ارائه یک طرح جدید احراز اصالت با حفظ گمنامی برای شبکه اینترنت اشیا

مصطفی مرادنیا [۱]، سید مرتضی پورنقی[۲]، بهروز خادم[۳].

۱- دانشجو کارشناسی ارشد مخابرات امن و رمزنگاری- دانشگاه جامع امام حسین(ع)- تهران- ایران

۲- استادیار- دانشگاه جامع امام حسین(ع)- تهران- ایران

۳- دانشیار- دانشگاه جامع امام حسین(ع)- تهران- ایران

چکیده

همزمان با گسترش دانش و فناوری اینترنت اشیا، چالش‌های امنیتی آن به طور جدی مورد توجه محققین قرار گرفته است. این چالش ها به خصوص در حوزه احراز اصالت برای مقاوم سازی در برابر انواع حملات جعل و در حوزه گمنامی برای مقابله با نفوذ اهمیت مضاعفی پیدا کرده اند. به طور دقیق تر شبکه اینترنت اشیا و پروتکل‌های احراز اصالت و گمنامی از طرف مهاجمان با تهدیداتی مانند انواع حملات جعل هویت، حمله تکرار، حمله مردی در میانه، انواع حملات انکار سرویس و حمله داخلی روبه‌رو هستند. بر اساس مطالعه انجام شده در این مقاله روشن شده است که هیچ‌کدام از طرح‌های مورد بررسی به طور کامل ویژگی‌های امنیتی موردنیاز مانند محرمانگی، حریم خصوصی، یکپارچگی، امنیت جلو رونده و عقب رونده، اتصال ناپذیری، مقیاس‌پذیری، دسترس‌پذیری و توافق کلید امن برای مقابله با حملات و تهدیدات متناظر را ندارند. در این مقاله پس از مقایسه تعدادی از جدیدترین پروتکل ها از منظر امنیت و کارایی، یک طرح جدید احراز اصالت، با قابلیت حفظ گمنامی پیشنهاد شده است که همه ویژگی‌های امنیتی نامبرده شده و موردنیاز برای مقاومت در برابر حملات متناظر را داشته باشد. برای اثبات صوری برخی از ویژگی های امنیتی از ابزار پرووریف نیز استفاده شده است. طرح پیشنهادی علاوه برافزایش امنیت توانسته است از جهت پیچیدگی محاسبات کارایی بهتری را نسبت به پروتکل های مورد بررسی ارائه نماید.

کلمات کلیدی: اینترنت اشیا، امنیت شبکه، احراز اصالت، گمنامی

۱. مقدمه

مفهوم اینترنت اشیا[۲] برای اولین بار در سال ۱۹۹۹ معرفی شد [۳]. در حال حاضر میلیون‌ها دستگاه در سرتاسر جهان به یکدیگر متصل شده و شبکه اینترنت اشیا را تشکیل داده اند. بدیهی است که تأمین امنیت چنین شبکه بزرگی از اهمیت خاصی برخوردار است و به یک چالش اساسی تبدیل‌شده است. یکی از مهم‌ترین مسائل امنیتی در این شبکه احراز هویت[۳] موجودیت‌ها است [۲]. معمولاً احراز اصالت به دو صورت انجام می‌گیرد. در حالت اول هویت طرفین توسط یک موجودیت سوم قابل‌اعتماد تائید می‌شود و در حالت دوم هویت طرفین به‌صورت مستقیم و توسط خود موجودیت‌ها تائید می‌شود [۵]. در اینترنت اشیا محدودیت‌های کمبود منابع وجود دارد؛ بنابراین باید از طرح‌هایی استفاده شود که سبک باشند [۵]. همچنین

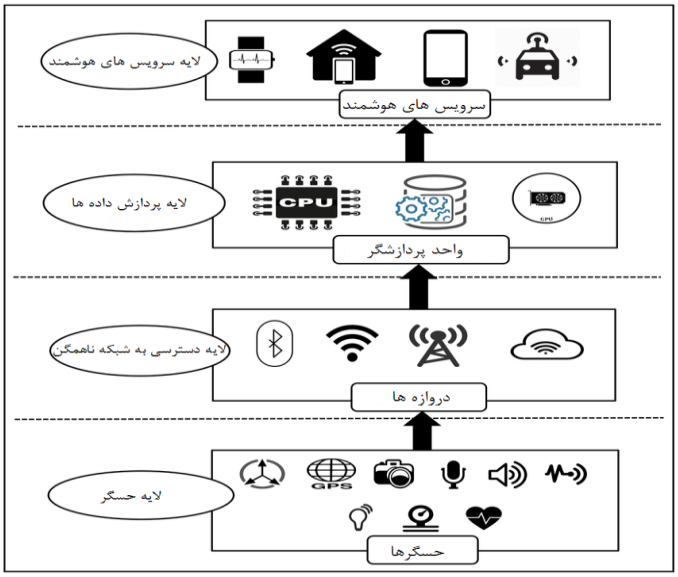
[1] **Corresponding author: Email: Mo.moradniya@gmail.com**
[2] Internet of things
[3] Authentication

برای تأمین امنیت بالاتر و جلوگیری از نفوذ به شبکه، گمنامی[1] موجودیت‌ها مهم است [۷]. ما در این مقاله یک طرح احراز اصالت کارا باقابلیت گمنامی برای اینترنت اشیا ارائه می‌دهیم. طرح پیشنهادی توانسته است ویژگی‌های امنیتی گمنامی، احراز هویت، محرمانگی[2]، توافق کلید امن[3]، عدم ردیابی[4]، مقیاس‌پذیری[5]، رازداری کامل روبه‌جلو[6] و یکپارچگی[7] را تأمین کند و در برابر حملات بازگشت[8]، مردی در میانه[9]، بسیاری از دستگاه‌های واردشده، حدس گذرواژه[10]، جعل هویت[11]، استراق سمع، ناهمگام سازی[12] و داخلی[13] مقاوم است. بسیاری از طرح‌های احراز اصالت برای حفظ تازگی پیام از مهرهای زمانی[14] استفاده می‌کنند. مهرهای زمانی در هر پیام فرستنده گنجانده‌شده است و گیرنده پیام را درصورتی‌که اختلاف‌زمانی بین دریافت و ارسال بیش از یک آستانه باشد، دور می‌زند؛ اما برای اندازه‌گیری دقیق این اختلاف‌زمانی، چنین طرح‌هایی نیاز به همگام‌سازی زمانی دقیق بین همه دستگاه‌ها دارند که برای دستیابی به آن نیاز به سربار اضافی دارد. اگر همگام‌سازی با شکست مواجه شود، مهاجم می‌تواند با استفاده از این واقعیت که شبکه نمی‌تواند به‌طور قابل‌اعتماد بین بسته‌های جدید و قدیمی تمایز قائل شود، حملات تکراری را انجام دهد [۸]. ازاین‌رو، در این مقاله، ما به دنبال طراحی یک پروتکل احراز هویت هستیم که از مهر زمانی استفاده نمی‌کند. قسمت‌های بعدی این مقاله به این شرح است: در بخش ۲، معماری شبکه اینترنت اشیا را معرفی می‌کنیم. در بخش ۳، پیشینه تحقیق، در بخش ۴، طرح پیشنهادی، در بخش ۵، تحلیل‌های امنیتی، در بخش ۶، اثبات رسمی امنیت، در بخش ۷ بررسی کارایی و در بخش ۸ مقاله، نتیجه کلی توضیح داده‌شده است.

۲. معماری مفروض

در این معماری ابتدا دستگاه‌های اینترنت اشیاء اطلاعات را جمع‌آوری می‌کنند و برای پردازش به فراهم آورنده سرویس ارسال می‌کنند. فراهم آورنده سرویس پس از پردازش، آن‌ها را برای کاربر ارسال می‌کند تا مورداستفاده قرار بگیرند [۹]. همچنین در این معماری دستگاه‌ها می‌توانند با یکدیگر در ارتباط باشند؛ بنابراین اهمیت احراز هویت برای امنیت اطلاعات کاملاً نمایان می‌شود. در این معماری برای تائید هویت ازیک‌طرف سوم که به نام سرویس‌دهنده قابل‌اعتماد شناخته می‌شود استفاده می‌کنیم.

[1] Anonymity
[2] confidentiality
[3] Secure key agreement
[4] No tracking
[5] Scalability
[6] Forward security
[7] integrity
[8] Reply attack
[9] man in the middle
[10] guess password
[11] impersonation
[12] Async
[13] Internal
[14] Time stamp



شکل ۲ – معماری مفروض شبکه

۳. پیشینه تحقیق

برای اولین بار مفهوم اینترنت اشیا در سال ۱۹۹۹ توسط کوین اشتون مورداستفاده قرار گرفت [۳]. کوین جهانی را توصیف می‌کرد که در آن هر چیزی، حتی اشیا بی‌جان نیز برای خود هویتی دیجیتالی دارند و با استفاده از کامپیوترها می‌توان آن‌ها را سازمان‌دهی و مدیریت کرد. در ابتدا به دلیل گسترده نبودن اینترنت در سطح جهانی این فناوری مورد استقبال قرار نگرفت اما پس از گذشت چند سال و گسترش زیاد اینترنت در جامعه این فناوری جای خود را در بین زندگی مردم پیدا کرد. طرح‌های اولیه IoT شامل نقایص و چالش‌های زیادی ازجمله موضوع حفظ امنیت بودند. محدودیت منابع در بسیاری از دستگاه‌های شبکه IoT بسیار رایج است و افشا هویت دستگاه‌های IoT می‌تواند اطلاعات حساس را فاش کند؛ بنابراین، کار آیی بالا (محاسبه و ارتباطات) و حفاظت از ناشناس بودن دو ویژگی مطلوب در احراز هویت اینترنت اشیاء و احراز هویت دستگاه به دستگاه (D2D)[1] هستند. گلدبرگ[2] و همکاران [۱۰] در سال ۲۰۱۲ پروتکل گمنامی ntor را ارائه کردند. این پروتکل مبادله کلید را با احراز هویت یک‌طرفه ایجاد می‌کند و گمنامی یک‌طرفه را ارائه می‌دهد. این پروتکل مبتنی بر رمزنگاری کلید عمومی و محرمانگی روبه‌جلو است. در طی سالیان اخیر محققین تمرکز ویژه‌ای بر روی چگونگی احراز اصالت در IoT با حفظ ویژگی گمنامی داشته‌اند و طرح‌های مختلفی را ارائه کرده‌اند. لی[3] و همکاران [۱۱] در سال ۲۰۱۷ یک طرح احراز هویت سه فاکتوری ارائه دادند. سه فاکتور معرفی‌شده در این طرح کارت هوشمند، رمز عبور و الگوی زیستی بود. این طرح قابلیت گمنامی را نیز فراهم می‌کرد. آن‌ها از یک طرح تعهد فازی برای رسیدگی به اطلاعات بیومتریک کاربر استفاده کرده‌اند. جانبابائی و همکاران [۱] در سال ۲۰۱۸ یک طرح احراز اصالت ارائه دادند که دارای قابلیت حفظ گمنامی طرفین ارتباط بود. جانبابائی طرح خود را در سه زمینه‌ی نیازمندی‌های اینترنت اشیا، بار محاسباتی و زمان اجرا و

جدول ۱- علائم و اختصارات

[1] Device to device
[2] Goldberg
[3] Li

شرح	نماد	شرح	نماد
کلید خصوصی بین دستگاه و سرویس‌دهنده	K_i	اعداد تصادفی دستگاه ۱	Q, n
نام مستعار دستگاه i ام	PN_i	پیام بررسی یکپارچگی پیام	H_{maci}
شناسه اصلی دستگاه i ام	ID_i	تابع چکیده ساز	$h(.)$
رمزنگاری و رمزگشایی متقارن	Enc, Dec	مقدار تصادفی دستگاه i ام	CC_i
عملگر الصاق	$\|\|$	مقدار تصادفی دستگاه ۲	C, e
کلید موقت صادرشده برای دستگاه‌ها توسط سرویس‌دهنده	K_{tmp}	مقدار خصوصی دستگاه ۱ برای به‌روزرسانی CC_1	PS_1
عملگرهای جمع بیتی	$\oplus$	مقدار خصوصی دستگاه ۲ برای بروز رسانی CC_2	PS_2
شناسه مستعار در مرحله توافق کلید	SN_i	مقادیر تصادفی برای تولید شناسه مستعار در توافق کلید	N_{12}, N_{21}
مرکز احراز اصالت	TTP	مدیر سیستم	SA
دستگاه iام	D_i	اعداد تصادفی برای تولید کید جلسه	x, y

مقاومت در برابر حملات مختلف با طرح‌های دیگر مقایسه کرده است و یک طرح جدید پیشنهاد کرده‌اند. متأسفانه طرح جانبابائی محرمانگی و رازداری روبه‌جلو را ارائه نمی‌دهد و امکان کشف کلید توسط مهاجم وجود دارد همچنین این طرح در برابر حملات جعل هویت و مردی در میانه مقاوم نیست. سابرامانی[1] و همکاران [۱۲] در سال ۲۰۱۹ یک طرح احراز هویت ناشناس جدید برای محاسبات ابری موبایل ارائه کرد. طرح پیشنهادی به کاربر تلفن همراه اجازه می‌دهد تا از طریق یک کلید خصوصی به ارائه‌دهندگان خدمات مختلف دسترسی پیدا کند. روش پیشنهادی همچنین از احراز هویت متقابل، اشتراک کلید، محرمانه بودن کاربر و عدم قابلیت ردیابی کاربر پشتیبانی می‌کند. تجزیه‌وتحلیل امنیتی نشان داده است که روش احراز هویت متقابل ناشناس در برابر اکثر تهدیدات مهم امنیتی مقاومت می‌کند و الزامات امنیتی مشترک را فراهم می‌کند. همچنین این طرح زمان احراز هویت را کاهش داده است. متأسفانه این طرح نمی‌تواند مدیریت کلید ایمن و کارآمد برای گروهی از کاربران را فراهم کند همچنین این پروتکل به دلیل استفاده از محاسبات جفت خطی، کارایی کمی را فراهم می‌کند و در برابر حملات جعل هویت، تکرار و مردی در میانه مقاوم نیست. کومار[2] و همکاران [۱۳] در سال ۲۰۲۰ در مقاله‌ای، یک پروتکل احراز اصالت امن را برای شبکه‌های IoT و سرویس‌دهنده ابری ارائه کرد که مبتنی بر خم‌های بیضوی است. آن‌ها خواص امنیتی پروتکل ارائه‌شده را بررسی کردند و با دیگر پروتکل‌های موجود ازنظر ویژگی‌های امنیتی، حفظ حریم خصوصی دستگاه، حمله جعل هویت، حمله بازگشت، حمله حدس گذرواژه، احراز هویت متقابل و همچنین کارایی پروتکل ارائه‌شده مورد مقایسه قراردادند و نشان دادند که در موارد محاسباتی، ارتباطی، سربار حافظه، کل زمان محاسباتی، امنیت و کارایی نسبت به پروتکل‌های دیگر برتری داشته است. طرح کومار در برابر حمله ناهمگام سازی مقاوم نیست. چن[3] [۴] در سال ۲۰۲۱ یک طرح احراز هویت برای اینترنت اشیا را ارائه کردند که دارای قابلیت گمنامی است و مبتنی بر چکیده ساز ترکیبی سطح ۲ هست. چن در مقاله خود مزایای طرح پیشنهادی را راندمان بالا ازنظر محاسبات و ارتباطات، ایجاد/همگام‌سازی آسان و کارآمد اسامی مستعار پویا، استحکام در برابر هر دو حملات انکار سرویس مبتنی بر همزمانی و اتصال ناپذیری، کاربرد آسان

[1] Subramani
[2] Kumar
[3] Chen

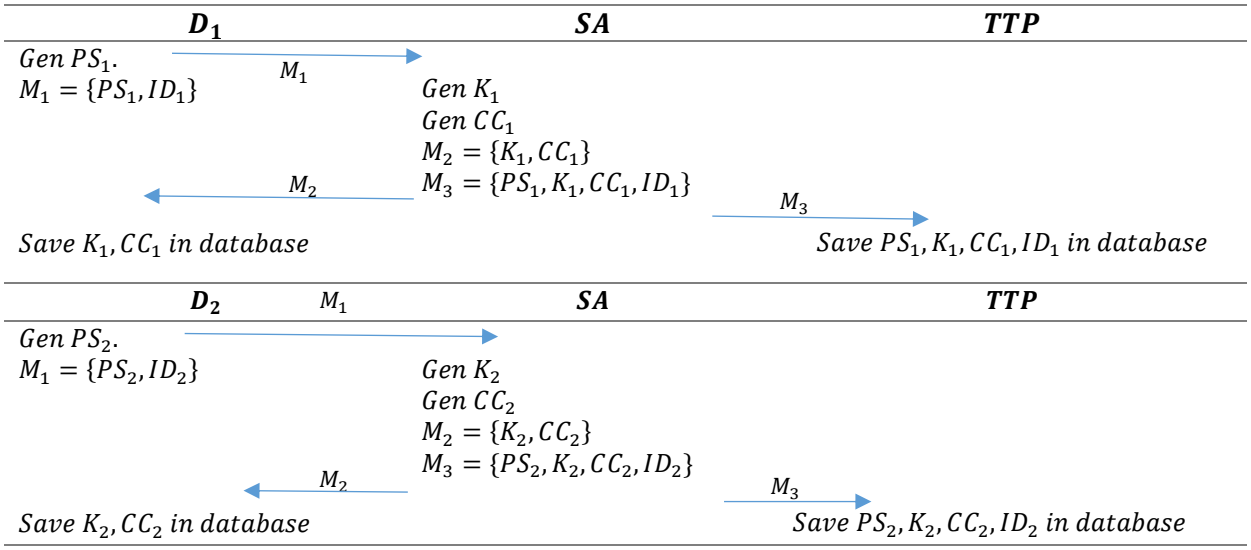
در معماری‌ها و استانداردهای موجود اینترنت اشیاء و تائید امنیت رسمی بیان کرده است. متأسفانه طرح چن در برابر حمله قطع سرویس مقاوم نیست. در سال ۲۰۲۰ گوپتا[1] و همکاران [۸] یک پروتکل احراز اصالت گمنام برای شهر هوشمند ارائه کرد که اکثر ویژگی‌های امنیتی و مقاومت در برابر اکثر حملات را دارد.

۴. طرح پیشنهادی

طرح پیشنهادی شامل سه مرحله ثبت‌نام، احراز اصالت و توافق کلید است. در مرحله ثبت‌نام دستگاه‌ها در مرکز قابل‌اعتماد ثبت‌نام می‌کنند. در این مرحله بین دستگاه و سرویس‌دهنده دو عدد تصادفی تبادل می‌شود. پس از ثبت‌نام دستگاه‌ها و سرویس‌دهنده می‌توانند بررسی هویت را آغاز نمایند. در صورت تائید هویت می‌توانند به‌صورت مستقیم با یکدیگر به یک کلید مشترک دست یابند. در جدول ۱ نمادهای اختصاری استفاده‌شده شرح داده‌شده است.

۱.۴. مرحله ثبت‌نام

در این فاز دستگاه‌ها توسط مدیر سیستم در مرکز مورد اعتماد ثبت می‌شوند . فرایند ثبت‌نام در کانال امن صورت می‌گیرد و در زیر شرح داده‌شده است.



شکل ۲ – مرحله ثبت‌نام دستگاه

گام ۱: $D_i \rightarrow SA$

ابتدا دستگاه یک مقدار تصادفی انتخاب می‌کند و به همراه شناسه اصلی خودش برای مدیر سیستم ارسال می‌کند.

[1] Gupta

گام ۲: $SA \rightarrow D_i$

مدیر سیستم کلید خصوصی دستگاه و مقدار تصادفی CC_i را تولید می‌کند و برای دستگاه ارسال می‌کند.

گام ۳: $SA \rightarrow TTP$

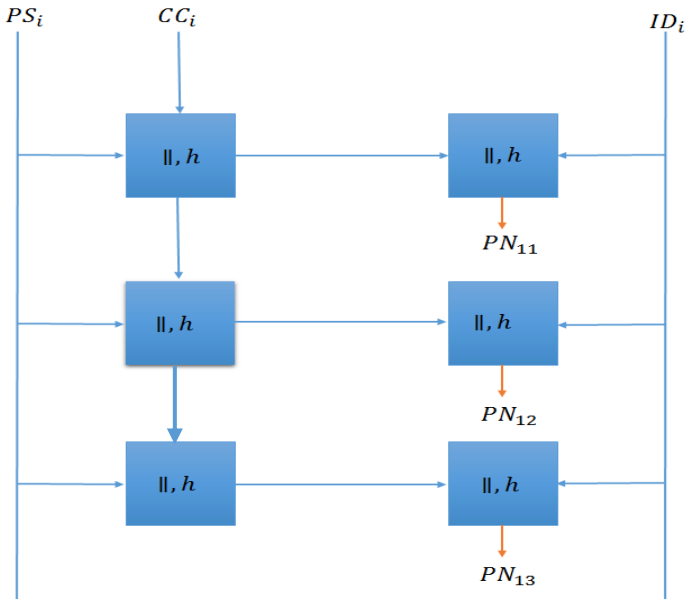
همچنین مدیر سیستم مقادیر کلید خصوصی دستگاه، شناسه اصلی دستگاه، مقدارهای تصادفی دستگاه و CC_i را برای سرویس‌دهنده ارسال می‌کند.

۲.۴. مرحله احراز اصالت

مرحله احراز اصالت شامل دو مرحله تولید نام‌های مستعار و مرحله احراز اصالت است.

۱.۲.۴. مرحله تولید نام‌های مستعار

در این مرحله ابتدا قبل از آغاز احراز اصالت دستگاه و سرویس‌دهنده نام‌های مستعار را تولید می‌نمایند و در پایگاه داده خود ذخیره می‌نمایند.



شکل ۳ – مرحله تولید نام‌های مستعار

این کار باعث می‌شود تا نیازی به هم‌زمان بودن دستگاه‌ها با سرویس‌دهنده نباشد. برای تولید نام مستعار دستگاه‌ها اعداد CC_i و PS_i را که در مرحله ثبت‌نام از مدیر سیستم دریافت نموده‌اند را از پایگاه داده خود دریافت می‌کنند و مقدار $C_{ij} = h(CC_i||PS_i)$ را محاسبه می‌کند و سپس نام مستعار را به‌صورت $PN_{ij} = h(CC_{ij}||ID_i)$ محاسبه می‌کند و در

پایگاه داده خود ذخیره می‌کند. همچنین سرویس‌دهنده این مراحل را برای هر دستگاه انجام می‌دهد و نام‌های مستعار را در پایگاه داده خود ذخیره می‌کند. مراحل تولید نام‌های مستعار در شکل ۳ نمایش داده‌شده است.

۱.۲.۴. مرحله احراز اصالت

در این مرحله دستگاه‌ها توسط سرویس‌دهنده احراز هویت می‌شوند و به هرکدام یک کلید موقت یکسان توسط سرویس‌دهنده داده می‌شود.

گام ۱: $D_1 \rightarrow TTP$

ابتدا دستگاه ۱ شناسه‌ی دستگاهی که نیاز به ارتباط با آن دارد را با کلید خصوصی خودش رمز می‌کند و سپس نام مستعار خود را تولید می‌کند. پس از تولید نام مستعار دو عدد تصادفی Q وn را تولید می‌کند و مقادیر موردنیاز برای احراز اصالت را محاسبه می‌کند. درنهایت از مقادیری که قرار است بر روی کانال فرستاده شود، به همراه CC_i برای حفظ تازگی و یکپارچگی چکیده گرفته می‌شود. درنهایت پیام M_1 برای TTP ارسال می‌گردد.

$Gen\ Q, n$
$R = h(K_1 \parallel Q)$
$F = h(R \parallel K_1 \parallel n)$
$b = F \oplus h(R \parallel Q)$
$H_{11} = h(R \parallel F \parallel CC_1)$
$y = h(K_1 \parallel H_{11}) \oplus Q$
$S = Enc_{K1}(ID_2 \parallel Q)$
$H_{mac1} = h(CC_1, b, y, H_{11}, PN_1, ID, S)$
$M_1 = H_{mac1} b, y, H_{11}, PN_{11}, S$

گام ۲: $TTP \rightarrow D_2$

TTP پس از دریافت پیام M_1 ، با مراجعه به جدول پایگاه داده خود، شناسه PN_1 را پیدا می‌کند و شناسه اصلی و کلید خصوصی بین یکدیگر را استخراج می‌کند. سپس یکپارچگی پیام را بررسی می‌کند اگر تائید شد شناسه دستگاه مقصد را رمزگشایی و سپس هویت دستگاه ۱ را بررسی می‌کند. اگر هویت دستگاه تائید شد، درخواست ارسال مقادیر احراز اصالت را برای دستگاه ۲ ارسال می‌نماید.

$verify\ H_{mac1} = H^*_{mac1}$
$Q = y \oplus h(K_1 \parallel H_{11})$
$ID_2 = Dec_{K1}(S)$
$R^* = h(K_1 || Q)$
$F^* = b \oplus h(R^* \parallel Q)$
$H^*_{11} = h(R^* \parallel F^* \parallel CC_1)$
$H^*_{11} =^? H_{11}$
$M_2 = Req, PN_{12}, PN_{21}$

گام ۳: $D_2 \rightarrow TTP$

دستگاه ۲ دو عدد تصادفی C و e را تولید می‌کند و با استفاده از کلید خصوصی و مقادیر تولیدشده، پارامترهای احراز اصالت

را تولید می‌کند. سپس از پیام‌های ارسالی به همراه CC_2 چکیده می‌گیرد و نام مستعار خود را محاسبه می‌کند و پیام M_3 برای TTP ارسال می‌کند.

$Gen\ C, e$
$E = h(K_2 \parallel C)$
$P = h(E \parallel K_2 \parallel e)$
$m = P \oplus h(E \parallel C)$
$H_{12} = h(E \parallel P \parallel CC_2)$
$l = h(K_2 \parallel H_{12}) \oplus C$
$H_{mac2} = h(CC_2, m, l, H_{12}, PN_{22})$
$M_3 = H_{mac2}, m, l, H_{12}, PN_{22}$

گام ۴: $TTP \rightarrow D_1$

TTP ابتدا یکپارچگی پیام را چک می‌کند در صورت تائید، هویت دستگاه ۲ را بررسی می‌کند.

$check\ H_{mac2} = H^*_{mac2}$
$C = l \oplus h(K_2 \parallel H_{12})$
$E^* = h(K_2 \parallel C)$
$P^* = m \oplus h(E^* \parallel C)$
$H^*_{12} = h(E^* \parallel P^* \parallel CC_2)$
$H^*_{12} =^? H_{12}$

سپس دو مقدار تصادفی N_1 و N_2 را تولید می‌نماید و کلید موقت K_{tmp} را تولید می‌نماید. درنهایت کلید موقت و مقادیر تصادفی N_{12} و N_{21} را به‌صورت رمز شده با کلید خصوصی برای دستگاه ۱ ارسال می‌نماید.

$Gen\ N_1, N_2, N_{12}, N_{21}.$
$K_{tmp} = h(N_1 \oplus \mathrm{N}_2)$
$e_1 = Enc_{K1}(K_{tmp}, N_{12}, N_{21})$
$E_1 = h(CC_1 \parallel e_1)$
$M_4 = e_1, E_1, PN_{13}, PN_{23}$

گام ۵: $TTP \rightarrow D_2$

کلید موقت K_{tmp} را به‌صورت رمز شده با کلید خصوصی، برای دستگاه ۲ ارسال می‌کند.

$e_2 = Enc_{K2}(K_{tmp}, N_{12}, N_{21})$
$E_2 = h(CC_2 \parallel e_2)$
$M_5 = e_2, E_2, PN_{23}$

گام ۶: D_1

دستگاه ۱ ابتدا یکپارچگی پیام را بررسی می‌کند اگر تائید شد مقدار کلید موقت را از طریق رمزگشایی به دست می‌آورد.

$Check\ E_1$
$Dec_{K_1}(e_1) = K_{tmp}, N_{12}, N_{21}$

گام ۷: D_2

دستگاه ۲ ابتدا یکپارچگی پیام را بررسی می‌کند اگر تائید شد مقدار کلید موقت را از طریق رمزگشایی به دست می‌آورد.

$Check\ E_2$
$Dec_{K_2}(e_2) = K_{tmp}, N_{12}, N_{21}$

در این پروتکل پس از دریافت موفقت آمیز مقادیر K_{tmp}, N_{12}, N_{21} دستگاه‌ها می‌توانند تا مدت‌زمان معینی با استفاده از این مقادیر یکدیگر را احراز اصالت نمایند و به یک کلید مشترک برسند. در شکل ۳ مراحل احراز اصالت نمایش داده‌شده است.

D_1	TTP	D_2
$Gen\ Q, n$ $R = h(K_1 \parallel Q)$ $F = h(R \parallel K_1 \parallel n)$ $b = F \oplus h(R \parallel Q)$ $H_{11} = h(R \parallel F \parallel CC_1)$ $y = h(K_1 \parallel H_{11}) \oplus Q$ $S = Enc_{K1}(ID_2 \parallel Q)$ $H_{mac1} = h(CC_1, b, y, H_{11}, PN_{11}, S)$	$H_{mac1}, b, y, H_{11}, PN_{11}, S \rightarrow$ $get\ K_1 and\ CC_1\ in\ database$ $verify\ H_{mac1} = H^*_{mac1}$ $Q = y \oplus h(K_1 \parallel H_{11})$ $ID_2 = Dec_{K1}(S)$ $R^* = h(K_1 \| Q)$ $F^* = b \oplus h(R^* \parallel Q)$ $H^*_{11} = h(R^* \parallel F^* \parallel CC_1)$ $H^*_{11} =^? H_{11}$	$Req, PN_{12}, PN_{21} \rightarrow$ $Gen\ C, e$ $E = h(K_2 \parallel C)$ $P = h(E \parallel K_2 \parallel e)$ $m = P \oplus h(E \parallel C)$ $H_{12} = h(E \parallel P \parallel CC_2)$ $l = h(K_2 \parallel H_{12}) \oplus C$ $H_{mac2} = h(CC_2, m, l, H_{12}, PN_{22})$
	$\leftarrow H_{mac2}, m, l, H_{12}, PN_{22}$ $check\ H_{mac2} = H^*_{mac2}$ $C = l \oplus h(K_2 \parallel H_{12})$ $E^* = h(K_2 \parallel C)$ $P^* = m \oplus h(E^* \parallel C)$ $H^*_{12} = h(E^* \parallel P^* \parallel CC_2)$ $H^*_{12} =^? H_{12}$ $Gen\ N_1, N_2, N_{12}, N_{21}.$ $K_{tmp} = h(N_1 \oplus N_2)$ $e_1 = Enc_{K1}(K_{tmp}, N_{12}, N_{21})$ $E_1 = h(CC_{1new} \parallel e_1)$ $e_2 = Enc_{K2}(K_{tmp}, N_{12}, N_{21})$ $E_2 = h(CC_{2new2} \parallel e_2)$	
	$\leftarrow e_1, E_1, PN_{13}, PN_{23}$	$e_2, E_2, PN_{1new}, PN_{23} \rightarrow$
$verify\ E_1$ $Dec_{K_1}(e_1) = K_{tmp}, N_{12}, N_{21}$ $Save\ in\ database\ SN_2 = h(K_{tmp} \parallel N_{21})$		$verify\ E_2$ $Dec_{K_2}(e_2) = K_{tmp}, N_{12}, N_{21}$ $Save\ in\ database\ SN_1 = h(K_{tmp} \parallel N_{12})$

شکل ۴ – مرحله احراز اصالت

۳.۴. مرحله توافق کلید

گام ۱: $D_1 \rightarrow D_2$

ابتدا دستگاه ۱ شناسه مستعار خودش و طرف مقابل را از پایگاه داده به دست می‌آورد و سپس یک مقدار تصادفی به نام x انتخاب می‌کند و $X = x.p$ را محاسبه می‌کند و به همراه $H_1 = h(K_{tmp} \parallel X)$ برای دستگاه ۲ ارسال می کند.

$SN_1 = h(K_{tmp}, N_{12})$
$SN_2 = h(K_{tmp}, N_{21})$
$Gen\ x$
$X = x.p$
$H_1 = h(K_{tmp} \parallel X)$

گام ۲: $D_2 \rightarrow D_1$

دستگاه ۲ ابتدا از پایگاه داده کلید K_{tmp} متناظر با دستگاه ۱ را به دست می‌آورد، سپس H_1 را بررسی می‌کند. اگر تائید شد y را به‌صورت تصادفی تولید می‌کند و $Y = y.p$ را محاسبه می‌کند و به همراه $H_2 = h(K_{tmp} \parallel Y)$ برای دستگاه ۲ ارسال می‌کند. درنهایت کلید جلسه را به‌صورت $K_{sess} = h(K_{tmp} \parallel xyp)$ به دست می‌آورد. در پایان نام‌های مستعار و کلید K_{tmp} را بروز رسانی می نماید.

$SN_1 = h(K_{tmp}, N_{12})$
$SN_2 = h(K_{tmp}, N_{21})$
$check\ H_1$
$Gen\ y$
$Y = y.p$
$H_2 = h(K_{tmp} \parallel Y)$
$K_{sess} = h(K_{tmp} \parallel xyp)$
$update$:
$K_{tmpnew} = h(K_{tmp} \parallel N_{12} \parallel N_{21})$
$SN_{1new} = h(K_{tmpnew} \parallel N_{12})$
$SN_{2new} = h(K_{tmpnew} \parallel N_{21})$

گام ۳: D_1

دستگاه ۱ ابتدا H_2 را بررسی می‌کند اگر تائید شد، کلید جلسه را به‌صورت $K_{sess} = h(K_{tmp} \parallel xyp)$ به دست می‌آورد. درنهایت نام‌های مستعار و کلید K_{tmp} را به‌روزرسانی می‌نماید.

$check\ H_2$
$K_{sess} = h(K_{tmp} \parallel xyp)$
$update$:
$K_{tmpnew} = h(K_{tmp} \parallel N_{12} \parallel N_{21})$
$SN_{1new} = h(K_{tmpnew} \parallel N_{12})$
$SN_{2new} = h(K_{tmpnew} \parallel N_{21})$

D_1		D_2
$SN_1 = h(K_{tmp}, N_{12})$ $SN_2 = h(K_{tmp}, N_{21})$		$SN_1 = h(K_{tmp}, N_{12})$ $SN_2 = h(K_{tmp}, N_{21})$
$Gen\ x$ $X = x.p$	X, H_1, SN_1, SN_2 →	
$H_1 = h(K_{tmp} \parallel X)$		$get\ K_{tmp}\ in\ database$ $check\ H_1$ $Gen\ y$ $Y = y.p$ $H_2 = h(K_{tmp} \parallel Y)$ $K_{sess} = h(K_{tmp} \parallel xyp)$
$check\ H_2$ $K_{sess} = h(K_{tmp} \parallel xyp)$	← Y, H_2, SN_2, SN_1	
$update$: $K_{tmpnew} = h(K_{tmp} \parallel N_{12} \parallel N_{21})$ $SN_{1new} = h(K_{tmpnew} \parallel N_{12})$ $SN_{2new} = h(K_{tmpnew} \parallel N_{21})$		$update$: $K_{tmpnew} = h(K_{tmp} \parallel N_{12} \parallel N_{21})$ $SN_{1new} = h(K_{tmpnew} \parallel N_{12})$ $SN_{2new} = h(K_{tmpnew} \parallel N_{21})$

شکل ۵ – مرحله توافق کلید

۵. تحلیل نظری امنیتی طرح پیشنهادی

در این بخش به بررسی برخی از ویژگی های امنیتی مهم و برخی از حملات متداول می‌پردازیم و مقاومت طرح پیشنهادی را در مقابل آن‌ها بررسی می‌کنیم.

۱.۵. ویژگی گمنامی

گمنامی پروتکل پیشنهادی مبتنی بر تولید نام‌های مستعار است. در گمنامی فقط دستگاه‌های مجاز می‌توانند شناسه اصلی دستگاه‌های موجود را داشته باشند ولی به‌هیچ‌عنوان شناسه اصلی دستگاه‌ها بر روی کانال منتقل نمی‌گردد. در این پروتکل در اولین ارتباط، دستگاه درخواست دهنده، شناسه اصلی دستگاه مقصد را به‌صورت رمز شده برای سرویس‌دهنده ارسال می‌کند و در بقیه شرایط فقط از نام مستعار برای ارتباط با یکدیگر استفاده می‌کنند. بنابراین در این پروتکل در هیچ شرایطی شناسه اصلی دستگاه‌ها بر روی کانال به‌صورت متن اصلی منتشر نمی‌شود و دستگاه‌ها نام مستعار خود را به نام PN_i، که مبتنی بر مسئله سخت ریاضیاتی توابع یک‌طرفه است، تولید می‌کنند و از این شناسه برای ارتباطات استفاده می‌کنند. در این پروتکل پس از هر بار استفاده شناسه مستعار باطل می‌شود و از شناسه مستعار جدید استفاده می‌گردد. این ویژگی باعث می‌گردد تا همواره شناسه مستعار به‌روزرسانی گردد و برای ارتباطات هم‌زمان، از دو شناسه مستعار متفاوت استفاده گردد.

۲.۵. ویژگی احراز اصالت

در این پروتکل به‌منظور احراز اصالت، دستگاه ۱ دو مقدار تصادفی $\mathrm{Q, n}$ را تولید می‌کند و مقادیر $R = h(K_1 \parallel Q)$، $F = h(R \parallel \mathrm{K_1} \parallel \mathrm{n})$، $b = F \oplus h(R \parallel Q)$، $y = h(K_1 \parallel H_{11}) \oplus$ و $H_{11} = h(R \parallel \mathrm{F} \parallel \mathrm{CC_1})$ را تولید می‌کند و مقادیر b، y و H_{11} را برای سرویس‌دهنده ارسال می‌کند. سرویس‌دهنده با استفاده از b و y و مقادیر محرمانه تبادل شده در مرحله ثبت‌نام، $R^* = h(K_1 || Q)$ و $F^* = b \oplus h(R^* \parallel Q)$ را محاسبه می‌کند و سپس H_{11}^* را محاسبه می‌کند.

درنهایت برای اثبات هویت دستگاه بررسی می‌کند که آیا H_{11} دریافتی با H_{11}^* برابر است یا خیر. اگر برابر بود هویت دستگاه تائید می‌شود و در غیر این صورت هویت دستگاه رد می‌شود. برای دستگاه ۲ نیز روند احراز اصالت به همین صورت است. دستگاه ۲ دو مقدار تصادفی C, e را تولید می‌کند و مقادیر $E = h(K_2 \parallel C)$، $P = h(E \parallel K_2 \parallel e)$، $m = P \oplus h(E \parallel C)$، $l = h(K_2 \parallel H_{12}) \oplus C$ و $H_{12} = h(E \parallel P \parallel CC_2)$ را تولید می‌کند و مقادیر m، l و H_{12} را برای سرویس‌دهنده ارسال می‌کند. سرویس‌دهنده با استفاده از m و l و مقادیر محرمانه تبادل شده در مرحله ثبت‌نام، $E^* = h(K_2 \parallel C)$ و $P^* = m \oplus h(E^* \parallel C)$ را محاسبه می‌کند و سپس H_{12}^* را محاسبه می‌کند. درنهایت برای اثبات هویت دستگاه بررسی می‌کند که آیا H_{12} دریافتی با H_{12}^* برابر است یا خیر. اگر برابر بود هویت دستگاه تائید می‌شود و در غیر این صورت هویت دستگاه رد می‌شود. در این پروتکل احراز اصالت مبتنی بر کلید خصوصی بین دستگاه و سرویس دهنده است که در مرحله ثبت نام از مدیر سیستم دریافت کرده اند.

۳.۵. ویژگی محرمانگی

در این پروتکل اگر مهاجم در مرحله توافق کلید قصد کند تا کلید جلسه را به دست آورد موفق نمی‌شود. زیرا اگر خواسته باشد تا کلید موقت K_{tmp} را به دست آورد باید پیام $e_1 = Enc_{K1}(K_{tmp}, N_{12}, N_{21})$ یا پیام $e_2 = Enc_{K2}(K_{tmp}, N_{12}, N_{21})$ را رمزگشایی کند، که به دلیل نداشتن کلید مخفی K_1 و K_2 نمی‌تواند این کار را انجام دهد. همچنین اگر به هر دلیلی کلیدهای مخفی را به دست آورد بازهم موفق نخواهد شد. زیرا باید از روی X و Y مقادیر x و y را به دست آورد که به دلیل مسئله سخت لگاریتم گسسته امکان‌پذیر نیست. بنابراین محرمانگی کلید جلسه حفظ می‌گردد.

۴.۵. ویژگی توافق کلید

در این پروتکل پس از احراز اصالت و دریافت کلید موقت K_{tmp} دستگاه‌ها می‌توانند از این کلید ، برای توافق کلید بین یکدیگر بدون دخالت سرویس‌دهنده، استفاده نمایند. کلید موقت K_{tmp} پس از مدتی استفاده باطل می‌گردد و دستگاه‌ها باید مجدد احراز اصالت نمایند. ایده توافق کلید مبتنی بر ایده توافق کلید دیفی هلمن با خم‌های بیضوی است. در این پروتکل دستگاه ۱، x را به‌صورت تصادفی تولید می‌کند و سپس $X = x.p$ را به همراه $H_1 = h(K_{tmp} \parallel X)$ برای حفظ یکپارچگی برای دستگاه ۲ ارسال می‌کند. دستگاه ۲ پس از بررسی H_1 مقدار y را به‌صورت تصادفی تولید می‌کند و سپس $Y = y.p$ را به همراه $H_2 = h(K_{tmp} \parallel Y)$ برای حفظ یکپارچگی، برای دستگاه ۱ ارسال می‌کند. درصورتی‌که بررسی H_2 موفق بود کلید جلسه مشترک به‌صورت $K_{sess} = h(K_{tmp} \parallel xyp)$ محاسبه می گردد.

۵.۵. ویژگی رازداری روبه‌جلو

در این پروتکل تولید و توافق کید به کلیدهای مخفی K_1 و K_2 وابسته نیست و به‌صورت مستقل و با اعداد تصادفی کلید جلسه تولید می‌گردد. بنابراین اگر کلیدهای مخفی K_1 و K_2 توسط مهاجم کشف گردد موفق به محاسبه کلید جلسه فعلی و جلسات قبل که از این کلیدهای مخفی استفاده‌شده است نخواهد شد. بنابراین رازداری روبه‌جلو را ارائه می‌دهد.

۶.۵. ویژگی یکپارچگی

در این پروتکل با استفاده از توابع چکیده ساز یکپارچگی پیام‌های تبادل شده حفظ می‌گردد.

۷.۵. ویژگی اتصال ناپذیری

اگر یک گره x به‌طور هم‌زمان با دو گره مختلف y و z ارتباط برقرار کند، آنگاه از هویت‌های پویا متفاوتی در پیام‌های مبادله شده با y و z استفاده می‌شود. همچنین در هر پیام ارتباطی با به‌روزرسانی مقدار CC_i یک شناسه مستعار جدید تولید می‌شود و مورداستفاده قرار می‌گیرد. بنابراین این پروتکل پیوند ناپذیر است.

۸.۵. حمله جعل هویت

در این پروتکل مهاجم برای جعل هویت باید حتماً سه پارامتر ID_i, K_i, CC_i را داشته باشد. حتی اگر یک مورد از این پارامترها نباشد حمله با شکست مواجه خواهد شد. اگر مهاجم سعی کند که مقادیر ID_i و CC_i را از طریق $PN_i = h(CC_i \parallel ID_i)$ به دست آورد به دلیل یک‌طرفه بودن توابع چکیده ساز موفق نخواهد شد. همچنین از روی مقدار $H_{ij} = h(R \parallel F \parallel CC_i)$ نیز به دلیل یک‌طرفه بودن تابع چکیده ساز و محرمانه بودن مقادیر R و F موفق به کشف CC_i نخواهد شد. همچنین برای یافتن کلید دستگاه ۱ باید مقادیر محرمانه $R = h(K_1 \parallel Q)$ و $F = h(R \parallel K_1 \parallel n)$ را به دست آورد. ازآنجایی‌که این مقادیر بر روی کانال منتقل نمی‌شوند امکان دسترسی به این مقادیر وجود ندارد. حتی اگر این مقادیر را به دست آورد به دلیل یک‌طرفه بودن توابع چکیده ساز امکان کشف کلید محرمانه وجود ندارد. همچنین از روی مقدار $y = h(K_1 \parallel H_{11}) \oplus Q$ نیز به دلیل محرمانه بودن مقدار تصادفی Q و یک‌طرفه بودن توابع چکیده ساز امکان کشف کلید محرمانه وجود ندارد. برای دستگاه ۲ نیز به همین صورت است. مهاجم برای یافتن کلید دستگاه ۲ باید مقادیر محرمانه $E = h(K_2 \parallel C)$ و $P = h(E \parallel K_2 \parallel e)$را به دست آورد. ازآنجایی‌که این مقادیر بر روی کانال منتقل نمی‌شوند امکان دسترسی به این مقادیر وجود ندارد. حتی اگر این مقادیر را به دست آورد به دلیل یک‌طرفه بودن توابع چکیده ساز امکان کشف کلید محرمانه وجود ندارد. همچنین از روی مقدار $l = h(K_2 \parallel H_{12}) \oplus C$ نیز به دلیل محرمانه بودن مقدار تصادفی C و یک‌طرفه بودن توابع چکیده ساز امکان کشف کلید محرمانه وجود ندارد.

۹.۵. حمله مردی در میانه

در این پروتکل اگر مهاجم در مرحله احراز اصالت در بین دستگاه ۱ و سرویس‌دهنده قرار بگیرد، و پیام‌های تبادل شده را باهدف به دست آوردن اطلاعات یا نفوذ دست‌کاری کند، موفق نمی‌شود. زیرا پیام‌هایی که در کانال منتقل می‌شود شامل b, y, H_{11}, PN_1 است. اگر $b = F \oplus h(R \parallel Q)$ را به صورت $b' = F' \oplus h(R \parallel Q)'$ تغییر دهد سرویس‌دهنده پیام را دریافت می‌نماید و $H_{mac1} = H^*_{mac1}$ را محاسبه می‌نماید زمانی که $H^*_{mac1} = h(CC_1, b', y, H_{11}, PN_1)$ را بررسی می‌کند متوجه حمله می‌گردد و جلسه را رد می‌کند. همین توضیح برای تغییر دادن y و H_{11} نیز صدق می‌کند.

همچنین اگر در مرحله آخر یعنی دریافت کلید موقت، مهاجم e_1 را تغییر دهد، دستگاه ۱ با چک کردن $E_1^* = h(CC_1 \parallel e'_1)$ متوجه می‌گردد که $E_1^* = E_1$ نیست و جلسه را رد می‌کند.

اگر مهاجم در مرحله احراز اصالت در بین دستگاه ۲ و سرویس‌دهنده قرار بگیرد، و پیام‌های تبادل شده را باهدف به دست آوردن اطلاعات یا نفوذ دست‌کاری کند، موفق نمی‌شود. زیرا پیام‌هایی که در کانال منتقل می‌شود شامل m, l, H_{12}, PN_2 است. اگر $m = P \oplus h(E \parallel C)$ را به صورت $m' = P' \oplus h(E \parallel C)'$ تغییر دهد سرویس‌دهنده پیام را دریافت می‌نماید و $H_{mac2} = H^*_{mac2}$ را محاسبه می‌نماید زمانی که $H^*_{mac2} = h(CC_2, m', l, H_{12}, PN_2)$ را بررسی می‌کند متوجه حمله می‌گردد و جلسه را رد می‌کند. همین توضیح برای تغییر دادن l و H_{12} نیز صدق می‌کند.

همچنین اگر در مرحله آخر دریافت کلید موقت مهاجم e_2 را تغییر دهد، دستگاه ۱ با چک کردن $E_2^* = h(CC_1 \parallel e'_2)$ متوجه می‌گردد که $E_2^* = E_2$ نیست و جلسه را رد می‌کند.

اگر مهاجم در مرحله توافق کلید بین دو دستگاه قرار بگیرد، اگر $X = x.p$ را به‌صورت $X' = x'.p$ تغییر دهد دستگاه ۲ با محاسبه $H_1^* = h(K_{tmp} \parallel X')$ و چک کردن $H_1^* =^? H_1$ متوجه تغییر می‌شود و جلسه را رد می‌کند.
همچنین اگر مهاجم $Y = y.p$ را به‌صورت $Y' = y'.p$ تغییر دهد دستگاه ۲ با محاسبه $H_2^* = h(K_{tmp} \parallel Y')$ و چک کردن $H_2^* =^? H_2$ متوجه تغییر می‌شود و جلسه را رد می‌کند.

۱۰.۵. حمله انکار سرویس

در این پروتکل اگر مهاجم باهدف از کار انداختن سرویس، پیام‌های نادرست برای سرویس‌دهنده ارسال نماید، در اولین مرحله با بررسی کردن مقادیر H_{maci}^* متوجه می‌گردد که این مشخصات با مشخصات هیچ دستگاهی سازگار نیست و متوجه حمله می‌گردد. همچنین اگر پیام‌های ارسالی از دستگاه‌ها را که مقادیر صحیح دارند را مکرر برای سرویس‌دهنده ارسال کند، ازآنجایی‌که CC_i پس از استفاده به‌روزرسانی می‌گردد، با بررسی H_{maci}^* متوجه می‌گردد که این مقادیر تکراری است و باطل‌شده است پس جلسه را رد و دستگاه را از سرویس خارج می‌کند.

۱۱.۵. حمله حدس گذرواژه

در این پروتکل از گذرواژه استفاده نمی‌گردد؛ بنابراین در برابر این حمله آسیب‌پذیر نیست.

۱۲.۵. حمله تکرار

در این پروتکل مقدار CC_i پس از هر بار استفاده به‌روزرسانی می‌گردد و مقدار CC_i قبلی باطل می‌گردد، اگر مهاجم پیام‌ها را ذخیره نماید و در زمان دیگری برای سرویس‌دهنده ارسال نماید، ازآنجایی‌که مقدار CC_i پیام باطل‌شده است متوجه حمله می‌گردد و جلسه را رد می‌نماید. اگر مهاجم در بخش تبادل کلید موقت، پیام‌های سرویس‌دهنده را ذخیره و مجدد برای دستگاه‌ها ارسال نماید. ازآنجایی‌که CC_i یک‌بار استفاده می‌گردد و با استفاده از تابع تولید دنباله تصادفی CC_i جدید تولید می‌کند،دستگاه با چک کردن $E_i^* = h(CC_{iold} \parallel e_i)$ متوجه حمله می‌گردد و جلسه را رد می‌نماید. همچنین در بخش توافق کلید اگر مهاجم حمله تکراری انجام دهد، موفق نخواهد شد. زیرا اگر مهاجم به هر دلیلی کلید جلسه را پیداکرده باشد و پیام X, H_1, PN_2 را برای دستگاه ۲ ارسال کند، تا با این کلید جلسه دیگری ایجاد کند، دستگاه ۲ عدد تصادفی y جدید تولید می‌کند و به یک کلید جلسه جدید می‌رسد. بنابراین به دلیل مستقل بودن کلیدهای جلسه از یکدیگر امکان اینکه مهاجم حمله را انجام دهد وجود ندارد.

۱۳.۵. حمله ناهمگام سازی

در این پروتکل اگر مهاجم یک اتصال ناموفق بین دستگاه و سرور ایجاد نماید، ازآنجایی‌که دستگاه منتظر دریافت پاسخ از سرور است، اگر پاسخی دریافت نکند، جهت جلوگیری از هدر رفتن منابع ارتباط قبلی را اتمام می‌کند و مجدد با استفاده از شناسه مستعار جلسه بعد که در پایگاه داده ذخیره‌شده است ارتباط را آغاز می‌نماید. ازآنجایی‌که شناسه‌های مستعار از قبل محاسبه می‌شوند و نیازی به‌به روز رسانی در هر ارتباط نیست، این کار باعث جلوگیری از ناهمگام شدن بین دستگاه‌ها و سرویس‌دهنده می‌شود.

جدول ۲- مقایسه امنیتی

ویژگی‌ها امنیتی	جانبابایی ۲۰۱۸	سابرامانی ۲۰۱۹	کومار ۲۰۲۰	چن ۲۰۲۱	گوپتا ۲۰۲۲	پیشنهادی
احراز اصالت	✓	×	✓	✓	✓	✓
گمنامی	✓	✓	✓	✓	✓	✓
محرمانگی	×	✓	✓	✓	✓	✓
توافق کلید امن	×	×	✓	×	✓	✓
دسترس‌پذیری	✓	✓	✓	✓	✓	✓
رازداری روبه‌جلو	×	✓	✓	✓	×	✓
اتصال ناپذیری	×	✓	✓	✓	✓	✓
جعل هویت	×	×	✓	✓	✓	✓
تکرار	✓	×	✓	✓	✓	✓
مردی در میانه	×	×	✓	✓	✓	✓
انکار سرویس	✓	✓	✓	✓	✓	✓
ناهمگام سازی	✓	✓	×	✓	✓	✓

۶. تحلیل عملی طرح پیشنهادی به روش صوری با ابزار پرووریف[1]

امنیت طرح با ابزار تحلیل خودکار پروتکل‌ها پرووریف اثبات‌شده است. نتایج ارزیابی در شکل ۳ نشان داده‌شده است.

```
--------------------------------------------------------------------
Verification summary:
Query not attacker(ID1[]) is true.
Query not attacker(ID2[]) is true.
Query not attacker(CC1[]) is true.
Query not attacker(Q[]) is true.
Query not attacker(n[]) is true.
Query not attacker(CC2[]) is true.
Query not attacker(C[]) is true.
Query not attacker(e[]) is true.
Query not attacker(N1[]) is true.
Query not attacker(N2[]) is true.
Query not attacker(k1[]) is true.
Query not attacker(k2[]) is true.
Query inj-event(end1) ==> inj-event(begin1) is true.
Query inj-event(end2) ==> inj-event(begin2) is true.
```

شکل ۶ – نتایج شبیه‌سازی

۷. ارزیابی طرح پیشنهادی و مقایسه پیچیدگی محاسباتی

در این بخش با بررسی و محاسبه فضای ذخیره‌سازی، سربار محاسباتی، مصرف انرژی گره حسگر و گره مرکزی و همچنین بررسی هزینه ارتباطی توسط پیام‌های ارسالی، کارایی طرح پیشنهادی مورد ارزیابی قرارگرفته شده است. در جدول ۳ پیچیدگی محاسباتی طرح ها نمایش داده‌شده است.

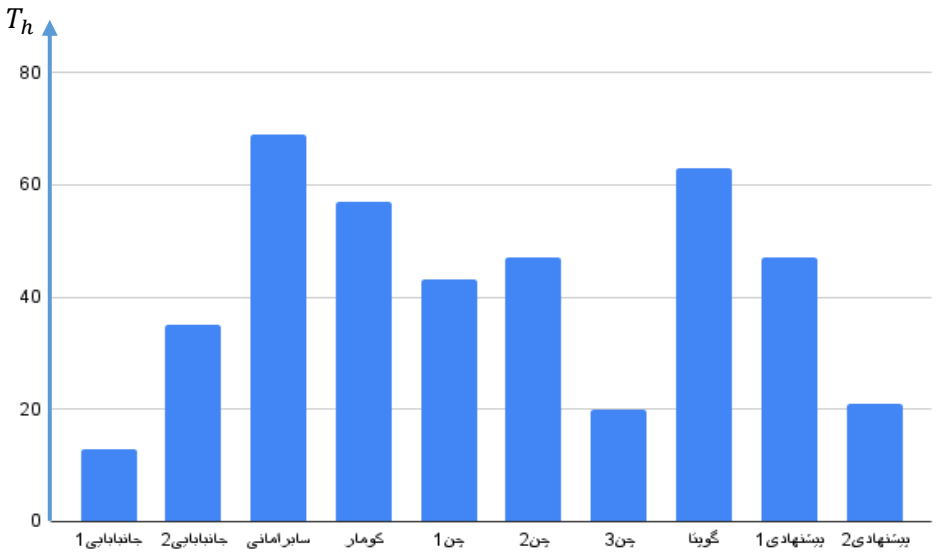
[1] Proverif

جدول ۳- مقایسه پیچیدگی محاسباتی

پروتکل	هزینه محاسباتی
جانبابایی[۱] پروتکل احراز اصالت در سرخوشه یکسان	$12T_h + 9T_{xor}$
جانبابایی[۱] پروتکل احراز اصالت در دو سرخوشه متفاوت	$34Th + 23Txor$
سابرامانی[۱۲]	$6T_{EPM} + 4Th + 3T_{ECA} + 2Tp$
کومار[۱۳]	$9Th + 8T_{EPM}$
چن[۴] پروتکل احراز اصالت توسط سرویس دهنده	$19Th + 6Tenc + 4T_{ECCM}$
چن[۴] پروتکل احراز اصالت مستقیم	$23T_h + 6T_{enc} + 4T_{ECCM}$
گوپتا[۸]	$23Th + 1T_{xor} + 10T_{Enc} + 10T_{Dec}$
پیشنهادی پروتکل احراز اصالت	$31T_h + 9T_{xor} + 3T_{Enc} + 3T_{Dec}$
پروتکل توافق کلید	**هزینه محاسباتی**
چن[۴] پروتکل توافق کلید	$8Th + 4T_{ECCM}$
پیشنهادی پروتکل توافق کلید	$16T_h + 4T_{ECCM}$

در این جدول T_{enc} زمان رمزگذاری، T_{xor}زمان محاسبه جمع در مبنای ۲، T_h زمان محاسبه چکیده پیام، T_{ECCM}زمان محاسبه خم بیضوی، T_{ECA} زمان جمع نقاط در خم بیضوی، T_{EPM} زمان ضرب نقاط در خم بیضوی و T_pزمان محاسبه جفت خطی است.

به‌صورت تقریبی زمان T_{ENC} دو برابر، T_{ECCM} سه ، T_{ECA} پنج برابر، T_{EPM} شش و T_p هفت برابر زمان محاسبه چکیده پیام یعنی T_h است.



شکل ۷– نمودار پیچیدگی محاسباتی

۸. نتیجه‌گیری

اینترنت اشیا مفهوم جدیدی است که در سال‌های اخیر، کاربردهای بسیار گسترده ای پیدا کرده و از این رو توجهات بسیاری از محققیان را به خود جلب کرده است. در این شبکه تمامی اشیا می‌توانند از طریق اینترنت با یکدیگر در ارتباط باشند. با افزایش ارتباطات در این شبکه، احراز اصالت به‌عنوان یکی از مسائل کلیدی این حوزه به شمار می‌آید که به علت محدودیت‌های محاسباتی در دستگاه‌های هوشمند و حسگرها بهتر است برای حل آن از راه‌حل‌های سبک استفاده شود. از طرفی یکی از مباحث مهم در اینترنت اشیا، مسئله گمنامی موجودیت‌ها در این شبکه است. طرح پیشنهادی در این مقاله یک طرح احراز اصالت باقابلیت گمنامی است که تمامی ویژگی‌های امنیتی موردنیاز در یک شبکه اینترنت اشیا مانند محرمانگی، حریم خصوصی، یکپارچگی، امنیت جلو رونده و عقب رونده، اتصال ناپذیری، مقیاس‌پذیری، دسترس‌پذیری و توافق کلید امن را فراهم می‌کند و در برابر حملات شناخته‌شده مانند انواع حملات جعل هویت، حمله تکرار، حمله مردی در میانه، انواع حملات انکار سرویس و حمله داخلی به این شبکه مقاوم است. در این طرح در فقط در صورتی کلید جلسه به اشتراک گذاشته می‌شود که هویت هر دو طرف برای سرویس‌دهنده اثبات‌شده باشد. شبیه سازی طرح و تحلیل آن با ابزار تحلیل پرووریف، نتایج نظری بدست آمده را تایید کرده اند.

۹. مراجع

[۱] جانبابایی، شادی، قرائی، حسین، م. زاده، ناصر، "ارائه طرح احراز اصالت سبک با قابلیت گمنامی و اعتماد در اینترنت اشیا," ۲۰۱۹.

[۲] ف. پدیداران مقدم و ب. ارجمندزاده، "مروری بر احراز هویت در اینترنت اشیاء" چهارمین کنفرانس سراسری دانش و فناوری مهندسی مکانیک و برق ایران، ۱۳۹۷.

[3] K. Ashton, "That ‘internet of things’ thing," RFID journal, vol. 22, no. 7, pp. 97-114, 2009.

[4] H.Y. Chien, "Two-Level-Composite-Hashing Facilitating Highly Efficient Anonymous IoT and D2D Authentication," Electronics, vol. 10, no. 7, p. 789, 2021.

[5] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and J.J. Schwartzmann, "A review on authentication methods," Australian Journal of Basic and Applied Sciences, vol. 7, no. 5, pp. 95-107, 2013.

[6] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment," IEEE Consumer Electronics Magazine, 2021.

[7] D. He, N. Kumar, J. Chen, C.C. Lee, N. Chilamkurti, and S.S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21, no. 1, pp. 49-60, 2015.

[8] A. Gupta and G. S. Kasbekar, "Secure, Anonymity-Preserving and Lightweight Mutual Authentication and Key Agreement Protocol for Home Automation IoT Networks," in 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2022, pp. 375-383: IEEE.

[9] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li, "A novel secure architecture for the internet of things," in 2011 Fifth International Conference on Genetic and Evolutionary Computing, 2011, pp. 311-314: IEEE.

[10] I. Goldberg, D. Stebila, and B. Ustaoglu, "Anonymity and one-way authentication in key exchange protocols," Designs, Codes and Cryptography, vol. 67, no. 2, pp. 245-269, 2013.
[11] C.T. Li, T.Y. Wu, C.L. Chen, C.C. Lee, and C.M .Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," Sensors, vol. 17, no. 7, p. 1482, 2017.
[12] S. Jegadeesan et al. "An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications," Sustainable Cities and Society, vol. 49 ,p. 101522, 2019.
[13] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," Journal of Reliable Intelligent Environments, vol. 6, no. 2, pp. 79-94, 2020.
[14] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia ,and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, 2015, pp. 37-42.
[15] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar" ,A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, vol. 80, pp. 483-495, 2018.
[16] R. El Abbadi and H. Jamouli, "Takagi–Sugeno Fuzzy Control for a Nonlinear Networked System Exposed to a Replay Attack," Mathematical Problems in Engineering, vol. 2021, 2021.
[17] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," Nuclear Engineering and Technology, vol. 50, no. 5, pp. 780-787, 2018.
[18] K. Jindal, S. Dalal, and K. K. Sharma, "Analyzing spoofing attacks in wireless networks," in 2014 Fourth International Conference on Advanced Computing & Communication Technologies, 2014, pp. 398-402: IEEE.