دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۲، جلد ۲۱، شماره ۲ (۵۱–۵۹)
https://monadi.isc.org.ir

ارائه‌شده در بیستیمن کنفرانس بین‌المللی انجمن رمز ایران در سازمان پژوهش‌های علمی و صنعتی ایران، ۸ و ۹ شهریور ۱۴۰۲

حمله کشف کلید عملی روی پروتکل احراز اصالت و توافق کلید SecAuthUAV در شبکه پهپادها و ارائه یک پروتکل بهبود یافته★

جواد علیزاده* و سیدهادی نورانی اصل

مرکز علم و فناوری فتح، دانشکده رایانه، شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
شبکه پهپادها
پروتکل احراز اصالت و توافق کلید
حمله کشف کلید
حمله جعل

dor: 20.1001.1.24763047.1402.12.2.6.2

نوع مقاله: پژوهشی

چکیده

مفهوم اینترنت هواپیماهای بدون سرنشین (IoD)، به معنی استفاده از وسایل نقلیه هوایی بدون سرنشین (UAVها) یا پرنده‌های هدایت‌پذیر از راه دور (پهپادها) تحت اینترنت است. این مفهوم که می‌توان آن را یک کاربرد خاص از مفهوم اینترنت اشیا (IoT) دانست، در برابر فرصت‌هایی که ایجاد می‌کند باعث آسیب‌پذیری‌های امنیتی نیز می‌شود. برای جلوگیری از این آسیب‌ها لازم است از پروتکل‌های احراز اصالت و توافق کلید در ارتباطات پهپادها استفاده شود. در سال ۲۰۲۰ علادی و همکاران یک پروتکل احراز اصالت و توافق کلید مبتنی بر توابع کپی‌ناپذیر فیزیکی به نام SecAutUAV ارائه و امنیت طرح خود را با استفاده از روش‌های غیرصوری و صوری بررسی کردند. در این مقاله نشان داده می‌شود پروتکل علادی و همکاران در برابر حمله کشف کلید ضعف اساسی دارد و یک مهاجم می‌تواند با استفاده از اطلاعات یک نشست، کلید نشست پهپاد با ایستگاه زمینی و پهپاد با پهپاد را به طور عملی به دست آورد. به علاوه، حمله کشف مقادیر محرمانه n بیتی با پیچیدگی محاسباتی برابر $2 \times 2^{\frac{n}{2}}$ روی این پروتکل ارائه می‌شود که کوچکتر از پیچیدگی جستجوی جامع است. مهاجم می‌تواند با استفاده از این مقادیر، جعل و ردیابی پهپاد را انجام دهد. برای رفع ضعف‌های امنیتی پروتکل SecAutUAV، یک پروتکل جدید، پیشنهاد و با SecAutUAV مقایسه می‌شود. برای ارزیابی امنیتی پروتکل پیشنهادی از روش‌های غیرصوری و صوری مبتنی بر ابزار ProVerif استفاده شده است. برای مقایسه کارآیی دو پروتکل نیز از روش شمارش تعداد عملگرها و توابع آنها استفاده شده است. نتایج ارزیابی‌ها نشان می‌دهد پروتکل جدید در مقایسه با پروتکل SecAutUAV، امن و کارآ است.

© ۱۴۰۲ انجمن رمز ایران

۱ مقدمه

امروزه برای تسهیل در ارتباطات از شبکه‌های کامپیوتری به صورت گسترده استفاده می‌شود. نفوذ این شبکه‌ها در بخش‌های مختلف زندگی انسان به اندازه‌ای گسترش پیدا کرده است که تصور زندگی بدون آن تقریباً ناممکن است. مفهوم اینترنت اشیا (IoT [1]) که در حال فراگیر شدن است، یک مصداق مهم از پیشرفت فناوری‌ها در حوزه شبکه‌های کامپیوتری است

[1] Internet of Things

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

*نویسنده مسئول.
آدرس‌های رایانامه: jaalizadeh@ihu.ac.ir (جواد علیزاده)، hadinorani@ihu.ac.ir (سیدهادی نورانی اصل)

© ۱۴۰۲ تمامی حقوق متعلق به انجمن رمز ایران است.

[۱]. به طوری که در حال حاضر این فناوری در جنبه‌های مختلف مانند سلامت پزشکی، کشاورزی و سیستم‌های نظارتی کاربردهای بسیار پیدا کرده است.

اینترنت پرنده‌های هدایت‌پذیر از راه دور[1] (پهپادها) که با نام IoD مطرح می‌شود و به معنی کنترل و استفاده از وسایل نقلیه هوایی بدون سرنشین (UAV[2]) تحت شبکه‌های کامپیوتری است، یک نمونه کاربردی از مفهوم IoT می‌باشد که تاثیرهای غیرقابل انکار در حوزه‌های کشاورزی، هوانوردی، نظارت و نظامی دارد [۲]. اگرچه این فناوری باعث پیشرفت‌هایی در حوزه ارتباطات شده است، اما نباید از تهدیدات امنیتی حاصل از آن غافل ماند. برای جلوگیری از این تهدیدات لازم است تا امنیت اطلاعات و ارتباطات در استفاده از یک پهپاد یا شبکه پهپادها تامین شود. به این معنی که پهپادها احراز اصالت شوند و از روش‌های تأمین محرمانگی اطلاعات مانند رمزنگاری برای ارسال و دریافت داده‌های مهم و حیاتی خود استفاده کنند. مشابه اکثر فناوری‌های ارتباطی، در ارتباطات پهپادی نیز برای احراز اصالت پهپادها و سرویس‌دهنده‌های زمینی و توافق کلید محرمانه میان آنها از پروتکل‌های احراز اصالت و توافق کلید استفاده می‌شود. معمولاً این پروتکل‌ها از سه بخش ثبت‌نام اولیه و اشتراک برخی داده‌های آغازین، فرآیند احراز اصالت و توافق کلید در طول یک نشست و به‌روزرسانی مقادیر برای استفاده در نشست‌های بعدی تشکیل شده‌اند [۳].

از آنجا که در پهپادها محدودیت منابع محاسباتی و ذخیره‌سازی وجود دارد، بنابراین لازم است پروتکل‌های مورد استفاده از نوع سبک‌وزن باشند. در سال‌های اخیر پروتکل‌های سبک‌وزن متنوعی برای استفاده در ارتباطات پهپادی یا شبکه پهپادها ارائه شده است. تمام این پروتکل‌ها تلاش می‌کنند تا ویژگی‌های امنیتی مانند احراز اصالت، محرمانگی و نیز حریم خصوصی کاربران را تامین کنند [۴] و در برابر حملات مهم و شناخته شده مانند کشف کلید، جعل، مردی در میانه، انکار سرویس و غیره مقاوم باشند [۵]. به عنوان نمونه در سال ۲۰۱۸ چن[3] و همکاران [۶] یک طرح تصدیق گمنام بی‌واسطه[4] با ویژگی احراز اصالت دو طرفه در شبکه پهپادها ارائه کردند. بنا به ادعای طراحان، طرح ایشان با در نظر گرفتن محدودیت‌های محاسباتی و منابع پهپادها، یک طرح مناسب و امن است. با این حال راه‌حل آن‌ها مبتنی بر استفاده از ماژول‌های پلتفرم مطمئن (TPM[5]) است که باید در سیستم‌ها ادغام شوند. از آنجا که TPMها پردازنده‌های تخصصی گران‌قیمتی هستند، طرح چن و همکاران یک طرح پرهزینه به حساب می‌آید. عبدالله[6] و همکاران [۷] در سال ۲۰۱۹ یک طرح سبک‌وزن برای شبکه‌های پهپادهای نظارتی ارائه کردند. اگرچه این طرح از مزیت سبک‌وزن بودن برخوردار است ولی باید توجه کرد که یک طرح احراز اصالت یک‌طرفه است. سمال[7] و همکاران [۸] در سال ۲۰۱۸ یک پروتکل توافق کلید همراه با احراز اصالت، بدون استفاده از گواهی برای شبکه پهپادها ارائه کردند. این کار براساس زوج‌سازی دوخطی[8] و رمزنگاری مبتنی بر خم بیضوی[9] ارائه شده است و جزو طرح‌های سبک‌وزن قرار نمی‌گیرد. در سال ۲۰۱۹، اسرینیواس[10] و همکاران [۹] یک طرح احراز اصالت سبک‌وزن به نام TCALAS برای شبکه پهپادها ارائه کردند. آنها امنیت طرح خود را در مدل واقعی یا تصادفی[11] و همچنین با استفاده از روش‌های مبتنی بر ابزارهای تحلیل خودکار مورد بررسی قرار دادند. زیشان[12] و همکاران [۱۰] در سال ۲۰۱۹، طرح TCALAS را مورد ارزیابی قرار دادند و علاوه بر ارائه برخی حملات روی آن، گفتند که این طرح تنها برای حالتی که یک ناحیه پرواز موجود باشد، مناسب است. ایشان یک طرح بهبود یافته به نام iTCALAS ارائه کردند که ضعف‌های امنیتی طرح TCALAS را برطرف می‌کرد و می‌توانست برای چند ناحیه پروازی عملی و کاربردی باشد. در سال ۲۰۲۱ برا[13] و همکاران [۱۱] طرح iTCALAS را مطالعه و نشان دادند که این طرح برخی ضعف‌های امنیتی مانند لو رفتن کلید نشست دارد. سپس ایشان یک طرح کنترل دسترسی مبتنی بر بلاک‌چین برای تشخیص UAVها و پروازهای غیرمجاز ارائه کردند. برا و همکاران امنیت طرح خود را در مدل واقعی یا تصادفی اثبات نمودند.

طرح‌های احراز اصالت شبکه پهپادها که تا اینجا معرفی شدند روی تامین ویژگی احراز اصالت و مقاومت در برابر حملات پروتکل و شبکه تمرکز داشتند و آسیب‌پذیری در برابر حملات فیزیکی و حملات دستکاری گره را مورد بحث قرار ندادند. برای تامین این هدف، در سال ۲۰۲۰ علادی[14] و همکاران [۱۲] یک طرح احراز اصالت و توافق کلید دو طرفه سبک‌وزن مبتنی بر توابع کپی‌ناپذیر فیزیکی (PUF[15]) به نام SecAuthUAV ارائه کردند. اگرچه این طرح برای استفاده میان یک UAV با ایستگاه زمینی طراحی شده است اما می‌توان آن را میان دو UAV هم به کار برد. آنها امنیت پروتکل خود را با استفاده از منطق مائو بوید[16] [۱۳] مورد بررسی قرار دادند و ادعا کردند طرحشان در برابر حملات شناخته شده مانند حملات کشف کلید و جعل امن است. در این مقاله امنیت پروتکل SecAuthUAV مورد مطالعه قرار می‌گیرد و نشان داده می‌شود علی‌رغم ادعای طراحان، این پروتکل نمی‌تواند در برابر حملاتی مانند کشف کلید، کشف مقادیر محرمانه، جعل و ردیابی مقاوم باشد. بعد از مشخص کردن نقاط ضعف پروتکل SecAuthUAV، یک نسخه بهبود یافته از این پروتکل ارائه می‌شود. به طوری که نسخه جدید در برابر حملات شناخته شده مهم مقاوم باشد. برای اطمینان بیشتر از امنیت پروتکل جدید، امنیت آن به روش صوری[17] و با استفاده از ابزار خودکار ProVerif نیز مورد بررسی قرار می‌گیرد. نتایج این ارزیابی نشان می‌دهد این پروتکل نشت اطلاعات ندارد. علاوه بر این، دو طرح SecAuthUAV و بهبود یافته از نظر سرعت محاسباتی و کارآیی نیز باهم مقایسه می‌شوند که نتایج نشان از کارآیی بالای طرح بهبود یافته در مقایسه با طرح اصلی دارد. نتایج مقایسه دو پروتکل از لحاظ امنیت و کارآیی به ترتیب در جدول‌های ۱ و ۳ خلاصه شده است.

ادامه مقاله به این صورت سازمان‌دهی شده است که در بخش ۲، پروتکل SecAuthUAV توصیف می‌شود. در بخش ۳، این پروتکل مورد

[1] Internet of Drones [2] Unmanned Aerial Vehicles [3] Chen [4] Direct Anonymous Attestation (DAA) [5] Trusted Platform Modules [6] Abdallah [7] Semal

[8] Bilinear Pairing [9] Elliptical Curve Cryptography [10] Srinivas [11] Real-Or-Random [12] Zeeshan [13] Bera [14] Tejasvi Alladi [15] Physically Unclonable Functions (PUF) [16] Mao Boyd [17] Formal

جدول ۱. مقاومت پروتکل SecAuthUAV و پروتکل بهبود یافته در برابر برخی حملات شناخته شده

حمله	SecAuthUAV	طرح بهبود یافته
حمله کشف کلید نشست	✘	✔
حمله کشف مقادیر محرمانه	✘	✔
حمله جعل پهپاد	✘	✔
حمله ردیابی پهپاد	✘	✔

جدول ۲. مقایسه کارآیی پروتکل SecAuthUAV و پروتکل بهبود یافته با توجه به نوع و تعداد عملگرهای آنها

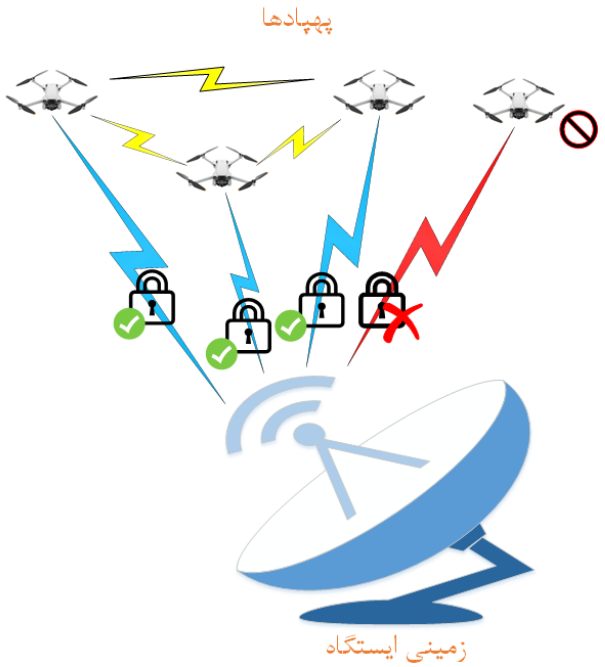
طرح	تعداد توابع و عملگر لازم				
	XOR	تکشمار	تابع چکیده‌ساز	تابع PUF	الحاق
SecAuthUAV	۱۶	۳	۸	۲	۲۵
بهبود یافته	۳	۱	۸	۲	۱۴

ارزیابی امنیتی قرارگرفته و حمله‌های کشف کلید، کشف مقادیر محرمانه، جعل و ردیابی روی آن اعمال می‌شود. در بخش ۴، یک نسخه بهبود یافته از پروتکل SecAuthUAV ارائه می‌شود.در این بخش همچنین پروتکل بهبود یافته به روش غیرصوری و روش صوری مبتنی بر استفاده از ابزار ProVerif مورد ارزیابی امنیتی قرار می‌گیرد. در نهایت جمع‌بندی و نتیجه‌گیری مقاله در بخش ۵ بیان می‌شود.

۲ توصیف پروتکل SecAuthUAV

پروتکل SecAuthUAV در یک شبکه ارتباطی میان پهپادها با ایستگاه زمینی و یا دو پهپاد با یکدیگر، با هدف احراز اصالت متقابل و توافق کلید به کار می‌رود. معماری شبکه ذکر شده را می‌توان مطابق شکل ۱ در نظر گرفت. قابلیت اصلی پروتکل SecAuthUAV این است که یک پهپاد قانونی بتواند اصالت خود را برای ایستگاه زمینی احراز کند و علاوه بر این از اصالت ایستگاه زمینی قانونی نیز مطمئن شود. بعد از این کار نیز یک کلید نشست میان پهپاد و ایستگاه زمینی توافق می‌شود. برای اینکه دو پهپاد با استفاده از پروتکل SecAuthUAV از اصالت یکدیگر مطمئن شده و میان خود یک کلید محرمانه توافق کنند، لازم است تا آنها از اطلاعاتی که در مرحله احراز اصالت و توافق کلید پهپاد و ایستگاه زمینی تولید می‌شود، استفاده نمایند.

پروتکل SecAuthUAV یک پروتکل مبتنی بر توابع کپی‌ناپذیر فیزیکی (PUF) است که منظور از آن، توابعی هستند که روی پهپادها پیاده‌سازی می‌شوند و غیر قابل کپی هستند. این توابع برای هر ورودی منحصر به فرد مانند C، یک خروجی منحصر به فرد مانند R تولید می‌کنند. به طوری که با داشتن یا نداشتن C، امکان حدس یا کپی کردن R وجود ندارد. مشابه اکثر پروتکل‌های احراز اصالت و توافق کلید، پروتکل SecAuthUAV نیز از سه مرحله ثبت‌نام، احراز اصالت و توافق کلید و به‌روزرسانی تشکیل شده است که در ادامه توصیف می‌شوند. برای توصیف این مراحل از نمادگذاری جدول ؟؟ استفاده شده است.



شکل ۱. معماری شبکه ارتباطات میان پهپادها و ایستگاه زمینی در پروتکل SecAuthUAV

جدول ۳. نمادگذاری برای توصیف پروتکل SecAuthUAV

توضیحات	نمادها
شناسه موقت پهپاد	PID_i^t
شناسه ایستگاه زمینی	GID
تابع کپی‌ناپذیر فیزیکی	PUF
الحاق	$\|$
عملگر XOR	$\oplus$
تابع چکیده ساز	$H()$
مهر زمانی	T_i
کلید نشست	SK_i
تکشمار	N_X
زوج چالش و پاسخ پهپاد	(C, R)
ایستگاه زمینی	GS

۱.۲ ثبت نام

در شروع پروتکل SecAuthUAV لازم است تا پهپاد توسط ایستگاه زمینی معتبر ثبت نام شود. برای این منظور ابتدا یک زوج چالش و پاسخ مانند (C, R) توسط تابع PUF روی پهپاد، تولید می‌شود. سپس یک شناسه موقت برای پهپاد مانند PID_i^t در نظر گرفته شده و همراه با زوج چالش و پاسخ (C, R) به صورت امن در پایگاه داده ایستگاه زمینی ذخیره می‌شود. همچنین شناسه معتبر ایستگاه زمینی، یعنی GID نیز در حافظه پهپاد ذخیره می‌شود.

شکل ۲. مراحل احراز اصالت و توافق کلید و به‌روزرسانی پروتکل SecAuthUAV

پهپاد		ایستگاه زمینی
تولید N_A		
$\{PID_i^t, N_A, H(R\|PID_i^t\|N_A)\}$	$\Longrightarrow$	دریافت R از پایگاه داده
		بررسی
		$H(R\|PID_i^t\|N_A)$
		$R = (K_1, K_2)$
		تولید N_B
		$X_1 = N_A \oplus K_2$
		$Y_2 = N_B \oplus X_1 \oplus K_1$
		$Q = (Y_2\|X_1) \oplus (K_2\|K_1)$
$R = (K_1, K_2)$	$\Longleftarrow$	$\{Q, H(Q\|GID\|N_B\|N_A)\}$
$Y_2\|X_1 = K_2\|K_1 \oplus Q$		
$N_B = Y_2 \oplus X_1 \oplus K_1$		
$N_A = X_1 \oplus K_2$		
بررسی		
$H(Q\|GID\|N_B\|N_A)$		
تولید N_C		
تولید C' از N_C		
$R' = PUF(C')$		
$M' = R' \oplus K_2\|K_1$		
$N' = N_C \oplus K_1$		
$(SK_i) = (K_1 \oplus N_B)\|(K_2 \oplus N_C)$		
$PID_i' = H(K_2\|PID_i^t\|K_1)$		
$\{M', N', H(R'\|PID_i^t\|N_B\|N_C\|SK_i)\}$		
	$\Longrightarrow$	$R' = M' \oplus K2\|K1$
		$N_C = N' \oplus K_1$
		$(SK_i) = (K_1 \oplus N_B)\|(K_2 \oplus N_C)$
		بررسی
		$H(R'\|PID_i^t\|N_B\|N_C\|SK_i)$
		$PID_i' = H(K_2\|PID_i^t\|K_1)$
		جایگزین کردن R و PID_i^t با R' و PID_i'

۲.۲ احراز اصالت متقابل پهپاد و ایستگاه زمینی و توافق کلید میان آنها همراه با به‌روزرسانی مقادیر

در این مرحله یک پهپاد و ایستگاه زمینی قانونی می‌توانند به صورت متقابل اصالت یکدیگر را احراز نموده و میان خود یک کلید محرمانه توافق کنند. با استفاده از نمادگذاری جدول ؟؟ توصیف این پروتکل به صورت خلاصه در شکل ۲ آورده شده است.

با توجه به شکل ۲، در مرحله احراز اصالت و توافق کلید پهپاد با ایستگاه زمینی، پهپاد یک مقدار تک‌شمار مانند N_A را تولید می‌کند و با استفاده از زوج چالش و پاسخ که از مرحله ثبت نام در اختیار دارد، مقدار $PID_i^t, N_A, H(R\|PID_i^t\|N_A)$ را برای ایستگاه زمینی ارسال می‌کند. ایستگاه زمینی با توجه به PID_i^t، مقدار R متناظر پهپاد را از پایگاه داده خود فراخوانی کرده و با بررسی مقدار تابع چکیده‌ساز دریافتی از پهپاد، اصالت آن را تایید می‌کند. سپس ایستگاه زمینی، R را به دو بخش K_1 و K_2 تقسیم می‌کند و با تولید تک‌شمار N_B، محاسبات مشخص شده در شکل ۲ را انجام و مقدار $Q, H(Q\|GID\|N_B\|N_A)$ را برای پهپاد می‌فرستد. به طور مشابه، پهپاد نیز R را به دو بخش K_1 و K_2 تقسیم می‌کند و با استفاده از مقادیر دریافتی از ایستگاه زمینی و محاسبات مشخص شده در شکل ۲ مقدار N_B را محاسبه کرده و با بررسی مقدار تابع چکیده‌ساز دریافتی از ایستگاه زمینی، اصالت آن را تایید می‌کند. بعد از این کار نیز یک مقدار تک‌شمار جدید مانند N_C تولید کرده و کلید نشست $(SK_i) = (K_1 \oplus N_B)\|(K_2 \oplus N_C)$ را حساب می‌کند. در نهایت پهپاد N_C را به شکل امن برای ایستگاه زمینی می‌فرستد تا ایستگاه زمینی هم بتواند کلید نشست مشترک با پهپاد را محاسبه کند. با توجه به محاسبات شکل ۲ پهپاد مقادیر زوج چالش و پاسخ و شناسه موقت خود را به‌روز می‌کند و مقدار جدید R' را به شکل امن برای ایستگاه زمینی می‌فرستد تا بعد از محاسبه شناسه موقت جدید پهپاد یعنی PID_i' توسط ایستگاه زمینی، دو مقدار R' و PID_i' جایگزین مقدارهای R و PID_i^t قبلی در پایگاه داده ایستگاه زمینی شوند.

۳ ارزیابی امنیتی پروتکل SecAuthUAV

برای ارزیابی پروتکل SecAuthUAV از مدل مهاجم دالو یائو[1] [۱۴] استفاده می‌شود. در این مدل، مهاجم مورد نظر یک مهاجم فعال است که می‌تواند پیام‌های تبادل شده در کانال را شنود و ذخیره کرده و حتی تغییر دهد. این مهاجم می‌تواند از اعضای شبکه نیز باشد که به عنوان مهاجم داخلی تعریف می‌شود. یک مهاجم می‌تواند به صورت عملی، کلید نشست میان ایستگاه زمینی و پهپاد را به دست آورد و اطلاعات محرمانه میان آنها را شنود کند. علاوه بر این او می‌تواند اطلاعات محرمانه یک پهپاد را به دست آورده و آن را جعل و ردیابی کند. این حملات قابل تعمیم به حمله‌های موفق روی ارتباطات پهپاد و پهپاد خواهند بود.

۱.۳ حمله کشف کلید نشست

مهم‌ترین حمله روی پروتکل SecAuthUAV، حمله کشف کلید است که در آن مهاجم می‌تواند کلید هر نشست را به صورت عملی به دست آورد. این حمله تنها با استفاده از اطلاعات نشست کنونی، قابل محاسبه است.

برای توضیح این حمله، رابطه محاسبه کلید نشست میان پهپاد و ایستگاه زمینی را به صورت رابطه (۱) در نظر بگیرید.

$$(SK_i) = (K_1 \oplus N_B)\|(K_2 \oplus N_C) \qquad (۱)$$

از طرفی با توجه به محاسبات در سمت ایستگاه زمینی، $Y_2 = N_B \oplus X_1 \oplus K_1$ است که از روی آن رابطه (۲) به صورت زیر به دست می‌آید.

$$Y_2 \oplus X_1 = K_1 \oplus N_B \qquad (۲)$$

از محاسبات در سمت ایستگاه زمینی می‌توان رابطه (۳) را در نظر گرفت.

$$X_1 = N_A \oplus K_2 \qquad (۳)$$

با جاگذاری (۳) در رابطه (۲)، رابطه (۴) به صورت زیر حاصل می‌شود.

$$Y_2 \oplus N_A \oplus K_2 = K_1 \oplus N_B \qquad (۴)$$

[1] Dolev-Yao

از طرف دیگر با توجه به محاسبات سمت پهپاد و $N' = N_C \oplus K_1$ در آن رابطه (۵) را به صورت زیر می‌توان نوشت.

$$N_C = N' \oplus K_1 \quad (۵)$$

با جاگذاری (۴) و (۵) در (۱)، این رابطه به شکل (۶) بازنویسی می‌شود.

$$(SK_i) = (Y_2 \oplus N_A \oplus K_2)\|(K_2 \oplus N' \oplus K_1) \quad (۶)$$

مهاجم در زمان ارسال اطلاعات از طرف ایستگاه زمینی به سمت پهپاد، $Q = (Y_2\|X_1) \oplus (K_2\|K_1)$ را شنود می‌کند. با توجه به ویژگی‌های عملگرهای XOR و الحاق، رابطه اخیر را به صورت رابطه (۷) می‌توان بازنویسی کرد.

$$Q = (Y_2 \oplus K_2)\|(X_1 \oplus K_1) \quad (۷)$$

به عبارت دیگر مهاجم با شنود Q مقدار $Y_2 \oplus K_2$ را در اختیار دارد. از طرف دیگر مهاجم در شروع پروتکل، زمان ارسال اطلاعات از سمت پهپاد به سمت ایستگاه زمینی، مقدار N_A را نیز شنود کرده است. بنابراین مهاجم می‌تواند مقدار $Y_2 \oplus N_A \oplus K_2$ را حساب کند که با توجه به رابطه (۶) یک نیمه از کلید نشست است. برای محاسبه نیمه دوم کلید نشست، یعنی مقدار $K_2 \oplus N' \oplus K_1$ در رابطه (۶)، مهاجم محاسبات خود را به این صورت ادامه می‌دهد که ابتدا رابطه (۲) را مطابق رابطه (۸) بازنویسی می‌کند.

$$N_B = Y_2 \oplus X_1 \oplus K_1 \quad (۸)$$

حال مقدار K_2 را دو بار در سمت راست رابطه (۸) XOR می‌کند. این تغییر در رابطه (۹) آورده شده است.

$$N_B = (Y_2 \oplus K_2) \oplus (X_1 \oplus K_1 \oplus K_2) \quad (۹)$$

با توجه به رابطه (۳)، رابطه (۹) به صورت رابطه (۱۰) بازنویسی می‌شود.

$$N_B = (Y_2 \oplus K_2) \oplus (N_A \oplus K_1) \quad (۱۰)$$

مهاجم طرفین دو رابطه (۹) و (۱۰) را با همدیگر XOR کرده و رابطه (۱۱) را به صورت زیر به دست می‌آورد.

$$\begin{aligned} 0 &= (X_1 \oplus K_1 \oplus K_2) \oplus (N_A \oplus K_1) \Rightarrow \\ 0 &= (X_1 \oplus K_1) \oplus N_A \oplus (K_1 \oplus K_2) \end{aligned} \quad (۱۱)$$

۲.۳ حمله به دست آوردن مقدار محرمانه R یک پهپاد توسط مهاجم داخلی

با توجه به اینکه امنیت پروتکل SecAuthUAV کاملاً مبتنی بر محرمانگی R است، اگر این امر نقض شود، مهاجم می‌تواند حملات دیگری مانند حمله جعل و حمله ردیابی نیز انجام دهد. اگر R مقدار n بیتی داشته باشد، مهاجم داخلی می‌تواند این مقدار را با پیچیدگی محاسباتی $2 \times 2^{\frac{n}{2}}$ حساب کند. در حالی که جستجوی جامع آن پیچیدگی محاسباتی برابر 2^n دارد. منظور از مهاجم داخلی، یک پهپاد غیر از پهپاد قربانی است که قبلاً در شبکه پهپادها ثبت نام کرده و GID ایستگاه زمینی را در اختیار دارد. در این حمله مهاجم مقدار $\{Q, H(Q\|GID\|N_B\|N_A)\}$ را شنود می‌کند و $H(Q\|GID\|N_B\|N_A)$ را با توجه به رابطه (۱۰) به صورت رابطه (۱۲) بازنویسی می‌کند.

$$z = H(Q\|GID\|(Y_2 \oplus K_2) \oplus (N_A \oplus K_1)\|N_A) \quad (۱۲)$$

حال مهاجم تمام مولفه‌های لازم برای محاسبه مقدار چکیده‌سازی، به جز K_1 را در اختیار دارد. از طرف دیگر مهاجم مقدار چکیده‌ساز را هم از پروتکل SecAuthUAV شنود کرده است که در رابطه (۱۲) برابر z در نظر گرفته شده است. بنابراین مهاجم می‌تواند روی K_1 جستجوی جامع انجام دهد و با وارد کردن آن در سمت راست رابطه (۱۲) و مقایسه خروجی با مقدار z در سمت چپ رابطه (۱۲)، مقدار صحیح K_1 را به دست آورد. برای به دست آوردن مقدار صحیح K_2 با جستجوی جامع نیز، ابتدا مهاجم با در اختیار داشتن کلید نشست از حمله کشف کلید و مقدار K_1 و با توجه به رابطه (۱)، مقدار N_B را حساب می‌کند. سپس با توجه به رابطه (۷) مقدار X_1 را حساب می‌کند. حال در رابطه (۱۲) به جای N_A، مقدار $X_1 \oplus K_2$ را وارد کرده و مشابه جستجوی جامع K_1، این بار جستجوی جامع K_2 را انجام می‌دهد.

۳.۳ حمله جعل پهپاد

از آنجا که در شروع پروتکل، شناسه موقت پهپاد یعنی PID_{i^t} به صورت آشکار از طرف پهپاد به سمت ایستگاه زمینی ارسال می‌شود، مهاجم می‌تواند این مقدار را شنود کند و با در اختیار داشتن مقدار محرمانه R پهپاد را جعل نماید. به این صورت که مهاجم در نشست زمان t یک پهپاد با ایستگاه زمینی، ابتدا M' را شنود کرده و با توجه به اینکه K_1 و K_2 را در اختیار دارد، مقدار R' را با توجه به رابطه $M' = R' \oplus K_2\|K_1$ محاسبه می‌کند. همچنین او می‌تواند شناسه موقت جدید پهپاد قربانی را با توجه به رابطه $PID'_i = H(K_2\|PID_i^t\|K_1)$ حساب کند. حال مهاجم با در اختیار داشتن R' و PID'_i می‌تواند در زمان $t+1$ شروع کننده ارتباط با ایستگاه زمینی، به جای پهپاد قربانی باشد.

۴.۳ حمله ردیابی

از آنجا که مهاجم شناسه موقت پهپاد را شنود کرده و در اختیار دارد و همچنین می‌تواند همانند خود پهپاد آن را به‌روز کند، بنابراین در هر نشستی او می‌تواند مقدار $H(R\|PID_i^t\|N_A)$ را برای هر پهپاد محاسبه کند و ارتباطات آن را ردیابی نماید.

۴ پروتکل بهبودیافته و ارزیابی آن

در این بخش، یک پروتکل جدید با توجه به اصول طراحی پروتکل SecAuthUAV، مبتنی بر توابع کپی‌ناپذیر فیزیکی طوری ارائه می‌شود که در برابر حملات بحث شده، مقاوم باشد. این پروتکل نیز شامل سه مرحله ثبت‌نام، احراز اصالت و توافق کلید و مرحله به‌روزرسانی است که در شکل ۳ خلاصه شده است.

شکل ۳. مراحل پروتکل پیشنهادی

مراحل	پهپاد		ایستگاه زمینی
مرحله ثبت‌نام	(PID_i^t, C, R, GID)		(PID_i^t, C, R)
مرحله احرازهویت و توافق کلید	$R = PUF(C), T_1$ $H_1 = H(PID_i^t \| R \| T_1)$ $\{PID_i^t, H_1, T_1\}$	$\Longrightarrow$	T_2 $T_2 - T_1 \leq \Delta T$ بررسی چکیده‌ساز $H(PID_i^t \| R \| T_1)$ $SK = R$ T_3 $H_2 = H(GID \| R \| T_3)$
	T_4 $T_4 - T_3 \leq \Delta T$ بررسی چکیده‌ساز $H(GID \| R \| T_3)$ $SK = R$	$\Longleftarrow$	$\{H_2, T_3\}$
مرحله به‌روزرسانی	تولید N'_C تولید (C') از N'_C $R' = PUF(C')$ $tempR' = R' \oplus R$ T_5 $H_3 =$ $H(tempR' \| (R \oplus 1) \| T_5)$ $PID'_i = H(PID_i^t \| R')$ $\{H_3, tempR', T_5\}$	$\Longrightarrow$	T_6 $T_6 - T_5 \leq \Delta T$ بررسی چکیده‌ساز $H(tempR' \| (R \oplus 1) \| T_5)$ $R' = R \oplus tempR'$ $PID'_i = H(PID_i^t \| R')$

۱.۴ ارزیابی امنیتی پروتکل پیشنهادی

برای ارزیابی امنیتی پروتکل پیشنهادی از دو روش غیرصوری، به معنای بررسی مقاومت پروتکل در برابر حملات شناخته شده و روش صوری مبتنی بر ابزار ProVerif استفاده می‌شود.

۱.۱.۴ مقاومت در برابر حمله نقاب‌گذاری و مردی در میانه

از آنجا که مهاجم در پروتکل پیشنهادی نمی‌تواند به زوج چالش و پاسخ تابع کپی‌ناپذیر فیزیکی پهپاد دسترسی داشته باشد، بنابراین نمی‌تواند خود را به جای ایستگاه زمینی یا یک پهپاد قانونی معرفی کند.

۲.۱.۴ حمله تکرار

تلاش‌های مهاجم برای استفاده از پیام‌های قدیمی ایستگاه زمینی یا پهپاد با شکست مواجه می‌شود. زیرا در هر نشست یک زوج چالش و پاسخ جدید استفاده می‌شود و تازگی پیام‌های دریافتی و ارسالی با استفاده از مهر زمانی سنجیده می‌شود.

۳.۱.۴ حمله شبیه‌سازی و دستکاری پهپاد

از آنجا که توابع کپی‌ناپذیر فیزیکی تعبیه شده در پهپاد، قابل کپی کردن و استفاده مجدد نیستند، مهاجم نمی‌تواند یک پهپاد را شبیه‌سازی یا دستکاری کند.

۴.۱.۴ حمله کشف کلید نشست

در پروتکل پیشنهادی کلید نشست معادل با پاسخ تابع کپی‌ناپذیر فیزیکی یک پهپاد در نظر گرفته شده است که در ابتدا در مرحله ثبت‌نام میان پهپاد و ایستگاه زمینی به صورت امن به اشتراک گذاشته شده و برای نشست‌های بعدی توسط پهپاد به‌روز شده و به صورت امن برای ایستگاه زمینی ارسال می‌شود. با توجه به روش تأمین امنیت در مرحله ثبت نام و مرحله ارسال مقدار به‌روز شده، پروتکل نشتی خاصی از این مؤلفه ندارد.

۵.۱.۴ حمله انکار سرویس

در پروتکل پیشنهادی، مهاجم نمی‌تواند با روش‌هایی باعث عدم سرویس‌دهی ایستگاه زمینی به پهپاد یا قطع ارتباط پهپاد با ایستگاه زمینی شود. زیرا هم پهپاد و هم ایستگاه زمینی بعد از دریافت پیام‌ها ابتدا اعتبار مهرزمانی و دست نخوردگی پیام را بررسی کرده و سپس اقدام به به‌روزرسانی و تبادل کلید نشست می‌شوند.

۶.۱.۴ امنیت پیشرو و پسرو

تأمین امنیت پیشرو و پسرو در طرح‌های احراز اصالت مبتنی بر استفاده از توابع چکیده‌ساز و حتی رمزهای متقارن، همیشه جزو چالش‌های اساسی بوده است. به طوری که برای تأمین این نوع امنیت در طرح‌های ذکر شده لازم است تا شرایط و محدودیت‌هایی برای مهاجم در نظر گرفته شود. در طرح پیشنهادی نیز شرط تأمین امنیت پیشرو و پسرو این است که مهاجم اطلاعات برخی از نشست‌ها را از دست داده باشد. به این معنی که اگر مهاجم نتواند کلید نشست زمان t را در اختیار داشته باشد، آنگاه نمی‌تواند کلید نشست زمان $t+1$ را حساب کند.

۷.۱.۴ ارزیابی صوری با استفاده از ابزار ProVerif

در این مقاله پروتکل پیشنهادی با استفاده از ابزار ProVerif [۱۵] نیز مورد ارزیابی قرار گرفت که کدهای مربوط به آن در شکل ۴ ارائه شده

شکل ۴. کدهای پروتکل بهبودیافته برای ارزیابی با ابزار ProVerif

```
free C1:channel.
free R:bitstring[private].
free c:bitstring[private].
free c':bitstring[private].
free R':bitstring[private].
free H1:bitstring.
free H1':bitstring.
free H2:bitstring.
free H2':bitstring.
free H3:bitstring.
free H3':bitstring.
free GID:bitstring.
free TUIDI:bitstring.
free SKI:bitstring[private].
free t1:bitstring.
free t3:bitstring.
free t5:bitstring.
free tempR':bitstring.
(*.....*)
fun
xor(bitstring,bitstring):bits
tring.
equation forall
p:bitstring,u:bitstring;
xor(xor(p,u),u)=p.
fun
concat(bitstring,bitstring):
bitstring.
fun h(bitstring):bitstring.
fun puf(bitstring):bitstring.
(*.....*)
query attacker(R).
query attacker(R').
query attacker(SKI).
query inj-event(A2)==>inj-
event(A1).
query inj-event(B2)==>inj-
event(B1).
query inj-event(D2)==>inj-
event(D1).
(*.....*)
event A1.
event A2.
event B1.
event B2.
event D1.
event D2.
(*.....*)
let ui=
let R=puf(c) in
let
H1=h(concat(R,concat(TUIDI,t1))
) in
event A1;
out(C1,(t1,H1));
in(C1,y:bitstring);
let
H2'=h(concat(GID,concat(R,t3)))
in
if H2=H2' then
event B2;
let SKI=R in
new nonce:bitstring;
let R'=puf(c') in
let tempR'=xor(R',R) in
let
H3=h(concat(tempR',concat(R,t5)
)) in
event D1;
out(C1,(H3,tempR',t5));
0.
(*.....*)
let GS=
in(C1,x:bitstring);
let
H1'=h(concat(R,concat(TUIDI,t1)
)) in
if H1=H1' then
event A2;
let SKI=R in
let
H2=h(concat(GID,concat(R,t3)))
in
event B1;
out(C1,(t3,H2));
in(C1,z:bitstring);
let R'=xor(tempR',R) in
let
H3'=h(concat(tempR',concat(R,t5
))) in
if H3'=H3 then
event D2;
0.
process
ui|GS
```

است. نتایج این ارزیابی نشان می‌دهد از نظر تحلیل و ارزیابی با روش خودکار مبتنی بر ProVerif، پروتکل پیشنهادی ضعف خاصی ندارد.

۵ نتیجه‌گیری

در این مقاله، پروتکل SecAuthUAV مورد تحلیل و ارزیابی امنیتی قرار گرفت. نشان داده شد این پروتکل نمی‌تواند کلید نشست را به صورت امن به اشتراک بگذارد و یک مهاجم می‌تواند به صورت عملی این کلید را به دست آورد. همچنین یک حمله کشف مقدار محرمانه R با پیچیدگی کمتر از جستجوی جامع ارائه و نشان داده شد یک مهاجم می‌تواند با در اختیار داشتن این مقدار، پهپاد را جعل و ردیابی نماید. در بخش دوم این مقاله، یک پروتکل احراز اصالت و توافق کلید بهبود یافته مبتنی بر توابع کپی‌ناپذیر فیزیکی ارائه شد. پروتکل جدید علاوه بر این که از لحاظ امنیتی مورد ارزیابی قرار گرفت، از جهت کارآیی نیز با پروتکل SecAuthUAV مقایسه شد. به طوری که نتایج مقایسه‌ها نشان از امنیت و کارآیی بالای پروتکل بهبودیافته در مقایسه با پروتکل علادی و همکاران دارد.

مراجع

[1] ITU, Recommendation ITU-T Y. 2060: Overview of the internet of things. *International Telecommunication Union*, 2012.

[2] Gupta, Lav, Jain, Raj, and Vaszkun, Gabor. Survey of important issues in uav communication networks. *IEEE communications surveys & tutorials*, 18(2):1123–1152, 2015.

[3] Idrus, Syed Zulkarnain Syed, Cherrier, Estelle, Rosenberger, Christophe, and Schwartzmann, Jean-Jacques. A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5):95–107, 2013.

[4] Vasilomanolakis, Emmanouil, Daubert, Jörg, Luthra, Manisha, Gazis, Vangelis, Wiesmaier, Alex, and Kikiras, Panayotis. On the security and privacy of internet of things architectures and systems. in *2015 international workshop on secure internet of things (SIoT)*, pp. 49–57. IEEE, 2015.

[5] Panda, Prabhat Kumar and Chattopadhyay, Sudipta. A secure mutual authentication protocol for iot environment. *Journal of Reliable Intelligent Environments*, 6:79–94, 2020.

[6] Chen, Liquan, Qian, Sijie, Lim, Ming, and Wang, Shihui. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems. *China communications*, 15(5):61–76, 2018.

[7] Abdallah, Asmaa, Ali, M Zulfiker, Mišić, Jelena, and Mišić, Vojislav B. Efficient security scheme for disaster surveillance uav communication networks. *Information*, 10(2):43, 2019.

[8] Semal, Benjamin, Markantonakis, Konstantinos, and Akram, Raja Naeem. A certificateless group authenticated key agreement protocol for secure communication in untrusted uav networks. in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pp. 1–8. IEEE, 2018.

[9] Srinivas, Jangirala, Das, Ashok Kumar, Kumar, Neeraj, and Rodrigues, Joel JPC. Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. *IEEE Transactions on Vehicular Technology*, 68(7):6903–6916, 2019.

[10] Ali, Zeeshan, Chaudhry, Shehzad Ashraf, Ramzan, Muhammad Sher, and Al-Turjman, Fadi. Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. *IEEE Access*, 8:43711–43724, 2020.

[11] Bera, Basudeb, Das, Ashok Kumar, and Sutrala, Anil Kumar. Private blockchain-based access control mechanism for unauthorized uav detection and mitigation in internet of drones environment. *Computer Communications*, 166:91–109, 2021.

[12] Alladi, Tejasvi, Bansal, Gaurang, Chamola, Vinay, Guizani, Mohsen, et al. Secauthuav: A novel authentica-

tion scheme for uav-ground station and uav-uav communication. *IEEE Transactions on Vehicular Technology*, 69(12):15068–15077, 2020.

[13] Mao, Wenbo and Boyd, Colin. Towards formal analysis of security protocols. in *[1993] Proceedings Computer Security Foundations Workshop VI*, pp. 147–158. IEEE, 1993.

[14] Dolev, Danny and Yao, Andrew. On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208, 1983.

[15] Blanchet, Bruno, Smyth, Ben, Cheval, Vincent, and Sylvestre, Marc. Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutorial. *Version from*, pp. 05–16, 2018.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2023, Volume 21, Number 2 (pp. 51–59)
https://monadi.isc.org.ir

Presented at the ISCISC 2023 in Iranian Research Organization for Science & Technology, Tehran, Iran

Practical key recovery attack on authentication and key agreement protocol SecAuthUAV in a network of drones and provide an improved protocol★

Javad Alizadeh * and Seyyed Hadi Noorani Asl

Fath Center, Faculty of Computer, Network and Communication, Imam Hosein University, Tehran, Iran

ARTICLE INFO.

Keywords:
Network of drones
Authentication and key agreement protocol
Key recovery attack
Forgery attack

dor: 20.1001.1.24763047.1402.12.2.6.2

Type: Research paper

ABSTRACT

The Internet of Drones (IoD) refers to the use of unmanned aerial vehicles (UAVs) connected to the Internet. This concept is a specific application of IoT. The IoD may offer opportunities, but it also poses security vulnerabilities. It is necessary to use authentication and key agreement protocols in drone communications to prevent these vulnerabilities. In 2020, Alladi et al presented an authentication and key agreement protocol based on physical unclonable functions called SecAutUAV. They analyzed the security of their scheme through both formal and informal methods. In this paper, we demonstrate the vulnerability of the SecAuthUAV protocol to a key recovery attack. An adversary can obtain a session key between a drone and a ground station by intercepting and analyzing the session data. In addition, we present a secret value recovery attack with complexity $2 \times 2^{\frac{n}{2}}$, which is lower than the complexity of brute force attacks. An adversary could spoof and track the drone by using these values. In order to improve the security and efficiency of SecAuthUAV, we present a new version and compare it to the original. We utilize both the informal method and formal-based ProVerif to analyze the security of the latest protocol. To compare the efficiency of the new protocol and SecAuthUAV, we counted their number of operators and functions. The new protocol is more secure and efficient than SecAutUAV.

© 2023 ISC

★ The ISCISC 2023 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: jaalizadeh@ihu.ac.ir (Javad Alizadeh), hadinorani@ihu.ac.ir (Seyyed Hadi Noorani Asl)
© 2023 ISC. All rights reserved.