



طرحی امن و کارا برای احراز هویت کاربران در شبکه های حسگر بی سیم مبتنی بر مفهوم اینترنت اشیا

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

۱- دانشجوی کارشناسی ارشد شبکه های 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 اشیا اصطلاحی است برای توصیف دنیایی که در آن اشیا قادر خواهند بود با اتصال به اینترنت یا به کمک ابزارهای ارتباطی، با سایر اشیا تعامل داشته باشند و اطلاعات خود را باهم و یا با انسان ها به اشتراک بگذارند و کلاس جدیدی از قابلیت ها، برنامه های کاربردی و سرویس ها را ارائه دهند. دنیایی که در آن تمامی اشیا و دستگاه های نامتجانس قابلیت آدرس دهی و در نتیجه قابلیت کنترل پذیری دارند. شبکه های حسگر بی سیم در یک چنین محیطی نقش مهمی را بازی می کند چراکه حسگرها جزء کلیدی اینترنت اشیا محسوب شده و شامل یک میدان گسترده از این کاربردها است. محققان در تلاش اند که چگونه می توانند شبکه های حسگر بی سیم را به صورت بهتری در محیط اینترنت اشیا یکپارچه کنند. یکی از جنبه های این یکپارچگی دیدگاه امنیت است. اخیراً محمد سبزی نژاد و ترکانویچ طرح کارآمدی برای احراز هویت کاربران و توافق کلید در شبکه های حسگر بی سیم نامتجانس مبتنی بر مفهوم اینترنت اشیا ارائه دادند. اگرچه طرح ارائه شده توسط سبزی نژاد و ترکانویچ کارآمد است، اما با تحلیل و بررسی های صورت گرفته مشخص شد که این طرح ناامن بوده و در مقابل برخی حملات رمزنگاری آسیب پذیر است. در این مقاله ضعف های امنیتی طرح سبزی نژاد و ترکانویچ نشان داده شده و سپس طرحی امن و کارا برای احراز هویت کاربران ارائه می شود.

کلمات کلیدی: اینترنت اشیا، شبکه های حسگر بی سیم، احراز هویت، توافق کلید.

۱. مقدمه

ورود غیرمجاز به یک سیستم، همواره مورد توجه مهاجمین و نفوذ گران بوده است. نفوذ به این سیستم ها در عین حال که منافع بسیاری برای مهاجمان به ارمغان می آورد، ممکن است خسارات جبران ناپذیری را به سازمان ها و اشخاص تحمیل کند. یکی از مهم ترین راهکارها برای مقابله با این گونه تهدیدات و برای افزایش ایمنی شبکه ها استفاده از پروتکل های احراز هویت است. احراز هویت، یکی از مهم ترین و اساسی ترین گام ها 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]. به عنوان مثال در حالتی که اصالت یک پیام مدنظر است، سرویس احراز هویت باید به دریافت کننده 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 می شود. به عبارتی مکانیزم های احراز هویت روش هایی برای کنترل ورود کاربران از طریق یک شبکه ارتباطی ناامن به یک کارگزار هستند. بنابراین استفاده از یک پروتکل کارا و مستحکم بدین منظور، می تواند از بسیاری از حمله های مهاجمان جلوگیری کند. اگر امنیت کافی به هنگام احراز هویت برآورده نگردد، یک مهاجم که به خطوط ارتباطی دسترسی دارد، می تواند با انجام حمله هایی همچون حمله جعل، حمله تکرار، حمله نشست های موازی، حمله واژه نامه، حمله حدس پسورد و غیره به صورت غیرمجاز وارد سیستم گردد و از خدمات آن سوءاستفاده کند. در نتیجه مکانیزم احراز هویت باید توانایی مقابله با چنین حمله هایی را داشته باشد. همچنین یکی از مهم ترین ملاحظات در طراحی پروتکل های احراز هویت، توجه به محیطی است که این پروتکل ها مورد کاربرد قرار خواهند گرفت. محیط های مختلف دارای محدودیت های مختلفی هستند. مانند محدودیت پردازشی، محدودیت فضای پیاده سازی، محدودیت توان مصرفی و محدودیت هزینه پیاده سازی [۲]. هر سیستم یا هر محیطی دارای خصوصیات و اقتضائات خاصی است که بایستی توسط طراحان مکانیزم های احراز هویت مورد توجه قرار گیرد. علاوه بر این برآورده کردن پاره ای از ویژگی های امنیتی همچون گمنامی کاربر، امنیت پیشرو، اصلاح پذیری، عدم تمیز پیام و محرمانگی، افزایش سطح ایمنی طرح و رضایت کاربران خود را در پی دارد که در بسیاری از مکانیزم ها در نظر گرفته نمی شود [۳]. روش های احراز هویت مبتنی بر کلمه عبور به دلیل سادگی و هزینه کم، رایج ترین مکانیزم احراز هویت در محیط های هوشمند به شمار می روند، ولی میزان اطمینان از عملکرد این طرح ها تنها به میزان محرمانگی کلمه عبور بستگی دارد و با فاش شدن کلمه عبور امنیت طرح به کلی از بین می رود [۴]. برای رفع این کاستی اخیراً مکانیزم های احراز هویت مبتنی بر دو یا چند فاکتور امنیتی مورد توجه قرار گرفته است. یکی از این مکانیزم ها، استفاده از کارت هوشمند به همراه کلمه عبور است. مزایای بالقوه کارت هوشمند، کاربرد آن را در طرح های احراز هویت توجیه می کند [۵]. این مزایا عبارتند از:

- کارت هوشمند قابل حمل است.
- حافظه قابل خواندن و نوشتن دارد، بنابراین می تواند داده های محرمانه ای 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 می دهد.

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

- کاربرد کارت هوشمند محدود به محیط هایی است که در آن ها امکاناتی برای مبادله اطلاعات با کارت هوشمند وجود داشته باشد (دستگاه کارت خان).
- توان محاسباتی کارت هوشمند محدود است و برای پیاده سازی الگوریتم هایی که هزینه محاسباتی زیادی دارند (همچون رمزنگاری نامتقارن) مناسب نیست.
- امکان گم شدن یا دزدیده شدن و در نتیجه سوءاستفاده از آن ها وجود دارد.

اخیراً سبزی نژاد و ترکانویچ [۶] مکانیزمی سبک و کارا برای توافق کلید و احراز هویت دوطرفه کاربران در ^۱WSN نامتجانس مبتنی بر مفهوم اینترنت اشیا^۲ ارائه دادند که در آن کاربران از راه دور می توانند بدون ارتباط اولیه با ^۳GWN با گره مورد نظر ارتباط برقرار کنند. ما این طرح را جهت سهولت ^۴UAKAS می نامیم. در این طرح از گره ^۳GWN به عنوان یک جزء سوم برای کمک در فرایند احراز هویت استفاده می شود. این در حالی است که در اکثر طرح های 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 ارائه شده توسط سبزی نژاد و ترکانویچ احراز هویت دوطرفه مابین کاربر، گره انتهایی و GWN را تضمین می کند. همچنین طرح ارائه شده توسط سبزی نژاد و همکارانش به دلیل اینکه تنها از محاسبات hash و XOR استفاده می کند، مناسب محیط هایی 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 می کند.

از این رو بخش دوم مروری دارد بر طرح ارائه شده توسط سبزی نژاد و ترکانویچ، در بخش سوم پس از انجام تحلیل امنیتی و حمله به طرح ارائه شده ی پیشین، تعدادی از آسیب پذیری ها و ضعف های امنیتی طرح ارائه شده نشان داده شده است. در بخش چهارم راه حل ارائه می شود. در بخش پنجم پس از انجام مقایسه ای از ویژگی های امنیتی طرح پیشنهادی با طرح ارائه شده ی پیشین، امن و کارا بودن طرح پیشنهادی مورد بررسی قرار می گیرد. بخش ششم نیز به نتیجه گیری اختصاص دارد. لازم به ذکر است لیست علائم و اختصارات در پیوست ۱ در انتهای مقاله ذکر شده است.

۲. مروری بر طرح سبزی نژاد و ترکانویچ

طرح ارائه شده توسط سبزی نژاد و ترکانویچ کاربر را قادر می سازد تا با گره مورد نظرش در شبکه ارتباط برقرار کند. این همان ویژگی خاصی است که در محیط اینترنت اشیا انتظارش را داریم، جایی که تمامی دستگاه ها مانند حسگرها، گوشی های هوشمند، ساعت های هوشمند، خودروهای هوشمند و... از طریق اینترنت به هم متصل می شوند [۸ و ۷]. بنابراین در یک چنین سناریویی، کاربر قادر است بدون نیاز به اتصال به گره GWN، با گره مورد نظر ارتباط برقرار کرده و داده رد و بدل نماید. در این طرح از گره GWN به عنوان یک جزء سوم برای کمک در فرایند احراز هویت استفاده می شود.

مزیت دیگر این طرح، معماری سبک وزن آن است زیرا از عملگرهای محاسباتی ساده و کم هزینه مانند توابع هش یک طرفه و XOR استفاده می کند که مناسب شبکه های دارای منابع محدود مانند شبکه های حسگر بی سیم و اینترنت اشیا است. در این قسمت برای فهم بهتر مطالبی که در ادامه خواهد آمد، مروری بر طرح ارائه شده توسط سبزی نژاد و ترکانویچ خواهیم داشت. طرح ارائه شده توسط سبزی نژاد و ترکانویچ طرحی کاراست که از چهار فاز اصلی: فاز قبل از راه اندازی، فاز ثبت نام، فاز ورود و فاز احراز هویت تشکیل شده است.

۲.۱. فاز قبل از راه اندازی (فاز قبل از استقرار)

این فاز که به فاز نصب هم معروف است به صورت آفلاین توسط مدیر شبکه اجرا می شود. در طول این فاز، هر گره حسگر $\{S_j | 1 \leq j \leq m\}$ با یک شناسه (SID_j) و یک کلید رمز امن به صورت تصادفی تولید شده (X_{GWN-S_j}) ، تعریف شده است. لازم به ذکر است که این کلید (X_{GWN-S_j}) با گره GWN به اشتراک گذاشته شده و در حافظه گره حسگر ذخیره شده است. برای گره GWN نیز یک کلید رمز خیلی امن تصادفی (X_{GWN}) که تنها توسط خود گره GWN شناخته می شود، تعریف می شود. این کلید نیز به صورت امن در حافظه گره GWN ذخیره می شود. علاوه بر این، گره GWN کلید امن به اشتراک گذاشته شده بین خود و گره های حسگر را در خود ذخیره می کند $\{X_{GWN-S_j} | 1 \leq j \leq m\}$. هدف از کلید به اشتراک گذاشته شده (X_{GWN-S_j}) استفاده از آن در فاز ثبت نام است. لازم به ذکر است که کلید به اشتراک گذاشته شده بین حسگرها و گره GWN (X_{GWN-S_j}) را می توان بعد از فاز ثبت نام حذف کرد. این کار گره GWN را قادر می سازد تعداد بیشتری گره حسگر را بدون پر شدن حافظه به شبکه اضافه کند، چراکه ما در این گونه شبکه ها دارای محدودیت حافظه هستیم.

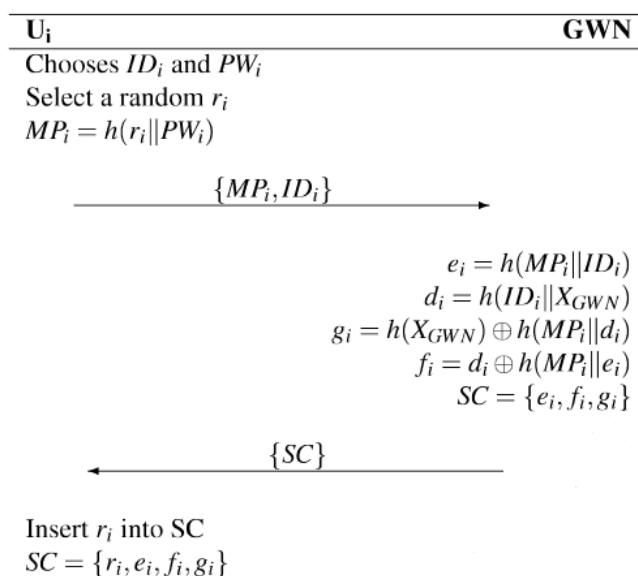


۲.۲. فاز ثبت نام

فاز ثبت نام در طرح ارائه شده توسط سبزی نژاد و ترکانویچ به دو بخش تقسیم می شود. بخش ثبت نام کاربر و بخش ثبت نام گره حسگر. هر گره حسگر پس از استقرار در محیط مورد استفاده باید برای احراز هویت و تأیید قانونی بودن آن، در گره GWN ثبت نام کند. همچنین کاربران قبل از اینکه بتوانند به گره حسگر خاصی متصل شده و به آن دسترسی داشته باشند، باید در شبکه ثبت نام کنند. فرایند ثبت نام کاربر از طریق یک کانال امن به وسیله گره GWN انجام می شود. همچنین پس از تکمیل فرایند ثبت نام، یک کارت هوشمند در اختیار کاربر قرار می گیرد. توضیحات کامل فاز ثبت نام کاربر در طرح ارائه شده به صورت زیر است:

▪ ثبت نام کاربر

در این طرح کاربر U_i با انتخاب شناسه و گذرواژه و همچنین یک عدد تصادفی فرایند ثبت نام را آغاز می کند. سپس کاربر U_i با محاسبه $MP_i = h(r_i || PW_i)$ گذرواژه خود را می پوشاند. پس از محاسبه MP_i کاربر U_i پیام $\{MP_i, ID_i\}$ را از طریق کانالی امن به گره GWN ارسال می کند. پس از دریافت پیام ثبت نام از U_i گره GWN در صورت تصمیم به ثبت نام 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 می کند. پس از آن گره GWN مقادیر $\{e_i, f_i, g_i\}$ را در حافظه کارت هوشمند (SC) ذخیره کرده و آن را برای کاربر U_i ارسال می کند. در انتها کاربر U_i مقدار r_i را در کارت هوشمند ذخیره کرده و فاز ثبت نام کاربر به پایان می رسد. نمایشی از این فاز در شکل ۱ آمده است.



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

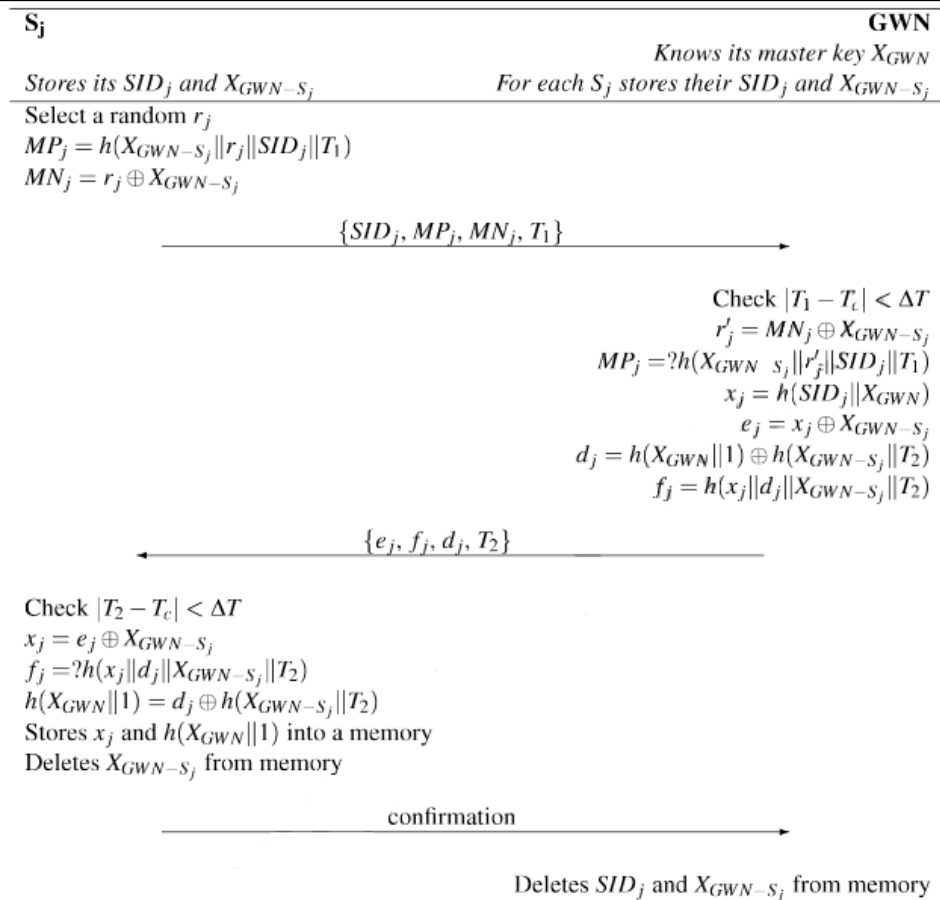
¹ Smart Card



■ ثبت نام گره حسگر

همان طور 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 می شوند. حال هر حسگر باید خود را از طریق کانالی غیر امن (فضای آزاد) در گره GWN ثبت نام کند. برای این کار گره S_j ابتدا با انتخاب عدد تصادفی r_j و محاسبه $\{SID_j, MP_j, MN_j = r_j \oplus X_{GWN-Sj} \text{ و } MP_j = h(X_{GWN-Sj} || r_j || SID_j || T_1)\}$ برچسب زمانی گره S_j در زمان حاضر است. گره GWN پس از دریافت پیام ثبت نام از طرف گره S_j اعتبار و صحت برچسب زمانی را بررسی می کند ($|T_1 - T_c| < \Delta t$). اگر صحت برچسب زمانی مورد تأیید نبود، GWN عملیات دیگری انجام نمی دهد و پیام عدم پذیرش را برای گره S_j ارسال می کند. در غیر این صورت GWN ، مقدار $r'_j = MN_j \oplus X_{GWN-Sj}$ و MP'_j را محاسبه کرده و سپس بررسی می کند که آیا MP'_j محاسبه شده 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 می کند. پس از آن گره GWN مقادیر d_j, e_j, x_j و f_j را محاسبه می کند. حال گره GWN پیامی شامل $\{e_j, f_j, d_j, T_2\}$ را از طریق کانال عمومی به گره S_j ارسال می کند.

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



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

۳.۲. فاز ورود

همان طور که پیش تر 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 به منظور ایجاد یک ارتباط امن بین کاربر و گره حسگر مورد استفاده قرار می گیرد 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 می شود. برای این کار کاربر U_i کارت را درون کارت خوان قرار داده و شناسه ID_i و گذرواژه PW_i خود را وارد می کند. سپس نیاز است که کارت هوشمند از طریق اطلاعاتی که در خود ذخیره دارد، صحت هویت مالک کارت را مشخص کند. برای این کار ابتدا SC ابتدا $MP_i = h(r_i || PW_i)$ را با توجه به گذرواژه وارد شده 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 می کند. اگر مقدار e_i به دست آمده با مقدار اصلی e_i برابر بود، SC قانونی بودن کاربر U_i را تأیید می کند و فرایند فاز ورود پایان می پذیرد.

۴.۲. فاز احراز هویت

بعد از ورود موفق، SC خود را برای فرایند احراز هویت آماده می کند. در ادامه روند فوق، SC ابتدا مقادیر $d_i = f_i \oplus$ و سپس $h(MP_i || e_i)$ را محاسبه می کند. بعد از آن SC از سه مقدار کمکی M_1, M_2 و



M_3 برای ارسال نتیجه ی محاسبات خود به گره GWN از طریق کانال عمومی استفاده می کند. SC پس از محاسبه مقدار $M_2 = K_i \oplus$ یک عدد تصادفی (K_i) با آنتروپی بالا^۱ انتخاب کرده و سپس مقادیر $M_1 = ID_i' \oplus h(h(X_{GWN} || T_1))$ و $M_3 = h(M_1 || M_2 || K_i || T_1)$ را محاسبه می کند. لازم به ذکر است محاسبه مقدار M_1 به منظور پوشاندن شناسه کاربر U_i ، و هدف از محاسبه مقدار M_2 پوشاندن K_i که بخشی از اجزای تشکیل دهنده کلید نشست محسوب می شود، 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 می کند.

حسگر S_j پس از دریافت پیام احراز هویت از کاربر U_i فرایند واری و تصدیق هویت را به گره GWN محول می کند. اما قبل از واگذار کردن این فرایند، با بررسی برچسب زمانی $|T_1 - T_c| < \Delta t$ از احتمال وجود حمله تکرار اطمینان حاصل می کند. همچنین نیاز است در صورت تأیید برچسب زمانی، مقادیر $ESID_j$ و M_4 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 $ESID_j = SID_j \oplus h(h(X_{GWN} || 1)T_2)$ ، یک عدد تصادفی با آنتروپی بالا (K_j) انتخاب می کند که این عدد بخش دوم کلید نشست مورد توافق ما را تشکیل می دهد. 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 می شود. همچنین مقدار M_4 بعداً برای استخراج K_j توسط گره GWN مورد استفاده قرار می گیرد. 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 می کند.

گره GWN پس از دریافت پیام احراز هویت از گره S_j ابتدا برای اطمینان از احتمال وجود حمله تکرار برچسب زمانی را بررسی می کند. 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 می کند. برای این کار گره GWN ابتدا شناسه گره حسگر $SID_j' = ESID_j \oplus h(h(X_{GWN} || 1)T_2)$ را با مقادیر دریافتی و کلید رمز امن خود (X_{GWN}) محاسبه کرده و با استفاده از نتیجه آن مقادیر $x_j' = h(SID_j' || T_1 || T_2)$ و سپس $K_j' = M_4 \oplus h(x_j' || T_1 || T_2)$ را به دست می آورد. 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 $M_5 = ?$ از قانونی بودن گره S_j اطمینان حاصل می کند.

پس از احراز هویت گره حسگر نوبت به اطمینان از قانونی بودن کاربر U_i می رسد. 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 می دهد، به دست می آورد. 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 $M_3 = ?$ از قانونی بودن کاربر U_i که فرایند احراز هویت را آغاز کرده است اطمینان حاصل می کند.

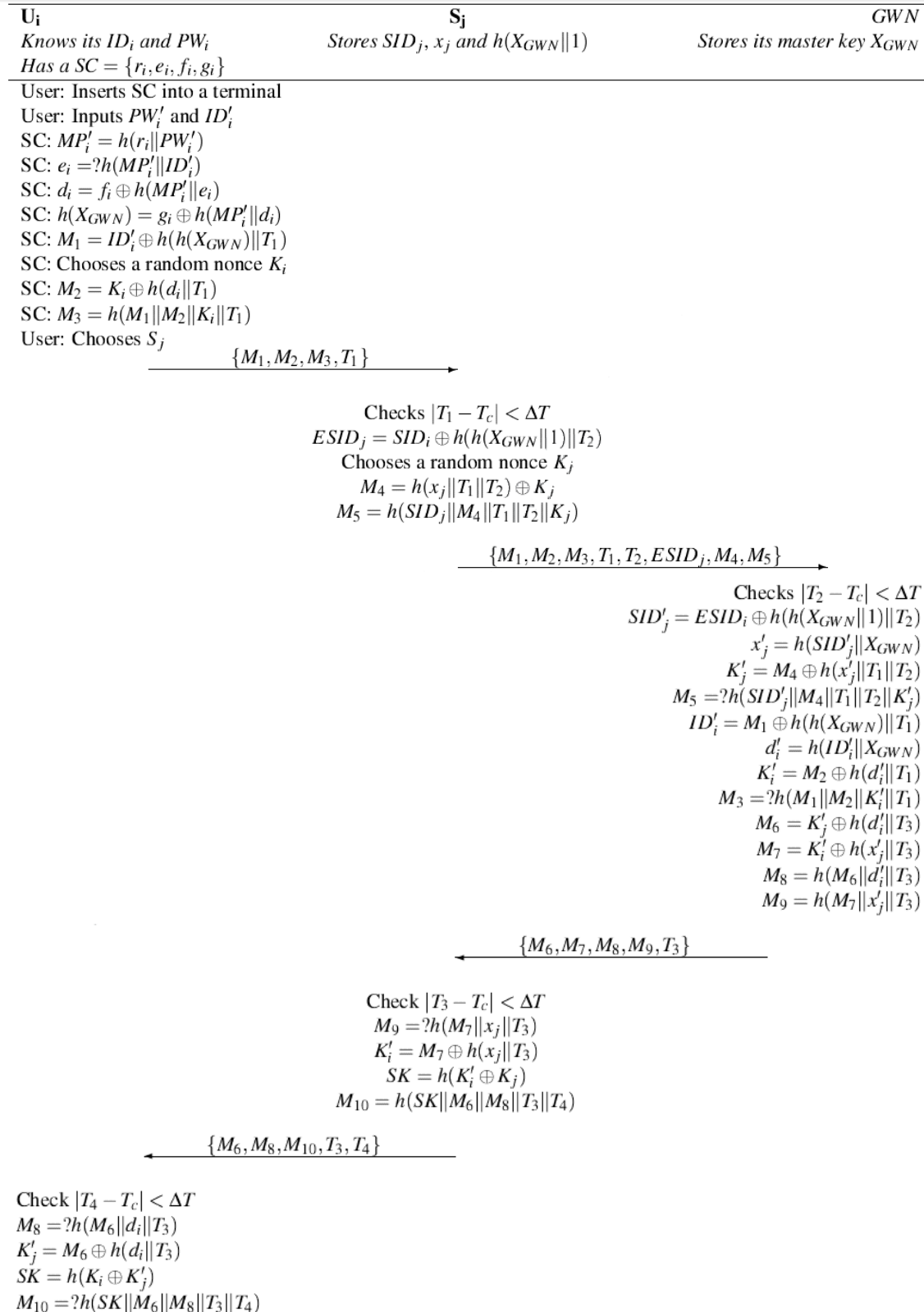
در ادامه و پس از احراز هویت موفق گره S_j و کاربر U_i ، گره GWN شروع به ایجاد پیام تأیید برای ارسال به گره S_j می کند. برای این کار گره GWN ابتدا با محاسبه $M_6 = K_j' \oplus h(d_i' || T_3)$ و $M_7 = K_i' \oplus h(x_j' || T_3)$ مقادیر K_i و K_j محاسبه شده را می پوشاند. سپس گره GWN با محاسبه دو مقدار $M_8 = h(M_6 || d_i' || T_3)$ 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 می کند. در اینجا گره GWN وظیفه اش را به عنوان جزء سوم کمک کننده در فرایند احراز هویت به اتمام می رساند.

^۱ 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 در نتیجه قانونی بودن گره GWN را تأیید می کند. 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 می کند. 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 می کند.

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 $M_8 = ?$ قانونی بودن گره GWN را تأیید می کند. 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 می کند. 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 $M_{10} = ?$ از قانونی بودن گره S_j اطمینان حاصل می کند. در این لحظه فاز احراز هویت با موفقیت به پایان می رسد. نمایشی کاملی از این فاز در شکل ۳ آمده است.



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 می کند. علی رغم ادعای نویسندگان این طرح، مبنی بر امنیت بالای آن ثابت شد که این طرح با ضعف های جدی و مهمی روبروست که در زیر به آن ها اشاره شده است.

۳.۱. کشف گذرواژه کاربر

طرح ارائه شده توسط سبزی نژاد و ترکانویچ یک طرح احراز هویت دو فاکتوره است که از کارت هوشمند و گذرواژه استفاده می کند. زمانی که این کارت هوشمند بنا به هر دلیلی (گم شدن/دزدیده شدن) به دست مهاجم بیافتد، او می تواند به اطلاعات حساس درون کارت $SC = \{r_i, e_i, f_i, g_i\}$ دسترسی پیدا کند. در این لحظه مهاجم می تواند در فاز ورود (Login) و با در دست داشتن مقدار r_i و امتحان کردن حالت های مختلفی از گذرواژه (PW'_i) ، مقدار $MP'_i = h(r_i || PW'_i)$ را به دست می آورد. امتحان کردن حالت های مختلفی از گذرواژه می تواند از طریق حمله دیکشنری^۱ انجام پذیرد. سپس مهاجم از مقدار MP'_i به دست آمده برای محاسبه $d_i = f_i \oplus h(MP'_i || e_i)$ استفاده می کند. لازم به ذکر است، مهاجم مقادیر f_i و e_i را از SC استخراج کرده است. پس از آن چون کاربر U_i پیام $\{M_1, M_2, M_3, T_1\}$ را از طریق کانال عمومی ناامن به گره S_j ارسال می کند، مهاجم قادر است این پیام را شنود کند. از این رو مهاجم می تواند مقدار $K_i = M_2 \oplus h(d_i || T_1)$ را به دست آورد. سپس مهاجم با استفاده از K_i به دست آمده مقدار $M'_3 = h(M_1 || M_2 || K_i || T_1)$ را محاسبه کرده و سپس مقدار M'_3 محاسبه شده را با مقدار M_3 شنود شده از کانال عمومی ناامن مقایسه می کند ($M'_3 = M_3$). اگر مقادیر ذکر شده برابر بود مهاجم اطمینان حاصل می کند که عملیات حدس گذرواژه موفقیت آمیز بوده است. تا این لحظه مهاجم موفق شده است گذرواژه کاربر و بخش کلید نشست کاربر (K_i) را به دست آورد. خلاصه ای از مراحل حمله حدس گذرواژه به صورت 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 $M'_3 = M_3$ ، مهاجم اطمینان حاصل می کند که عملیات حدس گذرواژه موفقیت آمیز بوده است.

۳.۲. کشف شناسه کاربر

پس از کشف گذرواژه کاربر، مهاجم می تواند شناسه کاربر را با امتحان کردن حالت های متفاوتی از ID_i در $e_i = h(MP'_i || ID_i)$ به دست آورد. امتحان کردن حالت های مختلفی از شناسه کاربر (ID') می تواند 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 می کند. با توجه به حمله اشاره شده در این بخش، باید دقت داشت که طول شناسه به اندازه کافی بزرگ انتخاب شود تا پروتکل در برابر چنین حملاتی امن باشد (طول شناسه حداقل ۱۲۸ بیت).

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 می تواند مقدار $d_i = f_i \oplus h(MP'_i \parallel e_i)$ و در نتیجه $h(X_{GWN}) = g_i \oplus h(MP'_i \parallel d_i)$ را محاسبه کند. لازم به ذکر است او مقادیر e_i ، f_i و g_i را از کارت هوشمند استخراج می کند. حال فرد مهاجم مقادیر T_1 و M_1 را هنگامی که کاربر U_i پیام $\{M_1, M_2, M_3, T_1\}$ را از طریق کانال ناامن به S_j ارسال می کند، شنود می کند. در انتها مهاجم می تواند مقدار $ID_i = M_1 \oplus h(h(X_{GWN}) \parallel T_1)$ را محاسبه کند. بنابراین طرح ارائه شده توسط سبزی نژاد و ترکانویچ برخلاف ادعای آن ها گمنامی کاربر را رعایت نمی کند.

۳.۴. کشف کلید نشست

همان طور که در قسمت (۳.۱) ذکر شد، مهاجم با محاسبه مقدار $K_i = M_2 \oplus h(d_i \parallel T_1)$ موفق می شود به بخش کلید نشست کاربر (K_i) دسترسی پیدا کند. پس از آن، مهاجم می تواند مقدار M_6 را در فاز احراز هویت، هنگامی که گره GWN پیام تأیید را به گره S_j از طریق کانال عمومی ناامن ارسال می کند، شنود کند. در این لحظه او موفق می شود با اطلاعات به دست آمده مقدار $K'_j = M_6 \oplus h(d'_i \parallel T_3)$ 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 هنگامی که GWN پیام تأیید را برای گره حسگر ارسال می کند، 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 $M^*_2 = K_i \oplus h(d_i \parallel T_1)$ را محاسبه می کند. سپس او از مقدار M^*_2 محاسبه شده استفاده کرده و مقدار $M^*_3 = h(M_1 \parallel M^*_2 \parallel K_i \parallel T_1)$ را به دست می آورد. لازم به ذکر است مهاجم مقادیر M_1 و T_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 می کرد، شنود می کند. حال فرد مهاجم پیام $\{M_1, M^*_2, M^*_3, T_1\}$ را به گره حسگر مورد نظر ارسال می کند. گره حسگر S_j پس از دریافت پیام برچسب زمانی $(|T_1 - T_c| < \Delta t)$ را برای جلوگیری از حمله تکرار بررسی می کند. اگر برچسب زمانی مورد تأیید بود گره حسگر مقدار $ESID_j$ را محاسبه می کند. 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 می کند.

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



۴. طرح UKAS امن و کارا

در این بخش طرحی بهبودیافته بر مبنای طرح ارائه شده توسط سبزی نژاد و ترکانویچ برای احراز هویت کاربران و توافق کلید در شبکه های حسگر بی سیم نامتجانس مبتنی بر مفهوم اینترنت اشیا ارائه می شود. طرح UKAS امن ارائه شده علاوه بر حذف تمامی آسیب پذیری ها و ضعف های امنیتی ذکر شده دارای عملکرد و کارایی یکسانی با طرح ارائه شده توسط سبزی نژاد و ترکانویچ است؛ به طوری که نهایت احتیاط در بهبود امنیتی طرح در نظر گرفته شده است. همچنین طرح ارائه شده از چهار فاز اصلی: فاز قبل از راه اندازی، فاز ثبت نام، فاز ورود و فاز احراز هویت تشکیل شده است که در ادامه به تشریح آن ها پرداخته می شود.

۴.۱. فاز قبل از راه اندازی (فاز قبل از استقرار)

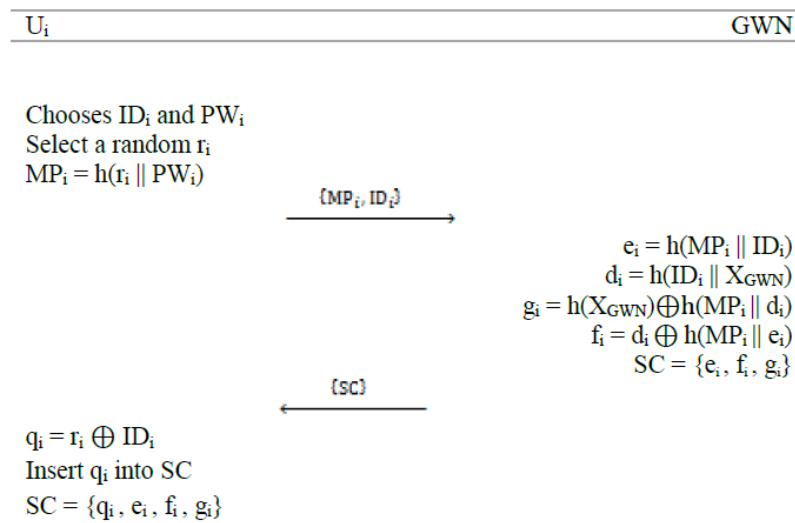
فاز قبل از راه اندازی طرح ارائه شده همانند طرح ارائه شده پیشین است که در بخش (۲.۱) توضیح داده شد. در طول این فاز، گره GWN یک کلید به اشتراک گذاشته شده $\{X_{GWN-Sj} | 1 \leq j \leq m\}$ را برای هر گره S_j تولید و ذخیره می کند. هدف از کلید به اشتراک گذاشته شده (X_{GWN-Sj}) استفاده از آن در فاز ثبت نام است. کلید به اشتراک گذاشته شده بین حسگرها و گره GWN (X_{GWN-Sj}) را می توان بعد از فاز ثبت نام حذف کرد. این کار گره GWN را قادر می سازد تعداد بیشتری گره حسگر را بدون پر شدن حافظه به شبکه اضافه کند؛ چراکه ما در این گونه شبکه ها دارای محدودیت منابع (حافظه) هستیم.

۴.۲. فاز ثبت نام

فاز ثبت نام طرح UKAS امن با تغییرات جزئی و هوشمندانه ای نسبت به طرح ارائه شده پیشین ارائه شده است. فاز ثبت نام گره حسگر در این فاز همانند طرح ارائه شده پیشین است، لذا از بیان آن در این قسمت خودداری می کنیم.

• ثبت نام 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 می کند. 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 می کند. پس از آن گره GWN مقدارهای $f_i = d_i \oplus h(MP_i || X_{GWN})$ و $g_i = h(X_{GWN} \oplus h(MP_i || d_i))$ را به دست آورده و سپس مقادیر $\{e_i, f_i, g_i\}$ را در حافظه کارت هوشمند ذخیره می کند و آن را برای کاربر U_i ارسال می کند. 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 می کند. با این حساب عملیات ثبت نام کاربر پایان می پذیرد. لازم به ذکر است محاسبه مقدار q_i به منظور عدم ذخیره آشکار مقدار r_i در کارت هوشمند است و این عمل باعث می شود در صورت دزدیده شدن یا گم شدن کارت، مهاجم نتواند به مقدار r_i دست پیدا کند. نمایش دقیقی از این فاز در شکل ۴ آمده است.



شکل ۴. فاز ثبت نام کاربر طرح ارائه شده

۳.۴. فاز ورود و احراز هویت

فاز ورود و احراز هویت طرح ارائه شده نیز مبتنی بر طرح ارائه شده توسط سبزی نژاد و ترکانویچ است که پیش از این در (۳-۱-۴) شرح داده شد. همان طور که در فاز ثبت نام اشاره شد، مقادیر ذخیره شده در کارت هوشمند شامل $SC = \{q_i, e_i, f_i, g_i\}$ است. مهم ترین تغییر قابل ملاحظه بین طرح ارائه شده 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، نمی تواند 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 نمی تواند 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 $d_i = f_i \oplus h(MP'_i || e_i)$ نمی تواند به بخش کلید نشست کاربر (K_i) در رابطه $K_i = M2 \oplus h(d_i || T1)$ و در نتیجه 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 $h(X_{GWN} // I)$	Stores its master key X_{GWN}
<p>User: Inserts SC into a terminal User: Inputs PW'_i and ID'_i $SC: r'_i = ID'_i \oplus q_i$ $SC: MP'_i = h(r'_i // PW'_i)$ $SC: e_i = ?h(MP'_i // ID'_i)$ $SC: d_i = f_i \oplus h(MP'_i // e_i)$ $SC: h(X_{GWN}) = g_i \oplus h(MP'_i // d_i)$ $SC: M_1 = ID'_i \oplus h(h(X_{GWN}) // T_1)$ $SC: \text{Chooses a random nonce } K_i$ $SC: M_2 = K_i \oplus h(d_i // T_1)$ $SC: M_3 = h(M_1 // M_2 // K_i // T_1)$ User: Chooses S_j</p>		
<p>$\xrightarrow{\{M_1, M_2, M_3, T_1\}}$</p> <p>Checks $T_1 - T_c < \Delta T$</p> <p>$ESID_j = SID_j \oplus h(h(X_{GWN} // I) // T_2)$ Chooses a random nonce K_j $M_4 = h(x_j // T_1 // T_2) \oplus K_j$ $M_5 = h(SID_j // M_4 // T_1 // T_2 // K_j)$</p> <p>$\xrightarrow{\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}}$</p> <p>Checks $T_2 - T_c < \Delta T$</p> <p>$SID'_j = ESID_j \oplus h(h(X_{GWN} // I) // T_2)$ $x'_j = h(SID'_j // X_{GWN})$ $K'_j = M_4 \oplus h(x'_j // T_1 // T_2)$ $M_5 = ?h(SID'_j // M_4 // T_1 // T_2 // K'_j)$ $ID'_i = M_1 \oplus h(h(X_{GWN}) // T_1)$ $d'_i = h(ID'_i // X_{GWN})$ $K'_i = M_2 \oplus h(d'_i // T_1)$ $M_3 = ?h(M_1 // M_2 // K'_i // T_1)$ $M_6 = K'_j \oplus h(d'_i // T_3)$ $M_7 = K'_i \oplus h(x'_j // T_3)$ $M_8 = h(M_6 // d'_i // T_3)$ $M_9 = h(M_7 // x'_j // T_3)$ $M_{11} = K_i \oplus h(d_i // T_3)$</p> <p>$\xleftarrow{\{M_6, M_7, M_8, M_9, M_{11}, T_3\}}$</p> <p>Checks $T_3 - T_c < \Delta T$</p> <p>$M_9 = ?h(M_7 // x_j // T_3)$ $K'_i = M_7 \oplus h(x_j // T_3)$ $SK = h(K'_i \oplus K_j)$ $M_{10} = h(SK // M_6 // M_8 // T_3 // T_4)$</p> <p>$\xleftarrow{\{M_6, M_8, M_{10}, T_3, T_4\}}$</p> <p>Checks $T_4 - T_c < \Delta T$</p> <p>$M_8 = ?h(M_6 // d_i // T_3)$ $K'_j = M_6 \oplus h(d_i // T_3)$ $SK = h(K_i \oplus K'_j)$ $M_{10} = ?h(SK // M_6 // M_8 // T_3 // T_4)$</p>		

شکل ۵. فاز ورود و احراز هویت طرح ارائه شده



۵. تحلیل امنیتی طرح ارائه شده

پس از ارائه طرح UAKAS توسط سبزی نژاد و ترکانویچ، علی رغم کارا و مناسب بودن این طرح برای پیاده سازی در محیط های شبکه های حسگر بی سیم مبتنی بر مفهوم اینترنت اشیاء، این طرح نتوانست نیازهای امنیتی مورد نیاز 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 ارائه شده توسط سبزی نژاد و ترکانویچ برای احراز هویت متقابل گره ها و کاربران ارائه شد که علاوه بر در نظر گرفتن محدودیت های محیط مذکور، اشکالات طرح پیشین را با در نظر گرفتن نیازمندی های امنیتی برطرف کرد. در این بخش پس از انجام مقایسه ای از ویژگی های امنیتی طرح پیشنهادی با طرح ارائه شده پیشین، امن و کارا بودن طرح پیشنهادی مورد بررسی قرار می گیرد.

۵.۱. مقایسه ویژگی های امنیتی

طرح UAKAS امن ارائه شده حفاظت از شناسه و گذرواژه کاربر، گمنامی کاربر، احراز هویت متقابل و توافق کلید را برای ما فراهم می کند. همچنین در برابر حمله سرقت کارت هوشمند، افشای پارامترهای مهم امنیتی و حمله جعل کاربر که جزء کاستی ها و نقص های جدی طرح سبزی نژاد و ترکانویچ محسوب می شود، مقاوم است. از این رو طرح UAKAS امن ارائه شده امنیت بیشتری را با حفظ همان میزان کارایی و عملکرد برای ما فراهم می کند. مقایسه ای از ویژگی های امنیتی طرح UAKAS امن ارائه شده و طرح ارائه شده توسط سبزی نژاد و ترکانویچ در جدول ۱ آمده است.

جدول ۱. مقایسه ویژگی های امنیتی طرح ارائه شده و طرح ارائه شده توسط سبزی نژاد و ترکانویچ

ویژگی های امنیتی	طرح ارائه شده توسط سبزی نژاد و ترکانویچ	طرح UAKAS امن ارائه شده
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 می تواند تمامی پارامترهای ذخیره شده در کارت $SC = \{r_i, e_i, f_i, g_i\}$ را به کمک حملات فیزیکی [۹] استخراج کند و سپس با استفاده از آن ها حمله ی کشف گذرواژه یا شناسه کاربر را پیاده سازی کند و همچنین شروعی باشد برای سایر تهدیدهای دیگر. بنابراین انتخاب و محاسبه هوشمندانه پارامترهای ذخیره شده در کارت هوشمند از نکات ضروری است که از پیاده سازی این گونه حمله ها جلوگیری به عمل می آورد.

همان طور که در طرح ارائه شده توسط سبزی نژاد و ترکانویچ مشاهده شد، پارامتر عدد تصادفی r_i باعث می شد تا مهاجم بتواند با انجام یکسری محاسبات، شناسه و گذرواژه کاربر را کشف کند. برای جلوگیری از این کار، در فاز ثبت نام 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 می کند. لازم به ذکر است محاسبه مقدار q_i به منظور عدم ذخیره آشکار مقدار r_i در کارت هوشمند است و این عمل باعث می شود در صورت دزدیده شدن یا گم شدن کارت، مهاجم نتواند به مقدار r_i دست پیدا کند.

۵.۱.۲. محافظت از گذرواژه

همان گونه که در بخش (۳.۱) توضیح داده شد مهاجم پس از دسترسی به اطلاعات کارت هوشمند می تواند با دست داشتن مقدار r_i مقدار گذرواژه را به دست می آورد. این در حالی است که در UAKAS امن ارائه شده کاربر با محاسبه مقدار $q_i = r_i \oplus ID_i$ در فاز ثبت نام و قرار دادن مقدار q_i به جای r_i در کارت هوشمند مانع از دسترسی فرد مهاجم به مقدار r_i می شود. در این صورت فرد مهاجم برای محاسبه مقدار $MP'_i = h(r'_i \parallel PW'_i)$ 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 به طور باورنکردنی افزایش می دهد.

۵.۱.۳. محافظت از شناسه

با توجه به بخش قبل (۵.۱.۲) متوجه می شویم که در صورتی که پیچیدگی کار برای محاسبه مقدار MP'_i زیاد شود (چراکه حدس گذرواژه و شناسه با توجه به حداقل طول ۶۴ بیتی هر کدام از آن ها غیرممکن است)، فرد مهاجم نمی تواند مقدار $e_i = ? h(MP'_i \parallel ID_i)$ را به سادگی محاسبه کند. به بیان ساده تر فرد مهاجم برای محاسبه $MP'_i = h((ID'_i \oplus PW'_i) \parallel PW'_i)$ باید ID'_i و PW'_i که هر کدام حداقل ۶۴ بیت طول دارد را حدس بزند. لازم به ذکر است که طول شناسه و گذرواژه در طرح سبزی نژاد ۶۴ بیت است [۸۶].

۵.۱.۴. گمنامی کاربر

به دلیل اینکه تمامی اجزای موجود در شبکه از طریق کانال ناامن با یکدیگر ارتباط برقرار می کنند، مهاجم می تواند به سادگی کانال را شنود کند. در صورتی که فرد مهاجم نتواند به مقادیر درون کارت (مانند r_i) دسترسی پیدا کرده 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 هیچ کدام از فازهای این طرح شناسه کاربر (ID_i) به صورت محافظت نشده بر روی کانال عمومی ناامن ارسال نشده است. این نشان می دهد که طرح UAKAS امن ارائه شده گمنامی کاربر را رعایت می کند.



۵.۱. ۵. محافظت از کلید نشست

به دلیل اینکه طرح ارائه شده 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 به صورت متقابل توافق می کنند و هرکدام از آن ها به صورت جداگانه مقدار $SK = h(K_i \oplus K_j)$ را در فاز احراز هویت محاسبه می کنند. 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 می کند). حال باید در نظر داشت چون اجزای موجود در شبکه از طریق کانال ناامن با یکدیگر ارتباط برقرار می کنند، مهاجم می تواند به سادگی کانال را شنود کند. از این رو باید نهایت دقت در مبادلات طرح صورت گیرد تا فرد مهاجم نتواند با شنود کانال ناامن به مقادیری دست پیدا کند که در نتیجه منجر به کشف کلید نشست شود. در طرح ارائه شده توسط سبزی نژاد و ترکانویچ مهاجم با دسترسی به اطلاعات درون کارت هوشمند و کشف گذرواژه و سپس محاسبه MP'_i و d_i می تواند به مقدار $K_i = M_2 \oplus h(d_i \parallel T_1)$ دست پیدا کند. همچنین او با شنود M_6 و T_3 از کانال مقدار $K'_j = M_6 \oplus h(d'_i \parallel T_3)$ را محاسبه می کرد و در نهایت $SK = h(K_i \oplus K'_j)$ را به دست می آورد. در طرح UAKAS امن ارائه شده، کاربر با قرار دادن q_i به جای r_i در کارت، کار را برای محاسبه مقدار d_i بسیار سخت کرد به طوری که می توان ادعا کرد این کار نشدنی است! در این صورت فرد مهاجم نمی تواند هیچ کدام از مقادیر K_i و K_j را محاسبه کند.

۵.۱. ۶. حمله جعل کاربر

همان طور که تاکنون ملاحظه شد عامل اصلی تمامی تهدیدها و حملات به وجود آمده، مربوط به پارامتر r_i ذخیره شده درون کارت هوشمند است. حمله جعل کاربر هم از این قاعده مستثنی نبوده و همان گونه که در بخش (۵.۳) به صورت کامل توضیح داده شد، فرد مهاجم با در دست 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 ذخیره شده در کارت هوشمند از نکات ضروری طراحی طرح های احراز هویت است که از پیاده سازی این گونه حمله ها جلوگیری به عمل می آورد".

۶. نتیجه گیری

در این مقاله طرحی امن و کارا برای احراز هویت متقابل و توافق کلید در شبکه های حسگر بی سیم مبتنی بر مفهوم اینترنت اشیا ارائه شده است. طرح ارائه شده مبتنی بر طرح سبزی نژاد و ترکانویچ است. از این رو تلاش شده است با در نظر گرفتن نیازمندی های امنیتی ضعف ها و آسیب پذیری های ذکر شده در مقاله برطرف گردد. در این مقاله ابتدا تعدادی از ضعف های امنیتی طرح سبزی نژاد و ترکانویچ بیان شده است و سپس طرحی بهبود یافته برای احراز هویت دوطرفه و توافق کلید ارائه شده است. طرح ارائه شده ویژگی هایی همچون محافظت از شناسه و گذرواژه، گمنامی کاربر، احراز هویت متقابل و توافق کلید را فراهم می کند و همچنین در برابر حمله هایی مانند سرقت کارت هوشمند، افشای پارامترهای مهم امنیتی و حمله جعل کاربر که از کاستی ها و نقص های طرح سبزی نژاد و ترکانویچ محسوب می شود، 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-S_j}	پسورد امن به اشتراک گذاشته شده بین GWN و حسگر S_j
X_{GWN-U_i}	پسورد امن به اشتراک گذاشته شده 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 یک طرفه
\oplus, \parallel	XOR، عملگر الحاق
MI_i, MP_i	پوشاندن (Mask) شناسه و کلمه عبور کاربر