دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۲ (۴۴-۵۱)
https://monadi.isc.org.ir

ارائه‌شده در نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه گیلان، ۹ و ۱۰ شهریور ۱۴۰۱

تحلیل امنیتی یک پروتکل تبادل کلید و احراز اصالت گمنام در شبکه حسگرهای پوششی★

صبا مرندی* و فرخ لقا معظمی گودرزی

پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
شبکه حسگرهای پوششی
احراز هویت متقابل
تبادل کلید
حمله‌ی جعل هویت گره حسگر

dor: 20.1001.1.24763047.1401.11.2.5.4

نوع مقاله: پژوهشی

چکیده

در زمینه‌ی پزشکی شبکه حسگرهای پوششی شبکه‌ی حسگرهایی است که روی بدن یا داخل بدن انسان‌ها قرار می‌گیرند و سرویس‌های آسان و بهینه‌ای را برای بیماران و پرسنل پزشکی فراهم می‌کنند. اطلاعات فیزیولوژیکی بیماران بسیار حساس و شخصی می‌باشد، بنابراین تبادل آنها از طریق کانال ناامن نیازمند گمنامی، عدم وابستگی و حفظ حریم خصوصی می‌باشد. علاوه بر این، شبکه حسگرهای پوششی زیرمجموعه‌ای از شبکه اینترنت اشیا است که به دلیل داشتن منابع محدود نیازمند پروتکل‌های سبکی هستند که اصالت، تمامیت و صحت اطلاعات آنها را تضمین کنند، بنابراین پروتکل‌های زیادی برای تامین امنیت این بستر توسط محققان ارائه شده است که برخی از آنها دارای مشکلات امنیتی هستند. این موضوع باعث به وجود آمدن زمینه تحقیقاتی گسترده‌ای روی این مساله‌ها شده است. اخیرا آنکور گوپتا و همکارانش پروتکل احراز هویت متقابل و تبادل کلید سبکی را ارائه داده‌اند و امن بودن آن را در برابر حملات شناخته شده اثبات کرده‌اند. ما در این مقاله نشان می‌دهیم که پروتکل پیشنهادی آنها در برابر حمله جعل هویت گره حسگر دارای ضعف می‌باشد و لذا امنیت مورد نیاز این بستر را فراهم نمی‌کند و به ارائه طرحی برای جلوگیری از این امر می‌پردازیم.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

شبکه اینترنت اشیا امکان ارتباط بین وسیله‌ها و تبادل اطلاعات بین آنها را فراهم می‌کند که امروزه به دلیل ساده بودن، کم هزینه بودن و قابل گسترش بودن مورد توجه بسیاری از زمینه‌های صنعتی و تجاری قرار گرفته‌است. یکی از کاربردهای گسترده این شبکه سیستم‌های نظارت بر سلامت حسگرهای پوششی [1] می‌باشد [۱]، که سرویس‌های گوناگونی را به بیماران و دکترها ارائه می‌دهد. شبکه حسگرهای پوششی [2] زیرمجموعه‌ای از این شبکه گسترده هستند که از حسگرهای ارزان قیمت دارای حافظه و توان محاسباتی پایین تشکیل می‌شوند. این حسگرها که در داخل یا روی بدن انسان یا لباس قرار می‌گیرند، سیگنال‌های مختلف ساطع شده از بدن را اندازه‌گیری کرده و آنها را از طریق کانال بی‌سیم به نقاط مختلف مانند بیمارستان‌ها و یا سیستم‌های نظارت خانگی ارسال می‌کنند. این ارتباط بی‌سیم، اطلاعات شخصی و حیاتی را در معرض حملات بسیار زیادی قرار می‌دهد. بنابراین حفظ امنیت این شبکه‌یکی از چالش‌های اساسی است که توجه کثیری از محققان را به خود جلب کرده است.

جلوگیری از رخ دادن این حملات و برقراری امنیت نیازمند درک عمیق و درستی از معماری شبکه حسگرهای پوششی می‌باشد. شکل ۱

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

*نویسنده مسئول
آدرس‌های رایانامه: sabamarandi@icloud.com (صبا مرندی)، f_moazemi@sbu.ac.ir (فرخ لقا معظمی گودرزی)

© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] WHMS

[2] WBAN

نشان‌دهنده‌ی معماری شبکه متمرکز با یک سرور محلی است. در حالت کلی این شبکه از سه لایه با دو مسیر ارتباطی تشکیل شده است تا ارسال اطلاعات از یک مسیر طولانی بدون نیاز به انرژی و توان زیاد امکان‌پذیر باشد [۲]. لایه‌ی اول گره مرتبه دو یا گره حسگر [۱] نام دارد که دارای کمترین توان پردازشی و حافظه است. این لایه تمامی اطلاعات بیولوژیکی را اعم از وضعیت فشار خون، درجه حرارت بدن، ضربان قلب و ... به دومین لایه تحت عنوان گره مرتبه اول یا گره میانی [۲] مانند تلفن همراه، تبلت و ... ارسال می‌کند، که به مسیر ارتباطی بین این دو گره Intra-BAN گفته می‌شود.

گره‌های میانی تمامی اطلاعات دریافت شده از حسگرها را به سمت سومین لایه، گره هاب [۳]، هدایت می‌کنند که این گره با داشتن بیشترین توان محاسباتی و حافظه مانند سرور، تمامی‌اطلاعات ارسال شده را برای پردازش به مدیریت سیستم یا مراکز بهداشتی- درمانی تحویل می‌دهد. به این مسیر ارتباطی که دور از بدن شکل می‌گیرد و نیازمند توان محاسباتی بالایی می‌باشد، Inter-BAN گفته می‌شود. که تامین امنیت این دو مسیر یکی از اهداف پژوهشی محققان می‌باشد [۳].

در این مقاله ابتدا برخی از کارهای انجام‌شده در این زمینه را در بخش ۲ بررسی می‌کنیم. در بخش ۳ به معرفی پروتکل گوپتا و همکارانش خواهیم پرداخت و در بخش ۴ و ۵ به ترتیب حمله اعمال‌شده را شرح داده، به توضیح روش جلوگیری از آن می‌پردازیم و در بخش پایانی نیز یک جمع بندی کلی از مقاله را ارائه خواهیم داد.

۲ کارهای پیشین

در شبکه حسگرهای پوششی تبادل اطلاعات از طریق شبکه بی‌سیم صورت می‌گیرد. بنابراین داده‌ها در معرض حملات بسیار زیادی قرار می‌گیرند. چون اطلاعات موجود در این شبکه محرمانه و شخصی می‌باشند، در سال‌های اخیر تحقیقات گسترده‌ای در زمینه‌ی بهبود امنیت پروتکل‌های احراز هویت و توزیع کلید انجام شده است، که توجه کثیری از این پروتکل‌ها، توزیع کلید بر پایه‌ی سیستم های رمزنگاری مانند AES، RSA، ECC و ... بوده است [۲]. سیستم‌های رمزنگاری سنتی علی‌رغم تامین امنیت بالا، نیازمند منابع و زیرساخت‌های بسیار قوی ارتباطی و محاسباتی می‌باشند. لذا برای استفاده در شبکه‌ی حسگرهای پوششی با توان محدود مناسب نمی‌باشند؛ بنابراین سیستم‌های رمزنگاری سبک متقارن [۴] امروزه مورد توجه بسیاری از محققان قرار گرفته است.

در سال ۲۰۱۷ لی و همکارانش [۴] پروتکل احراز هویت و توزیع کلید سبک وزن و گمنامی را ارائه کردند که امنیت مناسب‌تری نسبت به [۲] داشت. اگرچه این پروتکل گمنام امنیت رو به جلو و عقب [۵] را برآورده می‌کرد و در برابر حملات متعدد شناخته شده‌ای مانند حمله‌ی مرد میانی [۶]، حمله بازپخش [۷] و ... مقاوم بود، ولی در پی آن، آنالیزهای امنیتی عمیق‌تر اثبات کرد که این پروتکل در معرض خطراتی مانند به دست آوردن اطلاعات حافظه گره میانی [۸]، مشکل ذخیره کلید، جعل هویت [۹] گره حسگر و گره هاب می‌باشد و در حالت کلی فرض اعتماد به گره هاب در آن غیرواقعی است. در سال ۲۰۱۸ کویا و همکارانش [۵] به برطرف کردن این کمبودها با استفاده از سیگنال‌های فیزیولوژیکی پرداختند. چن و همکارانش در [۶] حمله‌های مشابه را در پروتکل لی و همکارانش پیدا کردند و در ادامه به اصلاح آن پرداختند تا گمنامی بهتر و امنیت بالاتری در مقابل حمله‌ی جعل هویت گره میانی ارائه دهند؛ ولی طرح آنها مانند [۴] در برابر حمله‌ی به دست آوردن اطلاعات حافظه گره میانی و جعل هویت گره هاب امن نیست و برای برنامه‌های عملی مناسب نمی‌باشد.در سال ۲۰۱۹ استاد شریف و همکارانش [۷] نشان دادند که [۴] دارای ضعف‌های امنیتی مانند رسیدن طرفین به کلیدهای نشست متفاوت [۱۰] و سخت بودن همگام‌سازی [۱۱] گره‌های حسگر است و طرحی مقاوم در برابر این آسیب‌ها ارائه دادند که گمنام بودن و غیر قابل ردیابی بودن [۱۲] نشست‌ها را تضمین می‌کند. در ادامه کومپارا و همکارانش در [۸] اثبات کردند که [۴] عدم وابستگی [۱۳] گره‌های حسگر را فراهم نمی‌کند و همچنین پروتکل [۵] به دلیل جمع‌آوری سیگنال‌های فیزیولوژیکی و لزوم همگام‌سازی گره‌های حسگر نیازمند توان محاسباتی بسیار بالایی می‌باشد. سپس زو و همکارانش در [۹] یک پروتکل سبک‌تر ارائه دادند که زیاد بودن توان محاسباتی [۵] را جبران کرده و در برابر حملات پارازیت [۱۴] و جعل هویت نسبت به پروتکل‌های مشابه امن‌تر بود؛ ولی با این حال در مقابل حمله‌ی بازپخش دارای ضعف می‌باشد.

در سال ۲۰۲۰ آنکور گوپتا و همکارانش در [۲] معتقد بودند که پروتکل لی و همکارانش ویژگی غیر قابل ردیابی بودن را برای نشست‌های مختلف فراهم نمی‌کند و به دست آوردن اطلاعات حافظه گره میانی، گره حسگر و گره هاب در آن امکان‌پذیر می‌باشد. بنابراین برای بهبود این ضعف‌های امنیتی، طرحی را ارائه کردند که در مدل حمله Dolev-Yao امن باشد. در این مقاله به بررسی آن از لحاظ امنیتی خواهیم پرداخت.

در حالت کلی ارائه دادن پروتکلی سبک که تمامی نیازهای امنیتی را در بستر شبکه حسگرهای پوششی یا به طور کلی شبکه اینترنت اشیا برآورده کند، موضوعی چالش برانگیز برای محققان این عرصه می‌باشد که در جدول ۱ به خلاصه‌ای از طرح‌های گذشته و آسیب‌پذیری آنها در برابر تعدادی از حملات شناخته شده اشاره شده است [۱۰].

۳ بررسی طرح آنکور گوپتا و همکاران

طرح آنکور گوپتا دارای ۴ مرحله با نام‌های مرحله اولیه، ثبت نام، احراز هویت و به‌روزرسانی گره پویا است. گره‌های IN، SN و HN سه نوع گره مختلف در این طرح شبکه هستند. IN همان گره مرتبه اول یا میانی مانند تلفن همراه، ساعت هوشمند، تبلت و ... است که اطلاعات به دست آمده از SN یا گره‌های حسگر را جمع‌آوری کرده و به گره هاب ارسال می‌کند. گره

[1] second level node (sensor node) [2] first level node (intermediate node) [3] hub node [4] lightweight symmetric cryptographic system [5] forward/backward secrecy

[6] man in the middle attack [7] reply attack [8] intermediate node capture attack [9] impersonation attack [10] wrong session key [11] synchronization [12] untraceability [13] linkability [14] jamming attack

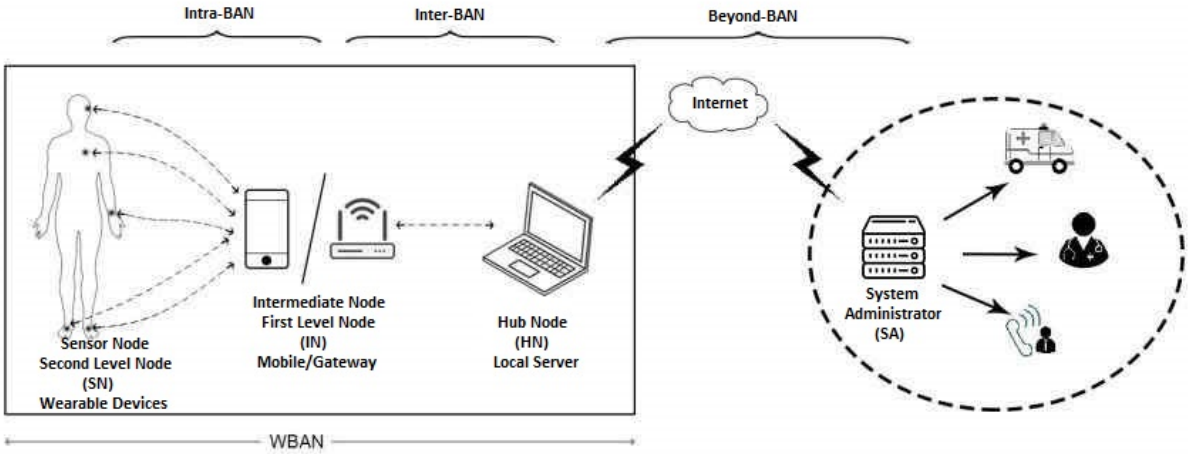

Figure 1 : Architecture of a WBAN system

شکل ۱. معماری شبکه حسگرهای پوششی

جدول ۱. مقایسه ویژگی‌های امنیتی طرح‌های ارائه‌شده

ویژگی‌ها	کومپارا و همکاران [۸]	گوپتا و همکاران [۲]	ابراهیم و همکاران [۱۱]	لی و همکاران [۴]	کویا و همکاران [۵]	چن و همکاران [۶]	زو و همکاران [۹]
گمنامی	✘	✔	✔	✘	✘	✘	✘
عدم وابستگی (unlinkability)	✔	✔	✔	✘	✔	✘	✔
حمله باز پخش	✔	✔	✔	✘	✔	✔	✔
حمله جعل هویت	✘	✘	✘	✘	✘	✘	✔
حمله شنود (eavesdropping attack)	✔	✔	✔	✔	✔	✔	✔
امنیت رو به جلو و رو به عقب	✔	✔	✔	✔	✔	✘	-
حمله مرد میانی	✘	✔	✔	✔	✔	✔	✔

هاب گره قدرتمندی از لحاظ محاسباتی و ارتباطی است که به سرورهای اصلی درمانی متصل می‌باشد. در جدول شماره ۲ تمامی نمادهای به کار رفته شده در این طرح نشان داده شده، است. مرحله احراز هویت پروتکل ارائه شده توسط گوپتا و همکارانش در شکل ۲ به صورت خلاصه نمایش داده شده است، که در ادامه به توضیح این مراحل می‌پردازیم.

مرحله اولیه: ابتدا SA کلید K_{hn} را برای گره هاب (HN) انتخاب می‌کند و آن را در حافظه این گره ذخیره می‌کند.

مرحله ثبت نام: SA گره‌های میانی و گره‌های حسگر را طی مراحل زیر ثبت نام می‌کند:

یک آدرس منحصر به فرد تحت عنوان id_n و یک کلید به نام K_n را برای گره حسگر و یک کلید مشترک خصوصی بین گره میانی و گره حسگر تحت عنوان X_{n-in} انتخاب می‌کند و سپس مقادیر زیر را محاسبه می‌کند:

$$a_n = id_n \oplus h(K_{hn}\|K_n),$$

$$b_n = K_{hn} \oplus K_n \oplus a_n,$$

$$c_n = h(K_{hn}\|id_n).$$

در ادامه یک آدرس منحصربه‌فرد نیز برای گره میانی تحت عنوان id_{in} انتخاب می‌کند و سرانجام پیام $\langle id_n, X_{n-in}, a_n, b_n, c_n\rangle$ را در حافظه‌ی گره حسگر (SN) و پیام $\langle id_in, X_{n-in}\rangle$ را در حافظه گره میانی (IN) ذخیره می‌کند.

نکته قابل توجه این است که K_n در هیچ حافظه ای توسط SA ذخیره نمی‌شود و فقط برای محاسبه کردن a_n و b_n از آن استفاده می‌شود.

فاز احراز هویت: SN عدد تصادفی r_n را انتخاب می‌کند و عبارات زیر را محاسبه می‌کند:

$$x_n = a_n \oplus id_n,\ y_n = x_n \oplus r_n.$$

سپس یک مهر زمانی به نام t_1 تولید می‌کند و مقادیر زیر را محاسبه می‌کند:

$$tid_n = ((id_n \oplus t_1)\|r_n),$$

جدول ۲. نمادهای به کار رفته شده در پروتکل آنکور گوپتا [۲]

Symbols	Explanations
SA	System Administrator
SN	Sensor Node
HN	Hub Node
IN	Intermediate Node
id_n	Identity of a sensor node
id_{in}	Identity of an intermediate node
tid_n	Temporary identity of a sensor node
K_{hn}	Secret Key of a hub node
K_n	Temporary secret key of sensor node
X_{n-in}	Long-Term shared secret key
t_i	Current timestamp
ΔT	Maximum transmission delay
K_s	Session key between SN and HN
h(·)	Cryptographic hash function
⊕	Bitwise XOR Operation
‖	Concatenation Operation

$$V_n = (X_{n-in}\|t_1).$$

در ادامه پیام $\langle tid_n, y_n, a_n, b_n, V_n, t_1\rangle$ را برای گره میانی از طریق کانال ناامن ارسال می‌کند.

گره میانی بعد از دریافت این پیام معتبر بودن مهر زمانی را با توجه به زمان دریافت اطلاعات از سوی خود t_c می‌سنجد، سپس عبارت زیر را محاسبه می‌کند و آن را با پیام دریافتی V_n مقایسه می‌کند:

$$V_n^* = h(X_{n-in}\|t_1).$$

در صورت نابرابری IN ارتباط را قطع می‌کند و در صورت برابری مهر زمانی t_2 را تولید کرده و عبارت $V_i = h(id_{in}\|t_2)$ را محاسبه می‌کند؛ در ادامه پیام $\langle tid_n, y_n, a_n, b_n, V_i, t_1, t_2\rangle$ را برای گره هاب از طریق کانال ناامن ارسال می‌کند. گره هاب بعد از دریافت این پیام معتبر بودن مهر زمانی را با توجه به زمان دریافت اطلاعات از سوی خود t_c می‌سنجد، سپس عبارت زیر را محاسبه می‌کند و آن را با پیام دریافتی V_i مقایسه می‌کند:

$$V_i^* = h(id_{in}\|t_2).$$

در صورت نابرابری HN ارتباط را قطع می‌کند و در صورت برابری عبارت‌های زیر را محاسبه می‌کند:

$$K_n^* = K_{hn} \oplus b_n \oplus a_n,$$
$$x_n^* = (K_{hn}\|K_n^*),$$
$$id_n^* = a_n \oplus x_n^*,\ r_n^* = y_n \oplus x_n^*.$$

سپس گره هاب آدرس موقت tid_n^* را از طریق عبارت زیر محاسبه کرده و آن را با پیام دریافتی tid_n مقایسه می‌کند:

$$tid_n^* = ((id_n^* \oplus t_1)\|r_n^*).$$

بعد از صحت اطلاعات فوق گره هاب یک K_n^+ و f_n را به صورت تصادفی تولید می‌کند و سپس مقادیر زیر را محاسبه می‌کند:

$$a_n^+ = id_n \oplus (K_{hn}\|K_n^+),$$
$$b_n^+ = K_{hn} \oplus K_n^+ \oplus a_n^+,$$
$$\alpha = (K_{hn}\|id_n) \oplus f_n,$$
$$\eta = ((K_{hn}\|id_n)\|f_n) \oplus a_n^+,$$
$$\mu = ((K_{hn}\|id_n)\|r_n) \oplus b_n^+,$$
$$\beta = (x_n\|r_n\|f_n\|\eta\|\mu).$$

در ادامه HN مهر زمانی حال حاضر را با نام t_3 تولید کرده و کلید نشست K_s را به طریق زیر محاسبه می‌کند:

$$K_s = (id_n\|r_n\|f_n\|(K_{hn}\|id_n)).$$

سپس مقدار عبارت $V_h = h(id_in\|t_3)$ را محاسبه کرده و پیام‌های $\langle \alpha, \beta, \eta, \mu, V_h, t_3\rangle$ را به سمت گره میانی باز می‌گرداند.

گره میانی بعد از دریافت این پیام معتبر بودن مهر زمانی را با توجه به زمان دریافت اطلاعات از سوی خود t_c می‌سنجد، سپس عبارت زیر را محاسبه می‌کند و آن را با پیام دریافتی V_h مقایسه می‌کند:

$$V_h^* = h(id_in\|t_3).$$

در صورت نابرابری IN ارتباط را قطع می‌کند و در صورت برابری مهر زمانی t_4 را تولید کرده و عبارت $V_i = h(X_{n-in}\|t_4)$ را حساب کرده و پیام $\langle \alpha, \beta, \eta, \mu, V_i, t_4\rangle$ را برای گره حسگر ارسال می‌کند.

گره حسگر معتبر بودن V_i را با محاسبه $V_i^* = h(X_{n-in}\|t_4)$ و مقایسه کردن آن با پیام دریافتی می‌سنجد و در صورت صحت اطلاعات عبارت‌های زیر را محاسبه می‌کند:

$$f_n^* = c_n \oplus \alpha,$$
$$\beta^* = (x_n\|r_n\|f_n^*\|\eta\|\mu).$$

و سپس آن را با β دریافتی در پیام مقایسه می‌کند و اگر صحت آن تأیید شد مقدار عبارت‌های زیر و کلید نشست را بدست می‌آورد. سپس a_n^+ و b_n^+ را در حافظه خود به‌روزرسانی می‌کند:

$$a_n^+ = (c_n\|f_n) \oplus \eta,$$
$$b_n^+ = (c_n\|r_n) \oplus \mu,$$
$$K_s = (id_n\|r_n\|f_n\|c_n).$$

فاز به‌روزرسانی گره پویا: در این حالت حسگر جدیدی درخواست پیوستن به شبکه موجود را دارد، بنابراین باید به صورت پویا وارد شبکه حسگرهای پوششی شود که جزئیات این مرحله در [۳] قابل مشاهده است.

۴ اعمال حمله جعل هویت گره حسگر

در این بخش مراحل اعمال حمله جعل هویت گره حسگر به طرح گوپتا و همکاران شرح داده می‌شود.

با توجه به آن که گره هاب a_n^+ و b_n^+ جدید که در انتهای پروتکل برای نشست جدید در حافظه گره حسگر ذخیره می‌شوند را در حافظه خود ذخیره نمی‌کند، لذا از آخرین تغییرات a_n و b_n در هر نشست اطلاعی ندارد و در صورت ارسال a_n و b_n مربوط به پروتکل‌های اجرا شده قبلی توسط گره میانی به گره هاب، گره هاب توانایی تشخیص قدیمی بودن آن‌ها را نخواهد داشت. همچنین با توجه به این که در عبارت $V_i = h(id_{in}\|t_۲)$ برای همه‌ی گره‌های حسگری که از یک گره میانی استفاده می‌کنند، در زمان $t_۲$ ثابت است، دشمن می‌تواند در گام اول به جای گره میانی، V_i مربوط به یکی از نشست‌های در حال اجرا را که در آن $t_۲ = t_c$ می‌باشد را در عبارت ارسالی خود به گره هاب جایگزین نماید.

در گام بعدی دشمن $t_۱$ مربوط به یکی از نشست‌های قبلی را با یک مقدار مشخص ϵ، XOR می‌کند تا آن را به زمان حال t_c نزدیک کند ($t_c > t_۲ > \epsilon \sim t_c - t_۱$). از آنجایی که در پروتکل مرجع زمان با برخی مقادیر XOR شده است؛ پس می‌توان گفت از جنس رشته می باشد و می‌توان آن را با مقدار ϵ که در دست خود مهاجم است XOR کرد. بنابراین پس از مشخص شدن مقدار ϵ در گام نهایی دشمن مقادیر $a_n \oplus \epsilon$، $b_n \oplus \epsilon$ و $t_۱ \oplus \epsilon$ را محاسبه نموده، در نهایت پیام

$$\langle tid_{n_{old}}, y_{n_{old}}, a_{n_{old}} \oplus \epsilon, b_{n_{old}} \oplus \epsilon, V_{i_{old}}, t_۱ \oplus \epsilon, t_۲ \rangle$$

را برای گره هاب ارسال می‌کند.

در ادامه گره هاب با دریافت این مقادیر ابتدا صحت مهر زمانی $|t_۲ - t_c| < \Delta t$ را چک می‌کند که با توجه به این امر که $t_۲$ از نشست در حال اجرای فعلی برداشته شده است و مقدار ϵ بستگی به مهاجم دارد و می‌تواند در آن تغییرات ایجاد کند، مورد تأیید قرار خواهد گرفت. همچنین V_i نیز مانند مهر زمانی مورد تأیید گره هاب قرار خواهد گرفت. در ادامه گره هاب مقادیر زیر را محاسبه می‌کند:

$$\begin{aligned}
K_n^* &= K_{hn} \oplus b_n \oplus \epsilon \oplus a_n \oplus \epsilon \\
&= K_{hn} \oplus b_n \oplus a_n, \\
x_n^* &= (K_{hn}\|K_n^*), \\
id_n^* &= a_n \oplus \epsilon \oplus x_n^*, \\
r_n^* &= y_n \oplus x_n^*, \\
tid_n^* &= ((id_n^* \oplus \epsilon \oplus t_۱ \oplus \epsilon)\|r_n^*) \\
&= ((id_n^* \oplus t_۱)\|r_n^*).
\end{aligned}$$

در این مرحله گره هاب بدون اینکه متوجه تکراری بودن پیام‌ها در نشست‌های قبلی بشود و بدون آنکه بداند V_i متعلق به گره حسگری است که در این نشست شرکت دارد یا نه، صحت اطلاعات را تأیید می‌کند و گره حسگر توسط گره هاب احراز هویت می‌شود و نهایتا دشمن به هدف خود می‌رسد.

۵ روش جلوگیری از حمله جعل هویت گره حسگر

در این بخش به ارائه روشی برای جلوگیری از حمله وارد شده به پروتکل احراز هویت و تبادل کلید متقابل آنکور گوپتا و همکارانش می‌پردازیم.

با توجه به این امر که در این پروتکل در مرحله دوم گره میانی علی‌رغم اثبات تازگی[1] پیام خود توسط مهر زمانی $t_۲$، هیچ اثباتی مبنی بر وابستگی پیام خود به نشست در حال اجرا و گره حسگر را به گره هاب ارائه نمی‌دهد و ثابت بودن V_i برای تمامی حسگرها باعث آسیب‌پذیر شدن پروتکل نسبت به حمله جعل هویت گره حسگر می‌شود . بنابراین دشمن می‌تواند با استفاده از V_i یکی از پروتکل های در حال اجرا این حمله را اعمال کند، چنانچه گره میانی در هنگام ارسال $V_i = h(id_{in}\|t_۲)$ مقادیر a_n ارسالی از طرف گره حسگر را نیز در محاسبات شرکت دهد، به این معنا که مقدار $V_i = h(id_{in}\|t_۲\|a_n)$ توسط گره میانی محاسبه کرده و برای گره هاب ارسال کند.

گره هاب بعد از دریافت این پیام، معتبر بودن مهر زمانی را با توجه به زمان دریافت اطلاعات از سوی خود $t(c)$ می‌سنجد، سپس عبارت زیر را محاسبه و آن را با پیام دریافتی V_i مقایسه می‌کند:

$$V_i^* = h(id_{in}\|t_۲\|a_n).$$

با توجه به وابستگی a_n به حسگر و همچنین رعایت توالی نشست‌ها توسط حسگر دشمن نمی‌تواند از V_i سایر نشست‌های در حال اجرای دیگر حسگرها سوءاستفاده نموده و حمله‌ی مذکور را اجرا کند، زیرا گره هاب هنگام مقایسه‌ی مقادیر V_i دریافتی و V_i^* محاسبه شده به تناقض رسیده و نشست را خاتمه می‌دهد.

۶ نتیجه‌گیری

انتقال اطلاعات حساس و شخصی در شبکه حسگرهای پوششی نیازمند برقراری امنیت توسط پروتکل‌هایی سبک و کارا می‌باشد، که در این مقاله به بررسی یکی از این طرح های امنیتی پرداخته شد. پس از بررسی‌های انجام شده مشخص شد که پروتکل آنکور گوپتا و همکارانش در برابر حمله‌ی جعل هویت گره حسگر دارای ضعف است و استفاده از آن باعث به وجود آمدن اختلالاتی در سیستم می‌شود؛ بنابراین نیازمند بهبود و اصلاح است. لذا به منظور حل این ضعف امنیتی ما روشی برای جلوگیری از به وقوع پیوستن این حمله ارائه کردیم و به بررسی آن پرداختیم. اگرچه سربار محاسباتی پروتکل گوپتا که با توجه به [۱] زیاد است با طرح پیشنهادی ما برای جلوگیری از حمله به مقدار جزئی افزایش پیدا می‌کند ولی به لحاظ امنیتی پروتکل امن‌تری نسبت به [۱] خواهیم داشت. در

[1] freshness

Sensor Node (SN)	Intermediate Node (MN)	Hub Node (HN)
Select r_n Generates timestamp t_1 Computes- $x_n = a_n \oplus id_n$ $y_n = x_n \oplus r_n$ $V_n = h(x_{n\text{-}in} \| t_1)$ $tid_n = h((id_n \oplus t_1) \| r_n)$		
$\xrightarrow{< tid_n, y_n, a_n, b_n, v_n, t_1 >}$	Checks = $\|t_1 - t_c\| < \triangle T$ Computes- $V_n^* = h(x_{n\text{-}in} \| t_1)$ $V_n^* = ? v_n$ Generates timestamp t_2 Computes- $V_i = h(id_{in} \| t_2)$	
	$\xrightarrow{< tid_n, y_n, a_n, b_n, v_i, t_1, t_2 >}$	Checks = $\|t_2 - t_c\| < \triangle T$ Calculates- $V_i^* = h(id_{in} \| t_2)$ $V_i^* = v_i$ Computes- $K_n^* = K_{hn} \oplus b_n \oplus a_n$ $x_n^* = h(K_{hn} \| K_n^*)$ $id_n^* = a_n \oplus x_n^*$ $r_n^* = y_n \oplus x_n^*$ $tid_n^* = h((id_n^* \oplus t_1) \| r_n^*)$ $tid_n = ? tid_n^*$ Selects f_n and new K_n^* Computes- $a_n^+ = id_n \oplus h(K_{hn} \| K_n^+)$ $b_n^+ = K_{hn} \oplus K_n^+ \oplus a_n^+$ $\alpha = h(K_{hn} \| id_n) \oplus f_n$ $\eta = h(h(K_{hn} \| id_n) \| f_n) \oplus a_n^+$ $\mu = h(h(K_{hn} \| id_n) \| r_n) \oplus b_n^+$ $\beta = h(x_n \| r_n \| f_n \| \eta \| \mu) \oplus b_n^+$ $K_s = h(id_n \| r_n \| f_n \| h(K_{hn} \| id_n))$ Generates timestamp t_3 $V_h = h(id_{in} \| t_3)$
	$\xleftarrow{< \alpha, \beta, \eta, \mu, V_h, t_3 >}$	
	Checks = $\|t_3 - t_c\| < \triangle T$ Computes- $V_h^* = h(id_{in} \| t_3)$ $V_h^* = ? V_h$ Generates timestamp t_4 Computes- $V_i = h(x_{n\text{-}in} \| t_4)$	
$\xleftarrow{< \alpha, \beta, \eta, \mu, V_h, t_3 >}$		
Checks = $\|t_4 - t_c\| < \triangle T$ Computes- $V_i^* = h(x_{n\text{-}in} \| t_4)$ $V_i^* = ? V_i$ Computes- $f_n^* = c_n \oplus \alpha$ $\beta^* = h(x_n \| r_n \| f_n^* \| \eta \| \mu) \oplus b_n^+$ $\beta = ? \beta^*$ Computes- $a_n^+ = h(c_n \| f_n) \oplus \eta$ $b_n^+ = h(c_n \| r_n) \oplus \mu$ $K_s = h(id_n \| r_n \| f_n \| c_n)$ Replaces- a_n and b_n with a_n^+ and b_n^+ Stores session key K_s		

شکل ۲. مروری بر مرحله احراز هویت پروتکل گوپتا و همکاران

کارهای آتی سعی بر سبک کردن این پروتکل با حفظ تمامی ویژگی‌های امنیتی خواهیم پرداخت.

مراجع

[1] Almuhaideb, Abdullah M and Alqudaihi, Kawther S. A lightweight and secure anonymity preserving protocol for wban. *IEEE Access*, 8:178183–178194, 2020.

[2] Gupta, Ankur, Tripathi, Meenakshi, and Sharma, Aakar. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in wban. *Computer Communications*, 160:311–325, 2020.

[3] Narwal, Bhawna and Mohapatra, Amar Kumar. Samaka: Secure and anonymous mutual authentication and key agreement scheme for wireless body area networks. *Arabian Journal for Science and Engineering*, 46(9):9197–9219, 2021.

[4] Li, Xiong, Ibrahim, Maged Hamada, Kumari, Saru, Sangaiah, Arun Kumar, Gupta, Vidushi, and Choo, Kim-Kwang Raymond. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, 129:429–443, 2017.

[5] Koya, Aneesh M and Deepthi, PP. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Computer Networks*, 140:138–151, 2018.

[6] Chen, Chien-Ming, Xiang, Bing, Wu, Tsu-Yang, and Wang, King-Hang. An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks. *Applied Sciences*, 8(7):1074, 2018.

[7] Ostad-Sharif, Arezou, Nikooghadam, Morteza, and Abbasinezhad-Mood, Dariush. Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks. *International Journal of Communication Systems*, 32(12):e3974, 2019.

[8] Kompara, Marko, Islam, SK Hafizul, and Hölbl, Marko. A robust and efficient mutual authentication and key agreement scheme with untraceability for wbans. *Computer networks*, 148:196–213, 2019.

[9] Xu, Zisang, Xu, Cheng, Chen, Haixian, and Yang, Fang. A lightweight anonymous mutual authentication and key agreement scheme for wban. *Concurrency and computation: Practice and experience*, 31(14):e5295, 2019.

[10] Thota, Sandeep Kumar Reddy, Mala, C, and Krishnan, Geetha. A lightweight and flexible mutual authentication and key agreement protocol for wearable sensing devices in wban. *International Journal of Pervasive Computing and Communications*, 2022.

[11] Ibrahim, Maged Hamada, Kumari, Saru, Das, Ashok Kumar, Wazid, Mohammad, and Odelu, Vanga. Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer methods and programs in biomedicine*, 135:37–50, 2016.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 2 (pp. 44–51)
https://monadi.isc.org.ir

Presented at the ISCISC 2022 in University of Giulan, Rasht, Iran

Security Analysis of an Anonymous Authentication and Key Agreement Scheme in Wireless Body Area Network★

Saba Marandi * and Farrokhlagha Moazzami

Cyberspace Research Institute, Shahid Beheshti University, Tehran, Iran

ARTICLE INFO.

Keywords:
WBAN
Mutual authentication
Key agreement
Sensor node impersonation attack

dor: 20.1001.1.24763047.1401.11.2.5.4

Type: research paper

ABSTRACT

In medical fields, a wearable body area sensors network is a network of sensors placed inside human bodies or on their skin. These multi-functional sensors provide all patients and medical personnel with optimized and comfortable services. The patient's physiological information transferred in this network is very sensitive and confidential; Therefore, transmitting through an insecure channel requires high anonymity, un-traceability, and privacy-preserving of personal data. Furthermore, the wearable body area network is a small part of the Internet of Things (IoT) community, and as the devices are resource-constraint, lightweight protocols are needed to guarantee the information's authenticity, confidentiality, and integrity. Hence, a large number of schemes were proposed by different researchers to improve the reliability of the protocols. Recently Ankur Gupta and his colleagues proposed a lightweight mutual authentication and key agreement protocol and proved its security against well-known attacks. In this paper, we will demonstrate that their proposed protocol is vulnerable to the sensor node impersonation attack and does not provide the necessary security for communicating data; Then, we will offer a new solution to overcome this problem.

© 2022 ISC

★ The ISCISC 2022 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: s.marandi@mail.sbu.ac.ir (Saba Marandi), f_moazemi@sbu.ac.ir (Farrokhlagha Moazzami)
© 2022 ISC. All rights reserved.