سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Fall 2023, 4 (3), 1-13
DOR:

Received: 2 July 2023
Accepted: 12 Aug 2023

مقاله پژوهشی

A New Protocol for Lightweight Anonymous Authentication with Leading Security in Wireless Sensor Networks Based on IoT

Maryam Rajabzadeh Asaar[1*], Pouya Derakhshan Barjoei[2]

1. Assistant Professor, Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran. (*Corresponding Author*) asaar@srbiau.ac.ir
2. Assistant Professor, Department of Electrical and Computer Engineering, Naein Branch, Islamic Azad University, Naein, Iran.pouya.derakhshan@srbiau.ac.ir

Abstract

Introduction: The Internet of Things includes an interconnected network that enables various types of communication and plays a critical role in the development of smart services to support and improve the activities of individuals and society. One of the most important concerns of those who use wireless networks is access information through the public channel considering security and privacy. Authentication is therefore important so that no entity, person, or non-virtual device can abuse the network and by maintaining the privacy of users who are using the network. Important information does not reach these people. Due to the fact that this research was aimed at providing a lightweight protocol, therefore, by checking and analyzing, we will show that the protocol proposed in this research is superior to the protocols of Fotuhi and colleagues in some aspects of security and computing [1]. The proposed protocol will be reviewed and shown, as claimed. It was found that the proposed protocol has both the characteristic of being lightweight and the characteristic of advanced security. By analyzing the security of the protocol, we showed that their proposed protocol is resistant to malicious port and asynchrony attacks.

Method: We presented a protocol that, in addition to the mentioned features, it also has the feature of two-way authentication. The proposed protocol model consists of three main components which all three entities have already been approved at the registration stage and can communicate with each other to verify their identity. The overall goal is for both the user and the sensor to verify each other's authorization, which is verified by the gateway. This protocol is safe against attacks and finally compared the proposed protocol with the previous and based protocol.

Results: our outcomes from the proposed method showed that the proposed protocol is 24% in computing overhead and 26% Improves telecommunication overhead.

Discussion: In this research, an attempt was made to provide a protocol that would bring sufficient security requirements without the use of a smart card. Also, unauthorized users cannot access the protocol stages by ways such as repetition attacks, identity forgery, lack of synchronization between the sensor and the user, the ability to track and capture the sensor.

Keywords: Internet of things, authentication, anonymity, advanced security, lightweight.

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

ارائه پروتکل نوین احرازهویت گمنام سبک‌وزن با امنیت پیشرو در شبکه‌های حسگر بی‌سیم مبتنی بر اینترنت اشیاء

تاریخ دریافت: ۱۱/ ۰٤/ ۱٤۰۲
تاریخ پذیرش: ۲۱/ ۰۵/ ۱٤۰۲

دورهٔ چهارم، پاییز ۱٤۰۲
شمارهٔ سوم، صص: ۱-۱۳

مریم رجب زاده عصار[1*]، پویا درخشان برجوئی[2]

۱. استادیار، گروه مهندسی برق، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. (نویسندهٔ مسئول) asaar@srbiau.ac.ir
۲. استادیار، گروه مهندسی برق، واحد نایین، دانشگاه آزاد اسلامی، نایین، ایران.

چکیده: در این مقاله یک پروتکل سبک‌وزن ارائه و پیشنهاد شده‌است که دارای محاسن امنیتی و محاسباتی جدیدی است. جهت مطالعه و بررسی از یک پروتکل پایه‌ای و مبنا بر اساس پروتکل پیشنهادی فتوحی و همکارانش که در مجله Computer Networks پیشنهاد شده‌است، استفاده‌کرده‌ایم. در این مقاله نشان‌دادیم که برخی از جنبه‌های امنیتی و محاسباتی پروتکل پیشنهادی نسبت به‌پروتکل‌های قبلی برتری‌هایی دارد. با بررسی و تحلیل پروتکل پیشنهادی نشان‌داده‌شد که مطابق ادعای گفته‌شده، پروتکل پیشنهادی هم ویژگی سبک‌وزن بودن و هم ویژگی امنیت پیشرو (حفظ امنیت کلیدهای نشست بعدی در صورت افشای یک کلید نشست) را داراست. با تحلیل امنیتی پروتکل فتوحی و همکارانش که در سال ۲۰۲۱ ارائه‌شده، نشان‌دادیم‌که پروتکل پیشنهادی آن‌ها در برابر حملات درگاه بدخواه و عدم همزمانی آسیب‌پذیر است. همچنین، پروتکل پیشنهادی علاوه بر ویژگی‌های مذکور، ویژگی احراز هویت دوطرفه را نیز داراست. این پروتکل در برابر حملات نیز امن است. درنهایت، پروتکل پیشنهادی را با پروتکل‌های مشابه مقایسه‌کرده و نشان داده‌شد که پروتکل پیشنهادی۲۴ ٪ در سربار محاسباتی و ۲۶٪ در سربار مخابراتی بهبود عملکرد را ایجاد کرده‌است.

واژه‌های کلیدی: اینترنت اشیاء، احراز هویت، گمنامی، امنیت پیشرو، سبک‌وزن.

۱. مقدمه

اینترنت اشیاء شامل یک شبکه به‌هم‌پیوسته است که انواع ارتباط را ممکن می‌سازد و نقش‌حساسی در توسعه سرویس‌های هوشمند برای پشتیبانی و بهبود فعالیت‌های افراد و جامعه دارد .یکی از مهم ترین دغدغه‌های کسانی که از شبکه‌های بی‌سیم استفاده می کنند نحوه دسترسی اطلاعات از طریق کانال عمومی، امنیت و حریم خصوصی است.احراز هویت، از این رو مهم است که هیچ نهاد، شخص یا دستگاه غیرمجازی نتواند از شبکه سوءاستفاده کند و با حفظ حریم خصوصی کاربرانی که در حال استفاده از شبکه هستند، اطلاعات مهمی به دست این افراد نرسد. در این تحقیق، تعدادی ازطرح‌هایی‌که بارویکرد حفظ امنیت اطلاعات، احرازهویت را انجام می‌دهند، بررسی شده است.با تحلیل و بررسی این طرح ها خوایم دید که کدام ویژگی‌ها برای شبکه تهدید تلقی می‌شود. ویژگی‌هایی‌که می‌توانند پروتکل پیشنهادی ما را به هدف نزدیک‌ترکنند، شامل حفظ گمنامی و همچنین پوشش‌دهی ویژگی امنیت پیشرو، با استفاده از ساده‌ترین و به‌اصطلاح سبکترین ابزار رمزنگاری هستند. با تحلیل امنیتی پروتکل فتوحی و همکاران نشان-دادیم که پروتکل پیشنهادی آن‌ها در برابر حملات درگاه بدخواه و عدم-همزمانی آسیب‌پذیر است و درنهایت، پروتکلی ارائه‌کردیم که علاوه بر ویژگی‌های مذکور ، ویژگی احراز هویت دوطرفه را نیز داراست. این پروتکل در برابر حملات، امن است و درنهایت پروتکل پیشنهای را با پروتکل فتوحی و همکاران مقایسه‌کرده و نشان‌دادیم که پروتکل پیشنهادی۲۴ ٪ در سربار محاسباتی و ۲۶٪ در سربار مخابراتی بهبود ایجاد می‌کند .

۲. کارهای مرتبط

در این قسمت برخی از پروتکل‌هایی که به‌منظور احراز هویت در شبکه‌های حسگر بی‌سیم و اینترنت اشیاء ارائه‌شدند را بررسی‌می‌کنیم . پروتکل‌های احراز هویت اخیر در زمینه اینترنت اشیاء می‌توانند به دو دسته تقسیم‌شوند: احراز هویت با صدور گواهینامه و احراز هویت بدون گواهینامه. دردسته اول، احرازهویت با استفاده از گواهینامه‌های دیجیتالی است. پورامبگ و همکاران[2] پروتکلی برای احرازهویت و تشکیل کلید نشست برای شبکه‌های حسگر بی‌سیم در اینترنت اشیاء ارائه‌دادند که شامل دو مرحله ثبت نام و احراز هویت است که در مرحله ثبت‌نام به هر کاربر و دستگاهی‌گواهینامه اختصاص داده می‌شود و در مرحله احراز هویت، کاربر سیستم برای گره حسگر احراز هویت‌شده و می‌تواند از اطلاعات حسگر استفاده‌کند این پروتکل به دلیل استفاده از خم‌های بیضوی از لحاظ مصرف انرژی بسیار مناسب است و با توجه به اینکه ادعاشده‌است که این پروتکل در مقابل برخی‌حملات امن است، اما ایرادهایی نیز به آن وارد است. به‌عنوان نمونه در این پروتکل، هویت کلید عمومی نهادی که گواهینامه‌ها را صادرمی‌کند تضمین نشده‌است و این یعنی هر شخصی می‌تواند با داشتن کلید بین‌حسگر و نهاد صدور گواهینامه‌ها، به‌راحتی خود را به‌عنوان این نهاد معرفی و جعل‌کند. گوپه و همکاران [3] پروتکل سبک وزنی برای احراز هویت ارائه‌کردند که این پروتکل بر مبنای کلید متقارن در شبکه‌های حسگر بی‌سیم بود. ادعای نویسندگان پروتکل این بود که این‌طرح در برابر حملاتی همچون سرقت کارت امن است و همچنین تضمین امنیت پیشرو از ویژگی‌های این‌طرح بود که در سال۲۰۱۹ توسط انورقانی وهمکاران [4] نشان‌داده شد که ادعای گوپه برای برقراری امنیت و حفظ اطلاعات شخصی چندان معتبر نیست.

دردسته دوم، پروتکل‌هایی قرارداده‌شدند که به گواهینامه نیازی ندارند. این دسته از پروتکل‌ها تنها ازعملگرهای ساده رمزنگاری مانند عمل‌الحاق، تابع چکیده‌ساز استفاده‌می‌کنند و به صرفه‌جویی در مصرف انرژی معروفند. خمیسا و همکاران[5] پروتکل احراز هویت فوق‌سبک-وزنی ارائه‌دادند که از امنیت بالا و سطح مصرف انرژی پایینی برخورداراست. می‌توان‌گفت این پروتکل کامل‌شده پروتکلی است‌که توسط خودشان ارائه‌شده‌بود. امنیت این پروتکل منوط بر یک مقدار خصوصی است که اگر مهاجم موفق‌شود این پارامتر را به‌دست‌آورد به‌راحتی می‌تواند به جای‌کاربران مجاز با گره‌های حسگر ارتباط برقرارکند که این موضوع می‌تواند نقطه ضعفی برای این پروتکل تلقی - شود. این مقدار می‌تواند توسط حالتی حدس زده‌شود و یا حتی بازیابی شود اما باید راهی‌باشد که حتی اگر این مقدار در دسترس مهاجمان قرارگرفت، نتوانند خللی به امنیت پروتکل واردکنند. در [6] کریمی و همکاران یک استراتژی متعادل‌سازی بار در طرح پیشنهادی مبتنی بر زمان پاسخ برای کنترل‌کننده‌های سوئیچ‌های مبتنی بر نرم افزار متعدد پیشنهاددادند که در مصرف انرژی تأثیرگذار بود. زند و همکاران در [7] ارتقای امنیت اینترنت اشیا در شبکه زیگبی را با الگوریتم پیشنهادی بررسی‌کردند. در [8] موسوی و همکاران طرح جدیدی برای مقاوم‌سازی الگوریتم‌های رمزنگاری و مقابله با حملات را نشان‌دادند. در [9-12] درخشان و همکاران بررسی مصرف انرژی و نوع انتقال داده را در شبکه-های غیرایستان بررسی و تداخل و حملات کاربران غیرمجاز را بررسی و مطالعه‌کردند.

۳. مروری بر پروتکل فتوحی و همکارانش [1]

یک پروتکل احراز هویت سبک‌وزن دوفاکتوره که دارای ویژگی‌های امنیت پیشرو است، ارائه‌شده که همچنین در برابر به‌دست‌آوردن یا جعل کلید توسط مهاجم و همچنین ردیابی، مقاوم است.

پروتکل فتوحی و همکارانش [1]، از ROR،OPNETو Proverifبرای اثبات امنیت، استفاده‌شده و کارایی پروتکل با پروتکل‌های پیشین مقایسه‌شده‌است. برای تحلیل این پروتکل سه فرضیه در نظر گرفته‌شده‌است :

فرضیه اول: تمام پیام‌هایی که در کانال عمومی رد و بدل می‌شوند می‌توانند توسط مهاجم استراق‌سمع، دستکاری یا بازپخش شوند و یا حتی از ارسال پیامی جلوگیری و یا پیامی توسط مهاجم تولید و اضافه شود. درباره پیام‌هایی که در کانال‌های خصوصی رد و بدل می‌شوند مهاجم هیچگونه دسترسی و آگاهی ندارد.

فرضیه دوم: با احتمال اینکه ممکن است دستگاه موبایل کاربر دزدیده شود، فرض‌می‌کنیم مهاجم می‌تواند اطلاعات داخل دستگاه موبایل را بازیابی‌کند.

فرضیه سوم: از آنجاکه مقادیر شناسه و رمز عبور کاربران توسط خودشان انتخاب‌می‌شود می‌تواند در زمان چندجمله‌ای، توسط مهاجم قابل‌حدس‌زدن باشد، همچنین مقادیر و دنباله‌های تصادفی، کلیدهای خصوصی و کلید نشست نمی‌توانند توسط مهاجم حدس‌زده‌شوند. این‌پروتکل‌دارای‌چهارمرحله اصلی‌است:

۱. مقداردهی‌اولیه ۲. ثبت‌نام ۳. احرازهویت ۴. تغییررمزعبور

جدول ۱ نمادهای‌مورداستفاده‌درپروتکل‌فتوحی‌وهمکارانش

نماد	تعریف
U_i , ID_i , PW_i	کاربرiام‌وشناسه‌ورمزعبورش
GID_j , G_j	شناسه‌وکلیدخصوصی‌درگاهjام$^{(GW_j)}$
SN_k , SID_k	حسگرkام‌وشناسه‌اش
N_l	تعدادمجموعه‌حسگرها
SG_k	کلیدخصوصی‌بین‌حسگرودرگاه
sk_u, sk_g, sk_s	کلیدهای‌نشست‌تولیدشده‌توسط‌کاربر،درگاه‌وحسگر
M_i	پیام‌های‌احرازهویت
CID_i, QID_k	دنباله‌های‌تصادفی‌موقتی‌کاربروحسگر
R_u, R_g, R_s, R_x, R_y, R_z	عددهای‌تصادفی‌موقتی
$h(.)$	تابع‌چکیده‌ساز
$\oplus$	یای‌انحصاری
$\|\|$	الحاق

۱،۳. مرحله مقداردهی اولیه

در این‌مرحله فرض‌شده که هر درگاه یک نهاد قابل‌اعتماد است که با GID_jشناخته‌شده و تمامی پیام‌ها بوسیله این درگاه‌ها انتقال‌می‌یابند . هر درگاه یک کلید خصوصی G_j نیزتولیدمی‌کند.

۲،۳. مرحله ثبت نام

این مرحله را به دو بخش تقسیم می‌کنیم:

۱-مرحله ثبت نام‌حسگر: هرحسگر SN_k دارای یک شناسه SID_k است. به‌علاوه هر مجموعه‌ای ازحسگرا متعلق به شبکه‌ای با شناسه خاص‌خودش N_lاست. هرحسگر با درگاه به‌طور مستقیم ارتباط می‌گیرد و دارای یک کلید خصوصی مشترک به نام SG_k هستند:

$SG_k= h(SID_k\| G_j\| Nl)$

سپس GW_j دوعدد تصادفی R_y و R_zو دنباله‌تصادفی QID_k را انتخاب‌کرده و مقادیر را $QID_k, SID_k, SG_k, GID_j, R_y, R_z$, را در حسگر قرارمی‌دهد و مقادیر $SID_k, QID_k, N_l, R_y,$ $h(R_z)$ را در پایگاه خود ذخیره‌می‌کند و درنهایت حسگر در محل مورد نظر قرارمی‌گیرد.

۲-مرحله ثبت نام‌کاربر: ثبت نام‌کاربر در درگاه‌طی سه مرحله اتفاق‌می‌افتد:

۱-کاربر U_iشناسه ID_i، رمزعبور PW_i و مقدارتصادفی R_0را انتخاب‌کرده و مقدار رمز عبور ماسک شده را بصورت $HPW_i=h(PW_i \| R_0)$ محاسبه‌می‌کندو ID_iو HPW_i را توسط کانال امن برای GW_jمی‌فرستد.

۲-درصورتی‌که ID_i از قبل‌در درگاه ثبت‌نام نشده‌باشد، GW_j برای U_i یک شناسه تصادفی CID_iو عدد تصادفی R_x تخصیص داده و همراه با مقادیر ID_iو HPW_i ذخیره و سپس A_1و A_2 را با استفاده از روابط(3-2), (3-1)محاسبه و مقادیر A_1, A_2 CID_i, GID_j,را برای U_i در یک‌کانال امن ارسال‌می‌کند.

$A_1 = h(CID_i \| R_x \| GID_j \| G_j) \oplus HPW_i$ (1)

$A_2 = h(ID_i \| G_j) \oplus h(ID_i \| HPW_i)$ (2)

۳- U_1 مقدار $A_3 = h(ID_i \| PW_i) \oplus R_0$ محاسبه و مقادیر $GIDj$, CID_i, A_3, A_2, A_1 موبایلش ذخیره‌می‌کند. اکنون کاربر آماده ورود به مرحله احرازهویت است.

۳،۳. مرحله احراز هویت

پس از مرحله ثبت‌نام، کاربر U_i ،حسگر مورد نظرش را انتخاب و IDi و PW_i را وارد دستگاه موبایل کرده، مقادیر $R_0=h(IDi \| PW_i) \oplus A_3$ و $HPW_i=h(PW_i \| R_0)$ محاسبه و پس ازآن با استفاده عددتصادفی R_u تولیدی و SID_k که‌کاربر اعلام کرده بود مقادیر B_4, B_3, B_2, B_1 از روابط زیر تشکیل و پیام $M_1=\{B_4, B_3, B_2, GID_i, CID_i\}$ برای درگاه ارسال‌می‌شود.

$B_1 = A_1 \oplus HPW_i$ (3)

$B_2 = B_1 \oplus HPW_i \oplus R_u$ (4)

$B_3 = SID_k \oplus h(ID_i \| R_u)$ (5)

$B_4 = h(CID_i \| GID_j \| SID_k \|B_1\| ID_i \| R_u)$ (6)

درستی CID_iو GID_j توسط GW_j بررسی‌شده و ID_i,R_xو HPW_iرا در صورت‌وجود، از پایگاه داده استخراج‌می‌کند. سپس روابط (7),(8)را محاسبه و دو عدد تصادفی R_gو R_z^{new} انتخاب‌کرده و پس‌از آن، GW_jبامحاسبه رابطه $B_3\oplus h(ID_i \| R_u)$ مقدار SID_k را به‌دست می آورد و R_y را نیز از پایگاه داده استخراج‌کرده و مقدار تصادفی QID_k^{new} را برای حسگر تولیدمی‌کند.

$B_1 = h(CID_i \| R_x \| GID_j \|G_j)$ (7)

$R_u = B_2 \oplus B_1 \oplus HPW_i$ (8)

درادامه، GW_jمقادیر SG_k,S, B_5, B_6, B_7, B_8 و B_9 را طبق روابط زیر تشکیل‌داده و پیام M_2 ={ QID_k , B_5 , B_6 , B_7 , B_8 , B_9 } را برای حسگر ارسال می‌کند .

$$SG_k = h(SID_k \| G_j \| N_i) \quad (9)$$
$$S = h(SG_k \| GID_j) \quad (10)$$
$$B_5 = (R_u \oplus HPW_i) \oplus S \oplus R_y \quad (11)$$
$$B_6 = R_g \oplus S \oplus SID_i \oplus R_y \quad (12)$$
$$B_7 = QID_k^{new} \oplus R_g \oplus R_y \quad (13)$$
$$B_8 = h(R_g \| R_y \| S) \oplus R_z^{new} \quad (14)$$
$$B_9 = h(QID_k \| B_7 \| B_8 \| SG_k \| R_u \oplus HPW_i \| R_g) \quad (15)$$

بعد از اینکه حسگر پیام را دریافت کرد، ابتدا QID_k را بررسی میکند و سپس با محاسبات زیر عدد تصادفی تولید می‌گردد.

$$S = h(SG_k \| GID_j) \quad (16)$$
$$(R_u \oplus HPW_i) = B_5 \oplus S \oplus R_y \quad (17)$$
$$R_g = B_6 \oplus S \oplus SID_i \oplus R_y \quad (18)$$

عدد تصادفی Rsراتولید و مقادیر زیر را حساب می‌کند:

$$R_z^{new} = h(R_g \| R_y \| S) \oplus B_8 \quad (19)$$
$$QID_k^{new} = B_7 \oplus R_g \oplus R_y \quad (20)$$

پس از محاسبه $B_{10} = R_g \oplus S \oplus R_z$, مقادیر $R^{new}_y = h(R_y)$, QID_k^{new}, R_z^{new} , را ذخیره می کند و کلید نشست یعنی $SKs = h(R_u \oplus HPW_i \| R_g \| R_s)$ را تولید و در نهایت با محاسبه B_{11} و B_{12} , پیام زیر را ارسال می‌کند.

$$M_3 = \{B_{10}, B_{11}, B_{12}\}$$
$$B_{11} = h(SG_k \| R_g) \oplus h(R_y) \oplus R_s \quad (21)$$
$$B_{12} = h(B_{10} \| B_{11} \| sk_s \| SID_k \| GID_j \| R_s) \quad (22)$$

به محض رسیدن پیام از طرف حسگر، GW_j با محاسبه $R'_y = h(R_y)$ و $R'_z = R_g \oplus S \oplus B_{10}$ و بررسی برابری مقدارها با مقدارهای ذخیره‌شده در پایگاه داده، $R'_y \oplus h(SG_k \| R_g) \oplus R_s = B_{11}$ و $SK_g = h(R_u \oplus HPW_i \| R_g \| R_s)$ را محاسبه‌می‌کند و درستی B_{12} را بررسی و یک CID_i^{new} برای Ui تولیدکرده و مقادیر QID^{new}_k و R_z^{new} را ذخیره‌می‌کند. به علاوه، R'_y را با R_y و $h(R_x)$ را با R_x جایگزین‌می‌کند. با محاسبه B_{13} ,B_{14} ,B_{15} ,B_{16} ,B_{17}, پیامM_4را برای Uiمی‌فرستد .

$$B_{13} = h(R_x) \| GID_j \| G_j) \oplus h(R_u \| HPW_i) \quad (23)$$
$$B_{14} = h(R_u \| ID_i) \oplus R_g \quad (24)$$
$$B_{15} = h(R_u \| R_g \| HPW_i) \oplus R_s \quad (25)$$
$$B_{16} = h(h(ID_i \| G_j) \| R_s) \oplus CID^{new}_i \quad (26)$$
$$B_{17} = h(sk_g \| ID_i \| B_{13} \| CID^{new}_i) \quad (27)$$

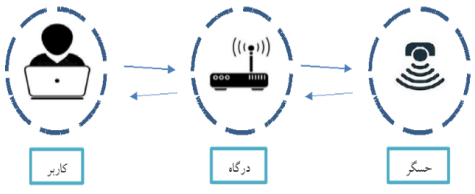
دستگاه موبایل U_i مقادیر R_sR_g و CID_i^{new} را بازیابی‌می‌کند و سپس کلید نشست SK_uرا محاسبه‌می‌کند و پس از بررسی درستی B_{17} مقادیر CID_i^{new} و A^{new}_1را ذخیره‌می‌کند.

اگر این حمله توسط مهاجم صورت‌بگیرد، در آخرین مرحله محاسبات انجام‌شده توسط درگاه مقدار CIDiبا مقدارCID_i^{new} جایگزین نمی‌شود و کاربر در ارتباط بعدی، پیامM_1 را برای درگاه ارسال می‌کند که شامل CID_i^{new}است و درگاه با دریافت آن باید قادر باشد درستی CID_i^{new} را بررسی‌کند که با توجه به توضیحات توانایی اجرا ندارد. همچنین آسیب‌پذیر بودن را باید درنظربگیریم. در این مقاله، فرض بر این است که درگاه کاملاً قابل‌اعتماد است که این خود فرضی بسیار قوی است.در این بخش با تعدیل فرض قابل‌اعتماد بودن درگاه، در جهت کاربردی کردن پروتکل فتوحی و همکاران این حمله درنظر گرفته‌شد.

دلیل نبود مکانیزمی که در آن کاربر بتواند صحت هویت حسگر درخواستی را بررسی‌کند، مهاجم در نقش درگاه بدخواه، بعد ازدریافت پیام M_1محاسبه و SID_k که شناسه حسگر k درخواستی توسط کاربر است می‌تواند خودسرانه با حسگر دیگری مانند SID^* ارتباط برقرارکند و نشست را بین‌کاربر و SID^*_k ایجادکند و چون درآخرین مرحله، کاربر فقط درستی B_{17} را برای بررسی صحت اطلاعات دریافتی درگاه بررسی می‌کند هرگز متوجه تغییر SID_k به SID^*_K نمی شود.

۴. مدل و ساختار پروتکل پیشنهادی

مدل پروتکل پیشنهادی از سه جزء اصلی تشکیل شده‌است که هر سه نهاد از قبل در مرحله ثبت‌نام مجاز بودنشان تأیید شده‌است و می‌توانند برای احراز هویت با هم در ارتباط باشند. هدف کلی این است که هم کاربر و هم حسگر از مجاز بودن یکدیگر مطمئن‌شوند که این امر به وسیله درگاه انجام و تأیید می‌شود. این پروتکل دارای چهار بخش اصلی شامل مرحله ثبت نام، مرحله احرازهویت، مرحله تغییر رمز عبور و مرحله اضافه‌شدن حسگر است.



شکل۱: مدل پروتکل پیشنهادی

با ارسال از کاربر، اگر مهاجم مانع رسیدن پیام M_4به کاربر شود، مقدار ذخیره‌شده در سمت درگاه با مقدار ذخیره‌شده آن در سمت کاربر متفاوت خواهدبود و در ارتباط بعدی درگاه قادر به بازیابی اطلاعات مربوط به CID_iارسالی از سمت کاربر نخواهدبود زیرا در آخرین ارتباط مقدارCID_i در حافظه درگاه به CID_i^{new}تغییرکرده‌است .

جدول ۲: نمادهای مورد استفاده در پروتکل پیشنهادی

نماد	تعریف
U_i , ID_i , PW_i	کاربر iام‌وشناسه‌ورمزعبورش
$R_1, R_2, R_3, R_4, S_1, S_2$	اعدادتصادفی
PID_i	شناسه‌ماسک‌شده‌کاربر iام
TID_i	شناسه‌موقتی‌کاربر iام
D_{ug}	مقدارمحرمانه‌بین‌درگاه‌وکاربر
D_{gs}	مقدارمحرمانه‌بین‌درگاه‌وحسگر
ID_{sn}	شناسه‌حسگر
sk_{us}	کلیدنشست‌بین‌کاربروحسگر
h(.)	تابع‌چکیده‌ساز
$\oplus$	یای‌انحصاری
$\|\|$	الحاق

۱،۴. مرحله ثبت نام پروتکل پیشنهادی

این‌قسمت‌خودشامل‌سه‌مرحله‌است.فرض‌براین‌است‌که‌دراین‌مرحله‌تمامی کانال‌های‌ارتباطی‌امن‌هستندوشنود آن‌ها غیرممکن‌است.

۱-کاربر شناسه ID_i را وارد دستگاه موبایل می‌کند و یک عدد تصادفی R_iرا انتخاب و$PID_i = h(ID_i \| h(R_1))$ را محاسبه و PID_i را برای درگاه ارسال‌می‌کند.

۲-درگاه برای هر کاربر، شناسه موقت TID_i را ایجادکرده و مقادیر $D_{ug} = h(PID_i \| TID_i \| S_1 \| S_2)$ و $ED_{ug} = (D_{ug} \| PID_i) \oplus h(S_1) \oplus h(S_2)$ را محاسبه‌می‌کند و سپس مقادیر ED_{ug} , TID_i رابرای کاربر توسط کانال امن ارسال-می‌کند.

۳-کاربر مقادیر

$A_1 = h(PW_i \| PID_i) \oplus D_{ug}$ و $A_2 = h(PW_i \| ID_i) \oplus h(R_1)$

و همین‌طور $A_3 = h(PW_i \| ID_i \| h(R_1) \| D_{ug})$ رامحاسبه و سپس مقادیر A_1, A_2, A_3, TID_i رادر دستگاه موبایل ذخیره می‌کند. در این مرحله نیز ID_{sn}, D_{gs}توسط درگاه تولیدمی‌شود که به ترتیب شناسه و مقدار محرمانه حسگری هستند که در شبکه ثبت نام می‌کند. این مقادیر توسط کانال امن برای حسگر ارسال و همچنین هم در درگاه و هم در حسگر ذخیره می‌شوند.

۲،۴. مرحله احرازهویت پروتکل پیشنهادی

در این مرحله مقادیر زیر به ترتیب مقایسه‌می‌شود. PWiو IDi توسط کاربر وارد می‌شود:

$h(R_1) = h(PW_i \| ID_i) \oplus A_2$ (28)

$PID_i = h(ID_i \| h(R_1))$ (29)

$D_{ug} = A_1 \oplus h(PW_i \| PID_i)$ (30)

$A'_3 = h(PW_i \| ID_i \| h(R_1) \| D_{ug})$ (31)

و درستی رابطه A'_3 و A_3 را بررسی‌می‌کند. اگر تساوی برقرار بود، دستگاه موبایل عدد تصادفی R_1 را تولید و مقادیرB_1 وB_2 را طبق روابط زیر، محاسبه‌می‌کند و پیام $M_1 = \{B_1 , B_2 \, TID_i\}$ را برای درگاه ارسال‌می‌کند.

$B_1 = h(PID_i \| D_{ug}) \oplus (h(R_2) \| ID_{sn})$ (32)

$B_2 = h(D_{ug} \| h(R_2) \| PID_i \| ID_{sn})$ (33)

درگاه با دریافت پیام M_1، تمامی مقادیر ذخیره‌شده متناظر با TID_iرا از پایگاه داده‌اش بازیابی‌می‌کند و روابط زیر را تشکیل‌می‌دهد

$D_{ug} \| PID_i = ED_{ug} \oplus h(S_1) \oplus h(S_2)$ (34)

$h(R_2) \| ID_{sn} = B1 \oplus h(PID_i \| Dug)$ (35)

$B'2 = h(Dug \| h(R2) \| PIDi \| IDsn)$ (36)

اکنون، درستی رابطه A_3 A'_3 را بررسی‌می‌کند. اگر تساوی برقرار بود، عدد تصادفیR_3 را انتخاب و مقادیرB_3 ,B_4 و sk_{us} را طبق روابط زیر محاسبه و پیام $M_2 = \{B_3, B_4\}$ را برای حسگر می‌فرستد.

$sk_{us} = h(h(R_3) \| (h(R_2) \| ID_{sn})$ (37)

$B_3 = h(D_{gs}) \oplus (h(R_3) \| sk_{us})$ (38)

$B_4 = h(D_{gs} \| h(R_3) \| sk_{us})$ (39)

حسگر با دریافت پیام از طرف درگاه، بلافاصله روابط زیر را محاسبه می‌کند.

$h(R_3) \| sk_{us} = h(D_{gs}) \oplus B_3$ (40)

$B'_4 = h(D_{gs} \| h(R_3) \| sk_{us})$ (41)

درستی رابطه B_4و B'_4را بررسی‌می‌کند. اگر تساوی برقرار بود، عدد تصادفی R_4 را انتخاب و مقادیر B_5 ,B_6 را طبق روابط زیر محاسبه و پیام $M_3 = \{B_5 , B_6\}$ را برای حسگر می‌فرستد.

$B_5 = h(D_{gs} \| ID_{sn}) \oplus h(R_4)$ (42)

$B_6 = h(D_{gs} \| h(R_3) \| h(R_4) \| sk_{us})$ (43)

اگر تساوی برقراربود، مقدارTID^{new}_i تولیدکرده و مقادیر B_7 ,B_8 و D_{ug}^{new} را طبق روابط زیر محاسبه و $M_4 = \{B_7, B_8\}$ برای‌کاربر می‌فرستد.

$h(R_4) = h(D_{gs} \| ID_{sn}) \oplus B_5$ (44)

$B'_6 = h(D_{gs} \| h(R_3) \| h(R_4) \| sk_{us})$ (45)

$D^{new}_{ug} = h(PID_i \| TID^{new} \| S_1 \| S_2)$ (46)

$B7 = h(Dug \| TIDi \| PIDi) \oplus Dnewug \| TIDnewi \| SKus)$ (47)

$B_8 = h(D_{ug}^{new} \| PID_i \| h(R_2) \| sk_{us} \| ID_{sn})$ (48)

اگرتساوی برقرار بود، رابطه B_9 را تشکیل‌می‌دهد، همچنین پیام$M_5 = \{B_9\}$ را برای درگاه می‌فرستد و مقادیرA_1وA_3 را با محاسبه A^{new}_1، A_2^{new} به‌روزرسانی می‌کند.

$D^{new}_{ug} \| TID_i^{new} \| SK_{us} = h(D_{ug} \| TID_i \| PID_i) \oplus B_7$ (49)

$B'_8 = h(D^{new}_{ug} \| PID_i \| h(R_2) \| SK_{us} \| ID_{sn})$ (50)

$B_9 = h(D_{ug} \| TID^{new}_i \| SK_{us} \| h(R_2))$ (51)

$A_1^{new} = h(PW_i \| PID_i) \oplus D^{new}_{ug})$ (52)

$A_3^{new} = h(PW_i \| ID_i \| h(R_1) \| D^{new}_{ug})$ (53)

درگاه با دریافت M_5، مقدار B'_9 را محاسبه و درستی رابطه B_9 B_9 رابررسی می‌کند.

$B_9 = h(D_{ug} \| TID_i^{new} \| SK_{us} \| R_2)$ (54)

$ED^{new}_{ug}=(D^{new}_{ug}||PID_i) \oplus h(S_1) \oplus h(S_2)$ (55)

درنهایت، اگر تساوی برقرا بود، مقادیر ED_{ug}و TID_iرا باTID^{new}_i و $ED_{ug}{}^{new}$ به‌روزرسانی می‌کند و احراز هویت به پایان می‌رسد.

۵.مرحله تغییر رمز عبور

کاربر، IDiوPWi را وارد دستگاه موبایل می‌کند، دستگاه پس از محاسبه روابط زیر، درستی رابطه A_3 , A'_3 را بررسی می‌کند. اگر تساوی برقرار باشد آنگاه کاربر رمز عبور جدید یعنیPW^{new}_i را وارد دستگاه می‌کند.

$h(R_1) = h(PW_i \| ID_i) \oplus A_2$ (56)

$PID_i = h (ID_i \| h(R_1))$ (57)

$D_{ug} = h(PW_i \| PID_i) \oplus A_1$ (58)

$A'_3 = h(PW_i \| ID_i \| h(R_1) \| D_{ug})$ (59)

عبور جدید مقادیر رابطه‌های زیر را محاسبه و مقادیر $A_1\ A_2\ A_3$ را با مقادیر $A_1{}^{new}\ A_2{}^{new}\ A_3{}^{new}$ به‌روزرسانی‌می‌کند .

$A_1{}^{new} = h(PW_i{}^{new} \| PID_i) \oplus D_{ug}$ (60)

$A_2{}^{new} = h(PW_i{}^{new} \| ID_i) \oplus h(R_1)$ (61)

$A_3{}^{new} = h(PW_i{}^{new} \| ID_i \| h(R_1) \| D_{ug})$ (62)

و مرحله تغییر رمز عبور، پایان‌می‌یابد.

۱,۵.مرحله اضافه شدن حسگر

درگاه، مسئول اضافه‌شدن یک حسگر جدید SN^{new}، به شبکه است. درگاه بعد از اضافه‌شدن یک شناسه $(ID_{SN}{}^{new})$ و کلید محرمانه مشترک$(DG_S{}^{new})$ برای هر حسگر جدید، هر دو را در حافظه حسگر جدید و خودش ذخیره‌می‌کند. در انتها، درگاه اعلام‌می‌کند که کاربران می‌توانند با SN^{new} ارتباط برقرارکرده و اطلاعات دریافت‌کنند.

کاربر	درگاه	حسگر
Idiو Pwi را وارد می کند $h(R_3)=h(PW_i \| ID_i) \oplus A_2$ $PID_i=h(ID_i \| h(R_1))$ $D_{ug} = A_1 \oplus h(PW_i \| PID_i)$ $A'_3 =h(PW_i \| ID_i \| h(R_1) \| D_{ug})$ $A'_3 \; A_3$ R_2 انتخاب $B_1=h(PID_i \| D_{ug}) \oplus (h(R_2) \| ID_{sn})$ ارسال پیام $M_1=\{B_1, B_2, TID_i\}$	$D_{ug} \| PID_i = ED_{ug} \oplus h(S_1) \oplus h(S_2)$ $h(R_2) \| ID_{sn} = B_1 \oplus h(PID_i \| D_{ug})$ $B'_2 = h(D_{ug} \| h(R_2) \| PID_i \| ID_{sn})$ $A_3 \; A'_3$ R_3 انتخاب $SK_{us} = h(h(R_3) \| (h(R_2) \| ID_{sn})$ $B_3 =h(D_{gs}) \oplus (h(R_3) \| SK_{us})$ $B_4 =h(D_{gs} \| h(R_3) \| SK_{us})$ ارسال پیام $M_2 =\{B_3, B_4\}$	$h(R3) \| SKus = h(Dgs) \oplus B3$ $B'4 = h(Dgs \| h(R3) \| SKus)$ $B4 \; B'4$ R4 انتخاب $B5 =h(Dgs \| IDsn) \oplus h(R4)$ $B6 =h(Dgs \| h(R3) \| h(R4) \| SKus)$ ارسال پیام $M3 =\{B5, B6\}$
$B'_8 \; B_8$ $D^{new}_{ug} \| TID^{new}_i \| SK_{us}=h(D_{ug} \| TID_i \| PID_i) \oplus B_7$ $B'_8= h(D^{new}_{ug} \| PID_i \| h(R_2) \| SK_{us} \| ID_{sn})$ $B_9=h(D^{new}_{ug} \| TID^{new}_i \| SK_{us} \| h(R_2))$ $A^{new}_1 =h(PW_i \| PID_i) \oplus D^{new}_{ug}$ $A^{new}_3=h(PW_i \| ID_i \| h(R_1) \| D^{new}_{ug})$ $A_1=A_1^{new}$ $A_3=A_3^{new}$ ارسال $m_5 =\{B_9\}$	$B'_6 \; B_6$ TID^{new}_i تولید $h(R_4)=h(D_{gs} \| ID_{sn}) \oplus B_5$ $B'_6=h(D_{gs} \| h(R_3) \| h(R_4) \| SK_{us})$ $D^{new}_{ug} = h(PID_i \| TID^{new}_i \| S_1 \| S_2)$ $B_7 =h(D_{ug} \| TID_i \| PID_i) \; D^{new}_{ug} \| TID^{new}_i \| SK_{us})$ $B_8=h(D^{new}_{ug} \| PID_i \| h(R_2) \| SK_{us} \| ID_{sn})$ ارسال پیام $M_4=\{B_7, B_8\}$	
	$B'_9 \; B_9$ $ED^{new}_{ug} =h(D_{ug} \| TID^{new}_{ug} \| SK_{us} \| h(R_2))$ $TID_i=TID^{new}_i$ $ED_{ug}=ED^{new}_{ug}$	

شکل ۲: مرحله احراز هویت پروتکل پیشنهادی

۲،۵.ویژگی‌های امنیتی پروتکل پیشنهادی

- **امنیت پیشرو**

پروتکل پیشنهادی دارای ویژگی امنیت پیشرو است، زیرا با افشای یک کلید نشست، کلیدهای نشست پیشین فاش‌نمی‌شوند[1,15]. در پروتکل پیشنهادی اگر کلید نشست را به‌دست‌بیاورد و همچنین مهاجم، تمام پیام‌های مبادله‌شده در کانال عمومی را نیز داشته‌باشد، باز هم به دلیل وجود مقادیرتصادفی R_2 و R_3 متفاوت در هر نشست، موفق به بازیابی کلیدهای نشست پیشین نخواهدشد. بنابراین، مهاجم در به‌دست‌آوردن مقدار کلیدهای نشست قبلی و بعدی موفق نخواهد بود [15].

- **غیرقابل ردیابی بودن حسگر**

پروتکل پیشنهادی هم این ویژگی را داراست چراکه شناسه حسگر به‌طور بدیهی درکانال رد و بدل نمی‌شود و در توابع چکیده‌ساز قرار داده می‌شوند.

- **سبک وزن بودن**

برای روند احرازهویت در این پروتکل از عملیات رمزنگاری ساده و اصطلاحاً سبک‌وزن مانند یای انحصاری و تابع چکیده‌ساز استفاده شده - است که در سربار و همچنین سرعت انجام عملیات تأثیر بسزایی دارد و می‌تواند مهر تأییدی برای اثبات سبک‌وزن بودن پروتکل پیشنهادی باشد.

- **تازگی**

به‌دلیل استفاده از مقادیر تصادف‌های که در هر بار اجرای پروتکل تغییر می‌یابند، پروتکل پیشنهادی دارای ویژگی تازگی است که این ویژگی می‌تواند از حمله تکرار یا همان بازپخش جلوگیری‌کند.

۳،۵.بررسی عملکرد پروتکل پیشنهادی در برابر حملات

مقاوم در برابر حمله عدم همزمانی

در هر پیام مبادله‌شده بین کاربر و درگاه، فقط یک پارامتر وجود دارد که متعلق به مرحله آخر ارتباطشان است و ارتباط بین‌درگاه و حسگر هم به این صورت است.

- **مقاوم در برابر حمله افشای کلید نشست**

در پروتکل پیشنهادی، کلید نشست در هر نشست با اعمال تابع چکیده‌ساز بر روی اعداد تصادفی R2, R3و IDsn ایجادمی‌شود که R2توسط کاربر و R3 توسط درگاه ایجادمی‌شود لازم به ذکر است که این مقادیر به‌گونه‌ای امن منتقل‌می‌شوند که مهاجم قادر به بازیابی آن‌ها از طریق کانال عمومی نخواهدبود.

- **مقاوم در برابر حمله جعل درگاه**

اگر مهاجمی بتواند پیام‌های معتبر M2و M4 را تولیدکند، می‌تواند درگاه را جعل‌کند. در پروتکل پیشنهادی، ایجاد پیام معتبر M2 ، مهاجم نیاز به داشتن S1و S2دارد تا بتواند IDsnو R2 را به‌دست‌آورد. همچنین نیاز دارد Dgs را به‌دست‌آورد تا بتواند B3 و B4معتبر را تولید کند. به‌طور مشابه، نیاز به مقادیر S1و S2 دارد و مقادیر IDsn,skusو Dug را محاسبه‌کند تا پیام M4 را تشکیل‌دهد.

- **مقاوم در برابر حمله جعل کاربر**

در پروتکل پیشنهادی، مهاجم باید قادر به تولید یک پیام معتبر $M_1=\{B_1, B_2, TID_i\}$باشد که بتواند این حمله را موفقیت‌آمیز انجام‌دهد، اما مقادیر محرمانه کاربر نظیر PID_iوD_{ug} و همچنین دستگاه موبایل‌کاربر را ندارد در نتیجه این‌حمله عملی نخواهدشد.

- **مقاوم در برابر حمله تسخیر حسگر**

در پروتکل پیشنهادی، اگر اطلاعات یک حسگر تغییر داده‌شود یا تسخیر شود، مهاجم قادرنخواهدبود اطلاعات سایر حسگرها را به‌دست‌آورد بود چون کلیدهای محرمانه مشترک و سایر مقادیر استفاده‌شده، تصادفی و متفاوت هستند.

- **مقاوم در برابر حمله درگاه بدخواه**

درگاه، شناسه حسگر موردنظر، در پیام ارسالی از طرف کاربر را نمی‌تواند تغییردهد، زیرا کاربر، صحت شناسه حسگر را با ارزیابی پیام B8 بررسی‌می‌کند، (PIDi || h(R2) || SKus || IDsn || B'8=h(Dnewug)واگر رابطه B8 B'8 برقرار بود آنگاه مراحل احراز هویت را ادامه‌می‌دهد.

بنابراین، اگردرگاه مقدار ID_{sn} را تغییردهد،کاربر می‌تواند نشست را خاتمه‌دهد ودرگاه قادرنخواهدبود نشستی بین‌کاربر وحسگر موردنظرخود تشکیل‌دهد.

- **مقاوم در برابر حمله ردیابی کاربر**

به‌دلیل استفاده از TIDiجدید در هر نشست، کاربر توسط مهاجم قابل ردیابی نیست.

- **مقاوم در برابر حمله جعل افشای کلید**

دراین‌حمله، مهاجم با داشتن‌کلید محرمانه بلندمدت می‌تواند خودش را به جای یک‌عضومعتبرجابزند، امادرپروتکل پیشنهادی به‌دلیل انتشار از مقادیر امنیتی‌کوتاه‌مدت نظیر R_2,R_3و R_4 که درهرنشست‌تغییر می‌کند،امکانپذیر نخواهدبود.

۴،۵.بررسی سربار محاسباتی پروتکل پیشنهادی

در جدول از لحاظ سربار محاسباتی پروتکل پیشنهادی را با پروتکل‌های مشابه دیگر مقایسه خواهیم‌کرد. در جدول زیر می‌توان به‌وضوح دید که پروتکل پیشنهادی سربار محاسباتی کمتری نسبت به پروتکل فتوحی و هم‌کارانش [1] دارد. همچنین، پروتکل پیشنهادی نسبت به پروتکل‌های [13]و[3] نیاز به زمان بیشتری برای احراز هویت دارد اما از آنجاکه، پروتکل‌های مذکور در مقابل حملات جدول امن نیستند، در نتیجه پروتکل پیشنهادی کاراتر خواهدبود.

با توجه به اینکه زمان مورد نیاز برای محاسبه بر اساسTh پیاده سازی شده در پروتکل فتوحی و همکارانش برابر با۰۰۰۳۲,۰ ثانیه در نظر گرفتیم. در جدول4 را خواهیم‌داشت و مشاهده‌می شود که از

لحاظ زمانی مرحله احراز هویت پروتکل پیشنهادی از پروتکل فتوحی وهمکارانش ۲,۵۶ میلی‌ثانیه سریعتر است.

۵,۵.بررسی سربار مخابراتی پروتکل پیشنهادی

برای محاسبه سربار مخابراتی پروتکل پیشنهادی و مقایسه آن با پروتکل فتوحی‌وهمکارانش، فرض‌می‌کنیم تمامی توابع چکیده‌ساز و شناسه‌های مورد استفاده در پروتکل پیشنهادی 160 بیتی و مقادیر تصادفی128 بیتی هستند در این‌صورت در مقایسه با پروتکل فتوحی‌وهمکارانش، جدول 4 را تشکیل‌داده و به بررسی می‌پردازیم. برای محاسبه سربار مخابراتی، دو کانال ارتباطی درگاه-کاربر و درگاه-حسگر، در مرحله احراز هویت داریم.
درکانال‌ارتباطی‌درگاه-کاربرداریم:

$$2|H|+|H|+|ID|+|H|$$

در نتیجه :

$$2(160)+160+160+160=800$$

بنابراین سربار مخابراتی‌کانال ارتباطی درگاه کاربر برابر است با 800 بیت. درکانال ارتباطی درگاه-حسگر داریم:

جدول ۲: مقایسه سربار محاسباتی پروتکل پیشنهادی با دیگر پروتکل‌ها

نماد		تعریف		
T_h		زمان متوسط برای محاسبه توابع چکیده ساز		
T_e		زمان متوسط برای محاسبه رمزنگاری و رمزگشایی		
T_f		زمان متوسط برای محاسبه تابع تعریف شده در پروتکل خمیسا		
پروتکل	درگاه	حسگر	کاربر	جمع
تورکانووی و همکاران [14]	14^{Th}	$7T_h$	$11T_h$	$32T_h$
فراش و همکاران[13]	$7T_h$	$5T_h$	$7T_h$	$19T_h$
گوپه و همکاران [3]	$9T_h$	$3T_h$	$7T_h$	$19T_h$
خمیسا و همکاران [5]	-	$T_e + T_f + T_h$	$T_e + T_f + T_h$	$(2T_e + T_f + T_h)$
انور قانی و همکاران [4]	$T_e + 3T_h$	T_h	$T_e + 2\ T_h$	$2T_e + 6T_h$
فتوحی و همکاران [1]	$17T_h$	$7T_h$	$10T_h$	$34T_h$
پروتکل پیشنهادی	11^{Th}	$6T_h$	$9T_h$	$26T_h$

جدول ۳ مقایسه زمان محاسبه سربار محاسباتی پروتکل پیشنهادی با پروتکل فتوحی و همکارانش

پروتکل	درگاه	حسگر	کاربر	جمع
فتوحی و همکاران [1]	5.44ms	2.24ms	3.2ms	10.88ms
پروتکل‌پیشنهادی	3.52ms	1.92ms	2.88ms	8.32ms

2|H|+|H|+2|H|+|H|+
|H|+|H|+|H|

در نتیجه:

2(160)+160+2(160)+160+160+160+160=1440

بنابراین سربار مخابراتی‌کانال ارتباطی درگاه-حسگر برابر است با 1440 بیت. با توجه به محاسبات و جدول زیر مشاهده می‌شود که پروتکل پیشنهادی، نسبت به پروتکل فتوحی و همکارانش [1] ، از نظر سربار مخابراتی نیز کاراتر خواهدبود.

جدول ۴:

مقایسه‌سربارمخابراتی‌پروتکل‌پیشنهادی‌باپروتکل‌فتوحی‌وهمکاران

پروتکل	جمع
فتوحی و همکاران [1]	3040bits
پروتکل‌پیشنهادی	2240bits

با توجه به مقایسه انجام‌شده در بالا مشاهده‌شد که پروتکل پیشنهادی۲۴٪ درسربار محاسباتی و۲۶٪ در سربار مخابراتی بهبود یافته‌است.

- **مقاوم در برابر حمله ردیابی:**

دراین‌حمله مهاجم قصد دارد کاربر را ردیابی‌کند اما موفق نخواهدشد چراکه کاربر شناسه یکبار مصرف داشته و در هر نشست به‌روزرسانی‌می‌شود.

- **مقاوم در برابر حمله جعل هویت:**

در این‌حمله مهاجم قصد دارد خود را به جای یکی از طرفین ارتباط جازده و طرف مقابل را فریب‌دهد که در پروتکل پیشنهادی ممکن نیست.

- **مقاوم در برابر حمله تکرار:**

در این حمله مهاجم از طریق ارسال مجدد پیام‌های معتبر شنودشده خواهان احراز هویت غیرمجاز است، که نمی‌تواند موفق شود زیرا همه پیام‌ها دارای مهر زمانی هستند.

بنابراین با توجه به جدول بالا نتیجه‌می‌گیریم که تنها پروتکل پیشنهادی در برابر حملات مذکور امن است.

- **مقاوم در برابر حمله درگاه بدخواه:**

در این حمله خود درگاه اقدام به اعمال مخرب می‌کند و نشستی‌که مدّنظر کاربر نیست تشکیل می‌دهد.

- **مقاوم در برابر حمله عدم همزمانی:**

در این حمله، نهادهای موجود در شبکه نمی‌توانند مقادیر خود را بطور همزمان با یکدیگر به‌روزرسانی کنند و نهادها در مقدار پارامترها با

یکدیگر دچار ناهماهنگی می‌شوند. مقایسه مقاوم‌بودن پروتکل پیشنهادی و دیگر پروتکل‌های سبک‌وزن در برابر حملات در جدول ۵ آورده شده-است.

۶. نتیجه‌گیری

در این تحقیق پروتکلی پیشنهاد شد که بدون استفاده از کارت هوشمند الزامات امنیتی کافی را برای کاربران به ارمغان بیاورد. همچنین کاربران غیرمجاز از راه‌هایی مانند حملات تکرار، جعل‌هویت، عدم همزمانی بین حسگر و کاربر، قابلیت ردیابی و تسخیر حسگر نتوانند به مراحل پروتکل دسترسی یابند، همچنین پروتکل پیشنهادی در مقایسه با پروتکل قبلی مقایسه‌شد و۲۴٪در سربار محاسباتی و۲۶٪ در سربار مخابراتی بهبود داشته‌است. بنا بر نتایج فوق پروتکل پیشنهادی در این تحقیق می‌تواند در زمینه اینترنت‌اشیاء و شبکه های‌حسگر بی‌سیم بسیار کارا باشد و مورد استفاده قرارگیرد.

جدول ۵: مقایسه پروتکل پیشنهادی و دیگر پروتکل‌ها

پروتکل	مقاوم بودن در برابر حملات				
	ردیابی	جعل هویت	عدم همزمانی	تکرار	درگاه بدخواه
تورکانووی و همکاران [14]	✓	✓	✗	✓	✗
گوپه و همکاران [3]	✓	✗	✗	✗	✗
خمیسا و همکاران [5]	✓	✗	✗	✗	✗
انور قانی و همکاران [4]	✓	✓	✗	✗	✗
فتوحی و همکاران [7]	✓	✓	✗	✓	✗
پروتکل پیشنهادی	✓	✓	✓	✓	✓

References

[1] Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks, 177, 107333.

[2] Porambage ،P. ،Schmitt ،C. ،Kumar ،P. ،Gurtov ،A. ،& Ylianttila ،M. (2014). PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. International Journal of Distributed Sensor Networks ، ۱۰(7)۳۵۷۴۳۰

[3] Gope ،P. ،& Hwang ،T. (2016). A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on industrial electronics۶۳ ،(11)-۷۱۲۴ ، ۷۱۳۲.

[4] Ghani ،A. ،Mansoor ،K. ،Mehmood ،S. ،Chaudhry ،S. A. ، Rahman ،A. U. ،& Najmus Saqib ،M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. International Journal of Communication Systems۳۲ ،(16) ، e4139.

[5] Khemissa ،H. ،Tandjaoui ،D. ،& Bouzefrane ،S. (2017 ،June). An ultra-lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things. In International conference on mobile ،secure ،and programmable networking (pp. 49-62). Springer ،Cham

[6] abbasi, N., & Karimi, S. (2022). Dynamic Migration of SDN-based Switches to Distribute Control Layer Load and Increase Efficiency Using Ryu Controller. Intelligent Multimedia Processing and Communication Systems (IMPCS), 3(4), 15-27.

[7] Zand, M., & Tahghighi Sharabian, M. (2020). Improvement of IOT Security in ZigBee Network Using AES256 Algorithm. Intelligent Multimedia Processing and Communication Systems (IMPCS), 1(2), 51-59.

[8] Mousavi, S.H., Safaeian, M., Ahmadi G.,A.H. (2022). A New Method in the Security of Encryption Systems by Unbalanced Gates. . Intelligent Multimedia Processing and Communication Systems (IMPCS), 3(2),39-50.

[9] Derakhshan P., G. Dadashzadeh, F. Razzazi,S. M. Razavizadeh. (2011) .Minimum power transmission design for cognitive radio networks in non-stationary environment. IEICE Journal Electronic Exp., Vol.8, No. 3.

[10] Derakhshan P., G. Dadashzadeh, F. Razzazi,S. M. Razavizadeh. (2011). Bio-inspired distributed beamforming for cognitive radio networks in non-stationary environment. IEICE Journal Electronic Exp., Vol.8, No. 6.

[11] Derakhshan P. (2011). Modified Spectrum Sensing and Awareness in Wireless Radio Networks," Int. Review on

Modeling and Simulations, I.RE.MO.S. Journal, pp. 718-722, Vol. 4. No. 2.

[12] Derakhshan P., G. Dadashzadeh, F. Razzazi,S. M. Razavizadeh. (2013). Power and Time Slot Allocation in Cognitive Relay Networks Using Particle Swarm Optimization. Hindawi Journal.

[13] 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.

[14] 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

[15] Bonyadi A., Rajabzadeh Asaar M., Derakhshan B. P.(2023). Security Analysis of a Lightweight Multifactor Authentication Scheme for Internet of Things Applications, 19th Conf. Inf. Tech. Compt. Comm. ITCT, June.