاسبات hash و XOR استفاده می‌کند، مناسب محیط‌هایی با منابع محدود همچون WSN مبتنی بر مفهوم اینترنت اشیاء است. این طرح یک مکانیزم احراز هویت دو فاکتوره بوده که از کارت هوشمند و گذرواژه استفاده می‌کند.

ازاین‌رو بخش دوم مروری دارد بر طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ، در بخش سوم پس از انجام تحلیل امنیتی و حمله به طرح ارائه‌شده‌ی پیشین، تعدادی از آسیب‌پذیری‌ها و ضعف‌های امنیتی طرح ارائه‌شده نشان داده‌شده است. در بخش چهارم راه‌حل ارائه می‌شود. در بخش پنجم پس از انجام مقایسه‌ای از ویژگی‌های امنیتی طرح پیشنهادی با طرح ارائه‌شده پیشین، امن و کارا بودن طرح پیشنهادی موردبررسی قرار می‌گیرد. بخش ششم نیز به نتیجه‌گیری اختصاص دارد. لازم به ذکر است لیست علائم و اختصارات در پیوست ۱ در انتهای مقاله ذکرشده است.

۲. مروری بر طرح سبزی نژاد و ترکانویچ

طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ کاربر را قادر می‌سازد تا با گره موردنظرش در شبکه ارتباط برقرار کند. این همان ویژگی خاصی است که در محیط اینترنت اشیا انتظارش را داریم، جایی که تمامی دستگاه‌ها مانند حسگرها، گوشی‌های هوشمند، ساعت‌های هوشمند، خودروهای هوشمند و... از طریق اینترنت به هم متصل می‌شوند[۷و۸] . بنابراین در یک چنین سناریویی، کاربر قادر است بدون نیاز به اتصال به گره GWN، با گره موردنظر ارتباط برقرار کرده و داده ردوبدل نماید. در این طرح از گره GWN به‌عنوان یک جزء سوم برای کمک در فرایند احراز هویت استفاده می‌شود.

مزیت دیگر این طرح، معماری سبک‌وزن آن است زیرا از عملگرهای محاسباتی ساده و کم‌هزینه مانند توابع هش یک‌طرفه و XOR استفاده می‌کند که مناسب شبکه‌های دارای منابع محدود مانند شبکه‌های حسگر بی‌سیم و اینترنت اشیاست. در این قسمت برای فهم بهتر مطالبی که در ادامه خواهد آمد، مروری بر طرح ارائه‌شده توسط سبزی‌نژاد و ترکانویچ خواهیم داشت. طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ طرحی کاراست که از چهار فاز اصلی: فاز قبل از راه‌اندازی، فاز ثبت‌نام، فاز ورود و فاز احراز هویت تشکیل شده است.

۲. ۱. فاز قبل از راه‌اندازی (فاز قبل از استقرار)

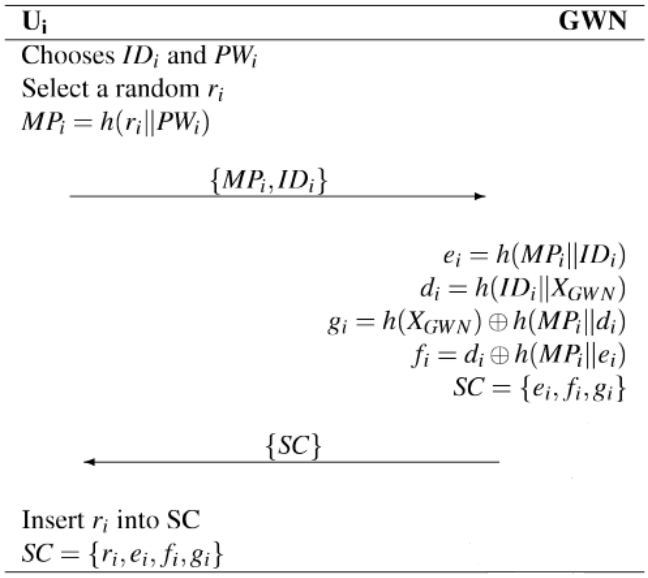
این فاز که به فاز نصب هم معروف است به‌صورت آفلاین توسط مدیر شبکه اجرا می‌شود. در طول این فاز، هر گره حسگر $\{S_j|1<=j<=m\}$ با یک شناسه (SID_j) و یک کلید رمز امن به‌صورت تصادفی تولیدشده (X_{GWN-Sj})، تعریف‌شده است.لازم به ذکر است که این کلید (X_{GWN-Sj}) با گره GWN به اشتراک گذاشته‌شده و در حافظه گره حسگر ذخیره‌شده است. برای گره GWN نیز یک کلید رمز خیلی امن تصادفی (X_{GWN}) که تنها توسط خود گره GWN شناخته می‌شود، تعریف می‌شود. این کلید نیز به‌صورت امن در حافظه گره GWN ذخیره می‌شود. علاوه بر این، گره GWN کلید امن به اشتراک گذاشته‌شده بین خود و گره‌های حسگر را در خود ذخیره می‌کند $\{X_{GWN-Sj} \mid 1<=j<=m\}$. هدف از کلید به اشتراک گذاشته‌شده (X_{GWN-Sj}) استفاده از آن در فاز ثبت‌نام است. لازم به ذکر است که کلید به اشتراک گذاشته‌شده بین حسگرها و گره GWN (X_{GWN-Sj}) را می‌توان بعد از فاز ثبت‌نام حذف کرد. این کار گره GWN را قادر می‌سازد تعداد بیشتری گره حسگر را بدون پر شدن حافظه به شبکه اضافه کند، چراکه ما در این‌گونه شبکه‌ها دارای محدودیت حافظه هستیم.

۲. ۲. فاز ثبت‌نام

فاز ثبت‌نام در طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ به دو بخش تقسیم می‌شود. بخش ثبت‌نام کاربر و بخش ثبت‌نام گره حسگر. هر گره حسگر پس از استقرار در محیط مورداستفاده باید برای احراز هویت و تائید قانونی بودن آن، در گره GWN ثبت‌نام کند. همچنین کاربران قبل از اینکه بتوانند به گره حسگر خاصی متصل شده و به آن دسترسی داشته باشند، باید در شبکه ثبت‌نام کنند. فرایند ثبت‌نام کاربر از طریق یک کانال امن به‌وسیله گره GWN انجام می‌شود. همچنین پس از تکمیل فرایند ثبت‌نام، یک کارت هوشمند در اختیار کاربر قرار می‌گیرد. توضیحات کامل فاز ثبت‌نام کاربر در طرح ارائه‌شده به‌صورت زیر است:

- **ثبت‌نام کاربر**

در این طرح کاربر U_i با انتخاب شناسه و گذرواژه و همچنین یک عدد تصادفی فرایند ثبت‌نام را آغاز می‌کند. سپس کاربر U_i با محاسبه $MP_i = h(r_i \| PW_i)$ گذرواژه خود را می‌پوشاند. پس از محاسبه MP_i کاربر U_i پیام $\{MP_i, ID_i\}$ را از طریق کانالی امن به گره GWN ارسال می‌کند. پس از دریافت پیام ثبت‌نام از U_i گره GWN در صورت تصمیم به ثبت‌نام کاربر، ابتدا $e_i = h(MP_i \| ID_i)$ و $d_i = h(ID_i \| X_{GWN})$ را با استفاده از کلید امن خودش (X_{GWN}) محاسبه کرده و سپس مقادیر $g_i = h(X_{GWN}) \oplus h(MP_i \| d_i)$ و $f_i = d_i \oplus h(MP_i \| e_i)$ را محاسبه می‌کند. پس‌ازآن گره GWN مقادیر $\{e_i, f_i, g_i\}$ را در حافظه کارت هوشمند (SC[1]) ذخیره کرده و آن را برای کاربر U_i ارسال می‌کند. در انتها کاربر U_i مقدار r_i را در کارت هوشمند ذخیره کرده و فاز ثبت‌نام کاربر به پایان می‌رسد. نمایشی از این فاز در شکل ۱ آمده است.



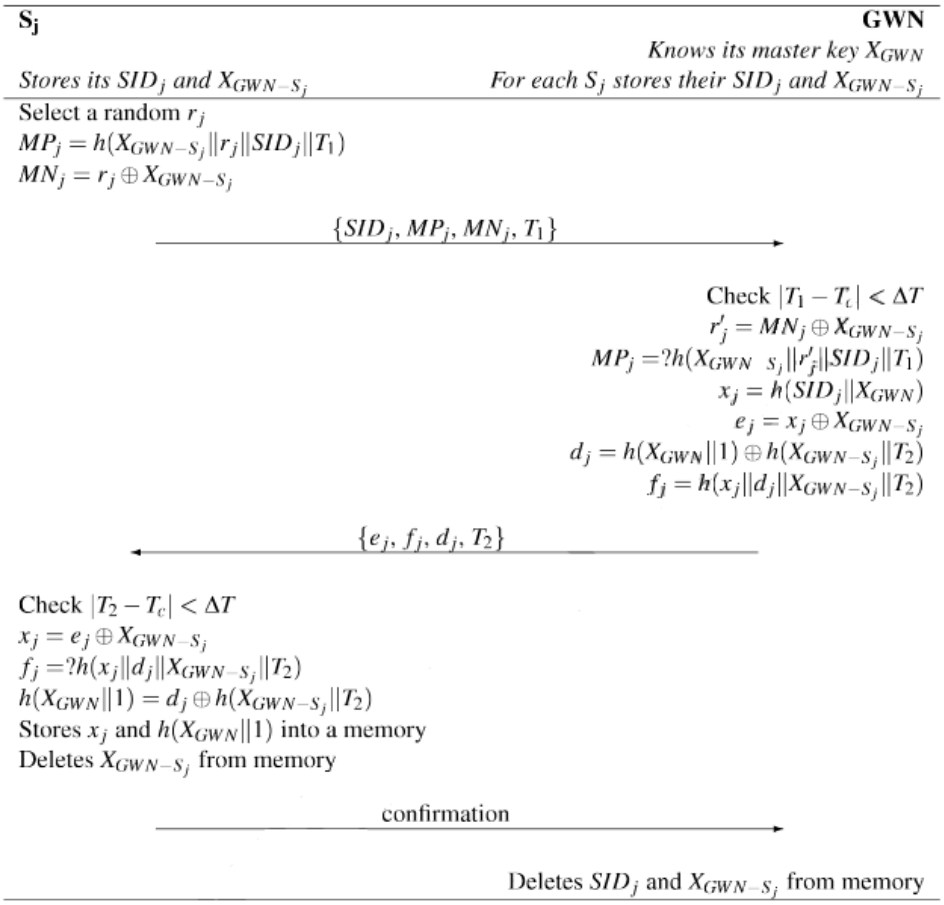
شکل ۱. فاز ثبت‌نام کاربر در طرح سبزی نژاد و ترکانویچ[۶]

[1] Smart Card

- **ثبت‌نام گره حسگر**

همان‌طور که در فاز استقرار ذکر شد، پس از پیکربندی هر حسگر با یک شناسه و کلید به اشتراک گذاشته شده بین خود و گره GWN (X_{GWN-Sj})، حسگرها در محیط موردنظر قرار داده می‌شوند. حال هر حسگر باید خود را از طریق کانالی غیر امن (فضای آزاد) در گره GWN ثبت‌نام کند. برای این کار گره S_j ابتدا با انتخاب عدد تصادفی r_j و محاسبه $MP_j = h(X_{GWN-Sj} || r_j || SID_j || T_1)$ و $MN_j = r_j \oplus X_{GWN-Sj}$ پیام ثبت‌نام $\{SID_j, MP_j, MN_j, T_1\}$ را از طریق کانالی ناامن به گره GWN ارسال می‌کند. T_1 برچسب زمانی گره S_j در زمان حاضر است. گره GWN پس از دریافت پیام ثبت‌نام از طرف گره S_j اعتبار و صحت برچسب زمانی را بررسی می‌کند ($|T_1-T_c| < \Delta t$). اگر صحت برچسب زمانی مورد تأیید نبود، GWN عملیات دیگری انجام نمی‌دهد و پیام عدم پذیرش را برای گره S_j ارسال می‌کند. در غیر این صورت GWN، مقدار $r'_j = MN_j \oplus X_{GWN-Sj}$ و MP'_j را محاسبه کرده و سپس بررسی می‌کند که آیا MP'_j محاسبه‌شده با مقدار اصلی MP_j دریافت شده برابر هستند یا خیر. اگر جواب مثبت بود و مقادیر باهم برابر بودند، گره GWN قانونی بودن گره حسگر S_j را تأیید می‌کند. پس‌ازآن گره GWN مقادیر x_j, e_j, d_j و f_j را محاسبه می‌کند. حال گره GWN پیامی شامل $\{e_j, f_j, d_j, T_2\}$ را از طریق کانال عمومی به گره S_j ارسال می‌کند.

گره S_j ابتدا صحت برچسب زمانی را برای جلوگیری از حمله تکرار بررسی می‌کند و سپس مقدار $x_j = e_j \oplus X_{GWN-Sj}$ و f'_j را به دست می‌آورد. در این لحظه گره S_j مقدار f'_j محاسبه شده را با f_j دریافتی مقایسه می‌کند. اگر مقادیر برابر بودند، گره حسگر S_j نیز متقابلاً موفق می‌شود گره GWN را احراز هویت کند. پس‌ازآن گره S_j مقدار $h(X_{GWN-Sj} || T_2)$ را محاسبه کرده و سپس مقدار x_j و $h(X_{GWN-Sj} || 1)$ را در $h(X_{GWN} || 1) = d_j \oplus h(X_{GWN-Sj} || T_2)$ حافظه ذخیره می‌کند. در انتها گره S_j کلید به اشتراک گذاشته‌شده (X_{GWN-Sj}) را حذف می‌کند و پیام تأییدیه را به گره GWN ارسال می‌کند. متقابلاً گره GWN، SID_j و کلید به اشتراک گذاشته‌شده(X_{GWN-Sj}) را از حافظه حذف می‌کند.



شکل ۲. فاز ثبت‌نام گره حسگر در طرح سبزی نژاد و ترکانویچ[۶]

۲. ۳. فاز ورود

همان‌طور که پیش‌تر ذکر شد، هدف از فاز احراز هویت قادر ساختن کاربر به ایجاد توافق بر روی یک کلید نشست امن با یک گره حسگر مشخص است، بدون اینکه نیازی به ارتباط مستقیم با گره GWN باشد. این کلید امن به‌منظور ایجاد یک ارتباط امن بین کاربر و گره حسگر مورداستفاده قرار می‌گیرد و هر دو طرف در ساخت آن نقش دارند.

قبل از شروع فرایند احراز هویت، کاربر U_i ابتدا باید به سیستم وارد شود(Login). این فرایند از طریق کارت هوشمند انجام می‌شود. برای این کار کاربر U_i کارت را درون کارت‌خوان قرار داده و شناسه ID'_i و گذرواژه PW'_i خود را وارد می‌کند. سپس نیاز است که کارت هوشمند از طریق اطلاعاتی که در خود ذخیره دارد، صحت هویت مالک کارت را مشخص کند. برای این کار SC ابتدا $MP'_i = h(r_i \| PW'_i)$ را با توجه به گذرواژه واردشده و مقدار تصادفی r_i که در خود ذخیره دارد به دست آورده و سپس مقدار $e'_i = h(MP'_i \| ID'_i)$ را محاسبه می‌کند. اگر مقدار e'_i به‌دست‌آمده با مقدار اصلی e_i برابر بود، SC قانونی بودن کاربر U_i را تأیید می‌کند و فرایند فاز ورود پایان می‌پذیرد.

۲. ۴. فاز احراز هویت

بعد از ورود موفق، SC خود را برای فرایند احراز هویت آماده می‌کند. در ادامه روند فوق، SC ابتدا مقادیر $d_i = f_i \oplus h(MP'_i \| e_i)$ و سپس $h(X_{GWN}) = g_i \oplus h(MP'_i \| d_i)$ را محاسبه می‌کند. بعدازآن SC از سه مقدار کمکی M_1, M_2 و

M_3برای ارسال نتیجه‌ی محاسبات خود به گره GWN از طریق کانال عمومی استفاده می‌کند. SC پس از محاسبه مقدار $M_1= ID'_i \oplus h(h(X_{GWN} \| T_1))$ یک عدد تصادفی (K_i) با آنتروپی بالا[1] انتخاب کرده و سپس مقادیر $M_2 = K_i \oplus h(d_i \| T_1)$ و $M_3 = h(M_1 \| M_2 \| K_i \| T_1)$ را محاسبه می‌کند. لازم به ذکر است محاسبه مقدار M_1 به‌منظور پوشاندن شناسه کاربر U_i، و هدف از محاسبه مقدار M_2 پوشاندن K_i که بخشی از اجزای تشکیل‌دهنده کلید نشست محسوب می‌شود، است. سرانجام SC پیام احراز هویت $\{M_1, M_2, M_3, T_1\}$ را از طریق کانال عمومی (ناامن) به گره GWN (از طریق گره) ارسال می‌کند.

حسگر S_j پس از دریافت پیام احراز هویت از کاربر U_i فرایند وارسی و تصدیق هویت را به گره GWN محول می‌کند. اما قبل از واگذار کردن این فرایند، با بررسی برچسب زمانی $|T_1-T_c| < \Delta t$ از احتمال وجود حمله تکرار اطمینان حاصل می‌کند. همچنین نیاز است در صورت تأیید برچسب زمانی، مقادیر $ESID_j$، M_4 وM_5 محاسبه شوند. هدف از محاسبه $ESID_j$ رعایت شرط گمنامی گره حسگر در حین ارسال روی کانال ناامن است. برای این کار حسگر S_j پس از محاسبه $ESID_j = SID_i \oplus h(h(X_{GWN} \| 1)T_2)$، یک عدد تصادفی با آنتروپی بالا (K_j) انتخاب می‌کند که این عدد بخش دوم کلید نشست موردتوافق ما را تشکیل می‌دهد. لازم به ذکر است از K_j برای محاسبه مقدار $M_4 = h(x_j \| T_1 \| T_2) \oplus K_j$ و $M_5 = h(SID_j \| M_4 \| T_1 \| T_2 \| K_j)$ استفاده می‌شود. همچنین مقدار M_4 بعداً برای استخراج K_j توسط گره GWN مورداستفاده قرار می‌گیرد. در انتها گره S_j پیام احراز هویت $\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$ را به گره GWN ارسال می‌کند.

گره GWN پس از دریافت پیام احراز هویت از گره S_j ابتدا برای اطمینان از احتمال وجود حمله تکرار برچسب زمانی را بررسی می‌کند. در صورت اطمینان، گره GWN فرایند احراز هویت را که شامل دو بخش احراز هویت گره S_j و احراز هویت کاربر U_i است، دنبال می‌کند. برای این کار گره GWN ابتدا شناسه گره حسگر $SID'_j = ESID_i \oplus h(h(X_{GWN} \| 1)T_2)$ را با مقادیر دریافتی و کلید رمز امن خود (X_{GWN}) محاسبه کرده و با استفاده از نتیجه آن مقادیر $x'_j = h(SID'_j \| X_{GWN})$ و سپس $K'_j = M_4 \oplus h(x'_j \| T_1 \| T_2)$ را به دست می‌آورد. در این لحظه گره GWN با محاسبه مقدار $M'_5 = h(SID'_j \| M_4 \| T_1 \| T_2 \| K'_j)$ و مقایسه آن با مقدار دریافتی M_5 ?= M'_5 از قانونی بودن گره S_j اطمینان حاصل می‌کند.

پس از احراز هویت گره حسگر نوبت به اطمینان از قانونی بودن کاربر U_i می‌رسد. این بخش از اهمیت بالایی در فرایند احراز هویت برخوردار است چراکه گره S_j تصدیق هویت کاربر را به گره GWN واگذار کرده است. برای این کار گره GWN ابتدا شناسه کاربر $ID'_i = M_1 \oplus h(h(X_{GWN}) \| T_1)$ را با مقادیر دریافتی و کلید رمز امن خود محاسبه کرده و با استفاده از نتیجه آن مقدار $d'_i = h(ID'_i \| X_{GWN})$ و سپس $K'_i = M_2 \oplus h(d'_i \| T_1)$ را که بخشی از کلید نشست را تشکیل می‌دهد، به دست می‌آورد. در این لحظه گره GWN با محاسبه مقدار $M'_3 = h(M_1 \| M_2 \| K'_i \| T_1)$ و مقایسه آن با مقدار دریافتی M_3 ?= M'_3 از قانونی بودن کاربر U_i که فرایند احراز هویت را آغاز کرده است اطمینان حاصل می‌کند.

در ادامه و پس از احراز هویت موفق گره S_j و کاربر U_i، گره GWN شروع به ایجاد پیام تأیید برای ارسال به گره S_j می‌کند. برای این کار گره GWN ابتدا با محاسبه $M_6 = K'_j \oplus h(d'_i \| T_3)$ و $M_7 = K'_i \oplus h(x'_j \| T_3)$ مقادیر K_i و K_j محاسبه‌شده را می‌پوشاند. سپس گره GWN با محاسبه دو مقدار $M_8 = h(M_6 \| d'_i \| T_3)$ و $M_9 = h(M_7 \| x'_j \| T_3)$ پیام تأییدیه را $\{M_6, M_7, M_8, M_9, T_3\}$ از طریق کانال عمومی به گره S_j ارسال می‌کند. در اینجا گره GWN وظیفه‌اش را به‌عنوان جزء سوم کمک‌کننده در فرایند احراز هویت به اتمام می‌رساند.

[1] علت انتخاب عدد تصادفی با آنتروپی بالا این است که K_i یکی از اجزای اصلی کلید نشست خواهد بود.

گره S_j پس از دریافت موفق پیام تأیید از گره GWN و بررسی برچسب زمانی $|T_3-T_c|< \Delta t$ برای جلوگیری از حمله تکرار، با محاسبه مقدار $M'_9 =?h(M_7 \parallel x_j \parallel T_3)$ و مقایسه نتیجه آن با مقدار دریافتی M_9 درستی پیام دریافتی و درنتیجه قانونی بودن گره GWN را تأیید می‌کند. در ادامه، گره S_j با محاسبه مقدار $K'_i = M_7 \oplus h(x_j \parallel T_3)$، بخش اول کلید نشست (مربوط به کاربر) را استخراج کرده و سپس کلید نشست نهایی $SK= h(K'_i \oplus K_j)$ را محاسبه می‌کند. در انتها گره S_j مقدار $M_{10} = h(SK \parallel M_6 \parallel M_8 \parallel T_3 \parallel T_4)$ را محاسبه کرده و سپس پیام تأییدیه $\{M_6, M_8, M_{10}, T_3, T_4\}$ را به کاربر U_i ارسال می‌کند.

کاربر پس از دریافت پیام تأییدیه ابتدا برچسب زمانی $(|T_4-T_c| < \Delta T)$ را برای اطمینان از عدم وجود حمله تکرار بررسی کرده و سپس با محاسبه مقدار $M'_8 = h(M_6 \parallel d_i \parallel T_3)$ و مقایسه نتیجه آن با مقدار دریافتی M_8 $M'_8 =?$ قانونی بودن گره GWN را تأیید می‌کند. همچنین کاربر U_i با محاسبه $K'_j =M_6 \oplus h(d_i \parallel T_3$ و استخراج بخش دوم کلید نشست (مربوط به گره S_j)، کلید نشست نهایی را محاسبه می‌کند. در انتها کاربر U_i با محاسبه مقدار $M'_{10} =h(SK \parallel M_6 \parallel M_8 \parallel T_3 \parallel T_4)$ و مقایسه آن با مقدار دریافتی M_{10} $M'_{10} =?$ از قانونی بودن گره S_j اطمینان حاصل می‌کند. در این لحظه فاز احراز هویت با موفقیت به پایان می‌رسد. نمایشی کاملی از این فاز در شکل ۳ آمده است.

$\mathbf{U_i}$	$\mathbf{S_j}$	GWN
Knows its ID_i *and* PW_i *Has a* $SC = \{r_i, e_i, f_i, g_i\}$	*Stores* SID_j, x_j *and* $h(X_{GWN}\|\|1)$	*Stores its master key* X_{GWN}

User: Inserts SC into a terminal
User: Inputs PW_i' and ID_i'
SC: $MP_i' = h(r_i||PW_i')$
SC: $e_i = ?h(MP_i'||ID_i')$
SC: $d_i = f_i \oplus h(MP_i'||e_i)$
SC: $h(X_{GWN}) = g_i \oplus h(MP_i'||d_i)$
SC: $M_1 = ID_i' \oplus h(h(X_{GWN})||T_1)$
SC: Chooses a random nonce K_i
SC: $M_2 = K_i \oplus h(d_i||T_1)$
SC: $M_3 = h(M_1||M_2||K_i||T_1)$
User: Chooses S_j

$$\xrightarrow{\{M_1, M_2, M_3, T_1\}}$$

Checks $|T_1 - T_c| < \Delta T$
$ESID_j = SID_i \oplus h(h(X_{GWN}||1)||T_2)$
Chooses a random nonce K_j
$M_4 = h(x_j||T_1||T_2) \oplus K_j$
$M_5 = h(SID_j||M_4||T_1||T_2||K_j)$

$$\xrightarrow{\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}}$$

Checks $|T_2 - T_c| < \Delta T$
$SID_j' = ESID_i \oplus h(h(X_{GWN}||1)||T_2)$
$x_j' = h(SID_j'||X_{GWN})$
$K_j' = M_4 \oplus h(x_j'||T_1||T_2)$
$M_5 = ?h(SID_j'||M_4||T_1||T_2||K_j')$
$ID_i' = M_1 \oplus h(h(X_{GWN})||T_1)$
$d_i' = h(ID_i'||X_{GWN})$
$K_i' = M_2 \oplus h(d_i'||T_1)$
$M_3 = ?h(M_1||M_2||K_i'||T_1)$
$M_6 = K_j' \oplus h(d_i'||T_3)$
$M_7 = K_i' \oplus h(x_j'||T_3)$
$M_8 = h(M_6||d_i'||T_3)$
$M_9 = h(M_7||x_j'||T_3)$

$$\xleftarrow{\{M_6, M_7, M_8, M_9, T_3\}}$$

Check $|T_3 - T_c| < \Delta T$
$M_9 = ?h(M_7||x_j||T_3)$
$K_i' = M_7 \oplus h(x_j||T_3)$
$SK = h(K_i' \oplus K_j)$
$M_{10} = h(SK||M_6||M_8||T_3||T_4)$

$$\xleftarrow{\{M_6, M_8, M_{10}, T_3, T_4\}}$$

Check $|T_4 - T_c| < \Delta T$
$M_8 = ?h(M_6||d_i||T_3)$
$K_j' = M_6 \oplus h(d_i||T_3)$
$SK = h(K_i \oplus K_j')$
$M_{10} = ?h(SK||M_6||M_8||T_3||T_4)$

شکل ۳. فاز ورود و احراز هویت در طرح سبزی نژاد و ترکانویچ[۶]

۳. تحلیل امنیتی و حمله به طرح UAKAS

UAKAS یک طرح سبک، کارا و مبتنی بر کارت هوشمند است که تنها از رمزنگاری متقارن، توابع محاسباتی هش و عملگرهای الحاق و XOR استفاده می‌کند. علی‌رغم ادعای نویسندگان این طرح، مبنی بر امنیت بالای آن ثابت شد که این طرح با ضعف‌های جدی و مهمی روبروست که در زیر به آن‌ها اشاره‌شده است.

۳. ۱. کشف گذرواژه کاربر

طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ یک طرح احراز هویت دو فاکتوره است که از کارت هوشمند و گذرواژه استفاده می‌کند. زمانی که این کارت هوشمند بنا به هر دلیلی (گم‌شدن/دزدیده شدن) به دست مهاجم بیافتد، او می‌تواند به اطلاعات حساس درون کارت $SC= \{r_i, e_i, f_i, g_i\}$ دسترسی پیدا کند. در این لحظه مهاجم می‌تواند در فاز ورود (Login) و با در دست داشتن مقدار r_i و امتحان کردن حالت‌های مختلفی از گذرواژه (PW'_i)، مقدار $MP'_i = h(r_i \| PW'_i)$ را به دست می‌آورد. امتحان کردن حالت‌های مختلفی از گذرواژه می‌تواند از طریق حمله دیکشنری[1] انجام پذیرد. سپس مهاجم از مقدار MP'_i به‌دست‌آمده برای محاسبه $d_i = f_i \oplus h(MP'_i \| e_i)$ استفاده می‌کند. لازم به ذکر است، مهاجم مقادیر f_i و e_i را از SC استخراج کرده است. پس‌ازآن چون کاربر U_i پیام $\{M_1, M_2, M_3, T_1\}$ را از طریق کانال عمومی ناامن به گره S_j ارسال می‌کند، مهاجم قادر است این پیام را شنود کند. ازاین‌رو مهاجم می‌تواند مقدار $K_i = M_2 \oplus h(d_i \| T_1)$ را به دست آورد. سپس مهاجم با استفاده از K_i به‌دست‌آمده مقدار $M'_3 = h(M_1 \| M_2 \| K_i \| T_1)$ را محاسبه کرده و سپس مقدار M'_3 محاسبه‌شده را با مقدار M_3 شنود شده از کانال عمومی ناامن مقایسه می‌کند($M'_3 =? M_3$). اگر مقادیر ذکرشده برابر بود مهاجم اطمینان حاصل می‌کند که عملیات حدس گذرواژه موفقیت‌آمیز بوده است.

تا این لحظه مهاجم موفق شده است گذرواژه کاربر و بخش کلید نشست کاربر (K_i) را به دست آورد.

خلاصه‌ای از مراحل حمله حدس گذرواژه به‌صورت زیر است:

- مرحله ۱: به دست آوردن SC و دسترسی به اطلاعات درون آن $SC= \{r_i, e_i, f_i, g_i\}$.
- مرحله ۲: حدس گذرواژه و محاسبه $MP'_i = h(r_i \| PW'_i)$.
- مرحله ۳: استفاده از مقدار MP'_i و محاسبه $d_i = f_i \oplus h(MP'_i \| e_i)$.
- مرحله ۴: استفاده از مقدار d_i و محاسبه $K_i = M_2 \oplus h(d_i \| T_1)$.
- مرحله ۵: استفاده از مقدار K_i و محاسبه $M'_3 = h(M_1 \| M_2 \| K_i \| T_1)$.
- مرحله ۶: اگر $M'3 = M3$، مهاجم اطمینان حاصل می‌کند که عملیات حدس گذرواژه موفقیت‌آمیز بوده است.

۳. ۲. کشف شناسه کاربر

پس از کشف گذرواژه کاربر، مهاجم می‌تواند شناسه کاربر را با امتحان کردن حالت‌های متفاوتی از ID_i در $e_i =? h(MP'_i \| ID_i)$ به دست آورد. امتحان کردن حالت‌های مختلفی از شناسه کاربر (ID') می‌تواند از طریق حمله دیکشنری انجام پذیرد. باید توجه داشت، مهاجم مقدار e_i را از SC استخراج و مقدار MP'_i را در مرحله ۲ کشف گذرواژه کاربر (۴-۲-۱) محاسبه می‌کند. با توجه به حمله اشاره‌شده در این بخش، باید دقت داشت که طول شناسه به‌اندازه کافی بزرگ انتخاب شود تا پروتکل در برابر چنین حملاتی امن باشد(طول شناسه حداقل ۱۲۸بیت).

[1] Dictionary attack (brute force attack)

۳. ۳. عدم رعایت گمنامی کاربر

پس از کشف (حدس صحیح) گذرواژه و سپس محاسبه مقدار MP'_i در بخش (۳. ۱) مهاجم می‌تواند مقدار $d_i = f_i \oplus h(MP'_i \| e_i)$ و درنتیجه $h(X_{GWN}) = g_i \oplus h(MP'_i \| d_i)$ را محاسبه کند. لازم به ذکر است او مقادیر e_i ، f_i و g_i را از کارت هوشمند استخراج می‌کند. حال فرد مهاجم مقادیر T_1 و M_1 را هنگامی‌که کاربر U_i پیام $\{M_1, M_2, M_3, T_1\}$ را از طریق کانال ناامن به S_j ارسال می‌کند، شنود می‌کند. در انتها مهاجم می‌تواند مقدار $ID_i = M_1 \oplus h(h(X_{GWN}) \| T_1)$ را محاسبه کند. بنابراین طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ برخلاف ادعای آن‌ها گمنامی کاربر را رعایت نمی‌کند.

۳. ۴. کشف کلید نشست

همان‌طور که در قسمت (۳. ۱) ذکر شد، مهاجم با محاسبه مقدار $K_i = M_2 \oplus h(d_i \| T_1)$ موفق می‌شود به بخش کلید نشست کاربر (K_i) دسترسی پیدا کند. پس‌ازآن، مهاجم می‌تواند مقدار M_6 را در فاز احراز هویت، هنگامی‌که گره GWN پیام تأیید را به گره S_j از طریق کانال عمومی ناامن ارسال می‌کند، شنود کند. در این لحظه او موفق می‌شود با اطلاعات به‌دست‌آمده مقدار $K'_j = M_6 \oplus h(d'_i \| T_3)$ را محاسبه کرده و سپس مقدار کلید نشست $SK = h(K_i \oplus K'_j)$ را به دست آورد. لازم به یادآوری است که مهاجم مقدار d_i را در مرحله ۳ کشف گذرواژه کاربر محاسبه و همچنین مقدار T_3 را هنگامی‌که GWN پیام تأیید را برای گره حسگر ارسال می‌کند، شنود کرده است.

۳. ۵. حمله جعل کاربر

پس از کشف گذرواژه صحیح کاربر و محاسبه مقدار d_i در قسمت (۳. ۱)، مهاجم با انتخاب یک عدد تصادفی K_i مقدار $M^*_2 = K_i \oplus h(d_i \| T_1)$ را محاسبه می‌کند. سپس او از مقدار M^*_2 محاسبه‌شده استفاده کرده و مقدار $M^*_3 = h(M_1 \| M^*_2 \| K_i \| T_1)$ را به دست می‌آورد. لازم به ذکر است مهاجم مقادیر M_1 وT_1 را در فاز احراز هویت زمانی که کاربر U_i پیام $\{M_1, M_2, M_3, T_1\}$را از طریق کانال عمومی ناامن به گره حسگر S_j ارسال می‌کرد، شنود می‌کند. حال فرد مهاجم پیام $\{M_1, M^*_2, M^*_3, T_1\}$ را به گره حسگر موردنظر ارسال می‌کند. گره حسگر S_j پس از دریافت پیام برچسب زمانی $(|T_1-T_c| < \Delta t)$ را برای جلوگیری از حمله تکرار بررسی می‌کند. اگر برچسب زمانی مورد تأیید بود گره حسگر مقدار $ESID_j$ را محاسبه می‌کند. سپس گره حسگر S_j یک عدد تصادفی (K_j) انتخاب کرده و پس از محاسبه مقدار M_4 و M_5 پیام $\{M_1, M^*_2, M^*_3, T_1, T_2, ESID_j, M_4, M_5\}$ را به GWN ارسال می‌کند.

گره GWN پس از بررسی برچسب زمانی $(|T_2-T_c| < \Delta t)$ مقادیر $ID'_i = M_1 \oplus h(h(X_{GWN}) \| T_1)$، $d'_i = h(ID'_i \| X_{GWN})$ و $K'_i = M^*_2 \oplus h(d'_i \| T_1)$ را محاسبه می‌کند. در انتها GWN با استفاده از مقادیر به‌دست‌آمده مقدار $M'_3 = h(M_1 \| M^*_2 \| K'_i \| T_1)$ را به دست می‌آورد و سپس بررسی می‌کند که آیا مقدار M'_3 به‌دست‌آمده با M^*_3 دریافت شده برابر است یا خیر $(M'_3 =? M^*_3)$. اگر $M'_3 = M^*_3$ بود گره GWN باور می‌کند که پیام از طرف کاربر معتبر U_i دریافت شده است!

۴. طرح UAKAS امن و کارا

در این بخش طرحی بهبودیافته برمبنای طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ برای احراز هویت کاربران و توافق کلید در شبکه‌های حسگر بی‌سیم نامتجانس مبتنی بر مفهوم اینترنت اشیا ارائه می‌شود. طرح UAKAS امن ارائه‌شده علاوه بر حذف تمامی آسیب‌پذیری‌ها و ضعف‌های امنیتی ذکرشده دارای عملکرد و کارایی یکسانی با طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ است؛ به‌طوری‌که نهایت احتیاط در بهبود امنیتی طرح در نظر گرفته‌شده است. همچنین طرح ارائه‌شده از چهار فاز اصلی: فاز قبل از راه‌اندازی، فاز ثبت‌نام، فاز ورود و فاز احراز هویت تشکیل‌شده است که در ادامه به تشریح آن‌ها پرداخته می‌شود.

۴. ۱. فاز قبل از راه‌اندازی (فاز قبل از استقرار)

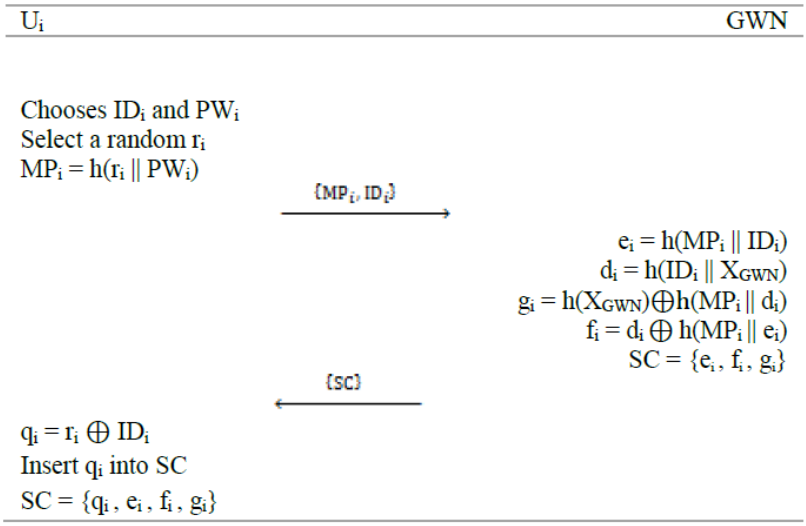
فاز قبل از راه‌اندازی طرح ارائه‌شده همانند طرح ارائه‌شده پیشین است که در بخش (۲. ۱) توضیح داده شد. در طول این فاز، گره GWN یک کلید به اشتراک گذاشته‌شده $\{X_{GWN-Sj} \mid 1<=j<=m\}$ را برای هر گره S_j تولید و ذخیره می‌کند. هدف از کلید به اشتراک گذاشته‌شده (X_{GWN-Sj}) استفاده از آن در فاز ثبت‌نام است. کلید به اشتراک گذاشته‌شده بین حسگرها و گره GWN (X_{GWN-Sj}) را می‌توان بعد از فاز ثبت‌نام حذف کرد. این کار گره GWN را قادر می‌سازد تعداد بیشتری گره حسگر را بدون پر شدن حافظه به شبکه اضافه کند؛ چراکه ما در این‌گونه شبکه‌ها دارای محدودیت منابع (حافظه) هستیم.

۴. ۲. فاز ثبت‌نام

فاز ثبت‌نام طرح UAKAS امن با تغییرات جزئی و هوشمندانه‌ای نسبت به طرح ارائه‌شده پیشین ارائه‌شده است. فاز ثبت‌نام گره حسگر در این فاز همانند طرح ارائه‌شده پیشین است، لذا از بیان آن در این قسمت خودداری می‌کنیم.

- **ثبت‌نام کاربر**

کاربر U_i پس از انتخاب شناسه ID_i و گذرواژه PW_i و تولید عدد تصادفی r_i مقدار $MP_i = h(r_i \| PW_i)$ را محاسبه کرده و سپس پیام $\{MP_i, ID_i\}$ را از طریق کانال عمومی برای گره GWN ارسال می‌کند. پس از دریافت پیام، گره GWN مقدار $e_i = h(MP_i \| ID_i)$ و $d_i = h(ID_i \| X_{GWN})$ را با استفاده از کلید امن خود (X_{GWN}) محاسبه می‌کند. پس‌ازآن گره GWN مقدارهای $g_i = h(X_{GWN}) \oplus h(MP_i \| d_i)$ و $f_i = d_i \oplus h(MP_i \|$ e_i) را به دست آورده و سپس مقادیر $\{e_i, f_i, g_i\}$ را در حافظه کارت هوشمند ذخیره می‌کند و آن را برای کاربر U_i ارسال می‌کند. در انتها کاربر U_i مقدار $q_i = r_i \oplus ID_i$ را محاسبه کرده و سپس q_i را در کارت هوشمند (SC = $\{q_i, e_i, f_i, g_i\}$) ذخیره می‌کند. با این حساب عملیات ثبت‌نام کاربر پایان می‌پذیرد. لازم به ذکر است محاسبه مقدار q_i به‌منظور عدم ذخیره آشکار مقدار r_i در کارت هوشمند است و این عمل باعث می‌شود در صورت دزدیده شدن یا گم‌شدن کارت، مهاجم نتواند به مقدار r_i دست پیدا کند. نمایش دقیقی از این فاز در شکل ۴ آمده است.



شکل ۴. فاز ثبت‌نام کاربر طرح ارائه‌شده

۴. ۳. فاز ورود و احراز هویت

فاز ورود و احراز هویت طرح ارائه‌شده نیز مبتنی بر طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ است که پیش‌ازاین در (۳-۱-۴) شرح داده شد. همان‌طور که در فاز ثبت‌نام اشاره شد، مقادیر ذخیره‌شده در کارت هوشمند شامل $SC = \{q_i, e_i, f_i, g_i\}$ است. مهم‌ترین تغییر قابل‌ملاحظه بین طرح ارائه‌شده و طرح پیشین این است که ما باید $r'_i = ID'_i \oplus q_i$ و $MP'_i = h(r'_i \| PW'_i)$ را قبل از بررسی $e_i = ?h\ (MP'_i \| ID'_i)$ محاسبه کنیم. در این حالت مهاجم به دلیل عدم دسترسی به مقدار r_i در هنگام دسترسی به اطلاعات درون کارت هوشمند، نمی‌تواند تنها با امتحان کردن حالات مختلفی از گذرواژه(حدس گذرواژه) در رابطه $MP'_i = h(r'_i \| PW'_i)$ به مقدار MP'_i دست پیدا کند. همچنین به دلیل عدم توانایی فرد مهاجم در محاسبه مقدار MP'_i ، او نمی‌تواند شناسه کاربر را با امتحان کردن حالات مختلفی از شناسه در رابطه $e_i = ?h\ (MP'_i \| ID'_i)$ به دست آورد. علاوه بر این مهاجم به دلیل عدم توانایی محاسبه $MP'_i = h(r'_i \| PW'_i)$ و سپس $d_i = f_i \oplus h(MP'_i \| e_i)$ نمی‌تواند به بخش کلید نشست کاربر (K_i) در رابطه $Ki = M2 \oplus h(di \| T1)$ و درنتیجه محاسبه مقدار نهایی کلید نشست $SK = h(K_i \oplus K'_j)$ دست پیدا کند. نمایش دقیقی از این فاز در شکل ۵ آمده است.

U_i	S_j	GWN
Knows its ID_i and PW_i Has a $SC = \{q_i, e_i, f_i, g_i\}$	Stores SID_j , x_j and $h(X_{GWN} \| \| 1)$	Stores its master key X_{GWN}
User: Inserts SC into a terminal User: Inputs PW'_i and ID'_i *SC:* $r'_i = ID'_i \oplus q_i$ *SC:* $MP'_i = h(r'_i \| \| PW'_i)$ *SC:* $e_i = ?h(MP'_i \| \| ID'_i)$ *SC:* $d_i = f_i \oplus h(MP'_i \| \| e_i)$ *SC:* $h(X_{GWN}) = g_i \oplus h(MP'_i \| \| d_i)$ *SC:* $M_1 = ID'_i \oplus h(h(X_{GWN}) \| \| T_1)$ *SC:* Chooses a random nonce K_i *SC:* $M_2 = K_i \oplus h(d_i \| \| T_1)$ *SC:* $M_3 = h(M_1 \| \| M_2 \| \| K_i \| \| T_1)$ User: Chooses S_j		
$\xrightarrow{\{M_1, M_2, M_3, T_1\}}$	Checks $\|T_1 - Tc\| < \Delta T$	
	$ESID_j = SID_j \oplus h(h(X_{GWN} \| \| 1) \| \| T_2)$ Chooses a random nonce K_j $M_4 = h(x_j \| \| T_1 \| \| T_2) \oplus K_j$ $M_5 = h(SID_j \| \| M_4 \| \| T_1 \| \| T_2 \| \| K_j)$	
	$\xrightarrow{\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}}$	Checks $\|T_2 - T_c\| < \Delta T$
		$SID'_j = ESID_j \oplus h(h(X_{GWN} \| \| 1) \| \| T_2)$ $x'_j = h(SID'_j \| \| X_{GWN})$ $K'_j = M_4 \oplus h(x'_j \| \| T_1 \| \| T_2)$ $M_5 = ?h(SID'_j \| \| M_4 \| \| T_1 \| \| T_2 \| \| K'_j)$ $ID'_i = M_1 \oplus h(h(X_{GWN}) \| \| T_1)$ $d'_i = h(ID'_i \| \| X_{GWN})$ $K'_i = M_2 \oplus h(d'_i \| \| T_1)$ $M_3 = ?h(M_1 \| \| M_2 \| \| K'_i \| \| T_1)$ $M_6 = K'_j \oplus h(d'_i \| \| T_3)$ $M_7 = K'_i \oplus h(x'_j \| \| T_3)$ $M_8 = h(M_6 \| \| d'_i \| \| T_3)$ $M_9 = h(M_7 \| \| x'_j \| \| T_3)$ $M_{11} = K_i \oplus h(d_i \| \| T_3)$
	Checks $\|T_3 - T_c\| < \Delta T$	$\xleftarrow{\{M_6, M_7, M_8, M_9, M_{11}, T_3\}}$
	$M_9 = ?h(M_7 \| \| x_j \| \| T_3)$ $K'_i = M_7 \oplus h(x_j \| \| T_3)$ $SK = h(K'_i \oplus K_j)$ $M_{10} = h(SK \| \| M_6 \| \| M_8 \| \| T_3 \| \| T_4)$	
Checks $\|T_4 - T_c\| < \Delta T$	$\xleftarrow{\{M_6, M_8, M_{10}, T_3, T_4\}}$	
$M_8 = ?h(M_6 \| \| d_i \| \| T_3)$ $K'_j = M_6 \oplus h(d_i \| \| T_3)$ $SK = h(K_i \oplus K'_j)$ $M_{10} = ?h(SK \| \| M_6 \| \| M_8 \| \| T_3 \| \| T_4)$		

شکل ۵. فاز ورود و احراز هویت طرح ارائه‌شده

۵. تحلیل امنیتی طرح ارائه‌شده

پس از ارائه طرح UAKAS توسط سبزی نژاد و ترکانویچ، علی‌رغم کارا و مناسب بودن این طرح برای پیاده‌سازی در محیط‌های شبکه‌های حسگر بی‌سیم مبتنی بر مفهوم اینترنت اشیاء، این طرح نتوانست نیازهای امنیتی موردنیاز را برآورده کند و دارای اشکالات امنیتی متفاوتی بود که در بخش سوم به آن پرداخته شد. در بخش چهارم طرح UAKAS امن و کارا مبتنی بر طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ برای احراز هویت متقابل گره‌ها و کاربران ارائه شد که علاوه بر در نظر گرفتن محدودیت‌های محیط مذکور، اشکالات طرح پیشین را با در نظر گرفتن نیازمندی‌های امنیتی برطرف کرد. در این بخش پس از انجام مقایسه‌ای از ویژگی‌های امنیتی طرح پیشنهادی با طرح ارائه‌شده پیشین، امن و کارا بودن طرح پیشنهادی موردبررسی قرار می‌گیرد.

۵. ۱. مقایسه ویژگی‌های امنیتی

طرح UAKAS امن ارائه‌شده حفاظت از شناسه و گذرواژه کاربر، گمنامی کاربر، احراز هویت متقابل و توافق کلید را برای ما فراهم می‌کند. همچنین در برابر حمله سرقت کارت هوشمند، افشای پارامترهای مهم امنیتی و حمله جعل کاربر که جزء کاستی‌ها و نقص‌های جدی طرح سبزی نژاد و ترکانویچ محسوب می‌شود، مقاوم است. ازاین‌رو طرح UAKAS امن ارائه‌شده امنیت بیشتری را با حفظ همان میزان کارایی و عملکرد برای ما فراهم می‌کند. مقایسه‌ای از ویژگی‌های امنیتی طرح UAKAS امن ارائه‌شده و طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ در جدول ۱ آمده است.

جدول ۱. مقایسه ویژگی‌های امنیتی طرح ارائه‌شده و طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ

ویژگی‌های امنیتی	طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ	طرح UAKAS امن ارائه‌شده
احراز هویت متقابل	بله	بله
توافق کلید	بله	بله
محافظت از شناسه و گذرواژه	خیر	بله
گمنامی کاربر	خیر	بله
گمنامی گره حسگر	بله	بله
مقاوم در برابر حمله سرقت SC	خیر	بله
محافظت از کلید نشست	خیر	بله
افشای پارامترهای مهم امنیتی	خیر	بله
حمله جعل کاربر	خیر	بله

۵. ۱. ۱. حمله سرقت کارت هوشمند

در سرقت کارت هوشمند فرض اولیه بر آن است که مهاجم توانسته کارت هوشمند را سرقت کند، لذا او می‌تواند تمامی پارامترهای ذخیره‌شده در کارت $SC= \{r_i, e_i, f_i, g_i\}$ را به کمک حملات فیزیکی [۹] استخراج کند و سپس با استفاده از آن‌ها حمله‌ی کشف گذرواژه یا شناسه کاربر را پیاده‌سازی کند و همچنین شروعی باشد برای سایر تهدیدهای دیگر. بنابراین انتخاب و محاسبه هوشمندانه پارامترهای ذخیره‌شده در کارت هوشمند از نکات ضروری است که از پیاده‌سازی این‌گونه حمله‌ها جلوگیری به عمل می‌آورد.

همان‌طور که در طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ مشاهده شد، پارامتر عدد تصادفی r_i باعث می‌شد تا مهاجم بتواند با انجام یکسری محاسبات، شناسه و گذرواژه کاربر را کشف کند. برای جلوگیری از این کار، در فاز ثبت‌نام کاربر، کاربر U_i مقدار $q_i = r_i \oplus ID_i$ را محاسبه کرده و سپس q_i را در کارت هوشمند $(SC = \{q_i, e_i, f_i, g_i\})$ ذخیره می‌کند. لازم به ذکر است محاسبه مقدار q_i به‌منظور عدم ذخیره آشکار مقدار r_i در کارت هوشمند است و این عمل باعث می‌شود در صورت دزدیده شدن یا گم‌شدن کارت، مهاجم نتواند به مقدار r_i دست پیدا کند.

۵. ۱. ۲. محافظت از گذرواژه

همان‌گونه که در بخش (۳. ۱) توضیح داده شد مهاجم پس از دسترسی به اطلاعات کارت هوشمند می‌توانست با در دست داشتن مقدار r_i، مقدار گذرواژه را به دست می‌آورد. این در حالی است که در UAKAS امن ارائه‌شده کاربر با محاسبه مقدار $q_i = r_i \oplus ID_i$ در فاز ثبت‌نام و قرار دادن مقدار q_i به‌جای r_i در کارت هوشمند مانع از دسترسی فرد مهاجم به مقدار r_i می‌شود. در این صورت فرد مهاجم برای محاسبه مقدار $MP'_i = h(r'_i \| PW'_i)$ از طریق حدس گذرواژه، ابتدا باید مقدار $r'_i = ID'_i \oplus q_i$ را به دست آورد، که این پیچیدگی کار را با توجه به حداقل ۶۴ بیتی بودن طول شناسه و گذرواژه برای فرد مهاجم به‌طور باورنکردنی افزایش می‌دهد.

۵. ۱. ۳. محافظت از شناسه

با توجه به بخش قبل (۵. ۱. ۲) متوجه می‌شویم که درصورتی‌که پیچیدگی کار برای محاسبه مقدار MP'_i زیاد شود(چراکه حدس گذرواژه و شناسه با توجه به حداقل طول ۶۴ بیتی هرکدام از آن‌ها غیرممکن است)، فرد مهاجم نمی‌تواند مقدار $e_i =? h(MP'_i \| ID_i)$ را به‌سادگی محاسبه کند. به بیان ساده‌تر فرد مهاجم برای محاسبه $MP'_i = h((ID'_i \oplus q_i) \| PW'_i)$ باید ID'_i و PW'_i که هرکدام حداقل ۶۴ بیت طول دارد را حدس بزند. لازم به ذکر است که طول شناسه و گذرواژه در طرح سبزی نژاد ۶۴ بیت است[۶و۸] .

۵. ۱. ۴. گمنامی کاربر

به دلیل اینکه تمامی اجزای موجود در شبکه از طریق کانال ناامن با یکدیگر ارتباط برقرار می‌کنند، مهاجم می‌تواند به‌سادگی کانال را شنود کند. درصورتی‌که فرد مهاجم نتواند به مقادیر درون کارت (مانند r_i) دسترسی پیداکرده و سپس گذرواژه را کشف کند، او نخواهد توانست با محاسبه به ترتیب MP'_i، d_i و $h(X_{GWN})$ به مقدار ID'_i دست پیدا کند. همچنین در هیچ‌کدام از فازهای این طرح شناسه کاربر (ID_i) به‌صورت محافظت نشده بر روی کانال عمومی ناامن ارسال نشده است. این نشان می‌دهد که طرح UAKAS امن ارائه‌شده گمنامی کاربر را رعایت می‌کند.

۵. ۱. ۵. محافظت از کلید نشست

به دلیل اینکه طرح ارائه‌شده یک طرح احراز هویت و توافق کلید است، فرایند توافق کلید از اهمیت بالایی برخوردار است. در این طرح، کاربر و گره حسگر بر روی یک کلید به‌صورت متقابل توافق می‌کنند و هرکدام از آن‌ها به‌صورت جداگانه مقدار $SK = h(K_i \oplus K_j)$ را در فاز احراز هویت محاسبه می‌کنند. این در حالی است که هرکدام از طرفین در ساخت کلید نشست مشارکت دارد(مقدار K_i را کاربر و مقدار K_j را گره حسگر تولید می‌کند). حال باید در نظر داشت چون اجزای موجود در شبکه از طریق کانال ناامن با یکدیگر ارتباط برقرار می‌کنند، مهاجم می‌تواند به‌سادگی کانال را شنود کند. ازاین‌رو باید نهایت دقت در مبادلات طرح صورت گیرد تا فرد مهاجم نتواند با شنود کانال ناامن به مقادیری دست پیدا کند که درنتیجه منجر به کشف کلید نشست شود. در طرح ارائه‌شده توسط سبزی نژاد و ترکانویچ مهاجم با دسترسی به اطلاعات درون کارت هوشمند و کشف گذرواژه و سپس محاسبه MP'_i و d_i می‌توانست به مقدار $K_i = M_2 \oplus h(d_i \| T_1)$ دست پیدا کند. همچنین او با شنود M_6 و T_3 از کانال مقدار $K'_j = M_6 \oplus h(d'_i \| T_3)$ را محاسبه می‌کرد و درنهایت $SK = h(K_i \oplus K_j)$ را به دست می‌آورد. در طرح UAKAS امن ارائه‌شده، کاربر با قرار دادن q_i به‌جای r_i در کارت، کار را برای محاسبه مقدار d_i بسیار سخت کرد به‌طوری‌که می‌توان ادعا کرد این کار نشدنی است! در این صورت فرد مهاجم نمی‌تواند هیچ‌کدام از مقادیر K_i و K_j را محاسبه کند.

۵. ۱. ۶. حمله جعل کاربر

همان‌طور که تاکنون ملاحظه شد عامل اصلی تمامی تهدیدها و حملات به وجود آمده، مربوط به پارامتر r_i ذخیره‌شده درون کارت هوشمند است. حمله جعل کاربر هم از این قاعده مستثنی نبوده و همان‌گونه که در بخش (۳. ۵) به‌صورت کامل توضیح داده شد، فرد مهاجم با دردست داشتن مقدار d_i و ایجاد یک عدد تصادفی K_i توانست کاری کند که گره GWN باور کند که پیام از طرف کاربر معتبر U_i دریافت شده است! و این یادآور این نکته است که "انتخاب و محاسبه هوشمندانه پارامترهای ذخیره‌شده در کارت هوشمند از نکات ضروری طراحی طرح‌های احراز هویت است که از پیاده‌سازی این‌گونه حمله‌ها جلوگیری به عمل می‌آورد".

۶. نتیجه‌گیری

در این مقاله طرحی امن و کارا برای احراز هویت متقابل و توافق کلید در شبکه‌های حسگر بی‌سیم مبتنی بر مفهوم اینترنت اشیاء ارائه‌شده است. طرح ارائه‌شده مبتنی بر طرح سبزی نژاد و ترکانویچ است. ازاین‌رو تلاش شده است با در نظر گرفتن نیازمندی‌های امنیتی ضعف‌ها و آسیب‌پذیری‌های ذکرشده در مقاله برطرف گردد. در این مقاله ابتدا تعدادی از ضعف‌های امنیتی طرح سبزی نژاد و ترکانویچ بیان‌شده است و سپس طرحی بهبودیافته برای احراز هویت دوطرفه و توافق کلید ارائه‌شده است. طرح ارائه‌شده ویژگی‌هایی همچون محافظت از شناسه و گذرواژه، گمنامی کاربر، احراز هویت متقابل و توافق کلید را فراهم می‌کند و همچنین در برابر حمله‌هایی مانند حمله سرقت کارت هوشمند، افشای پارامترهای مهم امنیتی و حمله جعل کاربر که از کاستی‌ها و نقص‌های طرح سبزی نژاد و ترکانویچ محسوب می‌شود، مقاوم است.

مراجع

1. He, D., Kumar, N., Chen, J., Lee, C. C., Chilamkurti, N., & Yeo, S. S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*.

2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4), 393-422.

3. Xue, K., Ma, C., Hong, P., & Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, *36*(1), 316-323.

4. Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160-1172.

5. Vaidya, B., Makrakis, D., & Mouftah, H. T. (2010, October). Improved two-factor user authentication in wireless sensor networks. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on* (pp. 600-606). IEEE.

6. Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks*, *36*, 152-176.

7. Bassi, A., & Horn, G. (2008). Internet of Things in 2020: A Roadmap for the Future. *European Commission: Information Society and Media*, *22*, 97-114.

8. Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, *20*, 96-112.

9. Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE transactions on computers*, *51*(5), 541-552.

پیوست ۱.

جدول ۲. لیست علائم و اختصارات

علائم	توضیحات
SC	کارت هوشمند (Smart card)
U_i	کاربر i
S_j	گره حسگر (Sensor node)
r_i, r_j	عدد تصادفی (nonce) برای کاربر و گره حسگر
GWN	گره Gateway
PW_i	رمز عبور کاربر
ID_i	شناسه کاربر
SID_j	شناسه گره حسگر
X_{GWN-Sj}	پسورد امن به اشتراک گذاشته‌شده بین GWN و حسگر S_j
X_{GWN-Ui}	پسورد امن به اشتراک گذاشته‌شده بین GWN و کاربر U_i
X_{GWN}	پسورد امن که تنها در اختیار گره GWN است.
T_i	برچسب(مهر) زمانی
ΔT	فاصله زمانی برای تأخیر انتقال مجاز
SK	کلید نشست پروتکل
h( )	تابع هش یک‌طرفه
$\oplus$, $\|\|$	XOR، عملگر الحاق
MI_i, MP_i	پوشاندن(Mask) شناسه و کلمه عبور کاربر