



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

Maryam Rajabzadeh Asaar<sup>1\*</sup>, Pouya Derakhshan Barjoei<sup>2</sup>

1. Assistant Professor, Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran. (*Corresponding Author*) [asaar@srbiau.ac.ir](mailto: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](mailto: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.



انجمن علمی تجارت الکترونیکی ایران

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند

Intelligent Multimedia Processing and Communication Systems (IMPCS)



واحد رنجان

## ارائه پروتکل نوین احراز هویت گمنام سبک‌وزن با امنیت پیشرو در شبکه‌های حسگر بی‌سیم مبتنی بر اینترنت اشیا

دوره چهارم، پاییز ۱۴۰۲  
شماره سوم، صص: ۱-۱۳

تاریخ دریافت: ۱۱/۰۴/۱۴۰۲  
تاریخ پذیرش: ۲۱/۰۵/۱۴۰۲

مریم رجب زاده عصار<sup>۱\*</sup>، پویا درخشان بر جوئی<sup>۲</sup>

۱. استادیار، گروه مهندسی برق، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول) [asaar@srbiau.ac.ir](mailto: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، استفاده کرده‌ایم. در این مقاله نشان دادیم که برخی از جنبه‌های امنیتی و محاسباتی پروتکل پیشنهادی نسبت به پروتکل‌های قبلی برتری‌هایی دارد. با بررسی و تحلیل پروتکل پیشنهادی نشان داده شد که مطابق ادعای گفته شده، 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 ارائه شده، نشان دادیم که 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. در نهایت، پروتکل پیشنهادی را با پروتکل‌های مشابه مقایسه کرده و نشان دادیم که پروتکل پیشنهادی ۲۴٪ در سربار محاسباتی و ۲۶٪ در سربار مخابراتی بهبود عملکرد را ایجاد کرده‌است.

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

## ۱. مقدمه

اینترنت اشیاء شامل یک شبکه به هم پیوسته است که انواع ارتباط را ممکن می‌سازد و نقش حساسی در توسعه سرویس‌های هوشمند برای پشتیبانی و بهبود فعالیت‌های افراد و جامعه دارد. یکی از مهم‌ترین دغدغه‌های کسانی که از شبکه‌های بی‌سیم استفاده می‌کنند 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 از طرح‌هایی که با رویکرد حفظ امنیت اطلاعات، احراز هویت را انجام می‌دهند، بررسی شده است. با تحلیل و بررسی این طرح‌ها خواهیم دید که کدام ویژگی‌ها برای شبکه تهدید تلقی می‌شود. ویژگی‌هایی که می‌توانند پروتکل پیشنهادی ما را به هدف نزدیک‌تر کنند، شامل حفظ گمنامی و همچنین پوشش‌دهی ویژگی امنیت پیشرو، با استفاده از ساده‌ترین و به اصطلاح 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 در نهایت، پروتکلی ارائه کردیم که علاوه بر ویژگی‌های مذکور، ویژگی احراز هویت دوطرفه را نیز داراست. این پروتکل در برابر حملات، امن است و در نهایت پروتکل پیشنهادی را با پروتکل فتوحی و همکاران مقایسه کرده و نشان دادیم که پروتکل پیشنهادی ۲۴٪ در سربار محاسباتی و ۲۶٪ در سربار مخابراتی بهبود ایجاد می‌کند.

## ۲. کارهای مرتبط

در این قسمت برخی از پروتکل‌هایی که به منظور احراز هویت در شبکه‌های حسگر بی‌سیم و اینترنت اشیاء ارائه شدند را بررسی می‌کنیم. پروتکل‌های احراز هویت اخیر در زمینه اینترنت اشیاء می‌توانند به دو دسته تقسیم شوند: احراز هویت با صدور گواهینامه و احراز هویت بدون گواهینامه. در دسته اول، احراز هویت با استفاده از گواهینامه‌های دیجیتال است. پورامیگ و همکاران [2] پروتکلی برای احراز هویت و تشکیل کلید نشست برای شبکه‌های حسگر بی‌سیم در اینترنت اشیاء ارائه دادند که شامل دو مرحله ثبت نام و احراز هویت است که در مرحله ثبت نام به هر کاربر و دستگاهی گواهینامه اختصاص داده می‌شود و در مرحله احراز هویت، کاربر سیستم برای گره حسگر احراز هویت شده و می‌تواند از اطلاعات حسگر استفاده کند این پروتکل به دلیل استفاده از خم‌های بیضوی از لحاظ مصرف انرژی بسیار مناسب است و با توجه به اینکه ادعا شده است که این پروتکل در مقابل برخی حملات امن است، اما ایرادهایی نیز به آن وارد است. به عنوان نمونه در این پروتکل، هویت کلید عمومی نهادی که گواهینامه‌ها را صادر می‌کند تضمین نشده است و این یعنی هر شخصی می‌تواند با داشتن کلید بین حسگر و نهاد صدور گواهینامه‌ها، به راحتی خود را به عنوان این نهاد معرفی و جعل کند. گویه

و همکاران [3] پروتکل سبک وزنی برای احراز هویت ارائه کردند که این پروتکل بر مبنای کلید متقارن در شبکه‌های حسگر بی‌سیم بود. ادعای نویسندگان پروتکل این بود که این طرح در برابر حملاتی همچون سرقت کارت امن است و همچنین تضمین امنیت پیشرو از ویژگی‌های این طرح بود که در سال ۲۰۱۹ توسط انورقانی و همکاران [4] نشان داده شد که ادعای گویه برای برقراری امنیت و حفظ اطلاعات شخصی چندان معتبر نیست.

در دسته دوم، پروتکل‌هایی قرار داده شدند که به گواهینامه نیازی ندارند. این دسته از پروتکل‌ها تنها از عملگرهای ساده رمزنگاری مانند عمل الحاق، تابع چکیده‌ساز استفاده می‌کنند و به صرفه‌جویی در مصرف انرژی معروفند. خمیسا و همکاران [5] پروتکل احراز هویت فوق سبک-وزنی ارائه دادند که از امنیت بالا و سطح مصرف انرژی پایینی برخوردار است. می‌توان گفت این پروتکل کامل شده پروتکلی است که توسط خودشان ارائه شده بود. امنیت این پروتکل منوط بر یک مقدار خصوصی است که اگر مهاجم موفق شود این پارامتر را به دست آورد به راحتی می‌تواند به جای کاربر مجاز با گره‌های حسگر ارتباط برقرار کند که این موضوع می‌تواند نقطه ضعفی برای این پروتکل تلقی شود. این مقدار می‌تواند توسط حالتی حدس زده شود و یا حتی بازیابی شود اما باید راهی باشد که حتی اگر این مقدار در دسترس مهاجمان قرار گرفت، نتوانند خللی به امنیت پروتکل وارد کنند. در [6] کریمی و همکاران یک استراتژی متعادل سازی بار در طرح پیشنهادی مبتنی بر زمان پاسخ برای کنترل‌کننده‌های سوئیچ‌های مبتنی بر نرم افزار متعدد پیشنهاد دادند که در مصرف انرژی تأثیرگذار بود. زند و همکاران در [7] ارتقای امنیت اینترنت اشیاء در شبکه زیگی را با الگوریتم پیشنهادی بررسی کردند. در [8] موسوی و همکاران طرح جدیدی برای مقاوم سازی الگوریتم‌های رمزنگاری و مقابله با حملات را نشان دادند. در [9-12] درخشان و همکاران بررسی مصرف انرژی و نوع انتقال داده را در شبکه‌های غیرایستاد بررسی و تداخل و حملات کاربر غیرمجاز را بررسی و مطالعه کردند.

## ۳. مروری بر پروتکل فتوحی و همکارانش [1]

یک پروتکل احراز هویت سبک‌وزن دوفاکتوره که دارای ویژگی‌های امنیت پیشرو است، ارائه شده که همچنین در برابر به دست آوردن یا جعل کلید توسط مهاجم و همچنین ردیابی، مقاوم است. پروتکل فتوحی و همکارانش [1]، از ROR.OPNET و Proverif برای اثبات امنیت، استفاده شده و کارایی پروتکل با پروتکل‌های پیشین مقایسه شده است. برای تحلیل این پروتکل سه فرضیه در نظر گرفته شده است:

فرضیه اول: تمام پیام‌هایی که در کانال عمومی رد و بدل می‌شوند می‌توانند توسط مهاجم استراق سمع، 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.

$R_z$  را در حسگر قرار می‌دهد و مقادیر  $SID_k, QID_k, N_1, R_y$ ، مورد نظر قرار می‌گیرد.

۲- مرحله ثبت نام کاربر: ثبت نام کاربر در درگاه طی سه مرحله اتفاق می‌افتد:

۱- کاربر  $U_i$  شناسه  $ID_i$ ، رمز عبور  $PW_i$  و مقدار تصادفی  $R_0$  را انتخاب کرده و مقدار رمز عبور ماسک شده را بصورت  $HPW_i = h(PW_i || R_0)$  محاسبه می‌کند و  $ID_i$  و  $HPW_i$  را توسط کانال امن برای  $GW_j$  می‌فرستد.

۲- در صورتی که  $ID_i$  از قبل در درگاه ثبت نام نشده باشد،  $GW_j$  برای  $U_i$  یک شناسه تصادفی  $CID_i$  و عدد تصادفی  $R_x$  تخصیص داده و همراه با مقادیر  $ID_i$  و  $HPW_i$  ذخیره و سپس  $A_1$  و  $A_2$  را با استفاده از روابط (2-3)، (1-3) محاسبه و مقادیر  $A_1, A_2, CID_i, GID_j$  را برای  $U_i$  در یک کانال امن ارسال می‌کند.

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

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

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

### ۳.۳. مرحله احراز هویت

پس از مرحله ثبت نام، کاربر  $U_i$ ، حسگر مورد نظرش را انتخاب و  $ID_i$  و  $PW_i$  را وارد دستگاه موبایل کرده، مقادیر  $R_0 = h(ID_i || PW_i) \oplus A_3$  و  $HPW_i = h(PW_i || R_0)$  محاسبه و پس از آن با استفاده عدد تصادفی  $R_u$  تولیدی و  $SID_k$  که کاربر اعلام کرده بود مقادیر  $B_1, B_2, B_3, B_4$  از روابط زیر تشکیل و پیام  $M_1 = \{B_4, B_3, B_2, GID_i, CID_i\}$  برای درگاه ارسال می‌شود.

$$B_1 = A_1 \oplus HPW_i \quad (3)$$

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

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

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

درستی  $CID_i$  و  $GID_j$  توسط  $GW_j$  بررسی شده و  $ID_i, R_x$  و  $HPW_i$  را در صورت وجود، از پایگاه داده استخراج می‌کند. سپس روابط (7)، (8) را محاسبه و دو عدد تصادفی  $R_g$  و  $R_z^{new}$  انتخاب کرده و پس از آن،  $GW_j$  با محاسبه رابطه

$$B_3 \oplus h(ID_i || R_u) \quad (7)$$

از پایگاه داده استخراج کرده و مقدار تصادفی  $QID_k^{new}$  را برای حسگر تولید می‌کند.

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

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

فرضیه دوم: با احتمال اینکه ممکن است دستگاه موبایل کاربر دزدیده شود، فرض می‌کنیم مهاجم می‌تواند اطلاعات داخل دستگاه موبایل را بازیابی کند.

فرضیه سوم: از آنجاکه مقادیر شناسه و رمز عبور کاربران توسط خودشان انتخاب می‌شود می‌تواند در زمان چند جمله‌ای، توسط مهاجم قابل حدس زدن باشد، همچنین مقادیر و دنباله‌های تصادفی، کلیدهای خصوصی و کلید نشست نمی‌توانند توسط مهاجم حدس زده شوند. این پروتکل دارای چهار مرحله اصلی است:

۱. مقداردهی اولیه ۲. ثبت نام ۳. احراز هویت ۴. تغییر رمز عبور

جدول ۱ نمادهای مورد استفاده در پروتکل فتوحی و همکارانش

نماد	تعریف
$U_i, ID_i, PW_i$	کاربر نام و شناسه و رمز عبورش
$GID_j, G_j$	شناسه و کلید خصوصی درگاه نام $(GW_j)$
$SN_k, SID_k$	حسگر نام و شناسه اش
$N_1$	تعداد مجموعه حسگرها
$SG_k$	کلید خصوصی بین حسگر و درگاه
$sk_u, sk_g, sk_s$	کلیدهای نشست تولید شده توسط کاربر، درگاه و حسگر
$M_i$	پیام‌های احراز هویت
$CID_i, QID_k$	دنباله‌های تصادفی موقتی کاربر و حسگر
$R_u, R_g, R_s, R_x, R_y, R_z$	عددهای تصادفی موقتی
$h(\cdot)$	تابع چکیده ساز
$\oplus$	یای انحصاری
$\parallel$	الحاق

### ۱.۳. مرحله مقداردهی اولیه

در این مرحله فرض شده که هر درگاه یک نهاد قابل اعتماد است که با  $GID_j$  شناخته شده و تمامی پیام‌ها بوسیله این درگاه‌ها انتقال می‌یابند. هر درگاه یک کلید خصوصی  $G_j$  نیز تولید می‌کند.

### ۲.۳. مرحله ثبت نام

این مرحله را به دو بخش تقسیم می‌کنیم:

۱- مرحله ثبت نام حسگر: هر حسگر  $SN_k$  دارای یک شناسه  $SID_k$  است. به علاوه هر مجموعه‌ای از حسگر متعلق به شبکه‌ای با شناسه خاص خودش  $N_1$  است. هر حسگر با درگاه به طور مستقیم ارتباط می‌گیرد و دارای یک کلید خصوصی مشترک به نام  $SG_k$  هستند:  $SG_k = h(SID_k || G_j || N_1)$  سپس  $GW_j$  دو عدد تصادفی  $R_y$  و  $R_z$  و دنباله تصادفی  $QID_k$  را انتخاب کرده و مقادیر  $R_y, GID_j, R_z, SID_k, SG_k, QID_k$

در ادامه،  $GW_j$  مقادیر  $B_5, B_6, B_7, B_8, S, B_9$  را طبق روابط

زیر تشکیل داده و پیام

$$M_2 = \{ QID_k, B_5, B_6, B_7, B_8, B_9 \}$$

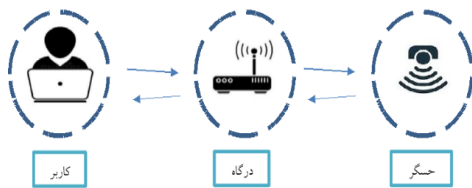
می کند .

دستگاه موبایل  $U_i$  مقادیر  $R_g$  و  $R_s$  و  $CID_i^{new}$  را بازیابی می کند و سپس کلید نشست  $SK_u$  را محاسبه می کند و پس از بررسی درستی  $B_{17}$  مقادیر  $CID_i^{new}$  و  $A_i^{new}$  را ذخیره می کند.

اگر این حمله توسط مهاجم صورت بگیرد، در آخرین مرحله محاسبات انجام شده توسط درگاه مقدار  $CID_i$  با مقدار  $CID_i^{new}$  جایگزین نمی شود و کاربر در ارتباط بعدی، پیام  $M_1$  را برای درگاه ارسال می کند که شامل  $CID_i^{new}$  است و درگاه با دریافت آن باید قادر باشد درستی  $CID_i^{new}$  را بررسی کند که با توجه به توضیحات توانایی اجرا ندارد. همچنین آسیب پذیر بودن را باید در نظر بگیریم. در این مقاله، فرض بر این است که درگاه کاملاً قابل اعتماد است که این خود فرضی بسیار قوی است. در این بخش با تعدیل فرض قابل اعتماد بودن درگاه، در جهت کاربردی کردن پروتکل فتوحی و همکاران این حمله در نظر گرفته شد. دلیل نبود مکانیزمی که در آن کاربر بتواند صحت هویت حسگر درخواستی را بررسی کند، مهاجم در نقش درگاه بدخواه، بعد از دریافت پیام  $M_1$  محاسبه  $SK_k$  که شناسه حسگر  $k$  درخواستی توسط کاربر است می تواند خودسرانه با حسگر دیگری مانند  $SID^*$  ارتباط برقرار کند و نشست را بین کاربر و  $SID^*$  ایجاد کند و چون در آخرین مرحله، کاربر فقط درستی  $B_{17}$  را برای بررسی صحت اطلاعات دریافتی درگاه بررسی می کند هرگز متوجه تغییر  $SID_k$  به  $SID^*$  نمی شود.

#### ۴. مدل و ساختار پروتکل پیشنهادی

مدل پروتکل پیشنهادی از سه جزء اصلی تشکیل شده است که هر سه نهاد از قبل در مرحله ثبت نام مجاز بودنشان تأیید شده است و می توانند برای احراز هویت با هم در ارتباط باشند. هدف کلی این است که هم کاربر و هم حسگر از مجاز بودن یکدیگر مطمئن شوند که این امر به وسیله درگاه انجام و تأیید می شود. این پروتکل دارای چهار بخش اصلی شامل مرحله ثبت نام، مرحله احراز هویت، مرحله تغییر رمز عبور و مرحله اضافه شدن حسگر است.



شکل ۱: مدل پروتکل پیشنهادی

با ارسال از کاربر، اگر مهاجم مانع رسیدن پیام  $M_4$  به کاربر شود، مقدار ذخیره شده در سمت درگاه با مقدار ذخیره شده آن در سمت کاربر متفاوت خواهد بود و در ارتباط بعدی درگاه قادر به بازیابی اطلاعات مربوط به  $CID_i$  ارسالی از سمت کاربر نخواهد بود زیرا در آخرین ارتباط مقدار  $CID_i$  در حافظه درگاه به  $CID_i^{new}$  تغییر کرده است.

$$SG_k = h(SID_k \parallel G_j \parallel N_i) \quad (9)$$

$$S = h(SG_k \parallel GID_j) \quad (10)$$

$$B_5 = (R_u \oplus HPW_i) \oplus S \oplus R_y \quad (11)$$

$$B_6 = R_g \oplus S \oplus SID_i \oplus R_y \quad (12)$$

$$B_7 = QID_k^{new} \oplus R_g \oplus R_y \quad (13)$$

$$B_8 = h(R_g \parallel R_y \parallel S) \oplus R_z^{new} \quad (14)$$

$$B_9 = h(QID_k \parallel B_7 \parallel B_8 \parallel SG_k \parallel R_u \oplus HPW_i \parallel R_g) \quad (15)$$

بعد از اینکه حسگر پیام را دریافت کرد، ابتدا  $QID_k$  را بررسی میکند

و سپس با محاسبات زیر عدد تصادفی تولید می گردد.

$$S = h(SG_k \parallel GID_j) \quad (16)$$

$$(R_u \oplus HPW_i) = B_5 \oplus S \oplus R_y \quad (17)$$

$$R_g = B_6 \oplus S \oplus SID_i \oplus R_y \quad (18)$$

عدد تصادفی  $R_s$  را تولید و مقادیر زیر را حساب می کند:

$$R_z^{new} = h(R_g \parallel R_y \parallel S) \oplus B_8 \quad (19)$$

$$QID_k^{new} = B_7 \oplus R_g \oplus R_y \quad (20)$$

پس از محاسبه  $B_{10} = R_g \oplus S \oplus R_z$  ، مقادیر  $R_y^{new} = h(R_y)$  ،

$SK_s$  ،  $R_z^{new}$  ،  $QID_k^{new}$  را ذخیره می کند و کلید نشست یعنی

$$B_{11} = h(R_u \oplus HPW_i \parallel R_g \parallel R_s) \quad (21)$$

$B_{12}$  ، پیام زیر را ارسال می کند.

$$M_3 = \{ B_{10}, B_{11}, B_{12} \}$$

$$B_{11} = h(SG_k \parallel R_g) \oplus h(R_y) \oplus R_s \quad (21)$$

$$B_{12} = h(B_{10} \parallel B_{11} \parallel sk_s \parallel SID_k \parallel GID_j \parallel R_s) \quad (22)$$

به محض رسیدن پیام از طرف حسگر،  $GW_j$  با محاسبه

$$R'_y = h(R_y) \quad \text{و} \quad R'_z = R_g \oplus S \oplus B_{10}$$

و بررسی برابری مقادیر با

مقادیر ذخیره شده در پایگاه داده،  $R'_y = h(R_g \parallel SG_k) \oplus R_s$  و

$$B_{11} = h(R_u \oplus HPW_i \parallel R_g \parallel R_s) \quad \text{و} \quad SK_g = h(R_u \oplus HPW_i \parallel R_g \parallel R_s)$$

را محاسبه می کند و درستی  $B_{12}$  را بررسی و یک  $CID_i^{new}$  برای  $U_i$  تولید کرده و مقادیر

$QID_k^{new}$  و  $R_z^{new}$  را ذخیره می کند. به علاوه،  $R'_y$  را با  $R_y$  و

$h(R_x)$  را با  $R_x$  جایگزین می کند. با محاسبه  $B_{13}, B_{14}, B_{15}, B_{16}$

$B_{17}$ ، پیام  $M_4$  را برای  $U_i$  می فرستد .

$$B_{13} = h(R_x \parallel GID_j \parallel G_j) \oplus h(R_u \parallel HPW_i) \quad (23)$$

$$B_{14} = h(R_u \parallel ID_i) \oplus R_g \quad (24)$$

$$B_{15} = h(R_u \parallel R_g \parallel HPW_i) \oplus R_s \quad (25)$$

$$B_{16} = h(h(ID_i \parallel G_j) \parallel R_s) \oplus CID_i^{new} \quad (26)$$

$$B_{17} = h(sk_g \parallel ID_i \parallel B_{13} \parallel CID_i^{new}) \quad (27)$$

روابط زیر، محاسبه می‌کند و پیام  $M_1 = \{B_1, B_2, TID_i\}$  را برای درگاه ارسال می‌کند.

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

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

درگاه با دریافت پیام  $M_1$ ، تمامی مقادیر ذخیره شده متناظر با  $TID_i$  را از پایگاه داده‌اش بازیابی می‌کند و روابط زیر را تشکیل می‌دهد

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

$$h(R_2) \parallel ID_{sn} = B_1 \oplus h(PID_i \parallel D_{ug}) \quad (35)$$

$$B'_2 = h(D_{ug} \parallel h(R_2) \parallel PID_i \parallel ID_{sn}) \quad (36)$$

اکنون، درستی رابطه  $A_3, A'_3$  را بررسی می‌کند. اگر تساوی برقرار بود، عدد تصادفی  $R_3$  را انتخاب و مقادیر  $B_3, B_4$  و  $sk_{us}$  را طبق روابط زیر محاسبه و پیام  $M_2 = \{B_3, B_4\}$  را برای حسگر می‌فرستد.

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

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

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

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

محاسبه می‌کند.

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

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

درستی رابطه  $B_4$  و  $B'_4$  را بررسی می‌کند. 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.

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

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

اگر تساوی برقرار بود، مقدار  $TID_i^{new}$  تولید کرده و مقادیر  $B_7, B_8$  و  $B$  و  $D_{ug}^{new}$  را طبق روابط زیر محاسبه و  $M_4 = \{B_7, B_8\}$  را برای کاربر

می‌فرستد.

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

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

$$D_{ug}^{new} = h(PID_i \parallel TID_i^{new} \parallel S_1 \parallel S_2) \quad (46)$$

$$B_7 = h(D_{ug} \parallel TID_i \parallel PID_i) \oplus D_{ug}^{new} \parallel TID_i^{new} \parallel SK_{us} \quad (47)$$

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

اگر تساوی برقرار بود، رابطه  $B_9$  را تشکیل می‌دهد، همچنین

پیام  $M_5 = \{B_9\}$  را برای درگاه می‌فرستد و مقادیر  $A_1, A_3$  را با محاسبه  $A_2^{new}, A_1^{new}$  به روزرسانی می‌کند.

$$D_{ug}^{new} \parallel TID_i^{new} \parallel SK_{us} = h(D_{ug} \parallel TID_i \parallel PID_i) \oplus B_7 \quad (49)$$

$$B'_8 = h(D_{ug}^{new} \parallel PID_i \parallel h(R_2) \parallel SK_{us} \parallel ID_{sn}) \quad (50)$$

$$B_9 = h(D_{ug} \parallel TID_i^{new} \parallel SK_{us} \parallel h(R_2)) \quad (51)$$

$$A_1^{new} = h(PW_i \parallel PID_i) \oplus D_{ug}^{new} \quad (52)$$

$$A_3^{new} = h(PW_i \parallel ID_i \parallel h(R_1) \parallel D_{ug}^{new}) \quad (53)$$

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

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

جدول ۲: نمادهای مورد استفاده در پروتکل پیشنهادی

نماد	تعریف
$U_i, ID_i, PW_i$	کاربر نام و شناسه و رمز عبور
$R_1, R_2, R_3, R_4, S_1, S_2$	اعداد تصادفی
$PID_i$	شناسه ماسک شده کاربر نام
$TID_i$	شناسه موقتی کاربر نام
$D_{ug}$	مقدار محرمانه بین درگاه و کاربر
$D_{gs}$	مقدار محرمانه بین درگاه و حسگر
$ID_{sn}$	شناسه حسگر
$sk_{us}$	کلید نشست بین کاربر و حسگر
$h(.)$	تابع چکیده ساز
$\oplus$	یای انحصاری
$\parallel$	الحاق

#### ۱.۴. مرحله ثبت نام پروتکل پیشنهادی

این قسمت خود شامل سه مرحله است. فرض بر این است که در این مرحله تمامی کانال‌های ارتباطی امن هستند و شنود آن‌ها غیرممکن است.

۱- کاربر شناسه  $ID_i$  را وارد دستگاه موبایل می‌کند و یک عدد تصادفی  $R_i$  را انتخاب و  $PID_i = h(ID_i \parallel h(R_i))$  را محاسبه و  $PID_i$  را برای درگاه ارسال می‌کند.

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

۳- کاربر مقادیر

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

و همین‌طور  $A_3 = h(PW_i \parallel ID_i \parallel h(R_1) \parallel D_{ug})$  را محاسبه و سپس مقادیر  $A_1, A_2, A_3, TID_i$  را در دستگاه موبایل ذخیره می‌کند. در این مرحله نیز  $ID_{sn}, D_{gs}$  توسط درگاه تولید می‌شود 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 احراز هویت پروتکل پیشنهادی

در این مرحله مقادیر زیر به ترتیب مقایسه می‌شود.  $ID_i$  و  $PW_i$  توسط کاربر وارد می‌شود:

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

$$PID_i = h(ID_i \parallel h(R_1)) \quad (29)$$

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

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

و درستی رابطه  $A_3$  و  $A'_3$  را بررسی می‌کند. اگر تساوی برقرار بود،

دستگاه موبایل عدد تصادفی  $R_1$  را تولید و مقادیر  $B_1$  و  $B_2$  را طبق

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

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

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

و مرحله تغییر رمز عبور، پایان می‌یابد.

#### ۱.۵. مرحله اضافه شدن حسگر

درگاه، مسئول اضافه شدن یک حسگر جدید  $SN^{new}$ ، به شبکه است. درگاه بعد از اضافه شدن 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 ذخیره می‌کند. در انتها، درگاه اعلام می‌کند که کاربران می‌توانند با  $SN^{new}$  ارتباط برقرار کرده و اطلاعات دریافت کنند.

$$ED_{ug}^{new} = (D_{ug}^{new} \parallel PID_i) \oplus h(S_1) \oplus h(S_2) \quad (55)$$

در نهایت، اگر تساوی برقرار بود، مقادیر  $ED_{ug}$  و  $TID_i$  را با  $TID_i^{new}$  و  $ED_{ug}^{new}$  به روزرسانی می‌کند و احراز هویت به پایان می‌رسد.

#### ۵. مرحله تغییر رمز عبور

کاربر،  $PW_i$  و  $ID_i$  را وارد دستگاه موبایل می‌کند، دستگاه پس از محاسبه روابط زیر، درستی رابطه  $A_3$ ،  $A_3'$ ،  $A_3$  را بررسی می‌کند. اگر تساوی برقرار باشد آنگاه کاربر رمز عبور جدید یعنی  $PW_i^{new}$  را وارد دستگاه می‌کند.

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

$$PID_i = h(ID_i \parallel h(R_1)) \quad (57)$$

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

$$A_3' = h(PW_i \parallel ID_i \parallel h(R_1) \parallel D_{ug}) \quad (59)$$

عبور جدید مقادیر رابطه‌های زیر را محاسبه و مقادیر  $A_1$   $A_2$   $A_3$

را با مقادیر  $A_1^{new}$   $A_2^{new}$   $A_3^{new}$  به روزرسانی می‌کند.

کاربر	درگاه	حسگر
<p> <math>I_d</math> و <math>P_w</math> را وارد می‌کند  <math>h(R_3) = h(PW_i \parallel ID_i) \oplus A_2</math>  <math>PID_i = h(ID_i \parallel h(R_1))</math>  <math>D_{ug} = A_1 \oplus h(PW_i \parallel PID_i)</math>  <math>A'_3 = h(PW_i \parallel ID_i \parallel h(R_1) \parallel D_{ug})</math>  <math>A_3</math>  <math>R_2</math> انتخاب  <math>B_1 = h(PID_i \parallel D_{ug}) \oplus (h(R_2) \parallel ID_{sn})</math>                      ارسال پیام  <math>M_1 = \{B_1, B_2, TID_i\}</math> </p>	<p> <math>D_{ug} \parallel PID_i = ED_{ug} \oplus h(S_1) \oplus h(S_2)</math>  <math>h(R_2) \parallel ID_{sn} = B_1 \oplus h(PID_i \parallel D_{ug})</math>  <math>B'_2 = h(D_{ug} \parallel h(R_2) \parallel PID_i \parallel ID_{sn})</math>  <math>A_3</math>  <math>A_3</math>  <math>R_3</math> انتخاب  <math>SK_{us} = h(h(R_3) \parallel (h(R_2) \parallel ID_{sn}))</math>  <math>B_3 = h(D_{gs} \oplus (h(R_3) \parallel SK_{us}))</math>  <math>B_4 = h(D_{gs} \parallel h(R_3) \parallel SK_{us})</math>                      ارسال پیام  <math>M_2 = \{B_3, B_4\}</math> </p>	<p> <math>h(R_3) \parallel SK_{us} = h(D_{gs}) \oplus B_3</math>  <math>B'_4 = h(D_{gs} \parallel h(R_3) \parallel SK_{us})</math>  <math>B_4</math>  <math>B'_4</math>  <math>R_4</math> انتخاب  <math>B_5 = h(D_{gs} \parallel ID_{sn}) \oplus h(R_4)</math>  <math>B_6 = h(D_{gs} \parallel h(R_3) \parallel h(R_4) \parallel SK_{us})</math>                      ارسال پیام  <math>M_3 = \{B_5, B_6\}</math> </p>
<p> <math>B'_8</math> <math>B_8</math>  <math>D^{new}_{ug} \parallel TID^{new}_i \parallel SK_{us} = h(D_{ug} \parallel TID_i \parallel PID_i) \oplus B_7</math>  <math>B'_8 = h(D^{new}_{ug} \parallel PID_i \parallel h(R_2) \parallel SK_{us} \parallel ID_{sn})</math>  <math>B_9 = h(D^{new}_{ug} \parallel TID^{new}_i \parallel SK_{us} \parallel h(R_2))</math>  <math>A^{new}_1 = h(PW_i \parallel PID_i) \oplus D^{new}_{ug}</math>  <math>A^{new}_3 = h(PW_i \parallel ID_i \parallel h(R_1) \parallel D^{new}_{ug})</math>  <math>A_1 = A_1^{new}</math>  <math>A_3 = A_3^{new}</math>                      ارسال <math>m_5 = \{B_9\}</math> </p>	<p> <math>B'_6</math> <math>B_6</math>  <math>TID^{new}_i</math> تولید  <math>h(R_4) = h(D_{gs} \parallel ID_{sn}) \oplus B_5</math>  <math>B'_6 = h(D_{gs} \parallel h(R_3) \parallel h(R_4) \parallel SK_{us})</math>  <math>D^{new}_{ug} = h(PID_i \parallel TID^{new}_i \parallel S_1 \parallel S_2)</math>  <math>B_7 = h(D_{ug} \parallel TID_i \parallel PID_i) \parallel D^{new}_{ug} \parallel TID^{new}_i \parallel SK_{us}</math>  <math>B_8 = h(D^{new}_{ug} \parallel PID_i \parallel h(R_2) \parallel SK_{us} \parallel ID_{sn})</math>                      ارسال پیام  <math>M_4 = \{B_7, B_8\}</math> </p>	
	<p> <math>B'_9</math> <math>B_9</math>  <math>ED^{new}_{ug} = h(D_{ug} \parallel TID^{new}_{ug} \parallel SK_{us} \parallel h(R_2))</math>  <math>TID_i = TID^{new}_i</math>  <math>ED_{ug} = ED^{new}_{ug}</math> </p>	

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 فاش نمی‌شوند [1,15]. در پروتکل پیشنهادی اگر کلید نشست را به دست بیاورد و همچنین مهاجم، تمام پیام‌های مبادله شده در کانال عمومی را نیز داشته باشد، باز هم به دلیل وجود مقادیر تصادفی  $R_2$  و  $R_3$  متفاوت در هر نشست، موفق به بازیابی کلیدهای نشست پیشین نخواهد شد. بنابراین، مهاجم در به دست آوردن مقدار کلیدهای نشست قبلی و بعدی موفق نخواهد بود [15].

### • غیرقابل ردیابی بودن حسگر

پروتکل پیشنهادی هم این ویژگی را داراست چراکه شناسه حسگر به طور بدیهی در کانال رد و بدل نمی‌شود و در توابع چکیده ساز قرار داده می‌شوند.

### • سبک وزن بودن

برای روند احراز هویت در این پروتکل از عملیات رمزنگاری ساده و اصطلاحاً سبک وزن مانند یای انحصاری و تابع چکیده ساز استفاده شده است که در سربار و همچنین سرعت انجام عملیات تأثیر بسزایی دارد و می‌تواند مهر تأییدی برای اثبات سبک وزن بودن پروتکل پیشنهادی باشد.

### • تازگی

به دلیل 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 جلوگیری کند.

## ۳.۵. بررسی عملکرد پروتکل پیشنهادی در برابر حملات

### مقاوم در برابر حمله عدم همزمانی

در هر پیام مبادله شده بین کاربر و درگاه، فقط یک پارامتر وجود دارد که متعلق به مرحله آخر ارتباطشان است و ارتباط بین درگاه 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 چکیده ساز بر روی اعداد تصادفی  $R_2$ ,  $R_3$  و  $ID_{sn}$  ایجاد می‌شود که  $R_2$  توسط کاربر و  $R_3$  توسط درگاه ایجاد می‌شود لازم به ذکر است که این مقادیر به گونه‌ای امن منتقل می‌شوند که مهاجم قادر به بازیابی آن‌ها از طریق کانال عمومی نخواهد بود.

### • مقاوم در برابر حمله جعل درگاه

اگر مهاجمی بتواند پیام‌های معتبر  $M_2$  و  $M_4$  را تولید کند، می‌تواند درگاه را جعل کند. در پروتکل پیشنهادی، ایجاد پیام معتبر  $M_2$ ، مهاجم نیاز به داشتن  $S_1$  و  $S_2$  دارد تا بتواند  $ID_{sn}$  را به دست آورد. همچنین نیاز دارد  $Dgs$  را به دست آورد تا بتواند  $B_3$  و  $B_4$  معتبر را تولید کند. به طور مشابه، نیاز به مقادیر  $S_1$  و  $S_2$

دارد و مقادیر  $ID_{sn}$ ,  $skus$  و  $Dug$  را محاسبه کند تا پیام  $M_4$  را تشکیل دهد.

### • 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 موفقیت آمیز انجام دهد، اما مقادیر محرمانه کاربر نظیر  $Dug$  و  $PID_i$  و همچنین دستگاه موبایل کاربر را ندارد در نتیجه این حمله عملی نخواهد شد.

### • مقاوم در برابر حمله تسخیر حسگر

در پروتکل پیشنهادی، اگر اطلاعات یک حسگر تغییر داده شود یا تسخیر شود، مهاجم قادر نخواهد بود اطلاعات سایر حسگرها را به دست آورد بود چون کلیدهای محرمانه مشترک و سایر مقادیر استفاده شده، تصادفی و متفاوت هستند.

### • مقاوم در برابر حمله درگاه بدخواه

درگاه، شناسه حسگر مورد نظر، در پیام ارسالی از طرف کاربر را نمی‌تواند تغییر دهد، زیرا کاربر، صحت شناسه حسگر را با ارزیابی پیام  $B_8$  بررسی می‌کند،  $(ID_{sn} || SKus || h(R_2) || PID_i)$  و اگر  $B_8 = h(Dnewug)$  و اگر رابطه  $B_8 = B_8'$  برقرار بود آنگاه مراحل احراز هویت را ادامه می‌دهد.

بنابراین، اگر درگاه مقدار  $ID_{sn}$  را تغییر دهد، کاربر می‌تواند نشست را خاتمه دهد و درگاه قادر نخواهد بود نشستی بین کاربر و حسگر مورد نظر خود تشکیل دهد.

### • مقاوم در برابر حمله ردیابی کاربر

به دلیل استفاده از  $TID_i$  جدید در هر نشست، کاربر توسط مهاجم قابل ردیابی نیست.

### • مقاوم در برابر حمله جعل افشای کلید

در این حمله، مهاجم با داشتن کلید محرمانه بلندمدت می‌تواند خودش را به جای یک عضو معتبر جا بزند، اما در پروتکل پیشنهادی به دلیل انتشار از مقادیر امنیتی کوتاه مدت نظیر  $R_2$ ,  $R_3$  و  $R_4$  که در هر نشست تغییر می‌کند، امکان پذیر نخواهد بود.

## ۴.۵. بررسی سربار محاسباتی پروتکل پیشنهادی

در جدول از لحاظ سربار محاسباتی پروتکل پیشنهادی را با پروتکل‌های مشابه دیگر مقایسه خواهیم کرد. در جدول زیر می‌توان به وضوح 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 خواهد بود.

با توجه به اینکه زمان مورد نیاز برای محاسبه بر اساس  $Th$  پیاده سازی شده در پروتکل فتوحی و همکارانش برابر با  $0.032$  ثانیه در نظر گرفتیم. در جدول 4 را خواهیم داشت و مشاهده می‌شود که از

لحاظ زمانی مرحله احراز هویت پروتکل پیشنهادی از پروتکل فتوحی و همکارانش ۲,۵۶ میلی ثانیه سریعتر است.

#### ۵.۵. بررسی سربار مخابراتی پروتکل پیشنهادی

برای محاسبه سربار مخابراتی پروتکل پیشنهادی و مقایسه آن با پروتکل فتوحی و همکارانش، فرض می‌کنیم تمامی توابع چکیده‌ساز و شناسه‌های مورد استفاده در پروتکل پیشنهادی 160 بیتی و مقادیر تصادفی 128 بیتی هستند در این صورت در مقایسه با پروتکل فتوحی و همکارانش، جدول 4 را تشکیل داده و به بررسی می‌پردازیم. برای محاسبه سربار مخابراتی، دو کانال ارتباطی درگاه-کاربر و درگاه-حسگر، در مرحله احراز هویت داریم. در کانال ارتباطی درگاه-کاربر داریم:

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

در نتیجه :

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

بنابراین سربار مخابراتی کانال ارتباطی درگاه کاربر برابر است با 800 بیت. در کانال ارتباطی درگاه-حسگر داریم:

جدول ۲: مقایسه سر بار محاسباتی پروتکل پیشنهادی با دیگر پروتکل ها

تعریف		نماد		
زمان متوسط برای محاسبه توابع چکیده ساز		$T_h$		
زمان متوسط برای محاسبه رمزنگاری و رمزگشایی		$T_e$		
زمان متوسط برای محاسبه تابع تعریف شده در پروتکل خمیسا		$T_f$		
پروتکل	درگاه	حسگر	کاربر	جمع
تورکانووی و همکاران [14]	$14T_h$	$7T_h$	$11T_h$	$32T_h$
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]	-	$T_e + T_f + T_h$	$T_e + T_f + T_h$	$(2T_e + T_f + T_h)$
انورقانی و همکاران [4]	$T_e + 3T_h$	$T_h$	$T_e + 2T_h$	$2T_e + 6T_h$
فتوحی و همکاران [1]	$17T_h$	$7T_h$	$10T_h$	$34T_h$
پروتکل پیشنهادی	$11T_h$	$6T_h$	$9T_h$	$26T_h$

جدول ۳ مقایسه زمان محاسبه سر بار 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
پروتکل پیشنهادی	3.52ms	1.92ms	2.88ms	8.32ms

در این حمله مهاجم قصد دارد کاربر را ردیابی کند اما موفق نخواهد شد چرا که کاربر شناسه یکبار مصرف داشته و در هر نشست به روزرسانی می شود.

**مقاوم در برابر حمله جعل هویت:**

در این حمله مهاجم قصد دارد خود را به جای یکی از طرفین ارتباط جازده و طرف مقابل را فریب دهد که در پروتکل پیشنهادی ممکن نیست.

**مقاوم در برابر حمله تکرار:**

در این حمله مهاجم از طریق ارسال مجدد پیام های معتبر شنود شده خواهان احراز هویت غیرمجاز است، که نمی تواند موفق شود زیرا همه پیام ها دارای مهر زمانی هستند. بنابراین با توجه به جدول بالا نتیجه می گیریم 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 می کند و نشستی که مدنظر کاربر نیست تشکیل می دهد.

**مقاوم در برابر حمله عدم همزمانی:**

در این حمله، نهادهای موجود در شبکه نمی توانند مقادیر خود را بطور همزمان با یکدیگر به روزرسانی کنند و نهادهای در مقدار پارامترها با

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

در نتیجه:

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

بنابراین سر بار مخابراتی کانال ارتباطی درگاه-حسگر برابر است با 1440 بیت. با توجه به محاسبات و جدول زیر مشاهده می شود که پروتکل پیشنهادی، نسبت به پروتکل فتوحی و همکارانش [1]، از نظر سر بار مخابراتی نیز کارتر خواهد بود.

**جدول ۴:**

مقایسه سر بار مخابراتی پروتکل پیشنهادی با پروتکل فتوحی و همکاران

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

با توجه به مقایسه انجام شده در بالا مشاهده شد که پروتکل پیشنهادی ۲۴٪ در سر بار محاسباتی و ۲۶٪ در سر بار مخابراتی بهبود یافته است.

**مقاوم در برابر حمله ردیابی:**

نتوانند به مراحل پروتکل دسترسی یابند، همچنین پروتکل پیشنهادی در مقایسه با پروتکل قبلی مقایسه شد و ۲۴٪ در سر بار محاسباتی و ۲۶٪ در سر بار مخابراتی بهبود داشته‌است. بنا بر نتایج فوق پروتکل پیشنهادی در این تحقیق می‌تواند در زمینه اینترنت‌اشیا و شبکه‌های حسگر بی‌سیم بسیار کارا باشد و مورد استفاده قرار گیرد.

یکدیگر دچار ناهماهنگی می‌شوند. مقایسه مقاوم بودن 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، جعل هویت، عدم همزمانی بین حسگر و کاربر، قابلیت ردیابی و تسخیر حسگر

جدول ۵: مقایسه پروتکل پیشنهادی و دیگر پروتکل‌ها

مقاوم بودن در برابر حملات					پروتکل
درگاه بدخواه	تکرار	عدم همزمانی	جعل هویت	ردیابی	
X	✓	X	✓	✓	تورکانووی و همکاران [14]
X	X	X	X	✓	گوپه و همکاران [3]
X	X	X	X	✓	خمیسا و همکاران [5]
X	X	X	✓	✓	انورقانی و همکاران [4]
X	✓	X	✓	✓	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*, 10(7), 357430.
- [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 electronics*, 63(11), 7124-7132.
- [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 Systems*, 16(4), 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.