دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۱-۹)
https://monadi.isc.org.ir

ارائه‌شده در هجدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه اصفهان، ۱۰ و ۱۱ شهریور ۱۴۰۰

حمله‌ی کشف کلید و جعل روی یک پروتکل توافق کلید همراه با احراز اصالت برای شبکه‌ی حسگر بی‌سیم★

امیر الهدادی غیاث‌آبادی* و جواد علیزاده

مرکز علم و فناوری فتح، دانشکده و پژوهشکده مهندسی کامپیوتر و قدرت سایبری، دانشگاه جامع امام حسین (ع)، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
شبکه‌ی حسگر بی‌سیم
پروتکل توافق کلید همراه با احراز اصالت
حمله‌ی کشف کلید
حمله‌ی جعل

dor: 20.1001.1.24763047.1401.11.1.1.8

نوع مقاله: پژوهشی

چکیده

با توسعه‌ی فناوری‌های اطلاعاتی و ارتباطی جدید مانند تحولات مربوط به کاربردهای اینترنت اشیا، اهمیت اطلاعات و حفظ امنیت آن بیش از پیش مورد توجه قرار می‌گیرد. پروتکل‌های توافق کلید و احراز اصالت نقش مهمی در تأمین امنیت اطلاعات دارند. یکی از مؤلفه‌های مهم که در بسیاری از کاربردهای اینترنت اشیا استفاده می‌شود، شبکه‌های حسگر بی‌سیم است که امنیت آن‌ها با استفاده از پروتکل‌های مناسب این شبکه‌ها تأمین می‌شود. در سال ۲۰۲۰ سیکاروار و داس یک پروتکل توافق کلید همراه با احراز اصالت برای شبکه‌های حسگر بی‌سیم ارائه و ادعا کردند این پروتکل در برابر حملات شناخته شده مانند حملات بازخوردی، کشف کلمه عبور و مردی در میانه امن است و با استفاده از آن می‌توان یک کلید را به صورت امن میان اعضای پروتکل به اشتراک گذاشت. در این مقاله نشان داده می‌شود کلید توافق شده با استفاده از پروتکل سیکاروار و داس، امن نیست و یک مهاجم می‌تواند به راحتی این کلید را به دست آورد. علاوه بر این نشان داده می‌شود پروتکل نمی‌تواند در برابر حملاتی مانند حمله‌ی کشف کلمه عبور و حمله‌ی جعل امن باشد.

۱ مقدمه

در سال‌های اخیر رشد و توسعه‌ی فناوری‌های اطلاعاتی و ارتباطی با سرعت قابل توجهی ادامه یافته است. یکی از نتایج این توسعه و پیشرفت، پیدایش فناوری‌های متحول کننده مانند فناوری اینترنت اشیا [1] است که باعث تغییر در شیوه‌ی زندگی بشر شده است. در حال حاضر کاربردهای بسیاری از اینترنت اشیا درگوشه و کنار جوامع بشری قابل مشاهده است. برای مثال، استفاده از حسگرها و ارتباط آن‌ها تحت شبکه اینترنت یا همان اینترنت حسگرها [2]، یک نمونه از کاربردهای ذکر شده است که در حوزه‌های مختلف مانند سلامتی و مراقبت‌های پزشکی، نظامی و صنعتی قابل مشاهده می‌باشد. شبکه‌های حسگر بی‌سیم [3] که شبکه‌ای از حسگرها با نوع ارتباط بی‌سیم است، یک نمونه عملی و قابل لمس از کاربرد اینترنت حسگرها می‌باشد [۱-۳] و همانند تمام فناوری‌های اطلاعاتی و ارتباطی چالش‌های امنیتی و کارآیی دارد. برای تأمین امنیت اطلاعات در این شبکه‌ها از الگوریتم‌ها و پروتکل‌های رمزنگاری مناسب استفاده می‌شود. به دلیل محدودیت منابع پیاده‌سازی در حسگرهایی که اندازه‌های نسبتاً کوچکی دارند، الگوریتم‌ها و پروتکل‌های ذکرشده می‌بایست طوری باشند که تا حد امکان نیاز به منابع و مساحت کمتری برای پیاده‌سازی داشته باشند. به عبارت دیگر آن‌ها باید از نوع سبک وزن باشند. با توجه به الزام استفاده از توابع ریاضیاتی ساده در الگوریتم‌ها و پروتکل‌های

★از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.

*نویسنده مسئول
آدرس‌های رایانامه: aalahdadi@ihu.ac.ir (امیر الهدادی غیاث‌آبادی)، jaalizadeh@ihu.ac.ir (جواد علیزاده)

[1] internet of thing

[2] internet od sensors [3] wireless sensor network

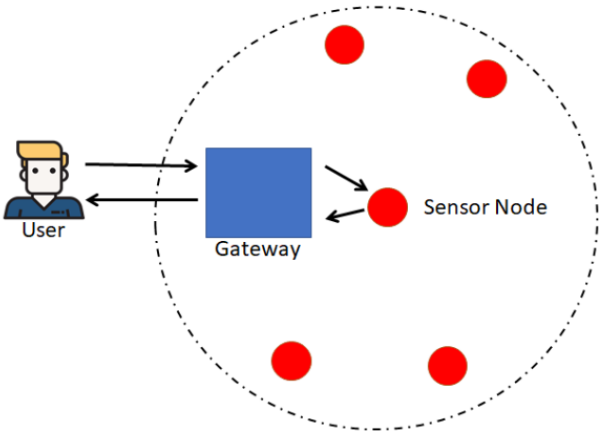
سبک‌وزن، اطمینان از امنیت آن‌ها در مقایسه با الگوریتم‌ها و پروتکل‌های غیر سبک وزن نیاز به دقت بیشتری دارد.

برای تأمین امنیت در یک شبکه‌ی حسگر بی‌سیم لازم است تا اعضای شبکه بتوانند به صورت امن همدیگر را احراز اصالت [۱] کنند و یک کلید محرمانه میان خود به اشتراک بگذارند تا با کاربرد آن در الگوریتم‌های رمزنگاری بتوانند محرمانگی و جامعیت داده‌های خود را تأمین کنند. برای دست‌یابی به اهداف احراز اصالت و توافق کلید [۲] در یک شبکه‌ی حسگر بی‌سیم می‌توان از پروتکل‌های احراز اصالت و توافق کلید و یا پروتکل‌های توافق کلید همراه با احراز اصالت [۳] استفاده کرد.

هرسال، کارها و مقالات متعددی در زمینه طراحی، پیاده‌سازی و تحلیل و ارزیابی پروتکل‌های توافق کلید همراه با احراز اصالت مناسب برای شبکه‌های حسگر بی‌سیم ارائه می‌شود که نشان می‌دهد توانمندی طراحان و تحلیل‌گران در این حوزه همراه با هم در حال رشد و تکوین است [۴–۶]. از این نمونه فعالیت‌ها می‌توان به [۷] در سال ۲۰۱۴ اشاره کرد که در آن فراش و همکاران برخی ضعف‌های امنیتی از طرح ترکانوویچ [۴] و همکاران [۸]، مانند امکان ردیابی کاربر [۵] و گمنام نبودن آن، آسیب‌پذیری در برابر حملات در مدل کارت هوشمند به سرقت رفته [۶] و مردی در میانه [۷] را گزارش دادند و سپس یک طرح جدید ارائه و ادعا کردند طرح آن‌ها ضعف‌های امنیتی مشابه با آنچه که در مورد طرح ترکانوویچ و همکاران گزارش شد، ندارد. با این وجود امین و همکاران [۹] در سال ۲۰۱۴ نشان دادند طرح فراش و همکاران برخلاف ادعای ایشان، در برابر برخی حملات شناخته‌شده مانند حمله‌ی جعل هویت کاربر [۸] و حملات در مدل کارت هوشمند به سرقت رفته ناامن است. به طور مشابه آن‌ها نیز یک پروتکل بهبودیافته را طوری ارائه کردند که ضعف‌های امنیتی ذکرشده را نداشته باشد. پروتکل امین و همکاران نیز در [۱۰] مورد تحلیل و ارزیابی قرار گرفت و بهبود داده شد. علاوه بر موارد ذکرشده، در سال‌های اخیر نیز پروتکل‌های سبک وزن متعددی برای استفاده در شبکه‌های حسگر بی‌سیم توسط طراحان، طراحی و توسط تحلیلگران ارزیابی‌شده است. ازجمله این پروتکل‌ها می‌توان به [۱۱–۱۴] اشاره کرد.

در سال ۲۰۱۵ چانگ [۹] و همکاران [۱۵] یک پروتکل توافق کلید همراه با احراز اصالت سبک وزن چهارمرحله‌ای ارائه و اثبات‌های امنیتی برای طرح خود ارائه کردند. در سال ۲۰۲۰ سیکاروار [۱۰] و داس [۱۱] [۱۶] طرح چانگ و همکاران را موردمطالعه و بررسی قرار دادند و تلاش کردند تا کارآیی این طرح را با حفظ سطح امنیتی آن ارتقا دهند. آن‌ها یک طرح بهبودیافته ازنقطه نظر کارآیی در مقایسه با طرح قبلی ارائه دادند و ادعا نمودند طرح آن‌ها در برابر حملات شناخته شده مانند حملات جعل و کشف کلمه عبور و حملات در مدل کارت هوشمند به سرقت رفته امن است و به طور امن می‌تواند یک کلید محرمانه را میان کاربران خود به اشتراک گذارد. برخلاف این ادعا می‌توان آسیب‌پذیری‌های جدی از این

[1] authentication [2] key agreement [3] Authenticated Key Agreement (AKA) [4] Turkanović [5] user traceability [6] stolen smart card [7] man in the middle [8] user impersonation [9] Chang [10] Sikarwar [11] Das



شکل ۱. مدل شبکه استفاده شده در پروتکل سیکاروار و داس [۱۶]

پروتکل به دست آورد و نشان داد این پروتکل یک طرح کاملاً ناامن است. برای مثال یک مهاجم می‌تواند کلید نشست توافق شده میان کاربران را به راحتی و به طور قطعی به دست آورد؛ یا اینکه یک مهاجم می‌تواند کلمه عبور کاربران را کشف و هویت ایشان را جعل نماید. با توجه به این موارد می‌توان نتیجه گرفت سیکاروار و داس برای بهبود کارآیی پروتکل چانگ و همکاران بده بستان میان کارآیی و امنیت را خوب رعایت نکرده‌اند و اگرچه یک پروتکل نسبتاً کارآتر در مقایسه با پروتکل قبلی ارائه داده‌اند ولی نتوانسته‌اند اهداف امنیتی پروتکل را تأمین کنند.

ادامه مطالب این مقاله به صورت زیر سازماندهی شده است. طرح سیکاروار و داس در بخش ۲ توصیف می‌شود. در بخش ۳، آسیب‌پذیری‌های این طرح مانند ضعف آن در برابر حمله‌ی کشف کلید، حمله‌ی کشف کلمه عبور و حملات جعل و حمله‌ی منع سرویس توضیح داده می‌شود. در نهایت جمع‌بندی و نتیجه‌گیری مقاله در بخش ۴ ارائه و دلایل ضعف امنیتی پروتکل سیکاروار و داس در برابر حملات ذکرشده خلاصه می‌شود.

۲ مرور پروتکل سیکاروار و داس

در این بخش پروتکل توافق کلید همراه با احراز اصالت سیکاروار و داس به صورت مختصر معرفی می‌شود. در این پروتکل برای احراز اصالت یک کاربر توسط یک گره حسگر از یک گره دروازه [۱۲] کمک گرفته می‌شود که کلیات این کار در شکل ۱ آورده شده است [۱۶].

پروتکل سیکاروار و داس یک طرح سبک وزن چهار مرحله‌ای مبتنی بر تابع چکیده‌ساز و عملگر xor است. با استفاده از این پروتکل می‌توان عمل احراز اصالت کاربر و توافق کلید میان کاربر و گره حسگر را به صورت همزمان انجام داد. در این پروتکل ابتدا کاربر اطلاعاتی از خود را برای گره حسگر ارسال کرده و درخواست برقراری ارتباط می‌دهد. گره حسگر شناسه‌ی کاربر و برخی اطلاعات ثبت شده از کاربر در مرحله‌ی ثبت نام را برای گره دروازه ارسال کرده و از وی برای احراز اصالت کاربر کمک می‌گیرد. به عبارت دیگر کار اصلی برای احراز اصالت کاربر را گره

[12] gateway node

جدول ۱. نمادگذاری برای توصیف پروتکل سیکاروار و داس

نماد	توضیحات
U_i	کاربر
ID_i	شناسه‌ی کاربر
PW_i	رمزعبور کاربر
SC_i	کارت هوشمند
GWN	گره دروازه
S_j	گره حسگر
SID_j	شناسه‌ی حسگر
X_{GWN}	کلید محرمانه‌ی گره دروازه
T_1, T_2, T_3, T_4	مهرهای زمانی
r_i, r'_i, K_i, K_j	اعداد تصادفی
$\|\|, \oplus, h()$	الحاق، xor، تابع چکیده‌ساز
SK_i	کلید نشست

دروازه انجام می‌دهد. گره دروازه بعد از تأیید هویت کاربر، این موضوع را به گره حسگر اطلاع می‌دهد و سپس گره حسگر اقدام به محاسبه یک کلید نشست محرمانه میان خود و کاربر نموده و آن را با استفاده از توابع چکیده‌ساز و به شکل امن برای کاربر ارسال می‌کند. حال کاربر و گره حسگر یک کلید محرمانه میان خود به اشتراک گذاشته‌اند و با استفاده از آن می‌توانند ارتباط امن داشته باشند.

پروتکل سیکاروار و داس چهار مرحله‌ی اصلی به ترتیب زیر دارد:

(۱) مرحله‌ی آماده‌سازی
(۲) مرحله‌ی ثبت‌نام
(۳) مرحله‌ی احراز اصالت و توافق کلید
(۴) مرحله‌ی تغییر کلمه عبور

در ادامه‌ی این مقاله برای توصیف مراحل پروتکل ذکرشده از نمادگذاری مطابق جدول ۱ استفاده می‌شود.

۱.۲ مرحله‌ی آماده‌سازی

در مرحله‌ی آماده‌سازی، برخی پارامترهای لازم برای گره دروازه و گره حسگر تولید می‌شود [۱۶]. این مرحله برای اطمینان از این امر است که گره دروازه اطلاعات لازم از گره حسگر را در اختیار دارد. در این مرحله گره دروازه کلید محرمانه‌ی خود یعنی X_{GWN} را انتخاب و گره حسگر شناسه‌ی خود یعنی SID_j را در نظر می‌گیرد. گره دروازه $f_j = h(SID_j \| X_{GWN})$ را حساب می‌کند. مقادیر SID_j و f_j در حافظه گره حسگر ذخیره می‌شوند. محاسبات این مرحله از پروتکل در جدول ۲ خلاصه شده است.

جدول ۲. مرحله‌ی آماده‌سازی پروتکل سیکاروار و داس

گره حسگر	گره دروازه
SID_j	X_{GWN}
$\leftarrow (SID_j)$	
	$f_j = h(SID_j \| X_{GWN})$
	$(SID_j, f_j) \rightarrow$
(SID_j, f_j)	

جدول ۳. مرحله‌ی ثبت‌نام پروتکل سیکاروار و داس

گره دروازه	کاربر
	ID_i, PW_i
	r_i
	$MP_i = h(r_i \| PW_i)$
	$(ID_i, Mp_i) \rightarrow$
r'_i	
$MI_i = h(r'_i \| ID_i)$	
$f_i = h(MI_i \| X_{GWN})$	
$e_i = MP_i \oplus f_i$	
$\leftarrow$ Smart Card $\{MI_i, e_i\}$	
	Smart Card $\{MI_i, e_i, r_i\}$

۲.۲ مرحله‌ی ثبت‌نام

در این مرحله برای استفاده از پروتکل، یک کاربر ثبت نام می‌کند و برای او یک کارت هوشمند صادر می‌شود که از آن برای ورود به پروتکل و شروع ارتباط با گره حسگر استفاده می‌کند. محاسبات لازم برای این مرحله در جدول ۳ آورده شده و جزئیات آن به شرح زیر است.

(۱) ابتدا کاربر شناسه‌ی ID_i و کلمه عبور PW_i را انتخاب و سپس عدد تصادفی r_i را تولید می‌کند. در ادامه مقدار $MP_i = h(r_i \| PW_i)$ را محاسبه و MP_i و ID_i را برای گره دروازه ارسال می‌کند.
(۲) گره دروازه عدد تصادفی r'_i را تولید کرده و مقادیر

$$MI_i = h(r'_i \| ID_i)$$
$$f_i = h(MI_i \| X_{GWN})$$
$$e_i = MP_i \oplus f_i$$

را محاسبه می‌کند. او دو عبارت (MI_i, e_i) را در یک کارت هوشمند ذخیره می‌کند و این کارت را برای کاربر می‌فرستد.
(۳) کاربر پس از دریافت کارت هوشمند عدد تصادفی r_i خود را به آن اضافه می‌کند.

۳.۲ مرحله‌ی احراز اصالت

در این مرحله تلاش می‌شود تا یک کاربر که درخواست برقراری ارتباط با یک گره حسگر بی‌سیم خاص را دارد احراز اصالت شود و یک کلید محرمانه میان کاربر و گره حسگر بی‌سیم به اشتراک گذاشته شود. برای این کار گره دروازه به‌عنوان یک مرجع قابل اعتماد برای کاربر و گره حسگر عمل می‌کند. مرحله‌ی احراز اصالت پروتکل سیکاروار و داس را می‌توان مطابق جدول ۴ در نظر گرفت که در آن

(۱) کاربر کارت هوشمند خود را در درگاه قرار می‌دهد و رمز عبور و شناسه‌ی خود را وارد می‌کند. سپس مقدار

$$Y_i = h(e_i \oplus h(r_i \| PW_i) \| T_1)$$

را محاسبه می‌کند که در آن T_1 مهر زمانی است. او عدد تصادفی K_i را تولید کرده و مقادیر $Z_i = K_i \oplus Y_i$ و $N_i = h(Y_i \| MI_i \| SID_j)$ را نیز محاسبه می‌کند. در انتها مقادیر (MI_i, N_i, Z_i, T_1) را برای گره حسگر ارسال می‌کند.

(۲) گره حسگر ابتدا مهر زمانی T_1 را بررسی می‌کند. سپس مقدار $A_j = f_j \oplus N_i \oplus T_2$ را حساب می‌کند که در آن T_2 یک مهر زمانی است. درنهایت $(MI_i, A_j, N_i, SID_j, T_1, T_2)$ را برای گره دروازه ارسال می‌کند.

(۳) گره دروازه بعد از بررسی مهرهای زمانی T_1 و T_2، محاسبات زیر را انجام می‌دهد:

$$A'_j = h(SID_j \| X_{GWN}) \oplus N_i \oplus T_2$$
$$Y'_i = h(h(MI_i \| X_{GWN}) \| T_1)$$
$$N'_i = h(Y' \| MI_i \| SID_j)$$

سپس بررسی می‌کند که تساوی $N'_i = N_i$ و $A'_j = A_j$ برقرار باشد. در این صورت کاربر احراز اصالت می‌شود و گره دروازه مقادیر زیر را حساب و همراه با مهر زمانی T_3 برای گره حسگر می‌فرستد.

$$F_ij = Y'_i \oplus h(f'_j \| T_3)$$
$$H_j = h(Y'_i)$$
$$E_i = h(f'_i \| N'_i)$$

(۴) گره حسگر مهر زمانی T_3 را بررسی و مقادیر زیر را حساب می‌کند

$$Y'_i = F_{ij} \oplus h(f_j \| T_3) \quad (۱)$$
$$H'_j = h(Y'_i) \quad (۲)$$

سپس تساوی $H'_j = H_j$ را بررسی می‌کند. اگر این تساوی صحیح باشد، هویت کاربر برای گره حسگر تأیید می‌شود و او مطابق جدول ۴ مقادیر (E_i, R_{ij}, T_4) را برای کاربر ارسال کرده و کلید نشست $SK_i = h(K_j \oplus K'_i)$ را حساب می‌کند.

(۵) کاربر مهر زمانی T_4 را بررسی می‌کند و $E'_i = h(f_i \| T_4)$ را محاسبه می‌کند. اگر تساوی $E'_i = E_i$ برقرار باشد هویت حسگر برای کاربر تأیید می‌شود و کاربر مقدار

$$K'_j = R_{ij} \oplus h(K_i \| T_4)$$

را محاسبه و درنهایت کلید نشست را به صورت

$$SK_i = h(K'_j \oplus K_i)$$

به دست می‌آورد.

۴.۲ مرحله‌ی تغییر کلمه عبور

در این مرحله، ابتدا کاربر کلمه عبور قدیمی و شناسه‌ی خود را وارد می‌کند. سپس درخواست تغییر کلمه عبور داده و کلمه عبور جدید خود یعنی PW_i^{new} را وارد می‌کند. مقادیر $MP_i^{new} = h(r_i \| PW_i^{new})$ و e_i^{new} محاسبه و در نهایت مقدار $e_i^{new} = e_i \oplus MP_i \oplus MP_i^{new}$ جایگزین e_i قبلی داخل کارت هوشمند می شود.

سیکاروار و داس ادعا کردند پروتکل ایشان که در بالا توصیف شد یک طرح امن بوده و از کارآیی لازم نیز برخوردار است. در بخش بعدی این مقاله نشان داده می‌شود این پروتکل برخی ضعف‌های امنیتی اساسی دارد که باعث می‌شود کاملاً ناامن باشد.

۳ ارزیابی امنیتی پروتکل سیکاروار و داس

در این بخش، امنیت پروتکل سیکاروار و داس مورد ارزیابی قرار می‌گیرد و نشان داده می‌شود این پروتکل نمی‌تواند در برابر حملات کشف کلید، کشف کلمه عبور، جعل و منع سرویس امن باشد. از آنجا که هدف اصلی این طرح، توافق کلید محرمانه میان اعضای شرکت‌کننده در آن است، بنابراین می‌توان نتیجه گرفت پروتکل سیکاروا و داس یک پروتکل کاملاً ناامن است و در عمل یک مهاجم می‌تواند به راحتی به کلید محرمانه‌ی توافق شده در این پروتکل دسترسی داشته باشد.

۱.۳ حمله‌ی کشف کلید

در این بخش یک حمله‌ی کشف کلید عملی روی پروتکل سیکاروار و داس شرح داده می‌شود. در این حمله مهاجم از اطلاعات تبادلی روی کانال ارتباطی عمومی میان اعضای پروتکل استفاده کرده و کلید محرمانه‌ی نشست را به دست می‌آورد. برای تشریح این حمله، مرحله‌ی احراز اصالت و توافق کلید پروتکل سیکاروار و داس را مطابق جدول ۴ در نظر بگیرید. در مرحله‌ای که کاربر پیام

$$(MI_i, N_i, Z_i, T_1)$$

را برای گره حسگر می‌فرستد، مهاجم مقدار Z_i را به دست می‌آورد. همچنین در مرحله‌ای که گره حسگر پیام

$$(MI_i, A_j, N_i, SID_j, T_1, T_2)$$

جدول ۴. مرحله‌ی احراز اصالت و توافق کلید پروتکل سیکاروار و داس

کاربر	گره حسگر	گره دروازه
Enter ID_i and Password PW_i		
$Y_i = h(e_i \oplus h(r_i \| PW_i) \| T_1)$		
Generate K_i		
$Z_i = K_i \oplus Y_i$		
$N_i = h(Y_i \| MI_i \| SID_j)$		
$(MI_i, N_i, Z_i, T_1) \rightarrow\rightarrow\rightarrow$		
	Verify T_1	
	$A_j = f_j \oplus N_i \oplus T_2$	
	$(MI_i, A_j, N_i, SID_j, T_1, T_2) \rightarrow\rightarrow\rightarrow$	
		Verify T_1, T_2
		$A'_j = h(SID_j \| X_{GWN}) \oplus N_i \oplus T_2$
		$Y'_i = h(h(MI_i \| X_{GWN}) \| T_1)$
		$N'_i = h(Y'_i \| MI_i \| SID_j)$
		$N'_i =? N_i$ and $A'_j =? A_j$
		$F_{ij} = Y'_i \oplus h(f_j \| T_2)$
		$H_j = h(Y'_i)$
		$E_i = h(f_i \| N'_i)$
		$\leftarrow\leftarrow\leftarrow (E_i, F_{ij}, H_j, T_2)$
	Verify T_3	
	$Y'_i = F_{ij} \oplus h(f_j \| T_2)$	
	$H'_j = h(Y'_i)$	
	$H'_j =? H_j$	
	Generate K_j	
	$K'_i = Z_i \oplus Y'_i$	
	$R_{ij} = h(K'_i \| T_4) \oplus K_j$	
	$\leftarrow\leftarrow\leftarrow (E_i, R_{ij}, T_4)$	
	$SK_i = h(K_j \oplus K'_i)$	
Verify T_4		
$E'_i = h(f_i \| N)$		
$E'_i =? E_i$		
$K'_j = R_{ij} \oplus h(K_i \| T_4)$		
$SK_i = h(K'_j \oplus K_i)$		

را برای گره دروازه ارسال می‌کند، مهاجم می‌تواند پارامترهای A_j، N_i و T_2 را به دست آورد. با توجه به اینکه گره حسگر، A_j را به صورت

$$A_j = f_j \oplus N_i \oplus T_2 \quad (۳)$$

حساب کرده است، بنابراین مهاجم می‌تواند مقدار f_j را به صورت زیر به دست آورد.

$$f_j = A_j \oplus N_i \oplus T_2 \quad (۴)$$

حال در مرحله‌ای که گره دروازه پیام

$$(E_i, F_{ij}, H_j, T_3)$$

را برای گره حسگر ارسال می‌کند، مهاجم می‌تواند دو مقدار T_3 و F_{ij}، را به دست آورد. با توجه به رابطه‌ی (۵) که در محاسبات مربوط به گره دروازه و گره حسگر از آن استفاده می‌شود و با داشتن مقدارهای f_j و T_3 مهاجم می‌تواند مقدار Y_i را مطابق رابطه‌ی (۶) حساب کند.

$$F_{ij} = Y_i \oplus h(f_j \| T_3) \quad (۵)$$

$$Y_i = F_{ij} \oplus h(f_j \| T_3) \quad (۶)$$

در مرحله‌ای که گره حسگر پیام

$$(E_i, R_{ij}, T_4)$$

را برای کاربر ارسال می‌کند، مهاجم مقدارهای T_4 و R_{ij} را به دست می‌آورد. با توجه به اینکه مهاجم مقدار Y_i را محاسبه کرده و مقدار Z_i را در اختیار دارد، می‌تواند با توجه به رابطه‌ی (۷) که در محاسبات مربوط به بخش‌های کاربر و گره حسگر پروتکل از آن استفاده می‌شود، مقدار K_i را مطابق رابطه‌ی (۸) حساب کند.

$$Z_i = K_i \oplus Y_i \quad (۷)$$

$$K_i = Z_i \oplus Y_i \quad (۸)$$

حال مهاجم می‌تواند با توجه به رابطه‌ی (۹) که در بخش محاسبات مربوط به گره حسگر از آن استفاده می‌شود، مقدار K_j را مطابق رابطه‌ی (۱۰) حساب کند.

$$R_{ij} = h(K_i \| T_4) \oplus K_j \quad (۹)$$

$$K_j = R_{ij} \oplus h(K_i \| T_4) \quad (۱۰)$$

درنهایت مهاجم با داشتن مقادیر K_i و K_j مقدار کلید نشست را به صورت

$$SK_i = h(K_j \oplus K_i)$$

حساب می‌کند که همان کلید نشست محرمانه‌ای است که میان کاربر و گره دروازه به اشتراک گذاشته شده است.

حمله‌ی کشف کلید روی پروتکل سیکاروار و داس که در این بخش توضیح داده شد، نشان می‌دهد این پروتکل کاملاً ناامن است و نمی‌تواند مهم‌ترین هدف خود که همان توافق کلید محرمانه میان اعضای مجاز است را برآورده کند. علاوه بر این ضعف، یک سری ضعف‌های دیگر نیز برای این پروتکل مشاهده شده است که در بخش‌های بعد تشریح می‌شوند.

۲.۳ حمله‌ی کشف کلمه عبور

در این بخش نشان داده می‌شود کلمه عبور کاربر هنگام استفاده از پروتکل سیکاروار و داس نمی‌تواند امن باقی بماند و توسط یک مهاجم قابل کشف است. در این پروتکل برای ثبت نام کاربر توسط گره دروازه، از یک کانال امن استفاده نشده است. بنابراین وقتی کاربر پیام (ID_i, Mp_i) را برای گره دروازه ارسال می‌کند، مهاجم می‌تواند این پیام را شنود کرده و آن را ذخیره نماید. در مدل حمله‌ی کارت هوشمند به سرقت رفته مهاجم می‌تواند به اطلاعات ذخیره‌شده در کارت هوشمند کاربر دسترسی داشته باشد. بنابراین او می‌تواند r_i تولیدشده توسط کاربر در مرحله‌ی ثبت نام را نیز به دست آورد. حال مهاجم با جستجوی کامل برای به دست آوردن کلمه عبور کاربر به صورت زیر عمل می‌کند.

(۱) یک مقدار تصادفی مانند PW_i' تولید می‌کند.
(۲) $(r_i \| PW_i')$ را حساب می‌کند.
(۳) اگر مقدار محاسبه شده در مرحله‌ی ۲، با مقدار MP_i برابر باشد، مهاجم PW_i' را به عنوان کلمه عبور کاربر ذخیره می‌کند. در غیر این صورت به مرحله‌ی ۱ می‌رود.

توجه: اگر در مرحله‌ی ثبت‌نام پروتکل سیکاروار و داس، از یک کانال امن استفاده شود، مهاجم با استفاده از حمله‌ی بالا، نمی‌تواند کلمه عبور کاربر را به دست آورد. با این وجود باز هم کلمه عبور کاربر تنها در اختیار او نخواهد بود. زیرا در این حالت گره دروازه می‌تواند حمله‌ی توضیح داده شده در بالا را اجرا نماید و به کلمه عبور کاربر دسترسی داشته باشد.

۳.۳ حمله‌ی جعل کاربر

اگرچه پروتکل سیکاروار و داس مبتنی بر استفاده از شناسه‌ی کاربر، کلمه عبور کاربر و کارت هوشمند کاربر است، اما با توجه به توضیحات این پروتکل روشن است که شناسه‌ی کاربر تنها در مرحله‌ی ثبت‌نام استفاده می‌شود و در مرحله‌ی احراز اصالت و توافق کلید کاربر از کلمه عبور و کارت هوشمند خود استفاده می‌کند. حال اگر مدل حمله، مدل کارت هوشمند به سرقت رفته در نظر گرفته شود، می‌توان فرض کرد اطلاعات کارت هوشمند کاربر در اختیار مهاجم قرارگرفته است و تنها پارامتر نامعلوم برای مهاجم کلمه عبور کاربر است. اگر مهاجم با توجه به حمله‌ی کشف کلمه عبور که در بخش ۲.۳ تشریح شد، کلمه عبور کاربر را به دست آورد، او توانسته است تمام اطلاعات لازم از کاربر برای شروع پروتکل را در اختیار بگیرد. بنابراین او خودش را به جای کاربر قانونی معرفی و درخواست خود را برای گره حسگر ارسال می‌کند. در نهایت هویت مهاجم به جای هویت کاربر واقعی از طرف گره حسگر و با کمک گره دروازه مورد پذیرش قرار گرفته و یک کلید نشست میان گره حسگر و مهاجم نیز تولید می‌شود که برای ارتباطات بعدی از آن استفاده می‌شود.

توجه: از آنجا که در پروتکل سیکاروار و داس $MP_i = h(r_i \| PW_i)$ است. مهاجم با به دست آوردن MP_i و بدون نیاز به کلمه عبور کاربر هم می‌تواند حمله‌ی جعل کاربر را انجام دهد. اگر فرض شود که در مرحله‌ی ثبت‌نام کاربر، از کانال امن استفاده شود که مهاجم نتواند MP_i و یا کلمه عبور کاربر را به دست آورد، در این صورت باز هم این پروتکل ناامن است. چراکه گره دروازه می‌تواند با داشتن MP_i یک کاربر خاص را برای گره حسگر جعل نماید و از ارتباطات محرمانه‌ی آن‌ها مطلع باشد.

۴.۳ حمله‌ی جعل گره حسگر

در پروتکل سیکاروار و داس، یک گره حسگر به راحتی قابل جعل است. توجه شود در این پروتکل وقتی یک درخواست از طرف کاربر برای گره حسگر ارسال می‌شود، گره حسگر ابتدا هویت خود را برای گره دروازه اثبات می‌کند و سپس با کمک گره دروازه تلاش می‌کند تا هویت کاربر را بررسی نماید. برای این کار گره حسگر از پارامتر محرمانه‌ی میان خود و گره دروازه که همان f_j است و در مرحله‌ی آماده‌سازی پروتکل سیکاروار و داس به صورت

$$f_j = h(SID_j \| X_{GWN})$$

محاسبه شده است، استفاده می‌کند. اما توجه شود گره حسگر پیام

$$(MI_i, A_j, N_i, SID_j, T_1, T_2)$$

را تحت یک کانال عمومی برای گره دروازه ارسال می‌کند. بنابراین یک مهاجم می‌تواند اطلاعات این پیام که شامل A_j، N_i، T_2 و SID_j است را ذخیره کند. با توجه به رابطه‌ی (۳) که به صورت زیر یادآوری می‌شود

$$A_j = f_j \oplus N_i \oplus T_2$$

مهاجم با در اختیار داشتن A_j، N_i و T_2 می‌تواند مقدار f_j (مقدار محرمانه‌ی مشترک میان گره حسگر و گره دروازه) را به دست آورد. حال مهاجم می‌تواند خود را به جای گره حسگر مورد نظر برای گره دروازه معرفی کند و گره دروازه نیز او را تأیید خواهد کرد.

۵.۳ حمله‌ی منع سرویس

پروتکل سیکاروار و داس در برابر حمله‌ی منع سرویس نیز آسیب‌پذیر است. برای توضیح بیشتر این حمله توجه کنید که در مرحله‌ی احراز اصالت و توافق کلید، گره حسگر در پایان محاسبات خود مقدار R_{ij} را حساب کرده و برای کاربر ارسال می‌کند. کاربر از این مقدار استفاده کرده و مقدار K'_j را حساب کرده و از آن برای تولید کلید نشست، یعنی SK_i استفاده می‌کند. با این وجود کاربر دست نخوردگی R_{ij} را بررسی نمی‌کند. بنابراین اگر مهاجم موقع ارسال پیام

$$(E_i, R_{ij}, T_4)$$

مقدار R_{ij} را با یک مقدار دیگر مانند R'_{ij} جایگزین کند، این موضوع توسط کاربر آشکار نمی‌شود. در نتیجه کاربر یک کلید نشست متفاوت با کلید نشست گره حسگر حساب می‌کند که این کار باعث اخلال در رمزگذاری و رمزگشایی پیام‌ها و ارتباط صحیح میان گره حسگر و کاربر می‌شود.

۴ نتیجه‌گیری

در این مقاله، امنیت پروتکل سیکاروار و داس که یک پروتکل توافق کلید همراه با احراز اصالت سبک وزن برای شبکه‌های حسگر بی‌سیم است موردمطالعه و بررسی قرار گرفت و ضعف‌های امنیتی آن تشریح شد. نشان داده شد این پروتکل برخلاف ادعای طراحان آن، در برابر حملات اساسی مانند حمله‌ی کشف کلید، حمله‌ی کشف کلمه عبور کاربر، حمله‌ی جعل کاربر و جعل گره حسگر و حمله‌ی منع سرویس ضعف‌های اساسی دارد. به طوری که در عمل نمی‌تواند اهداف اولیه‌ی خود را تأمین کند. یکی از دلایل مهم این ضعف‌ها، تمرکز بیش از حد طراحان روی افزایش کارآیی پروتکل است که باعث شده است تا بده بستان میان کارآیی و امنیت را به خوبی رعایت نکنند. در واقع ایشان با حذف برخی توابع و چکیده‌سازی‌های لازم تلاش کردند تا تعداد محاسبات پروتکل خود را کاهش دهند. حال آنکه این کار باعث کاهش امنیت این پروتکل و ایجاد ضعف‌های اساسی در آن شده است. برای بهبود امنیت طرح سیکاروار و داس در برابر حملاتی که ارائه شد، می‌توان تغییرات زیر را در نظر گرفت:

- برای ثبت نام کاربر از یک کانال امن استفاده شود.
- برای محاسبه مقدار $A_j = f_j \oplus N_i \oplus T_2$ از یک تابع چکیده‌ساز به صورت $A_j = h(f_j \oplus N_i \oplus T_2)$ استفاده شود.
- دست نخوردگی R_{ij} توسط کاربر کنترل شود.

توجه شود موارد ذکر شده در بالا راه حل‌های ابتدایی برای جلوگیری از موفقیت‌آمیز بودن حملاتی است که در این مقاله بحث شده است و این به معنی ادعا در مورد عدم وجود مسائل امنیتی دیگر در پروتکل سیکاروار و داس و نوع بهبود یافته‌ی آن نیست. بنابراین بهبود و مقاوم‌سازی دقیق این پروتکل می‌تواند در ادامه‌ی این مقاله مورد توجه قرار بگیرد.

مراجع

[1] Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, Arun Kumar Sangaiah, and Kim-Kwang Raymond Choo. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications*, 103:194–204, 2018.

[2] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S Morteza Pournaghi, and Mohammad-Ali Doostari. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot. *Computer Networks*, 177:107333, 2020.

[3] Hamza Khemissa and Djamel Tandjaoui. A novel

lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things. In *2016 Wireless Telecommunications Symposium (WTS)*, pages 1–6. IEEE, 2016.

[4] AmirHosein Adavoudi-Jolfaei, Maede Ashouri-Talouki, and Seyed Farhad Aghili. Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. *Peer-to-Peer Networking and Applications*, 12(1):43–59, 2019.

[5] Samir Athmani, Azeddine Bilami, and Djallel Eddine Boubiche. Edak: An efficient dynamic authentication and key management mechanism for heterogeneous wsns. *Future Generation Computer Systems*, 92:789–799, 2019.

[6] Yoney Kirsal Ever. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. *IEEE systems journal*, 13(1):456–467, 2018.

[7] Mohammad Sabzinejad Farash, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. 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, 2016.

[8] 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.

[9] Ruhul Amin, SK Hafizul Islam, GP Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, 101:42–62, 2016.

[10] Yanrong Lu, Lixiang Li, Haipeng Peng, and Yixian Yang. An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks. *Sensors*, 16(6):837, 2016.

[11] Iván Santos-González, Alexandra Rivero-García, Mike Burmester, Jorge Munilla, and Pino Caballero-Gil. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Information Systems*, 88:101423, 2020.

[12] Foroozan Ghosairi Darbandeh and Masoumeh Safkhani. A new lightweight user authentication and key agree-

ment scheme for wsn. *Wireless Personal Communications*, 114(4):3247–3269, 2020.

[13] Jiaqing Mo and Hang Chen. A lightweight secure user authentication and key agreement protocol for wireless sensor networks. *Security and Communication Networks*, 2019, 2019.

[14] Deepti Singh, Bijendra Kumar, Samayveer Singh, and Satish Chand. An efficient biometric based three-factor authentication scheme for wireless sensor network. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pages 875–879. IEEE, 2018.

[15] 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.

[16] Himani Sikarwar and Debasis Das. A lightweight and secure authentication protocol for wsn. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 475–480. IEEE, 2020.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 1 (pp. 1–9)
https://monadi.isc.org.ir

Presented at the ISCISC 2021 in University of Isfahan, Isfahan, Iran

Key Discovery and Forgery Attack on a Key Agreement Protocol with Authentication for Wireless Sensor Network★

Amir Allahdadi Ghiyasabadi * and Javad Alizadeh

Fat'h Science and Technology Center, Faculty and Research Institute of Computer Engineering and Cyber Power, Imam Hossein (AS) University, Tehran, Iran

ARTICLE INFO.

Keywords:
wireless sensor network
key agreement protocol with authentication
key discovery attack
forgery attack

dor: 20.1001.1.24763047.1401.11.1.1.8

Type: research paper

ABSTRACT

With the development of new information and communication technologies such as developments related to Internet of Things applications, the importance of information and maintaining its security is more and more considered. Key agreement and authentication protocols play an important role in ensuring information security. One of the important components used in many applications of the Internet of Things is wireless sensor networks, whose security is ensured by using appropriate protocols of these networks. In 2020, Sikarwar and Das presented a key agreement protocol with authentication for wireless sensor networks and claimed that this protocol is secure against well-known attacks such as feedback attacks, password discovery, and man-in-the-middle attacks. In this paper, it is shown that the Sikarvar and DOS protocol is not secure and an attacker can easily obtain this key. In addition, it is shown that the protocol cannot be secure against password discovery and spoofing attacks.

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: aalahdadi@ihu.ac.ir (Amir Allahdadi Ghiyasabadi), jaalizadeh@ihu.ac.ir (Javad Alizadeh)