دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۰، جلد ۱۹، شماره ۲ (۱-۱۱)
https://monadi.isc.org.ir

ارائه‌شده در هفدهمین کنفرانس بین المللی انجمن رمز ایران در دانشگاه علم و صنعت ایران، ۱۹ و ۲۰ شهریور ۱۳۹۹

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

علی اریش* و مائده عاشوری تلوکی

گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان

اطلاعات مقاله

کلمات کلیدی:
شبکه حسگر بی‌سیم
کشاورزی هوشمند
احراز اصالت
توافق کلید
سامانه نظارت کشاورزی
احراز اصالت سبک‌وزن
بررسی امنیتی

dor: 10.0000/000000000

نوع مقاله: پژوهشی

چکیده

شبکه حسگر بی‌سیم، کاربردهای زیادی دارد و در محیط‌های مختلف توسعه پیدا کرده‌اند. اما محدودیت‌های این شبکه‌ها شامل محدودیت انرژی و قدرت پردازشی حسگرها، محققان را با چالش‌های زیادی مواجه کرده است. یکی از چالش‌ها، مساله امنیت این نوع شبکه‌ها و به طور 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 نشست، امن بودن کلید نشست و امنیت رو به جلو کامل باشد و جلوی حمله‌های مهاجم را بگیرد. یک ویژگی مهم در طرح احراز اصالت این است که با ضبط حسگر مهاجم نتواند مقادیر خصوصی طرف‌های پروتکل را به دست آورد. چن و همکاران یک طرح احراز اصالت همراه با توافق کلید با استفاده از شبکه حسگر بی‌سیم برای سامانه 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 دست آوردن کلید نشست، جعل حسگر، نقض گمنامی کاربر و حسگر، نقض امنیت رو به جلو و رو به عقب و پیوند زدن نشست‌ها می‌شود، آسیب‌پذیر است. در ادامه مقاله، راهکار پیشنهادی جهت بهبود طرح چن و همکاران ارائه و طرح بهبودیافته مورد ارزیابی قرار خواهد گرفت.

© ۱۴۰۰ انجمن رمز ایران

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 تقسیم شده 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

★از کمیته علمی هفدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: ali.arish20@eng.ui.ac.ir (علی اریش)، m.ashouri@eng.ui.ac.ir (مائده عاشوری تلوکی)
© ۱۴۰۰ تمامی حقوق متعلق به انجمن رمز ایران است.

اصالت، به این معنا است که مهاجم با شنود در یک کانال ناامن، نتواند 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 نشست 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 [۳] بیان می‌شود، اثبات می‌شود که این طرح در برابر حمله ضبط حسگر آسیب‌پذیر است و مهاجم به کلید نشست می‌رسد. همچنین گمنامی کاربر و حسگر نقض خواهد شد و مهاجم نشست‌ها را به هم پیوند می‌زند. در آخر یک راهکار برای حل ضعف‌های طرح چن و همکاران [۳] ارائه و تحلیل می‌شود.

بخش‌های مختلف این مقاله به این صورت است: در بخش ۲ پیشینه تحقیق مرور می‌شود. بخش ۳ روش چن و همکاران [۳] بیان شده و در بخش ۴ تحلیل امنیتی روش چن و همکاران [۳] می‌شود. در بخش ۵ راهکار پیشنهادی ارائه می‌شود. در بخش ۶ تحلیل راهکار پیشنهادی انجام می‌شود. در بخش ۷ مقایسه امنیتی و کارایی انجام می‌شود. در بخش ۸ نقاط قوت و ضعف طرح پیشنهادی بیان می‌شود. درنهایت در بخش ۹ جمع‌بندی مقاله ارائه می‌شود.

۲ پیشینه تحقیق

در سال‌های اخیر طرح‌های احراز اصالت 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 مرحله ثبت‌نام، ورود و احراز اصالت بود. این طرح شامل ضعف‌هایی مانند: 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 مرحله‌های ثبت‌نام، ورود و احراز اصالت، مرحله 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 مرحله ثبت‌نام، ورود و احراز اصالت با توافق کلید و تغییر کلمه عبور ارائه دادند. در این طرح شناسه کاربر به صورت 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 مرحله 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 مرحله ثبت‌نام، ورود، احراز اصالت و تغییر کلمه عبور ارائه دادند. این طرح شامل ضعف‌هایی مانند حمله ضبط کارت هوشمند، جعل کاربر و نقض گمنامی کاربر است.

در سال ۲۰۱۸ علی و همکاران [۱۵] یک طرح احراز اصالت و توافق کلید برای سامانه‌های نظارت کشاورزی هوشمند ارائه دادند که شامل چهار 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 رو به جلو کامل است.

۱.۲ پیشینه حمله ضبط حسگر

در این حمله هدف مهاجم این است که با ضبط حسگر به مقادیر خصوصی سایر موجودیت‌ها یا کلید جلسه دست یابد. همچنین این حمله می‌تواند پیش‌زمینه حمله‌های دیگر مانند به دست آوردن کلید جلسه، نقض امنیت رو به جلو و رو به عقب و نقض گمنامی کاربر و حسگر باشد. یک راهکار برای جلوگیری از این حمله استفاده از رمزنگاری خم بیضوی است، ولی این راهکار برای حسگر بسیار سنگین و انرژی زیادی مصرف خواهد کرد که باعث کاهش طول عمر حسگر می‌شود [۱۶].

در سال ۲۰۱۲ داس و همکاران [۱۷] ادعا کردند که طرح‌های وونگ و همکاران [۱۰]، نیانگ و همکاران [۱۸]، هی و همکاران [۱۹]، فن و همکاران [۲۰]، چن و همکاران [۲۱] در برابر حمله ضبط حسگر، مقاوم نیستند. در سال ۲۰۱۵ چانگ و همکاران [۱۶] ادعا کردند که طرح ترکانویچ و همکاران [۲۲] در برابر حمله ضبط حسگر، مقاوم نیست. همچنین در طرحی دیگر در سال ۲۰۱۶ وو و همکاران [۲۳] ادعا کردند که طرح‌های وایدیا و همکاران [۲۴]، خان و همکاران [۱۱] نیز در برابر حمله ضبط حسگر، مقاوم نیستند. در سال ۲۰۱۷ وو و همکاران [۲۵] ادعا کردند که طرح لی و همکاران [۲۶] در برابر حمله ضبط حسگر، مقاوم نیست. در سال ۲۰۱۹ گوپتا و همکاران [۲۷] ادعا کردند که طرح‌های چانگ و همکاران [۱۶]، وو و همکاران [۲۸]، داس و همکاران [۲۹] در برابر حمله ضبط حسگر، مقاوم نیستند.

۳ طرح چن و همکاران

چن و همکاران [۳] در سال ۲۰۱۹ یک طرح احراز اصالت و توافق کلید سبک‌وزن با حفظ حریم‌خصوصی مبتنی بر شبکه حسگر بی‌سیم برای سامانه‌های نظارت کشاورزی ارائه داده‌اند. این طرح شامل شش مرحله برپایی سامانه، ثبت‌نام کاربر و متخصص کشاورزی، ورود، احراز اصالت و توافق کلید نشست، تغییر یا به‌روزرسانی کلمه عبور و اضافه کردن پویای گره است.

در مرحله برپایی سامانه، برای موجودیت‌ها کلید مشترک با BS ساخته می‌شود و شناسه حسگر توسط مدیر سامانه انتخاب می‌شود. در مرحله

[1] base station [2] gateway node

جدول ۱. نمادها [۳]

نماد	توضیح
U_i	کاربر یا متخصص کشاورزی
BS	ایستگاه پایه
GWN_j	گره درگاه
SN_j	گره حسگر
$ID_i, IDGWN_j, IDSN_j$	شناسه U_i، GWN_j و SN_j
PW_i	کلمه عبور U_i
F_i	زیست‌سنجشی U_i
A_i	کلید مشترک بین BS و U_i
X	کلید خصوصی BS
$XBS-GWN_j$	کلید مشترک بین BS و GWN_j
RI_j	کلید مشترک بین BS و SN_j
$RU, RBS, RGWN_j, RSN_j$	مقدار تصادفی U_i، BS، GWN_j و SN_j
SK	کلید نشست
T_i	تمبر زمان iام
$REP(\cdot)$	تابع بازگشت استخراج‌کننده
$h(\cdot)$	تابع چکیده‌ساز
$\|$	عمل جمع کننده
$\oplus$	جمع با پیمانه دو

ثبت‌نام، موجودیت کاربر یا متخصص کشاورزی یک شناسه و کلمه عبور انتخاب و خصوصیت زیست‌سنجشی خود را ثبت می‌کند، توسط BS ثبت‌نام می‌شود و مقادیر را کاربر در کارت هوشمند ذخیره می‌کند. در مرحله تغییر کلمه عبور کاربر با استفاده از شناسه و کلمه عبور فعلی، کلمه عبور جدید انتخاب می‌کند. در مرحله اضافه کردن پویای گره حسگر، مدیر سامانه برای حسگر کلید مشترک و شناسه را انتخاب می‌کند و در حافظه حسگر قرار می‌دهد.

در ادامه، مرحله ورود و احراز اصالت همراه با توافق کلید به صورت مشروح بیان خواهد شد. در جدول ۱ نمادهای مورد استفاده در طرح احراز اصالت آورده شده است.

۱.۳ مرحله ورود، احراز اصالت و توافق کلید

مراحل مرحله ورود، احراز اصالت و توافق کلید همان‌طور که در شکل ۱ نشان داده شده است، به صورت زیر است:

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

$$Rep(F_i, P_F) = X_F^*,\ RPW_i^*,\ h(A_i\|X)^*,\ \text{و}\ D_i^*$$

سپس بررسی می‌کند که آیا D_i^* با D_i داخل کارت هوشمند برابر است یا خیر. اگر برابر بود ادامه می‌دهد و در غیر این صورت، نشست به پایان می‌رسد.

مرحله ۲: U_i یک مقدار تصادفی RU را تولید و مقادیر DID_i و M_1 را محاسبه و مقادیر A_i، DID_i، T_1، M_1، $IDSN_j$، $IDGWN_j$ را برای BS از طریق کانال عمومی می‌فرستد.

مرحله ۳: BS بعد از دریافت مقادیر A_i، DID_i، T_1، M_1، $IDSN_j$، $IDGWN_j$ از طرف U_i، ابتدا بررسی می‌کند که زمان فعلی از زمانی که U_i فرستاده در حد مجاز است یا خیر. اگر مجاز نبود نشست به پایان می‌رسد. در غیر این صورت BS مقدار $ID\|RU$ و سپس M_1^* را محاسبه و M_1^* را با M_1 دریافتی مقایسه می‌کند. اگر برابر نبود نشست 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 RBS تولید و A_i^{new} را محاسبه می‌کند. سپس مقادیر M_2، M_3، M_4 و M_5 را محاسبه می‌کند و مقادیر M_1، M_2، M_3، M_4، M_5، T_3 را برای GWN_j از طریق کانال عمومی می‌فرستد.

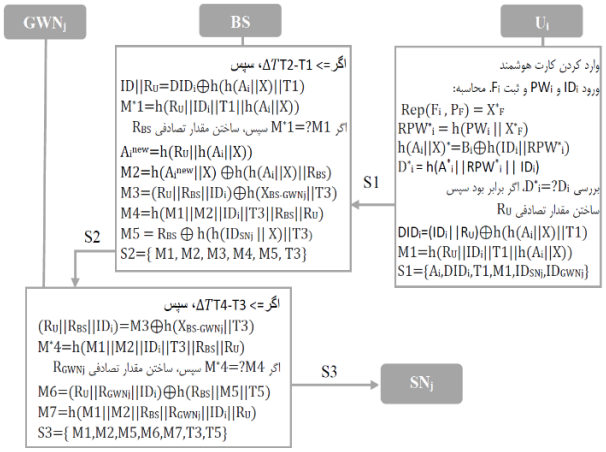
مرحله ۵: GWN_j پس از دریافت پیام از BS، T_3 را بررسی می‌کند. پس از بررسی، مقدار M_4^* را محاسبه و M_4^* را با M_4 دریافتی مقایسه می‌کند. اگر برابر نبودند، نشست به اتمام می‌رسد. در غیر این صورت، BS توسط GWN_j احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.

مرحله ۶: حال GWN_j یک مقدار تصادفی $RGWN_j$ را تولید می‌کند. سپس مقادیر M_6 و M_7 را محاسبه می‌کند و مقادیر M_1، M_2، M_5، M_6، M_7، T_3 و T_5 را برای حسگر SN_j می‌فرستد.

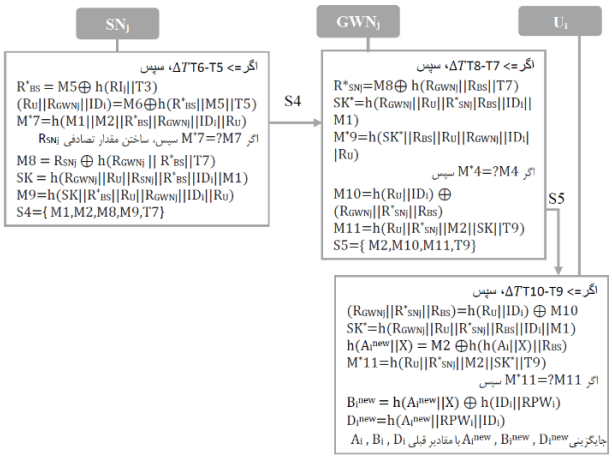
مرحله ۷: SN_j پس از دریافت پیام از GWN_j ابتدا $T5$ را بررسی می‌کند، سپس مقادیر $(R_U\|RGWN_j\|ID_i)R_{BS}^*$ و M_7^* را محاسبه می‌کند. آنگاه M_7^* را با M_7 دریافتی محاسبه می‌کند. اگر برابر نبود، نشست به اتمام می‌رسد. در غیر این صورت، GWN_j توسط SN_j احراز اصالت می‌شود و نشست ادامه پیدا می‌کند.

مرحله ۸: SN_j یک مقدار تصادفی RSN_j را تولید می‌کند و سپس SN_j مقادیر M_8، SK و M_9 را محاسبه می‌کند. آنگاه مقادیر M_1، M_2، M_8، M_9، T_7 را برای GWN_j می‌فرستد.

مرحله ۹: GWN_j پس از دریافت پیام از طرف SN_j بررسی می‌کند که $T_8 - T_7$ (T_8 زمان فعلی است) در بازه مجاز باشد. اگر مجاز نبود نشست به اتمام می‌رسد. در غیر این صورت GWN_j مقادیر $R_{SN_j}^*$، SK^* و M_9 را محاسبه می‌کند. سپس M_9^* را با M_9 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.



شکل ۱. بخش اول: ورود، احراز اصالت و توافق کلید در روش چن و همکاران [۳]



شکل ۲. بخش دوم: ورود، احراز اصالت و توافق کلید در روش چن و همکاران [۳]

مرحله ۱۰: حال GWN_j مقادیر M_{10} و M_{11} را محاسبه کرده و سپس مقادیر M_2، M_{10}، M_{11}، T_9 را برای U_i ارسال می‌کند.

مرحله ۱۱: U_i پس از دریافت پیام از GWN_j ابتدا بررسی می‌کند که T_9 در محدوده مجاز باشد. اگر مجاز نبود نشست به اتمام می‌رسد. در غیر این صورت U_i مقدار $(RGWN_j \| R^*_{SN_j} \| RBS)$، SK^* و $h(A_i^{new} \| X)$ و M^*_{11} را محاسبه می‌کند. حال M^*_{11} را با M_{11} 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

$$SK = h(RGWN_j \| RU \| RSN_j \| RBS \| ID_i \| M_1)$$

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.

۴ تجزیه و تحلیل روش چن و همکاران

در این بخش نشان داده می‌شود که طرح چن و همکاران [۳] 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 $IDSN_j$ و کلید مشترک بین حسگر و $BS(RI_j)$ است. مهاجم با داشتن این مقادیر می‌تواند مقادیر خصوصی را استخراج کند. در ادامه چگونگی حمله‌ها نشان داده خواهد شد.

۱.۴ به دست آوردن کلید نشست

در این نوع حمله، هدف مهاجم این است که با شنود پیام‌های نشست به کلید نشست برسد. مهاجم با حمله ضبط حسگر، به مقادیر حسگر (کلید مشترک بین حسگر و BS: RI_j) دسترسی یافته و سپس با شنود پیام‌های نشست به کلید نشست فعلی یا نشست‌های قبلی خواهد رسید. همچنین مهاجم با توجه به فاش بودن شناسه حسگر در پیامی که کاربر برای BS می‌فرستد به راحتی می‌تواند پیام‌های قبلی حسگر را تفکیک کند. مراحل حمله به‌قرار زیر است:

مرحله اول: مهاجم با شنود پیام GWN_j به SN_j که شامل M_5 و T_3 است و $M_5 = RBS \oplus h(RI_j \| T_3)$ می‌تواند به RBS برسد به این صورت: $RBS = M5 \oplus h(RI_j \| T_3)$ که RBS مقدار تصادفی ایستگاه است.

مرحله دوم: مهاجم با داشتن M_6، T_5، RBS و M_5 (درحالی‌که

$$M_6 = (RU \| RGWN_j \| ID_i) \oplus h(RBS \| M_5 \| T_5)$$

است) و با استفاده از رابطه زیر مقادیر RU، $RGWN_j$، ID_i را به دست می‌آورد:

$$(RU \| RGWN_j \| ID_i) = M_6 \oplus h(RBS \| M_5 \| T_5)$$

که RU مقدار تصادفی کاربر، ID_i شناسه کاربر و $RGWN_j$ مقدار تصادفی گره دروازه است.

مرحله سوم: مهاجم با شنود مقدار M_8 و T_7 (درحالی‌که

$$M_8 = RSN_j \oplus h(RBS \| M_5 \| T_7)$$

است) و با داشتن مقادیر مراحل قبل به RSN_j می‌رسد:

$$RSN_j = M_8 \oplus h(RBS \| M_5 \| T_7)$$

که RSN_j مقدار تصادفی حسگر است.

مرحله چهارم: حال مهاجم با داشتن مقادیر مراحل قبل می‌تواند کلید نشست را محاسبه کند:

$$SK = h(RGWN_j \| RU \| RSN_j \| RBS \| ID_i \| M_1)$$

۲.۴ نقض گمنامی حسگر

در این حمله، مهاجم قصد دارد که شناسه حسگر را به دست آورد تا باعث شود گمنامی حسگر نقض شود.

مهاجم در طرح چن و همکاران [۳]، پیام S_1 که به صورت فاش ارسال می‌شود را شنود می‌کند. همان‌طور بالا ذکر شد، در پیام S_1 شناسه حسگر به صورت فاش ارسال می‌شود. مهاجم با شنود این پیام و مقدار شناسه حسگر، گمنامی حسگر را نقض کرده است. در واقع شاید گمنامی حسگر در سامانه‌های نظارت کشاورزی مهم نباشد، ولی دشمن می‌تواند پیام‌های هر حسگر را جداگانه دسته‌بندی کند تا نیازی نباشد که محاسبات اضافه‌تری برای پیدا کردن نشست حسگر مورد نظر انجام دهد. این کار باعث می‌شود که حمله نقض امنیت رو به جلو و رو به عقب با محاسبات کمتری و سریع‌تر انجام شود.

۳.۴ نقض امنیت رو به جلو و رو به عقب

در این نوع حمله، مهاجم با داشتن مقادیر خصوصی می‌خواهد کلید نشست تمام نشست‌های قبلی که شنود کرده است را به دست بیاورد. همچنین می‌خواهد با داشتن این مقادیر خصوصی، کلید 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 جلسه‌های برسد. همچنین اگر مهاجم فقط اطلاعات را از حسگر استخراج کند و حسگر را در جای خود قرار دهد، می‌تواند کلید جلسه‌های 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 دست یابد، می‌تواند اطلاعات را با کلید نشست رمزگشایی کند:

$$DECSK(C) = M.$$

۴.۴ نقض گمنامی کاربر

هدف مهاجم در این نوع حمله این است که به شناسه یا مقدار یکتایی از یک کاربر دست یابد، تا گمنامی کاربر را از بین ببرد. مهاجم با داشتن کلید مشترک بین BS و SN_j و شنود مقدار M_5 و M_6 با استفاده از مراحل زیر به شناسه کاربر می‌رسد.

مرحله اول: مهاجم پیام بین GWN_j و SN_j را شنود می‌کند، که شامل M_5 و T_3 است $(M_5 = RBS \oplus h(RI_j \| T_3))$. حال با استفاده از رابطه $RBS = M_5 \oplus h(RI_j \| T_3)$ مقدار RBS را محاسبه می‌کند، که RBS مقدار تصادفی ایستگاه است.

مرحله دوم: مهاجم با داشتن مقادیر M_6، T_5، RBS و M_5 (در صورتی که

$$M_6 = (RU \| RGWN_j \| ID_i) \oplus h(RBS \| M_5 \| T_5)$$

است) مقادیر RU، $RGWN_j$، ID_i را به دست می‌آورد:

$$(RU \| RGWN_j \| ID_i) = M_6 \oplus h(RBS \| M_5 \| T_5)$$

با یافتن ID_i گمنامی کاربر از بین می‌رود.

۵.۴ پیوند زدن نشست‌های یک کاربر یا حسگر

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. این باعث می‌شود که حریم خصوصی یک موجودیت نقض شود.

با شنود مقدارهای M_5 و M_6 و طبق حمله نقض گمنامی کاربر، مهاجم می‌تواند به شناسه کاربر دست یابد. با این کار مهاجم می‌تواند نشست‌های مرتبط یک کاربر را به هم پیوند بزند.

با شنود پیام S_1، مهاجم می‌تواند به شناسه حسگر دست یابد و با این کار می‌تواند نشست‌های مرتبط یک حسگر را به هم پیوند بزند.

۶.۴ جعل حسگر

هدف مهاجم این است پیام‌هایی که حسگر تولید می‌کند را تولید کند و خود را به جای حسگر جا بزند.

مهاجم می‌تواند به جای حسگر قرار گیرد و با دریافت پیام از GWN_j و استخراج مقادیر خصوصی، مقادیر M_8، M_9 و T_7 را تولید کند، سپس خود را جای حسگر جا بزند و برای GWN_j پیام معتبر بفرستد.

۵ راهکار پیشنهادی

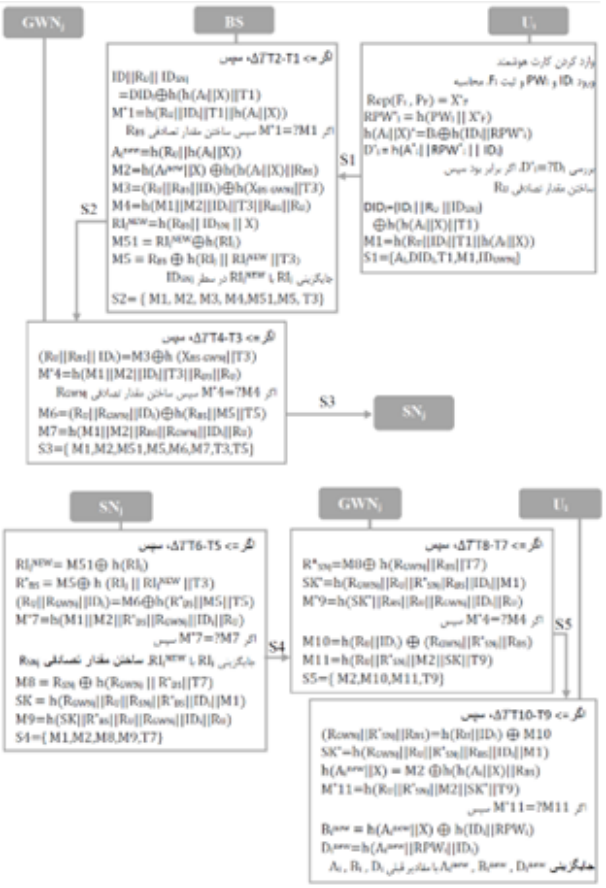
در این بخش، راهکاری برای بهبود طرح چن و همکاران [۳] ارائه می‌شود، تا این طرح در مقابل ضعف‌های نامبرده در بخش ۴ مقاوم شود. تغییرهای مرحله ورود، احراز اصالت و توافق کلید در هر مرحله به صورت زیر انجام می‌شود:

مرحله ۱: مانند طرح چن و همکاران [۳].

مرحله ۲: در پیام S_1 به جای ارسال شناسه حسگر به صورت فاش، شناسه حسگر به مقدار DID_i، اضافه می‌شود و شناسه حسگر از پیام S_1 حذف می‌شود. سپس پیام S_1 برای BS فرستاده می‌شود.

مرحله ۳: BS می‌تواند با توجه به مقادیر DID_i، به شناسه حسگر دست یابد.

مرحله ۴: پس از محاسبه M_4، BS کلید مشترک جدید بین حسگر و BS (RI_j^{NEW}) را محاسبه می‌کند. سپس مقدار M_{51} را تولید می‌کند که شامل مقادیر زیر است: کلید مشترک جدید بین حسگر و BS، مقدار چکیده (مقدار درهم) کلید مشترک بین حسگر و BS که در نشست قبل محاسبه شده است و در ستون مورد نظر جدول حسگرها در سمت BS وجود دارد. حال BS مقدار M_5 را تولید می‌کند که شامل XOR مقدار



شکل ۳. ورود، احراز اصالت و توافق کلید راهکار پیشنهادی

تصادفی BS با مقدار چکیده کلید مشترک نشست قبل بین حسگر و BS، کلید مشترک جدید بین حسگر و BS و برچسب زمانی $T_۳$ است. پس از محاسبه $M_۵$، BS کلید مشترک جدید بین حسگر و BS را در جدول حسگرها، ستون حسگر مورد نظر جایگزین مقدار قبل می‌کند. در این بخش مقدار $M_{۵۱}$ به $S_۲$ اضافه شده و سپس پیام $S_۲$ برای GWN_j ارسال می‌شود.

مرحله ۵: مانند طرح چن و همکاران [۳].

مرحله ۶: در پیام $S_۳$، مقدار $M_{۵۱}$ اضافه شده است و برای SNj فرستاده می‌شود.

مرحله ۷: SN_j پس از دریافت پیام $S_۳$، با توجه به $M_{۵۱}$، مقدار RI_j^{NEW} را به دست می‌آورد. در ادامه از طریق $M_۵$، به مقدار تصادفی BS می‌رسد. سپس مانند طرح چن و همکاران [۳] ادامه می‌یابد و مقادیر محاسبه می‌شود.

مرحله ۸: مانند طرح چن و همکاران [۳].

مرحله ۹: مانند طرح چن و همکاران [۳].

مرحله ۱۰: مانند طرح چن و همکاران [۳].

مرحله ۱۱: مانند طرح چن و همکاران [۳].

۱.۵ تغییرها نسبت به طرح چن و همکاران

- حذف شناسه حسگر از پیام $S_۱$.
- قرار دادن شناسه حسگر در مقدار DID_i.
- اضافه شدن جدول حسگرها در BS برای ذخیره کلید مشترک جدید بین حسگر و BS.
- اضافه شدن دو عمل چکیده و یک XOR در سمت BS.
- اضافه شدن کلید مشترک جدید بین حسگر و BS در مقدار $M_۵$ در سمت BS.
- اضافه شدن یک چکیده و یک XOR در سمت حسگر.
- ذخیره کلید مشترک جدید بین حسگر و BS در سمت حسگر.

۶ تحلیل امنیتی راهکار پیشنهادی

در این بخش، امنیت طرح پیشنهادی نسبت به ضعف‌های طرح چن و همکاران [۳] تحلیل می‌شود.

فرض کنید که مهاجم موفق شده است بعد از نشست iام، گره حسگر را ضبط کند. حال مهاجم مقادیر شناسه حسگر و $RI_j^{NEW_i} + ۱$ را در اختیار دارد. همچنین مهاجم نشست‌های مختلفی را شنود کرده است. با توجه به این فرض، رفتار طرح بهبودیافته، نسبت به حملات به دست آوردن کلید نشست، نقض گمنامی کاربر، نقض گمنامی حسگر، پیوند زدن نشست‌های یک کاربر یا یک حسگر، جعل حسگر و نقض امنیت رو به جلو و رو به عقب بررسی می‌شود.

۱.۶ به دست آوردن کلید جلسه

در این نوع حمله، هدف مهاجم این است که با شنود پیام‌های نشست به کلید نشست دست یابد. با در نظر گرفتن فرض بخش قبل، مهاجم باید دقیقا نشست قبلی این حسگر را پیدا کند، یعنی از بین هزاران نشستی که شنود کرده، نشست قبلی این حسگر را پیدا کند. ابتدا باید پیوندی در پیام‌ها پیدا کند یعنی شناسه حسگر را در پیام‌های ارسالی بیابد، در طرح چن و همکاران [۳] این امکان وجود داشت، زیرا در پیامی که کاربر برای BS ارسال می‌کرد شناسه حسگر به صورت فاش ارسال می‌شد ولی در طرح جدید، شناسه حسگر به صورت فاش ارسال نمی‌شود، بنابراین امکان یافتن نشست‌های قبلی این حسگر وجود ندارد.

حال فرض کنید که مهاجم به طریقی بتواند شناسه حسگر را در پیام‌ها به دست آورد و نشست قبلی این حسگر را پیدا کند. در این صورت مهاجم می‌خواهد مطابق عبارات زیر ابتدا به مقدار RBS برسد و سپس سایر مقادیر و کلید نشست را به دست آورد:

$$M_{۵۱} = RI_j^{NEW_i} + ۱ \oplus h(RI_j^{NEW_i})$$
$$M_۵ = RBS \oplus h(RI_j^{NEW_i} \| RI_j^{NEW_i} + ۱ \| T_۳)$$
$$SK = h(RGWN_j \| RU \| RSN_j \| R * BS \| ID_i \| M_۱)$$

همان‌طور که دیده می‌شود، مهاجم باید مقدار $RI_j^{NEW_i}$ را به دست

آورد، ولی از طریق $M_{۵۱}$ فقط چکیده این مقدار را در اختیار دارد. بنابراین مهاجم نمی‌تواند به مقدار $RI_j^{NEW_i}$ برسد، پس نمی‌تواند مقدار RBS را به دست آورد. با نداشتن RBS مهاجم نمی‌تواند کلید نشست را به دست آورد.

۲.۶ گمنامی حسگر

در این حمله، مهاجم قصد دارد که شناسه حسگر را به دست آورد تا باعث شود گمنامی حسگر نقض شود.

در راهکار بهبودیافته، در پیام $S_۱$ شناسه حسگر به صورت فاش در پیام ارسال نمی‌شود و در قسمت DID_i قرار می‌گیرد تا مهاجم به شناسه حسگر دست پیدا نکند.

۳.۶ امنیت رو به جلو و رو به عقب

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

با فرض ضبط شدن حسگر توسط مهاجم و شنود نشست‌های مختلف از حسگرهای مختلف، مانند به دست آوردن کلید نشست، باید ابتدا پیوندی بین شناسه داخل حسگر و پیام‌های شنود شده بیابد که با توجه به تامین گمنامی حسگر در پروتکل بهبودیافته، امکان این حمله وجود ندارد.

۴.۶ 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.

طبق بخش ۱.۶ مهاجم نمی‌تواند به RBS برسد، با نداشتن RBS مهاجم نمی‌تواند به مقادیر $M_۶$

$$((RU\|RGWN_j\|ID_i) = M_۶ \oplus h(R*BS\|M_۵\|T_۵))$$

که شامل شناسه کاربر است دست یابد و در نتیجه گمنامی کاربر حفظ می‌شود.

۵.۶ پیوند زدن نشست‌های یک کاربر یا حسگر

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، این امر باعث نقض حریم خصوصی آن موجودیت می‌شود.

با توجه به بخش‌های ۳.۶، ۴.۶ و تامین گمنامی کاربر و حسگر، این امکان وجود ندارد که مهاجم شناسه حسگر یا کاربر را به دست آورد. همچنین در تمامی پیام‌هایی که به صورت فاش ارسال می‌شود مقادیر تصادفی استفاده شده است که باعث می‌شود نشست‌های مختلف به یکدیگر پیوند زده نشوند.

۶.۶ حمله جعل حسگر

هدف مهاجم در این حمله این است که بتواند پیام‌های یک حسگر را تولید کند و خود را به جای حسگر جا بزند.

با توجه به اینکه مهاجم طبق حمله به دست آوردن کلید نشست در بخش ۱.۶، نمی‌تواند به مقدار RBS دست یابد، پس نمی‌تواند مقدارهای $M_۸$ و $M_۹$ را تولید کند، در نتیجه امکان جعل حسگر وجود ندارد.

۷ مقایسه امنیتی و کارایی

در این بخش طرح پیشنهادی با طرح‌های [۳، ۱۰-۱۵] از نظر امنیتی و کارایی مقایسه می‌شود.

۱.۷ مقایسه امنیتی

در جدول ۲ طرح پیشنهادی با طرح‌های [۳، ۱۰-۱۵] از نظر امنیتی مقایسه می‌شود. همچنین مشخص است که طرح چن و همکاران [۳] در برابر حملاتی ضعف دارد و طرح پیشنهادی در برابر آن حملات مقاوم است.

در ستون اول جدول ۲ خصوصیات امنیتی نوشته شده است که ۱) احراز اصالت متقابل، ۲) گمنامی کاربر، ۳) ردیابی کاربر، ۴) گمنامی حسگر، ۵) پیوند نشست‌ها، ۶) امنیت کلید نشست، ۷) امنیت رو به جلو، ۸) جعل حسگر، ۹) جعل دروازه، ۱۰) جعل کاربر، ۱۱) حمله تکرار، ۱۲) حمله داخلی، ۱۳) حمله منع خدمت، ۱۴) حدس برون‌خط کلمه عبور، ۱۵) دزدیدن کارت هوشمند، است.

۲.۷ مقایسه کارایی

یکی از چالش‌های مهم شبکه حسگر بی‌سیم، محدودیت انرژی است. یک طرح، اگر کمتر انرژی مصرف کند، کاراتر است و حسگر آن طرح عمر طولانی‌تری خواهد داشت. مصرف انرژی یک طرح، به محاسباتی که در آن طرح انجام می‌شود، بستگی دارد.

در این بخش، طرح پیشنهادی با طرح‌های [۳، ۱۰-۱۵] مقایسه می‌شود. مقایسه‌ها به تفکیک موجودیت‌ها است. در جدول ۳، T_H به معنای زمان انجام عملیات تابع درهم‌ساز، T_m به معنای زمان انجام ضرب اسکالر، T_s به معنای زمان انجام عملیات رمزنگاری متقارن است. همچنین هر عمل T_H، ۰/۰۰۰۴ ثانیه، T_m، ۷/۳۵۲۹ ثانیه و T_s، ۰/۱۳۰۳ ثانیه زمان خواهد برد.

در جدول ۳ دیده می‌شود که طرح پیشنهادی دارای سه عمل چکیده‌ساز بیشتر نسبت به طرح چن و همکاران [۳] است، اما از لحاظ امنیتی، طرح پیشنهادی امنیت بهتری را تامین می‌کند.

جدول ۲. مقایسه امنیتی

	[۱۰]	[۱۱]	[۱۲]	[۱۳]	[۱۴]	[۱۵]	[۳]	طرح پیشنهادی
۱	✘	✘	✔	✔	✔	✔	✔	✔
۲	✘	✔	✔	✘	✘	✘	✘	✔
۳	✘	✔	✔	✘	✘	✘	✔	✔
۴	✔	✔	✔	✔	✔	✔	✘	✔
۵	✔	✔	✘	✔	✘	✘	✘	✔
۶	✔	✔	✔	✔	✔	✔	✘	✔
۷	✔	✔	✔	✔	✔	✘	✘	✔
۸	✘	✔	✔	✔	✔	✘	✘	✔
۹	✔	✔	✔	✔	✔	✔	✔	✔
۱۰	✘	✔	✘	✘	✘	✔	✔	✔
۱۱	✔	✔	✔	✔	✔	✔	✔	✔
۱۲	✔	✘	✔	✔	✔	✘	✔	✔
۱۳	✔	✘	✔	✔	✔	✔	✔	✔
۱۴	✘	✔	✔	✔	✔	✔	✔	✔
۱۵	✔	✔	✔	✘	✘	✔	✔	✔

۸ نقاط قوت و ضعف

۱.۸ نقاط قوت

- مقاوم در برابر نقض گمنامی حسگر.
- مقاوم در برابر حمله‌های جعل موجودیت‌ها.
- عدم پیوند نشست‌ها.
- عدم به دست آوردن کلید نشست.
- دارای امنیت رو به جلو و روبه‌عقب.
- استفاده از این راهکار برای سایر کاربردهایی که ضعف ضبط گره حسگر دارند.

۲.۸ نقاط ضعف

- اضافه شدن جدول در سمت BS و هزینه جستجو در جدول.
- اضافه شدن دو عمل چکیده و یک XOR در سمت BS.
- اضافه شدن یک چکیده و یک XOR در سمت حسگر.
- بروز رسانی کلید مشترک جدید بین حسگر و BS در سمت حسگر.

۹ نتیجه‌گیری

در این مقاله طرح احراز اصالت چن و همکاران [۳] 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 نشست، نقض امنیت رو به جلو و رو به عقب، نقض گمنامی کاربر و حسگر، پیوند زدن نشست‌ها و حمله جعل حسگر شود.

در ادامه راهکار پیشنهادی این مقاله، جهت بهبود طرح ارائه شد تا ضعف‌های طرح چن و همکاران [۳] برطرف شود؛ سپس طرح بهبودیافته مورد ارزیابی قرار گرفت.

به عنوان راهکارهای آینده می‌توان به ارائه یک طرح جدید با تامین ویژگی‌های امنیتی مورد انتظار و کاراتر اشاره کرد.

مراجع

[1] Chee-Yee Chong and Srikanta P Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, 2003.

[2] Hua-Yi Lin. High effect secure data transmission mechanisms in wireless sensor networks using id-based key management scheme. *J. Convergence Inf. Technol.*, 4(1):77–83, 2009.

[3] Meriske Chen, Tian-Fu Lee, and Jiann-I Pan. An enhanced lightweight dynamic pseudonym identity based authentication and key agreement scheme using wireless sensor networks for agriculture monitoring. *Sensors*, 19(5):1146, 2019.

[4] Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment. *Journal of Network and Computer Applications*, 89:72–85, 2017.

[5] Prosanta Gope, Ashok Kumar Das, Neeraj Kumar, and Yongqiang Cheng. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. *IEEE transactions on industrial informatics*, 15(9):4957–4968, 2019.

[6] Mian Jan, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. Pawn: a payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29(17):e3986, 2017.

[7] Shaymaa Mahmood Naser and Muayad Sadik Croock. Proposed simulator based on developed lightweight au-

جدول ۳. مقایسه کارایی

	کاربر	ایستگاه پایه	دروازه	حسگر	جمع کل
[۱۰]	-	-	$۱T_H$	$۳T_H$	$۴T_H$
[۱۱]	$۴T_H$	-	$۳T_H$	TH۱	TH۸
[۱۲]	$۵T_H$	-	$۸T_H$	$۲T_H$	$۱۵T_H$
[۱۳]	$۸T_H$	-	$۹T_H$	$۷T_H$	$۲۴T_H$
[۱۴]	$۱۱T_H + ۲T_m$	-	$۱۰T_H$	$۳T_H + ۲T_m$	$۲۴T_H + ۴T_m$
[۱۵]	$۷T_H + ۲T_s$	$۳T_H + ۲T_s$	$۵T_H + ۴T_s$	$۴T_H + ۱T_s$	$۱۹T_H + ۹T_s$
[۳]	$۱۴T_H$	$۹T_H$	$۹T_H$	$۶T_H$	$۳۸T_H$
طرح پیشنهادی	$۱۴T_H$	$۱۱T_H$	$۹T_H$	$۷T_H$	$۴۱T_H$

2015.

[14] Fan Wu, Lili Xu, Saru Kumari, and Xiong Li. An improved and provably secure three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, 11(1):1–20, 2018.

[15] Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah, and Mauro Conti. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, 84:200–215, 2018.

[16] Chin-Chen Chang and Hai-Duong Le. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on wireless communications*, 15(1):357–366, 2015.

[17] Ashok Kumar Das, Pranay Sharma, Santanu Chatterjee, and Jamuna Kanta Sing. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, 35(5):1646–1656, 2012.

[18] DaeHun Nyang and Mun-Kyu Lee. Improvement of das's two-factor authentication protocol in wireless sensor networks. *Cryptology EPrint Archive*, 2009.

[19] Daojing He, Yi Gao, Sammy Chan, Chun Chen, and Jiajun Bu. An enhanced two-factor user authentication scheme in wireless sensor networks. *Ad Hoc Sens. Wirel. Networks*, 10(4):361–371, 2010.

[20] Rong Fan, Ling-Di Ping, Jian-Qing Fu, and Xue-Zeng Pan. A secure and efficient user authentication protocol for two-tiered wireless sensor networks. In *2010 Second Pacific-Asia Conference on Circuits, Communications and System*, volume 1, pages 425–428. IEEE, 2010.

thentication and key management protocol for wireless sensor network. *International Journal of Computing and Digital Systems*, 7(04):251–260, 2018.

[8] Rabia Riaz, Noor-ul-Ain Gillani, SanamShahla Rizvi, Sana Shokat, and Se Jin Kwon. Subbase: An authentication scheme for wireless sensor networks based on user biometrics. *Wireless Communications and Mobile Computing*, 2019, 2019.

[9] Ruhul Amin, SK Hafizul Islam, Neeraj Kumar, and Kim-Kwang Raymond Choo. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. *Journal of network and computer applications*, 104:133–144, 2018.

[10] Kirk HM Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang. A dynamic user authentication scheme for wireless sensor networks. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, volume 1, pages 8–pp. IEEE, 2006.

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

[12] Sang Guun Yoo, Keun Young Park, and Juho Kim. A security-performance-balanced user authentication scheme for wireless sensor networks. *International journal of distributed sensor networks*, 8(3):382810, 2012.

[13] Debiao He, Neeraj Kumar, and Naveen Chilamkurti. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences*, 321:263–277,

[21] Tien-Ho Chen and Wei-Kuan Shih. A robust mutual authentication protocol for wireless sensor networks. *ETRI journal*, 32(5):704–712, 2010.

[22] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. 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, 2014.

[23] Fan Wu, Lili Xu, Saru Kumari, and Xiong Li. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security. *Journal of Ambient Intelligence and Humanized Computing*, 8(1):101–116, 2017.

[24] Binod Vaidya, Dimitrios Makrakis, and Hussein T Mouftah. Improved two-factor user authentication in wireless sensor networks. In *2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications*, pages 600–606. IEEE, 2010.

[25] Fan Wu, Lili Xu, Saru Kumari, and Xiong Li. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimedia Systems*, 23(2):195–205, 2017.

[26] Xiong Li, Jianwei Niu, Saru Kumari, Junguo Liao, Wei Liang, and Muhammad Khurram Khan. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Security and Communication Networks*, 9(15):2643–2655, 2016.

[27] Ankur Gupta, Meenakshi Tripathi, Tabish Jamil Shaikh, and Aakar Sharma. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, 149:29–42, 2019.

[28] Fan Wu, Xiong Li, Lili Xu, Saru Kumari, Marimuthu Karuppiah, and Jian Shen. A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. *Computers & Electrical Engineering*, 63:168–181, 2017.

[29] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and YoungHo Park. Design of secure and lightweight authentication protocol for wearable devices environment. *IEEE journal of biomedical and health informatics*, 22(4):1310–1322, 2017.