EasyChair Preprint

№ 1837

Security Analysis of Lightweight Authentication Scheme with Key Agreement using Wireless Sensor Network for Agricultural Monitoring System

Ali Arish and Maede Ashouri-Talouki

November 5, 2019

تحلیل امنیتی طرح احراز اصالت سبک‌وزن همراه با توافق کلید با استفاده از شبکه حسگر بی‌سیم برای سیستم نظارت کشاورزی

علی اریش[۱]، مائده عاشوری تلوکی[۲]

[۱] دانشجوی کارشناسی ارشد، گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان
ali.arish20@eng.ui.ac.ir

[۲] استادیار، گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان
m.ashouri@eng.ui.ac.ir

چکیده

شبکه حسگر بی‌سیم کاربردهای زیادی در دنیای واقعی دارند و در محیط‌های مختلف توسعه پیداکرده‌اند. اما محدودیت‌های این شبکه‌ها شامل محدودیت انرژی و قدرت پردازشی حسگرها محققان را با چالش‌های زیادی مواجه کرده است. یکی از چالش‌های مهم، مساله امنیت این نوع شبکه‌ها و به‌طور خاص مساله احراز اصالت در شبکه حسگر بی‌سیم است. یک طرح احراز اصالت در شبکه حسگر بی‌سیم باید دارای ویژگی‌های امنیتی گمنامی، عدم پیوند نشست‌ها، توافق کلید جلسه، امن بودن کلید جلسه و امنیت روبه‌جلو کامل باشد و جلوی حملات مهاجم را بگیرد. یک ویژگی مهم در طرح احراز اصالت این است که با ضبط حسگر مهاجم نتواند مقادیر خصوصی طرف‌های پروتکل را به‌دست آورد. چن و همکاران یک طرح احراز اصالت همراه با توافق کلید با استفاده از شبکه حسگر بی‌سیم برای سیستم نظارت کشاورزی ارائه دادند و ادعا کردند که ویژگی‌های امنیتی را دارا است. در این مقاله اثبات می‌شود که طرح چن و همکاران در برابر حمله ضبط حسگر که منجر به بدست آوردن کلید جلسه، جعل حسگر، نقض گمنامی کاربر، نقض امنیت روبه‌جلو و رو به عقب و پیوند زدن نشست‌ها می‌شود، آسیب‌پذیر است.

کلمات کلیدی

شبکه حسگر بی سیم، کشاورزی هوشمند، احراز اصالت، توافق کلید، سیستم نظارت کشاورزی، احراز اصالت سبک‌وزن، بررسی امنیتی.

۱- مقدمه

کنترل و نظارت از راه دور باعث ایجاد شبکه حسگر بی‌سیم شده است. شبکه حسگر بی‌سیم با قرارگیری در هر محیطی باعث شد برنامه‌های متنوعی از این فناوری استفاده کنند [۱].

در سال‌های اخیر محققان زیادی در مورد چالش‌های موجود در شبکه حسگر بی‌سیم تحقیقاتی انجام داده‌اند. ازجمله چالش‌هایی که وجود دارد محدودیت انرژی و پردازش حسگر است که باعث ایجاد موضوعاتی بر روی سبک‌وزن شدن طرح‌ها شده است. چالش مهم دیگری که وجود دارد، چالش امنیتی است که خود به چندین بخش تقسیم‌شده است. دو چالش امنیتی مهم احراز اصالت و توافق کلید می‌باشند.

به دلیل اینکه شبکه حسگر بی‌سیم در محیط‌های بدون نظارت قرار دارد نیاز است که دسترسی مجاز به اطلاعات توسط موجودیت‌های معتبر انجام شود. همچنین یک نگرانی دیگر که وجود دارد این است که احراز اصالت موجودیت‌ها باید با توجه به محدودیت منابع انجام شود [۲]. در یک طرح احراز اصالت متقابل دو طرف پروتکل می‌خواهند از معتبر بودن طرف دیگر مطمئن شوند. حریم خصوصی در یک طرح احراز اصالت به این معنا است که مهاجم با شنود در یک کانال ناامن، شناسه موجودیت‌هایی که نیاز به حفظ حریم خصوصی دارند را استخراج یا نشست‌ها را به هم پیوند بزند. توافق کلید در این طرح به این معنا است که موجودیت‌ها بعد از احراز اصالت متقابل به یک کلید جلسه برسند تا در ارتباطات از طریق آن کلید اطلاعات را رمزگذاری و رمزگشایی کنند. در این مقاله روش چن و همکاران [۳] بیان می‌شود و این طرح تحلیل امنیتی می‌شود. در ادامه ضعف‌های طرح چن و همکاران بیان می‌شود [۳]، اثبات می‌شود که این طرح در برابر حمله ضبط حسگر آسیب‌پذیر است و مهاجم به کلید جلسه می‌رسد. همچنین گمنامی کاربر را از بین می‌رود و مهاجم نشست‌ها را به هم پیوند می‌زند.

بخش‌های مختلف این مقاله به این صورت است: در بخش ۲ پیشینه تحقیق مرور می‌شود. بخش ۳ روش چن و همکاران [۳] بیان‌شده و در بخش ۴ تحلیل امنیتی روش چن و همکاران [۳] می‌شود.، درنهایت در بخش ۵ جمع‌بندی مقاله ارائه می‌شود.

۲- پیشینه تحقیق

در سال‌های اخیر طرح‌های احراز اصالت امن مختلفی در شبکه حسگر بی‌سیم ارائه‌شده‌اند [۴-۹] که می‌توان برای کشاورزی هوشمند نیز استفاده کرد.

در سال ۲۰۰۶ وانگ و همکاران [۱۰] یک طرح احراز اصالت برای شبکه حسگر بی‌سیم ارائه دادند که شامل سه موجودیت کاربر، حسگر و گره درگاه بود. این طرح شامل سه فاز ثبت‌نام، ورود و احراز اصالت بود. این طرح شامل ضعف‌های: جعل حسگر، حدس کلمه عبور، عدم احراز اصالت متقابل، نقض گمنامی کاربر و عدم توافق کلید است. در سال ۲۰۱۰ خان و همکاران [۱۱] یک طرح احراز اصالت در شبکه حسگر بی‌سیم با استفاده از کارت هوشمند ارائه دادند. در این طرح علاوه بر فازهای ثبت‌نام، ورود و احراز اصالت، فاز تغییر کلمه عبور اضافه‌شده است. ضعف‌های طرح خان و همکاران [۱۱] شامل: حمله داخلی، حمله منع سرویس و عدم احراز اصالت متقابل است. در سال ۲۰۱۲ یو و همکاران [۱۲] یک طرح احراز اصالت در شبکه حسگر بی‌سیم شامل چهار فاز ثبت‌نام، ورود و احراز اصالت با توافق کلید و تغییر کلمه عبور ارائه دادند. در این طرح شناسه کاربر به‌صورت فاش ارسال می‌شود و گمنامی کاربر وجود ندارد. در سال ۲۰۱۵ هی و همکاران [۱۳] در شبکه حسگر بی‌سیم یک طرح احراز اصالت با سه فاز ثبت‌نام، ورود و احراز اصالت ارائه دادند. مهاجم در این طرح می‌تواند کاربر را جعل کند. همچنین این طرح دارای ضعف پیوند زدن نشست‌ها است. در سال ۲۰۱۸ وو و همکاران [۱۴] یک طرح احراز اصالت در شبکه حسگر بی‌سیم با چهار فاز ثبت‌نام، ورود، احراز اصالت و تغییر کلمه عبور ارائه دادند. این طرح شامل ضعف‌های: حمله دزدیدن کارت هوشمند، جعل کاربر و نقض گمنامی کاربر است.

در سال ۲۰۱۸ علی و همکاران [۱۵] یک طرح احراز اصالت و توافق کلید برای سیستم‌های نظارت بر کشاورزی هوشمند ارائه دادند که شامل ۴ موجودیت: کاربر، ایستگاه پایه[1] ، گره درگاه[2] و حسگر است. این طرح دارای ضعف‌های حمله داخلی، حمله جعل حسگر، نقض گمنامی کاربر و نقض امنیت روبه‌جلو کامل است.

۳- روش چن و همکاران

چن و همکاران [۳] در سال ۲۰۱۹ یک طرح احراز اصالت و توافق کلید سبک‌وزن با حفظ حریم خصوصی مبتنی بر شبکه حسگر بی‌سیم برای سیستم‌های نظارت کشاورزی ارائه داده‌اند. این طرح شامل شش فاز برپایی سیستم، ثبت‌نام کاربر و متخصص کشاورزی، ورود، احراز اصالت و توافق کلید جلسه، تغییر یا به‌روزرسانی کلمه عبور و اضافه کردن پویای گره است. در فاز برپایی سیستم، برای موجودیت‌ها کلید مشترک با ایستگاه پایه (BS) ساخته می‌شود و شناسه حسگر توسط مدیر سیستم انتخاب می‌شود. در فاز ثبت‌نام، موجودیت کاربر یا متخصص کشاورزی یک شناسه و کلمه عبور انتخاب و خصوصیت بیومتریک خود را ثبت می‌کند. توسط BS ثبت‌نام می‌شود و مقادیر را کاربر در کارت هوشمند ذخیره می‌کند. در فاز تغییر کلمه عبور کاربر با استفاده از شناسه و کلمه عبور فعلی، کلمه عبور جدید انتخاب می‌کند. در فاز اضافه کردن پویای گره حسگر، مدیر سیستم برای حسگر کلید مشترک و شناسه را انتخاب می‌کند و در حافظه حسگر قرار می‌دهد. در ادامه فاز ورود و احراز اصالت همراه با توافق کلید به‌صورت مشروح بیان خواهد شد. در جدول ۱ نمادهای مورداستفاده در طرح احراز اصالت آورده شده است.

جدول (۱): نمادها [۳]

نماد	توضیح
U_i	کاربر یا متخصص کشاورزی
BS	ایستگاه پایه
GWN_j	گره درگاه
SN_j	گره حسگر
ID_i, ID_{GWNj}, ID_{SNj}	شناسه U_i، GWN_j و SN_j
PW_i	کلمه عبور U_i
F_i	بیومتریک U_i
A_i	کلید مشترک بین BS و U_i
X	کلید خصوصی BS
$X_{BS-GWNj}$	کلید مشترک بین BS و GWN_j
RI_j	کلید مشترک بین BS و SN_j
R_U,R_{BS},R_{GWNj},R_{SNj}	مقدار تصادفی U_i، BS،GWN_j و SN_j
SK	کلید جلسه
T_i	تمبر زمان iام
REP(.)	تابع بازگشت استخراج‌کننده فازی
h(.)	تابع درهم‌ساز
||	عمل جمع کننده
$\oplus$	جمع با پیمانه دو

۳-۱- فاز ورود، احراز اصالت و توافق کلید

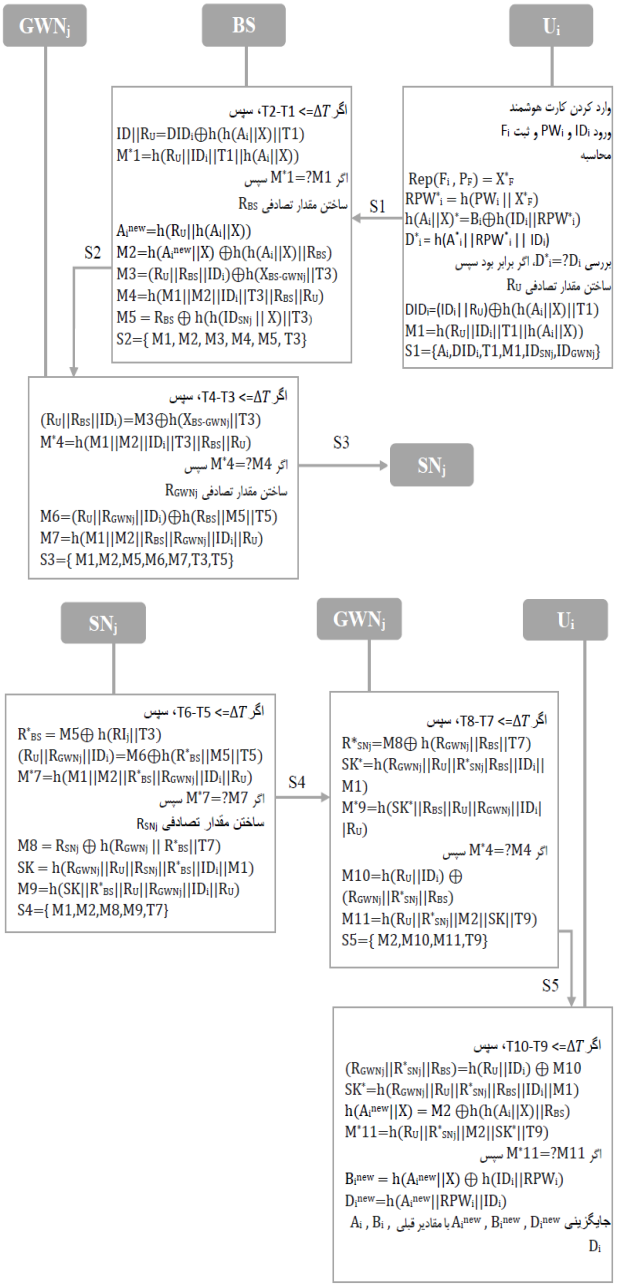
مراحل فاز ورود، احراز اصالت و توافق کلید همان‌طور که در شکل ۱ نشان داده‌شده است، به‌صورت زیر است:

- مرحله ۱: U_i کارت هوشمند خود را وارد کارت‌خوان کرده و سپس شناسه، کلمه عبور و خصوصیت بیومتریک را وارد می‌کند. حال کارت‌خوان مقادیر زیر را محاسبه می‌کند:

$$D^*_i \text{ و } h(A_i \,||\, X)^* \text{ ، } RPW^*_i \text{ ، } Rep(F_i, P_F) = X^*_F$$

سپس بررسی که آیا D^*_i با D_i داخل کارت هوشمند برابر است یا خیر. اگر برابر بود ادامه می‌دهد و در غیر این جلسه به پایان می‌رسد.

- مرحله ۲: U_i یک مقدار تصادفی R_U را تولید و مقادیر DIDi و M1 را محاسبه و مقادیر A_i, DID_i, T1, M1, ID_{SNj}, ID_{GWNj} را برای BS از طریق کانال عمومی می‌فرستد.
- مرحله ۳: BS بعد از دریافت مقادیر A_i, DID_i, T1, M1, ID_{SNj}, ID_{GWNj} از طرف U_i، ابتدا چک می‌کند که زمان فعلی از زمانی که U_i فرستاده در حد مجاز است یا خیر. اگر مجاز نبود جلسه به پایان می‌رسد. در غیر این صورت BS مقدار R_U ||ID و سپسM^*1 را محاسبه و M^*1 را با M1 دریافتی مقایسه می‌کند. اگر برابر نبود جلسه به پایان می‌رسد. در غیر این صورت U_i توسط BS احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.
- مرحله ۴: BS یک مقدار تصادفی R_{BS} تولید و A_i^{new} را محاسبه می‌کند. سپس مقادیر M2،M3،M4 و M5 را محاسبه و مقادیر M1, M2, M3, M4, M5, T3 را برای GWN_j از طریق کانال عمومی می‌فرستد.
- مرحله ۵: GWN_j پس از دریافت پیام از BS، T3 را بررسی می‌کند. پس از بررسی، مقادیر ($ID_i \,||\, R_{BS} \,||\, R_U$ و M^*4 را محاسبه و M^*4 را با M4 دریافتی مقایسه می‌کند. اگر برابر نبودند نشست به اتمام می‌رسد. در غیر این صورت BS توسط GWN_j احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.
- مرحله ۶: حال GWN_j یک مقدار تصادفی R_{GWNj} را تولید می‌کند. سپس مقادیر M6 و M7 را محاسبه و مقادیر M1,M2,M5,M6,M7,T3 T5 را برای حسگر SN_j می‌فرستد.
- مرحله ۷: SN_j پس از دریافت پیام از GWN_j ابتدا. T5 را بررسی می‌کند، سپس مقادیر R^*_{BS} ,$(R_U \,||\, R_{GWNj} \,||\, ID_i)$ و M^*7 را محاسبه می‌کند. آنگاه M^*7 را با M7 دریافتی محاسبه می‌کند. اگر برابر نبود نشست به اتمام می‌رسد. در غیر این صورت GWN_j توسط SN_j احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.
- مرحله ۸: SN_j یک مقدار تصادفی R_{SNj} را تولید و سپس SN_j مقادیر SK،M8 و M9 را محاسبه می‌کند. آنگاه مقادیر M1,M2,M8,M9,T7 را برای GWN_j می‌فرستد.
- مرحله ۹: GWN_j پس از دریافت پیام از طرف SN_j بررسی می‌کند که T8-T7 (T8 زمان فعلی است) در بازه مجاز باشد. اگر مجاز نبود نشست به اتمام می‌رسد. در غیر این صورت GWN_j مقادیر R^*_{SNj}،SK^* و M9 را محاسبه می‌کند. سپس M^*9 را با M9 دریافتی مقایسه می‌کند. اگر برابر نبود نشست به اتمام می‌رسد. در غیر این صورت SN_j توسط GWN_j احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.
- مرحله ۱۰: حال GWN_j مقادیر M10 و M11 را محاسبه کرده و سپس مقادیر M2,M10,M11,T9 را برای U_i ارسال می‌کند.
- مرحله ۱۱: U_i پس از دریافت پیام از GWN_j ابتدا بررسی می‌کند که T9 در محدوده مجاز باشد. اگر مجاز نبود نشست به اتمام می‌رسد. در غیر این صورت U_i مقدار $(R_{GWNj}||R^*_{SNj}||R_{BS})$، SK^* و $h(A_i^{new}||X)$ و M^*11 را محاسبه می‌کند. حال M^*11 را با M11 دریافتی مقایسه می‌کند. اگر برابر نبودند نشست به اتمام می‌رسد. در غیر این صورت GWN_j توسط U_i احراز اصالت می‌شود و احراز اصالت متقابل تکمیل می‌شود. آنگاه توافق کلید بین موجودیت‌ها انجام و کلید نشست $SK = h(R_{GWNj}||R_U||R_{SNj}||R_{BS}||ID_i||M1)$ است.
- مرحله ۱۲: U_i مقادیر جدید B_i^{new} و D_i^{new} را محاسبه می‌کند. سپس سه مقدار A_i^{new}, B_i^{new}, D_i^{new} را جایگزین A_i, B_i, D_i می‌کند.



شکل 1–ورود، احراز اصالت و توافق کلید در روش چن و همکاران

۴- تجزیه‌وتحلیل روش چن و همکاران

در این بخش نشان داده می‌شود که طرح چن و همکاران چگونه ناامن است. فرض آن است که مهاجم می‌تواند یک حسگر را ضبط کند و اطلاعات حسگر را استخراج کند. این اطلاعات شامل شناسه حسگر ID_{SNj} و کلید مشترک بین حسگر و ایستگاه پایه RI_j است. مهاجم با داشتن این مقادیر می‌تواند مقادیر خصوصی را استخراج کند. در ادامه چگونگی حملات نشان داده خواهد شد.

۴-۱- به دست آوردن کلید جلسه

در این نوع حمله، هدف مهاجم این است که با شنود پیام‌های نشست به کلید جلسه برسد. مهاجم با حمله دزدیدن یا ضبط حسگر، به مقادیر حسگر (کلید مشترک بین حسگر و ایستگاه پایه:RI_j) دسترسی یافته و سپس با شنود پیام‌های نشست به کلید جلسه نشست فعلی یا نشست‌های قبلی خواهد رسید. مراحل حمله به‌قرار زیر است:

- مرحله اول: مهاجم با شنود پیام GWN_j به SN_j که شامل $M5$ و $T3$ است و $M5 = R_{BS} \oplus h(RI_j \| T3)$ می‌تواند به R_{BS} برسد به این صورت: $R_{BS} = M5 \oplus h(RI_j \| T3)$ که R_{BS} مقدار تصادفی ایستگاه است.
- مرحله دوم: مهاجم با داشتن $M6,T5,R_{BS}$ و $M5$ (درحالی‌که $M6 = (R_U \| R_{GWNj} \| ID_i) \oplus h(R_{BS} \| M5 \| T5)$ است) و با استفاده از رابطه زیر مقادیر R_U,R_{GWNj},ID_i را به دست می‌آورد:
$(R_U \| R_{GWNj} \| ID_i)=M6 \oplus h(R_{BS}\|M5\|T5)$
که R_U مقدار تصادفی کاربر، ID_i شناسه کاربر و R_{GWNj} مقدار تصادفی گره دروازه است.
- مرحله سوم: مهاجم با شنود پیام $M8$ و $T7$ (درحالی‌که $M8=R_{SNj}\oplus h(R_{BS}\|M5\|T7)$ است) و با داشتن مقادیر مراحل قبل به R_{SNj} می‌رسد:
$R_{SNj}=M8\oplus h(R_{BS}\|M5\|T7)$ که R_{SNj} مقدار تصادفی حسگر است.
- مرحله چهارم: حال مهاجم با داشتن مقادیر مراحل قبل می‌تواند کلید جلسه را محاسبه کند:
$SK=h(R_{GWNj}\|R_U\|R_{SNj}\|R_{BS}\|ID_i\|M1)$

۴-۲- نقض امنیت روبه‌جلو و روبه‌عقب

در این نوع حمله، مهاجم با داشتن مقادیر خصوصی می‌خواهد کلید جلسه تمام نشست‌های قبلی که شنود کرده‌است را به دست بیاورد. همچنین می‌خواهد با داشتن این مقادیر خصوصی، کلید جلسه نشست‌های بعد که قرار است انجام شود را نیز به دست آورد.

مهاجم با شنود نشست‌های قبلی و با داشتن کلید مشترک بین BS و SN_j (RI_j) می‌تواند به کلید جلسات برسد. همچنین اگر مهاجم فقط اطلاعات را از حسگر استخراج کند و آن را در جای خود قرار دهد، می‌تواند کلید جلسات بعد را نیز تولید کند و پیام‌های بین کاربر و حسگر را رمزگشایی کند؛ زیرا پیام‌های ارتباطات بین موجودیت‌ها از طریق کلیدی که به توافق رسیده‌اند رمز می‌شود. پس اگر مهاجم به این کلید برسد می‌تواند اطلاعات را با کلید نشست رمزگشایی کند: $DEC_{SK}(C)=M$

۴-۳- نقض گمنامی کاربر

هدف مهاجم در این نوع حمله این است که به شناسه یا مقدار یکتایی از یک کاربر برسد تا گمنامی کاربر را از بین ببرد.

مهاجم با داشتن کلید مشترک بین BS و SN_j و شنود پیام $M5$ و $M6$ با استفاده از مراحل زیر به شناسه کاربر می‌رسد.

- مرحله اول: مهاجم پیام بین GWN_j و SN_j را شنود می‌کند، که شامل $M5$ و $T3$ است ($M5 = R_{BS} \oplus h(RI_j \| T3)$). حال با استفاده از رابطه $R_{BS} = M5 \oplus h(RI_j \| T3)$ مقدار R_{BS} را محاسبه می‌کند، که R_{BS} مقدار تصادفی ایستگاه است.

- مرحله دوم: مهاجم با داشتن مقادیر $M6,T5,R_{BS}$ و $M5$ (درصورتی‌که $M6 = (R_U \,||\, R_{GWNj} \,||\, ID_i) \oplus h(R_{BS} \,||\, M5 \,||T5)$ است) مقادیر R_U,R_{GWNj},ID_i را به دست می‌آورد:

$$(R_U \,||\, R_{GWNj} \,||\, ID_i)=M6 \oplus h(R_{BS}||M5||T5)$$

با یافتن ID_i گمنامی کاربر از بین می‌رود.

۴-۴- پیوند زدن نشست‌ها

هدف مهاجم در این حمله این است که با شنود پیام‌های چندین نشست بتواند آن‌ها را به هم پیوند بزند و ثابت کند که این نشست‌ها مربوط به یک موجودیت است و این باعث می‌شود که حریم خصوصی کاربر نقض شود.

با شنود پیام‌های $M5$ و $M6$ می‌تواند به شناسه کاربر برسد و با این کار می‌تواند نشست‌های مرتبط را به هم پیوند بزند.

۴-۵- جعل حسگر

مهاجم می‌تواند به‌جای حسگر قرار گیرد و با دریافت پیام از GWN_j و استخراج مقادیر خصوصی، مقادیر $M8, M9$ و $T7$ را تولید کند، سپس خود را جای حسگر جا بزند و برای GWN_j پیام معتبر بفرستد.

۵- نتیجه‌گیری

در این مقاله یک طرح احراز اصالت امن در شبکه حسگر بی‌سیم مورد ارزیابی امنیتی قرار گرفت و نشان داده شد که این طرح در برابر حمله ضبط حسگر و لو رفتن مقدار تصادفی BS ناامن است و می‌تواند باعث ایجاد ضعف‌هایی ازجمله: فاش شدن کلید جلسه، نقض امنیت روبه‌جلو و رو به عقب، نقض گمنامی کاربر، پیوند زدن نشست‌ها و حمله جعل حسگر شود.

مراجع

[1] Chong, C.-Y. and S.P. Kumar, *Sensor networks: evolution, opportunities, and challenges.* Proceedings of the IEEE, 2003. **91**(8): p. 1247-1256.

[2] Lin, H.-Y., *High effect secure data transmission mechanisms in wireless sensor networks using ID-based key management scheme.* Journal of convergence information technology, 2009. **4**(1): p. 77-83.

[3] Chen, M., T.-F. Lee, and J.-I. Pan, *An Enhanced Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring.* Sensors, 2019. **19**(5): p. 1146.

[4] Wu, F., et al., *An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment.* Journal of Network and Computer Applications, 2017. **89**: p. 72-85.

[5] Gope, P., et al., *Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks.* IEEE transactions on industrial informatics, 2019.

[6] Jan, M., et al., *PAWN: a payload-based mutual authentication scheme for wireless sensor networks.* Concurrency and Computation: Practice and Experience, 2017. **29**(17): p. e3986.

[7] Naser, S.M. and M.S. Croock, *Proposed Simulator Based on Developed Lightweight Authentication and Key Management Protocol for Wireless Sensor Network.* International Journal of Computing and Digital Systems, 2018. **7**(04): p. 251-260.

[8] Riaz, R., et al., *SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics.* Wireless Communications and Mobile Computing, 2019. **2019**.

[9] Amin, R., et al., *An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks.* Journal of Network and Computer Applications, 2018. **104**: p. 133-144.

[10] Wong, K.H., et al. *A dynamic user authentication scheme for wireless sensor networks*. in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*. 2006. IEEE.

[11] Khan, M.K. and K. Alghathbar, *Cryptanalysis and security improvements of' two-factor user authentication in wireless sensor networks'.* Sensors, 2010. **10**(3): p. 2450-2459.

[12] Yoo, S.G., K.Y. Park, and J. Kim, *A security-performance-balanced user authentication scheme for wireless sensor networks.* International journal of distributed sensor networks, 2012. **8**(3): p. 382810.

[13] He, D., N. Kumar, and N. Chilamkurti, *A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks.* Information Sciences, 2015. **321**: p.۲۷۷-۲۶۳ .

[14] Wu, F., et al., *An improved and provably secure three-factor user authentication scheme for wireless sensor networks.* Peer-to-Peer Networking and Applications, 2018. **11**(1): p. 1-20.

[15] Ali, R., et al., *A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring.* Future Generation Computer Systems, 2018. **84**: p. 200-215.

پانویس‌ها

[1] Base Station

[2] Gateway Node