

روشی جدید برای احراز هویت دوطرفه



در اینترنت اشیا

پیام محمودی نصر^{۱*} و حسین کیمیا^۲

^۱دانشکده مهندسی و فناوری، دانشگاه مازندران، مازندران، ایران

^۲مؤسسه آموزش عالی صنعتی مازندران، مازندران، ایران

چکیده

امروزه شاهد گسترش خدمات مختلف اینترنت اشیا در حوزه‌های مختلف از قبیل نظارت و سلامت هستیم. این خدمات از طریق دستگاه‌های هوشمند در هر مکان و زمانی می‌تواند در دسترس کاربران قرار گیرند. این در حالی است که این دسترسی‌ها می‌تواند مسأله امنیت و حریم خصوصی را به امری حساس و حیاتی تبدیل کند. گزارش‌های دریافتی نشان می‌دهد که تعداد دستگاه‌های اینترنت اشیا تا سال ۲۰۳۰ به عدد ۲۵/۴۴ بیلیون خواهد رسید و این در حالی است که ۲۶٪ حملات اینترنت اشیا در سال ۲۰۱۹ مربوط به عدم احراز هویت بوده است. به همین دلیل احراز هویت کاربران در اینترنت اشیا به یکی از حساس‌ترین مفاهیم امنیتی تبدیل شده است. در این مقاله یک پروتکل احراز هویت دوطرفه دستگاه‌به‌دستگاه برای شبکه‌های خانگی هوشمند، ارائه شده است. این پروتکل بر اساس رمزنگاری نامتقارن برای احراز هویت دستگاه‌های موجود در شبکه طراحی شده و در آن تمامی دستگاه‌ها یک کلید جلسه خصوصی مشترک دارند. برای حصول اطمینان از امنیت ارتباطها در هر جلسه، کلیدهای جلسه پس از هر جلسه ارتباطی، تغییر می‌کنند. برنامه‌نویسی طرح پیشنهادی به وسیله HLPSL، شبیه‌سازی و ارزیابی بهیچگی با ابزار SPAN و AVISPA انجام شده است. تحلیل‌های امنیتی نشان می‌دهد که پروتکل پیشنهادی در مقابل حملات امنیتی، پایداری خود را حفظ می‌کند.

واژگان کلیدی: اینترنت اشیا، پروتکل احراز هویت، رمزنگاری، امنیت، AVISPA.

A Mutual Authentication Method for Internet of Things

Payam Mahmoudi-Nasr^{*1} & Hossein Kimia²

¹Engineering and Technology Dep., University of Mazandaran, Mazandaran, Iran

²Mazandaran Institute of Technology, Mazandaran, Iran

Abstract

Today, we are witnessing the expansion of various Internet of Things (IoT) applications and services such as monitoring and health. These services are delivered to users via smart devices anywhere and anytime. Forecasts show that the IoT, which is controlled online in the user environment, will reach 25 billion devices worldwide by 2020.

Data security is one of the main concerns in the IoT. The IoT is supposed to deal with a population of about billions of objects, so the number of malicious attacks can be very high and alarming given the global connection (anyone access) and the wide availability (access to any place at any time). However, these accesses can make security and privacy critical. Reports show that 26% of IoT attacks in 2019 were related to non-authentication, which is why IoT authentication has become one of the most sensitive security concepts. IoT devices are usually left unattended and this makes it easy for an attacker to target such equipment. For example, security breaches and unwanted changes in patient's health parameters in smart health care systems can cause wrong treatments or even lead to his death. The fact that each device in the IoT knows who it is communicating with and at what level of access is one of the important aspects of security, especially in cases where various devices with different capabilities have to perform common tasks and cooperate with each other. IoT authentication is a trust model to protect control access and data when information travels between devices.

* Corresponding author

* نویسنده عهده‌دار مکاتبات

سال ۱۴۰۱ شماره ۲ پیاپی ۵۲

• تاریخ ارسال مقاله: ۱۳۹۹/۱/۲۷ • تاریخ پذیرش: ۱۴۰۰/۱/۲۹ • تاریخ انتشار: ۱۴۰۱/۷/۷ • نوع مطالعه: پژوهشی

فصلنامه

پژوهش‌های
پردازش داده

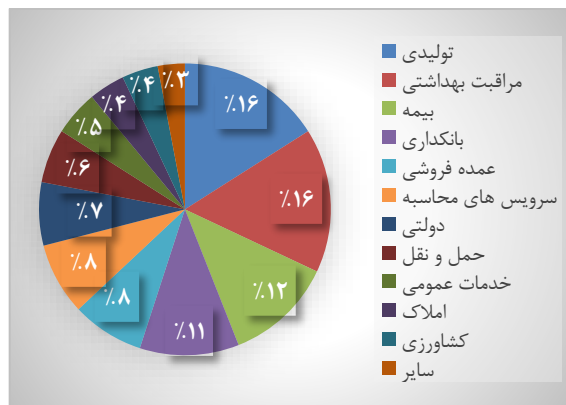
۷۳

So far, different methods have been proposed for authentication in the IoT network. These methods are usually based on the public key, private key, random key distribution, and hash function. A point that should be taken into account in IoT authentication is that IoT networks and devices have limited bandwidth, low memory, low processing power, and energy limitations. Therefore, the proposed method should pay special attention to such limitations. In addition, IoT authentication needs to ensure enhanced security features such as confidentiality, data integrity, reliability, maintainability, scalability, and privacy to their consumers.

This paper proposes a two-way or mutual authentication protocol in which both devices authenticate each other without human intervention in a smart home network. The proposed protocol is based on asymmetric encryption for authentication of devices, which have a shared private session key, along with hashing operations in the network. Also, to ensure the security of communications at each session, each device has a one-time private session key. The session keys are changed regularly to ensure the security of sessions between devices. The proposed protocol is programmed by HLPSL and simulated and verified by the SPAN and AVISPA tools. The security analysis results show the proposed protocol is extremely practical, and secure against potential attacks.

Keywords: Internet of Things, Authentication protocol, Cryptography, Security, AVISPA.

سامانه‌های هوشمند مراقبت از سلامتی و داده‌های معیوب ناقص/ نامرتب و بی‌نظم از پارامترهای سلامتی یک بیمار می‌تواند باعث درمان‌های ناخواسته/ اشتباه و یا حتی منجر به مرگ وی شود. این موضوع که هر دستگاهی در اینترنت اشیا بداند در حال ارتباط با چه کسی/ دستگاهی و در چه سطحی از دسترسی است، از جنبه‌های مهم امنیتی است، به‌خصوص در مواردی که وسایل متنوعی با قابلیت‌ها مختلف مجبور به انجام وظایف مشترک و همکاری با یکدیگر هستند؛ لذا می‌توان گفت احراز هویت از نخستین گام‌های امنیتی در اینترنت اشیا است.



(شکل ۱): موارد استفاده اینترنت اشیا.

(Figure-1): IoT categories.

امنیت داده‌ها یکی از دغدغه‌های اصلی در اینترنت اشیا است. اینترنت اشیا قرار است با جمعیتی حدود میلیاردی شیء سروکار داشته باشد؛ بنابراین تعداد حمله‌های مخرب با توجه به اتصال جهانی (دسترسی هر کسی) و دسترس‌پذیری گسترده (دسترسی به هر مکان در هر زمان) می‌تواند بسیار زیاد و نگران‌کننده باشد [3]. به‌عنوان مثال، نقض‌های امنیتی و تغییرات ناخواسته در

۱- مقدمه

اینترنت اشیا (IoT) در همین اواخر به شکل قابل‌توجهی شکوفا و باعث به‌وجود آمدن شرکت‌های نوپای فراوانی شده و بسیاری از شرکت‌ها و سازمان‌های بزرگ، زمان و منابع خود را در این بخش سرمایه‌گذاری کرده‌اند. زمینه‌های کاربرد اینترنت اشیا از خانه تا بیمارستان، اتوماسیون صنعتی، کشاورزی تا شبکه‌های توزیع برق بسیار متنوع و متفاوت است. وسایل مختلفی مانند دست‌بند‌های تناسب‌اندام، ضربان‌سنج‌ها، پمپ‌های انسولین، ساعت‌ها، ترموستات‌های خانگی و تلویزیون‌های هوشمند، ارتباط ماشین‌ها در محیط‌های صنعتی، تجهیزات جلوگیری/شناسایی برخورد اتومبیل‌ها، وسایل نقلیه بدون سرنشین و وسایل شبکه هوشمند برق همگی مثال‌هایی از کاربرد اینترنت اشیا است که امروزه تقاضای بیشتری دارند. اینترنت اشیا میزان اتصال تجهیزات را افزایش داده و باعث بهبود اقتصاد، کیفیت زندگی و حتی سلامتی می‌شود [1]. شکل (۱) زمینه‌های مختلف کاربردی اینترنت اشیا را نمایش می‌دهد. پیش‌بینی‌ها نشان می‌دهد که اینترنت اشیا و لوازمی که به‌صورت برخط در محیط اطراف کاربران کنترل می‌شوند تا سال ۲۰۲۰ به ۲۵ میلیارد دستگاه در سرتاسر دنیا خواهد رسید [2].

امنیت داده‌ها یکی از دغدغه‌های اصلی در اینترنت اشیا است. اینترنت اشیا قرار است با جمعیتی حدود میلیاردی شیء سروکار داشته باشد؛ بنابراین تعداد حمله‌های مخرب با توجه به اتصال جهانی (دسترسی هر کسی) و دسترس‌پذیری گسترده (دسترسی به هر مکان در هر زمان) می‌تواند بسیار زیاد و نگران‌کننده باشد [3]. به‌عنوان مثال، نقض‌های امنیتی و تغییرات ناخواسته در

شده تا شبکه ارتباطی امن را فراهم کند. در این روش همچنین یک روش آستانه پویا برای محاسبه امتیاز آستانه صداسنجی کاربر براساس ترکیب گاوسی ارائه شده است. پس از احراز هویت اولیه، کاربران متنی که روی صفحه نمایش آمده را می‌خوانند. این عمل باعث جلوگیری ورود مهاجمان به‌عنوان یک شخص دارای اعتبار می‌شود. می‌دانیم که احراز هویت به‌کمک صداسنجی دارای محاسبات رایانه‌ای بسیار است و لذا در این روش کارایی فدای امنیت خواهد شد. Ukil و همکاران [7] یک شمای تأیید امنیتی سبک‌وزن با استفاده از مدیریت حفاظت کلیدی ارائه کردند تا بتوانند کانالی امن برای سیستم‌های ردیابی وسایل نقلیه به‌وجود بیاورند. این پروتکل سبک‌وزن، به‌منظور افزایش کارایی، تبادل اطلاعات سنگین میان رایانه‌ها را کاهش داده و بر پایه اطلاعات مربوط به وسایل نقلیه است. Barreto و همکاران [8]، نشان می‌دهند که چگونه تجهیزات می‌توانند فرایند احراز هویت را در یک سناریوی سرویس ابری IoT انجام دهند. در این پژوهش، فقط دستگاه‌های ایمن IoT برای پیوستن به ارائه‌دهنده سرویس ابری IoT مورد تأیید هستند. پس از فرایند پیوستن به این سرویس، انواع احراز هویت بسته به سازنده، کاربر عادی و کاربر پیشرفته در دسترس است. سازندگان می‌توانند به‌صورت دوره‌ای برای انجام کارهایی از جمله به‌روزرسانی، انجام تنظیمات، رفع مشکل و ... به دستگاه‌های IoT متصل شوند. کاربران عادی می‌توانند از طریق پلتفرم سرویس ابری IoT به دستگاه‌های IoT متصل شوند، درحالی‌که کاربران پیشرفته می‌توانند دسترسی مستقیم به دستگاه‌ها داشته باشند. با این وجود، برای انجام چنین احراز هویت‌هایی، خود کاربران می‌بایست در سرویس ابری عملیات احراز هویت را انجام دهند. جانبابایی و همکاران [9] یک پروتکل احراز هویت سبک بر پایه گمنامی ارائه کرده‌اند. در این پروتکل برخی نیازمندی‌های امنیتی مورد توجه قرار گرفته و نشان داده شده که در مقابل حملات جعل هویت، تکرار و مردمیانی مقاوم است. در این پروتکل سعی شده تا با استفاده از توابع درهم‌ساز تا حد مقدور پروتکل سبک، تا در حس‌گرها قابل استفاده باشد. مایسا و همکاران [10] یک پروتکل احراز هویت با استفاده از توکن ارائه کرده‌اند. در این مقاله از توابع درهم‌ساز و تابه XOR برای آسانی عملیات پردازشی و سرعت بیشتر استفاده شده است. محدودیت این روش آن است که تنها برای دسترسی موقت به داده‌ها می‌تواند مورد استفاده قرار گیرد. کیسانگ

سامانه‌های هوشمند مراقبت از سلامتی و داده‌های معیوب/ناقص/نامرتب و بی‌نظم از پارامترهای سلامتی یک بیمار می‌تواند باعث درمان‌های ناخواسته/اشتباه و یا حتی منجر به مرگ وی شود. این موضوع که هر دستگاهی در اینترنت اشیا بداند در حال ارتباط با چه کسی/دستگاهی و در چه سطحی از دسترسی است، از جنبه‌های مهم امنیتی است، به‌خصوص در مواردی که وسایل متنوعی با قابلیت‌ها مختلف مجبور به انجام وظایف مشترک و همکاری با یکدیگر هستند؛ لذا می‌توان گفت احراز هویت از نخستین گام‌های امنیتی در اینترنت اشیا است.

احراز هویت، فرایند تأیید هویت یک وسیله و حصول اطمینان از منبع ارتباط است. با برقراری احراز هویت میان منابع، میزان فاکتور اطمینان در ارتباطات IoT افزایش‌یافته و از امنیت اطلاعات اطمینان حاصل می‌شود. مرسوم‌ترین روش احراز هویت بر اساس گواهی‌های انسانی مانند بیومتریک، ترکیب نام کاربری و رمز عبور، اطلاعات شخصی و یا نقش کاری در یک سازمان است. اینترنت اشیا یک شبکه ناهم‌گون است که در آن انواع ارتباطات میان دو دستگاه، دستگاه به انسان و یا انسان به دستگاه برقرار است. چالش دیگر موضوع سربار احراز هویت در ترافیک شبکه و صرف زمان برای برقراری آن است. دستگاه‌های متصل به اینترنت اشیا به‌طورعمومی توان پردازشی و حافظه محدودی دارند؛ بنابراین روش احراز هویتی که پیاده‌سازی می‌شود نیاز است که ظرفیت پایین پردازش و حافظه را به‌عنوان اولویت اصلی قرار دهد [4].

تاکنون مطالعات گسترده‌ای در خصوص اینترنت اشیا انجام‌گرفته که در میان آنها جنبه امنیتی اینترنت اشیا بیشتر مورد توجه قرار گرفته است. Crossman و همکاران [5] مدلی جدید برای تأیید کاربر یا دستگاه مبتنی بر کاربر ارائه کرده‌اند. در این مدل که به آن تأیید هوشمند دومرحله‌ای اطلاق شده، پس از این‌که کاربر رمز خود را وارد کرد، به جای تولید کد تأیید، یک رمز امنیتی داده می‌شود. این رمز امنیتی مانند یک کارت هوشمند به‌عنوان فاکتور دوم احراز هویت برای دریافت کلید رمزنگاری پویا استفاده می‌شود. Ren و همکاران [6] یک سیستم شناسایی صدا و احراز هویت اینترنتی براساس موبایل ارائه کرده‌اند که شامل دو زیر سیستم است. در این سیستم از تجهیزات Raspberry Pi به‌عنوان مرکز کنترل زیرسیستم‌ها استفاده می‌شود. این مرکز کنترل به‌وسیله یک شبکه خصوصی مجازی (VPN) به تلفن همراه متصل

بیشتر مورد استفاده است با استفاده از ابزار Avispa شبیه‌سازی و ارزیابی شده است.

و همکاران [11] یک پروتکل احراز هویت سبک مبتنی بر کلید مشترک را بدون نیاز به ذخیره‌سازی در پایگاه داده ارائه کرده‌اند. روش پیشنهادی که در کاربردهای پزشکی

(جدول-1): مقایسه تکنیک‌ها بر اساس مدل ارزیابی شده

(Table-1): Comparison of techniques based on evaluated model

پروتکل پیشنهادی	[18]	[3]	[19]	[6]	[17]	[7]	[20]	[5]	[20]	[21]	
پیاپی‌سازی				*	*			*			
شبیه‌سازی	*	*			*	*				*	
ارزیابی نظری	*		*	*	*	*	*		*	*	
بررسی عملکرد		*		*	*	*			*	*	

اطلاعات شخصی، اطلاعات هویتی، اطلاعات بانکی، اطلاعات کارت اعتباری یا اعتبارات امنیتی باشند که دسترسی به تجهیزات دیگری را فراهم کنند؛ این در حالی است که در سال ۲۰۱۴، شرکت هیولت پاکارد در مطالعه‌ای اعلام کرد که هفتاد درصد از متداول‌ترین دستگاه‌های اینترنت اشیا در کشور آمریکا به دلیل گذرواژه‌های ضعیف و یا اتصالات بدون رمزگذاری دارای آسیب‌پذیری‌های جدی هستند [13].

شکل (۲) معماری یک خانه هوشمند را نشان می‌دهد. همان‌طور که ملاحظه می‌شود، در این مدل از سرور رایانش ابری بهره برده شده است. البته رایانش ابری هنگامی یک راه‌حل قابل قبول و سودمند است که بتوانیم از دسترسی کامل و بدون وقفه به سرور ابر اطمینان حاصل کنیم. با توجه به محدودیت‌های موجود و به منظور پرکردن شکاف محدودیتی (پهنای باند، محدودیت‌های زمانی و مسائل مربوط به مقیاس‌پذیری)، امروزه رایانش مرزی به عنوان راه‌حل موفقیت‌آمیز معرفی شده است [14]. در این مدل داده‌ها به جای ابر یا مرکز داده دوردست، در دستگاه‌های محاسبات محلی جمع‌آوری و پردازش می‌شوند و لذا، داده‌ها به‌طور مکرر به سرور مرکزی برای پردازش ارسال نخواهند شد، بلکه هر دستگاه در شبکه محلی پردازش را انجام داده و سپس داده‌ها را به مرکز ارسال می‌کند. اگر چه این تجزیه و تحلیل بدون درنگ داده‌ها، امنیت به‌نسب بهتری را تضمین می‌کند، اما نیاز به این دارد که تمام دستگاه‌های مرزی از نظر محاسباتی قدرتمند و دارای ظرفیت حافظه بیشتری باشند. در این مدل دروازه، که وظیفه تبادل اطلاعات و ارتباطات بین دستگاه‌ها را به عهده دارد، به عنوان عنصر اصلی شبکه در IoT در نظر گرفته می‌شود. این عنصر به عنوان یک رابط عمل کرده و می‌تواند ترافیک ورودی و خروجی از شبکه‌های با محدودیت و بدون محدودیت را کنترل کند [15].

هدف اصلی این مقاله، ارائه یک پروتکل احراز هویت متقابل/دوطرفه دستگاه‌به‌دستگاه بدون دخالت انسان است. در این راستا به منظور انجام اعتبارسنجی دوطرفه، از رمزنگاری نامتقارن به همراه عملیات درهم‌سازی برای احراز هویت دستگاه‌های موجود در شبکه استفاده شده است. همچنین به منظور اطمینان از امنیت ارتباطها در هر نشست، تمامی دستگاه‌ها دارای یک کلید جلسه خصوصی، مشترک، و یک بار مصرف هستند. برای شبیه‌سازی و نمایش کارایی پروتکل پیشنهادی از نرم‌افزار شبیه‌ساز AVISPA به منظور پیاده‌سازی اجزای مختلف پروتکل استفاده شده است. تحلیل‌های امنیتی انجام شده نشان می‌دهد که پروتکل پیشنهادی در مقابل بسیاری از حملات امنیت خود را حفظ می‌کند. جدول (۱) مقایسه ارزیابی پروتکل پیشنهادی نسبت به کارهای پیشین را نشان می‌دهد.

۲- مفاهیم پایه

۲-۱- معماری خانه هوشمند

یک خانه هوشمند به خانه‌ای اطلاق می‌شود که دارای یک سامانه خودکار برای نظارت بر تمامی تجهیزاتی است که بدون دخالت انسان با یکدیگر در ارتباط هستند [12] مانند درجه حرارت، درب‌ها، مصرف انرژی، لوازم خانگی، و ... از آنجا که تمامی تجهیزات در یک خانه هوشمند با یکدیگر در ارتباطند (مانند لامپ‌ها، قفل‌های هوشمند، یخچال و فریزر، تلویزیون، لپ‌تاپ، ترموستات و غیره)، ایمنی و حفظ حریم خصوصی هر یک از آنها اهمیت زیادی دارد. چرا که اگر تنها یک دستگاه در معرض خطر باشد، مهاجم می‌تواند از این دستگاه به صورت یک نقطه مرکزی استفاده کرده و به شبکه‌ای که دستگاه عضوی از آن است وارد شده و در نهایت به منابع موجود در آن دسترسی پیدا کند. این دارایی‌ها یا منابع می‌توانند

سلسله‌مراتبی: از یک سامانه سلسله‌مراتبی احراز هویت استفاده می‌کند که در آن هر کاربر باتوجه به حق دسترسی خود می‌تواند به اطلاعات احراز هویت دسترسی داشته باشد.

یکنواخت: فرایند احراز هویت، بدون در نظر گرفتن سلسله‌مراتب اجرا می‌شود.

در روش دوم تکنیک‌های احراز هویت را باتوجه به مشخصات فرایند احراز هویت به شرح زیر طبقه‌بندی می‌کنند [3]:

۱. احراز هویت دوطرفه: بستگی به این دارد که احراز هویت متقابل صورت گرفته است یا احراز هویت یک‌طرفه.

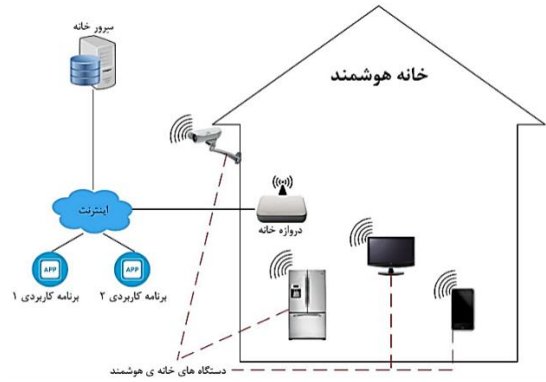
۲. نیازمندی به سخت‌افزار: آیا سخت‌افزاری برای کامل کردن فرایند احراز هویت نیاز است یا خیر.

۳. چندمدرکی: نیازمند این است که مدارک متعددی در سطوح مختلف برای تأیید صحت هویت کاربر یا دستگاه، تأیید شود.

۴. احراز هویت چندسطحی: نیازمند سطوح مختلف احراز هویت با مدارک متفاوت در هر سطح است.

۵. ثبت‌نام: نیازمند یک مرحله ثبت‌نام به‌منظور ثبت اطلاعات کاربر، دستگاه یا سرور است.

۶. مرحله برون‌خط: مرحله برون‌خط یا پیش‌راه‌اندازی برای آماده‌سازی شبکه و یا به‌روزرسانی‌ها نیاز است. جدول (۳) مقایسه روش استفاده شده در پژوهش‌های پیشین و روش پیشنهادی را نشان می‌دهد [16,17].



(شکل-۲): سیستم شبکه خانگی هوشمند در IoT
(Figure-2): Smart home architecture in IoT

۲-۲- طبقه‌بندی تکنیک‌های احراز هویت

به‌طور کلی تکنیک‌های احراز هویت را می‌توان به دو روش طبقه‌بندی کرد. در روش نخست، طبقه‌بندی باتوجه به چگونگی اعمال فرایند احراز هویت صورت می‌گیرد. جدول (۲) تقسیم‌بندی بالا را نمایش می‌دهد.

(جدول-۲): تکنیک‌های احراز هویت

(Table-2): Authentication techniques.

یکنواخت	سلسله‌مراتبی	
پروتکل پیشنهادی	[18], [8], [3]	متمرکز
[22], [21], [19], [7], [5]	[17]	توزیع شده

متمرکز: کاربران / دستگاه‌ها برای فراهم کردن مدارک لازم به یک سرور مرکزی قابل اعتماد متصل می‌شوند.

توزیع شده: اجزا به‌صورت جداگانه به‌منظور دستیابی به هدفی مشترک، با همکاران خود ارتباط برقرار کرده و هماهنگی لازم را ایجاد می‌کنند.

(جدول-۳): مقایسه تکنیک‌های احراز هویت

(Table-3): Comparison of authentication technique.

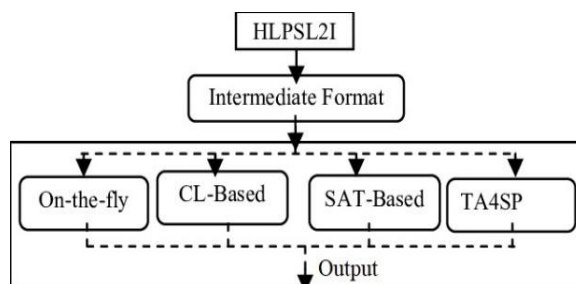
پروتکل پیشنهادی	[18]	[8]	[3]	[24]	[6]	[17]	[22]	[7]	[21]	[5]	[20]	[19]	
*			*					*	*			*	احراز هویت متقابل
		*	*				*	*		*			سخت‌فزار اضافی
*			*	*		*	*		*	*	*		چندمدرکی
	*			*						*			چندسطحی
*		*	*		*	*			*				ثبت‌نام
					*		*	*				*	مرحله برون‌خط

زبان سطح بالا، مبتنی بر نقش برای مدل‌سازی پروتکل‌های ارتباطی و امنیتی است. ویژگی‌های HLPSSL اجازه می‌دهد تا پروتکل بدون استفاده از تکنیک‌های خاص پیاده‌سازی شود، سپس پروتکل پیاده‌سازی شده به‌صورت خودکار توسط مترجم HLPSSL2IF به IF ترجمه

۲-۳- معماری AVISPA

معماری ابزار AVISPA در شکل (۳) نشان داده شده است. همان‌طور که ملاحظه می‌شود، ابتدا پروتکل امنیتی با استفاده از زبان HLPSSL پیاده‌سازی می‌شود. HLPSSL یک

می‌شود. این ترجمه‌ها، به‌عنوان ورودی برای پایانه‌های مختلف است که ابزار تحلیل AVISPA محسوب می‌شوند [23].



شکل-۳: معماری ابزار AVISPA
(Figure-3): AVISPA architecture

ابزار AVISPA دارای چهار پایانه برای پردازش ریاضی است:

OFMG: این ابزار برای پروتکل‌هایی است که در آن خواص جبری توابع رمزنگاری مهم هستند. این ابزار نه تنها می‌تواند برای جعل محرمانه پروتکل‌ها، یعنی شناسایی سریع حملات، به کار گرفته شود بلکه برای تأیید نیز مورد استفاده قرار می‌گیرد. به عبارت دیگر تأیید پروتکل برای تعداد محدودی از جلسات، بدون محدود کردن پیام‌هایی که دستگاه مزاحم می‌تواند تولید کند.

CL-AtSe: این ابزار یک سامانه مبتنی بر محدودیت است. به عبارتی بررسی‌های لازم را انجام می‌دهد تا مشخصات پروتکل امنیتی را به مجموعه‌ای از محدودیت‌ها تبدیل کند. بدین ترتیب می‌تواند به‌طور مؤثر برای یافتن حملات به پروتکل‌ها مورد استفاده قرار گیرد.

SATMC: این ابزار ترکیبی موفق از تکنیک‌های رمزگذاری است به‌عبارتی تلاش می‌کند تا یک فرمول پیشنهادی ارائه دهد که ناقض ویژگی‌های امنیتی است.

TA4SP: این ابزار یا به آسیب‌پذیری پروتکل اشاره می‌کند و یا میزان ثبات آن را به‌وسیله برآورد دقیق از قابلیت‌های دستگاه مهاجم پیش‌بینی می‌کند.

۴-۲- حملات امنیتی

مهم‌ترین حملات امنیتی به پروتکل‌های احراز هویت را می‌توان به شرح زیر خلاصه کرد:

حمله زمان‌سنجی: این حمله شیء مخربی را فعال کرده تا اطلاعات محرمانه در سامانه را با بررسی مدت زمانی که طول می‌کشد تا سامانه به پرس‌وجوهای مختلف پاسخ دهد، برملا کند و بر اساس آن شیوه پیاده‌سازی الگوریتم رمزنگاری را بفهمد.

(جدول-۴): فهرست نمادهای استفاده‌شده

(Table-4): List of symbols.

نشان گذاری	توضیحات
D_1	دستگاه ۱ اینترنت اشیا (فرضاً تلویزیون)
D_2	دستگاه ۲ اینترنت اشیا (فرضاً مایکروویو)
P_1	رمز عبور یکبار مصرف دستگاه D_1
G	دروازه
C	کنترل کننده
U_D	دستگاه شخصی کاربر
ID_1, ID_2	هویت دستگاه ۱ و ۲
K_{u1}, K_{u2}	کلید عمومی دستگاه ۱ و ۲
K'_{u1}, K'_{u2}	کلید خصوصی دستگاه ۱ و ۲
ID_g	هویت دروازه
K_{uG}, K_{uC}	کلید عمومی دروازه و کنترل کننده
IP_{v6}	هویت مجازی
T_c	برچسب زمان فعلی
N_1, N_2, N_3, N_4	Nonce ها - مجموعه بیت غیرقابل پیش‌بینی
H, H_1	Hash ها - تضمین عدم دستکاری پیام‌ها
$H(IP_{v6})$	درهم‌سازی IP_{v6} دستگاه اول
K_{12}	کلید مشترک میان دستگاه ۱ و ۲
$M \rightarrow N$	پیام ارسال شده از M به N
M^u	مقدار جدید M
$En\{M\}$	مقدار رمزنگاری شده M

حمله داخلی: این حمله زمانی رخ می‌دهد که یک عضو دارای صلاحیت، به سایر اعضای شبکه حمله می‌کند.

حمله جعل هویت: مهاجم از هویت و مدارک احراز هویت یک کاربر مورد اعتماد استفاده کرده تا بتواند به سایر موجودیت‌ها دسترسی پیدا کرده و پیام‌های مخربی را ارسال کند.

حمله بازپخش: مهاجم بسته‌ای ارسالی در شبکه را نزد خود ذخیره کرده تا پس از خروج کاربر اصلی از بازپخش آنها برای احراز هویت خود استفاده کند.

حمله تعویض / حدس رمز عبور: این حمله یکی از مخرب‌ترین تهدیدها است. در این حمله مهاجم از ضعف طرح امنیتی سوء استفاده کرده و با موفقیت رمز عبور موجودیت ثبت نام شده را تغییر / حدس می‌زند.

حمله جعل: یک مهاجم می‌تواند به‌عنوان کاربری قانونی ظاهر شود و به مدارک لازمه دسترسی پیدا کند.

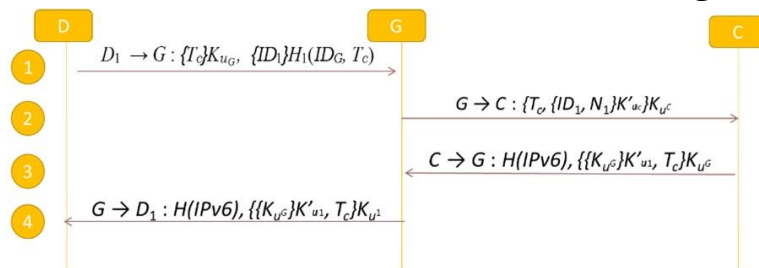
حمله شنود: مهاجم با گوش دادن به تبادلات میان دو موجودیت، به اطلاعات سری و محرمانه دست می‌یابد.

حمله منع سرویس: مهاجم به طور مداوم به گیرنده پیام ارسال کرده و منبع سیستم را مصرف می‌کند، به عبارت دیگر مهاجم با ارسال درخواست‌های بیش از حد منجر به از کار افتادن آن می‌شود.

۳-۱- مرحله پیش‌راه‌اندازی

این مرحله، در محل تولید دستگاه و پیش از رسیدن آن به دست فروشنده یا کاربر تحقق می‌یابد. در این مرحله تولیدکننده دستگاه را با اطلاعات و جزئیات رمزنگاری در رابطه با سرور ابری بارگذاری می‌کند. این عمل به ایجاد یک پل ارتباطی مطمئن میان تولیدکننده و دستگاه به جهت اجرای اعمالی از قبیل به‌روزرسانی نرم‌افزاری یا دانلود میان‌افزار کمک می‌کند؛ سپس کنترل‌کننده در سرور از راه دور هویت دستگاه (ID_1)، و با استفاده از یک مقدار تصادفی کلید عمومی، کلید خصوصی و یک رمز عبور یک‌بارمصرف (P_1) را برای دستگاه تولید، و آنها را با استفاده از یک کانال امن، بر روی دستگاه بارگذاری می‌کند به صورت زیر:

$$C \rightarrow D_1 : \text{En}\{ID_1, P_1, K_{u1}, K_{u1g}\} \quad (1)$$



(شکل-۴): مرحله راه‌اندازی
(Figure-4): Initialization part

دروازه پیام دریافتی را رمزگشایی کرده و برچسب زمانی را بررسی می‌کند. اگر صحیح باشد، مقدار $H_1(ID_G, T_C)$ که کلید رمزنگاری استفاده شده برای رمزنگاری و ID دستگاه D_1 بوده را محاسبه می‌کند. این گام در معادله پایین نشان داده شده است.

$$D_1 \rightarrow G : \{T_c\}K_{uG}, \{ID_1\}H_1(ID_G, T_c) \quad (3)$$

هنگامی که دروازه هویت دستگاه را به دست آورد، هویت دستگاه، برچسب زمانی فعلی و N_1 را که هرکدام به شکلی مناسب رمزنگاری شده‌اند، برای کنترل‌کننده در سرور از راه دور ارسال می‌کند.

$$G \rightarrow C : \{T_c, \{ID_1, N_1\}K'u, c\}K_{uG} \quad (4)$$

برچسب زمانی اطلاعاتی درباره زمان رخ دادن یک واقعه را منتقل می‌کند. Nonce مقداری است که تنها یک‌بار استفاده می‌شود. برچسب‌های زمانی و Nonce‌ها طوری انتخاب می‌شوند که از حملات بازپخش جلوگیری

حمله کارت هوشمند سرقت‌شده: مهاجم از اطلاعات موجود در کارت هوشمند کاربر خبر دارد و از آن برای احراز هویت موفق استفاده می‌کند.

حمله جدول رنگین کمائی: جدول رنگین کمائی، جدول جستجوی از پیش محاسبه شده از کلمات عبور رمز شده است. در این حمله مهاجم سعی می‌کند تا با استفاده از جدول رنگین کمائی یک کلمه عبور را با توجه به رمز آن بازیابی کند.

حمله جستجوی فراگیر: مهاجم برای بازیابی کلمات عبور جستجوی جامع و کاملی را با استفاده از روش سعی و خطا انجام می‌دهد.

۳- طراحی پروتکل پیشنهادی

پروتکل پیشنهادی دارای سه مرحله است که در ادامه به تشریح آنها می‌پردازیم. جدول (۴) علائم استفاده شده در پروتکل پیشنهادی را نشان می‌دهد.

۳-۲- مرحله راه‌اندازی

هنگامی که کاربر، دستگاه D_1 را دریافت می‌کند از سرور ابری اطلاعات احراز هویت را درخواست می‌کند تا بتواند به دستگاه دسترسی داشته باشد. کنترل‌کننده سرور ابری رمز عبور یک‌بارمصرف را به کاربر ارسال کرده تا به کاربر اجازه دسترسی به سرویس‌های D_1 را بدهد.

هنگامی که کاربر به سرویس‌های D_1 دسترسی پیدا کرد، دستگاه می‌تواند از طریق دروازه هوشمند G به سرور شبکه خانگی متصل شود. دستگاه شخصی کاربر، هویت دروازه هوشمند ID_G و کلید عمومی آن K_{uG} را به D_1 ارسال می‌کند.

$$U_D \rightarrow D_1 : ID_G, K_{uG} \quad (2)$$

دستگاه D_1 ، ID دروازه به همراه برچسب زمان فعلی را رمزنگاری کرده و برای دروازه ارسال می‌کند تا در شبکه خانگی ثبت شود. به هنگام دریافت داده از D_1 ،

کند. در ابتدا D_1 درخواست این ارتباط را برای دروازه ارسال می‌کند.

$$D_1 \rightarrow G : H(IPv6), \{T_c, D_2\}K_{uG} \quad (7)$$

دروازه برچسب زمانی را چک کرده و در صورت صحیح بودن، پایگاه داده را برای اطلاعاتی درباره D_2 بررسی و برای D_1 ارسال می‌کند. K_{12} که کلید مشترکی است که می‌تواند برای ارتباط میان D_1 و D_2 استفاده شود، پیوست شده با مقدار تصادفی یک بار مصرف N_2 ، برچسب زمانی فعلی و K_{uG} پیوست شده با K_{12} که با کلید خصوصی D_2 رمزنگاری شده، همگی با کلید عمومی دستگاه به صورت زیر رمزنگاری می‌شوند.

$$G \rightarrow D_1 : \{\{K_{uG}, K_{12}\}K_{u'1}, T_c, N_2, K_{12}\}K_{u'1} \quad (8)$$

D_1 ارسال شده برای D_1 توسط G ، به همین گونه برای D_2 ارسال می‌شود و این به D_2 تضمین می‌دهد که کلید واقعاً به وسیله دروازه به اشتراک گذاشته شده است. D_1 برچسب زمانی را بررسی کرده و در صورت صحت آن، کلید مشترک K_{12} را دریافت می‌کند. D_1 $\{K_{uG}, K_{12}\}K_{u'1}$ را برای D_2 به همراه مقدار تصادفی یک بار مصرف N_3 و برچسب زمانی فعلی، پیوست شده و رمزنگاری شده، ارسال می‌کند.

$$D_1 \rightarrow D_2 : \{\{K_{uG}, K_{12}\}K_{u'2}, \{N_3\}K_{12}, H_1(K_{12}, T_c)\}K_{u'2} \quad (9)$$

D_2 پیام دریافت شده را رمزگشایی کرده و K_{12} را از $\{K_{uG}, K_{12}\}K_{u'2}$ با اطمینان از اینکه به وسیله دروازه به دست آمده، دریافت می‌کند؛ سپس توسط کلید K_{12} مقدار N_3 را رمزگشایی می‌کند. D_2 از تابع درهم ساز و K_{12} آگاه است و در نهایت می‌تواند T_c را دریافت کرده و برچسب زمانی را چک کند.

D_2 با مقدار تصادفی و یک بار مصرف N_4 ، که پیوست شده با مقدار دریافتی N_3 است به D_1 پاسخ می‌دهد. هنگامی که D_1 ، N_3 را به همراه برچسب زمانی معتبر رمزنگاری شده با کلید مشترک دریافت می‌کند، D_2 را معتبر در نظر می‌گیرد. برای اعتباربخشیدن خودش به D_2 ، D_1 با مقدار N_4 رمزنگاری شده با کلید مشترکی که فقط دو دستگاه از آن آگاه‌اند، به D_2 پاسخ می‌دهد. هر دو این گام‌ها در معادلات زیر نشان داده شده‌اند.

$$D_2 \rightarrow D_1 : \{\{N_3, N_4\}K_{u'1}, T_c\}K_{12} \quad (10)$$

$$D_1 \rightarrow D_2 : \{N_4\}K_{12} \quad (11)$$

کنند. کنترل‌کننده در سرور ابری، برچسب زمانی دریافت شده را با برچسب زمانی فعلی چک می‌کند. در صورت صحت، N_1 را می‌گیرد و تضمین می‌دهد که تاکنون دریافت نشده است و سپس ID دستگاه را دریافت می‌کند. کنترل‌کننده یک هویت مجازی IP_{v6} برای D_1 ایجاد کرده و آن را در پایگاه داده خود با ID متناظرش ذخیره می‌کند؛ سپس مقادیر به هم پیوسته درهم‌سازی شده IP_{v6} ، کلید عمومی دروازه که با کلید خصوصی دستگاه رمزنگاری شده و با برچسب زمانی فعلی پیوست شده، با کلید عمومی دروازه رمزنگاری کرده و برای دروازه می‌فرستد. طبق رابطه زیر:

$$C \rightarrow G : H(IPv6), \{\{K_{uG}\}K_{u'1}, T_c\}K_{u'1} \quad (5)$$

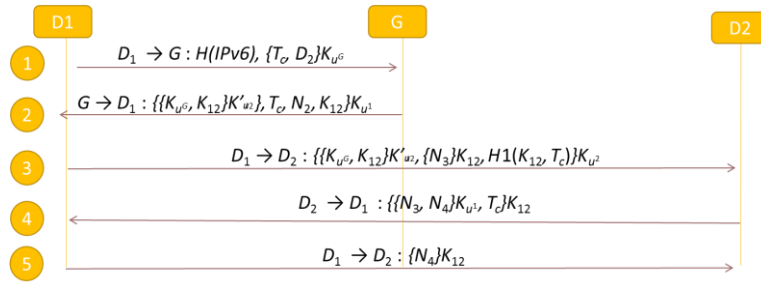
در گام بعد، G برچسب زمانی را تأیید کرده و $H(IP_{v6})$ را به همراه ID متناظرش یعنی ID_1 در پایگاه داده خود ذخیره می‌کند؛ سپس دروازه $H(IP_{v6})$ و کلید عمومی خودش که با کلید خصوصی دستگاه که از کنترل‌کننده دریافت و رمزنگاری شده، و برچسب زمانی فعلی را که همگی با کلید عمومی D_1 رمزنگاری شده‌اند، برای D_1 ارسال می‌کند. D_1 برچسب زمانی دریافت شده را بررسی کرده و در صورت صحیح بودن، $H(IP_{v6})$ را در حافظه خود ذخیره می‌کند. این گام با معادله زیر نشان داده شده است:

$$G \rightarrow D_1 : H(IPv6), \{\{K_{uG}\}K_{u'1}, T_c\}K_{u'1} \quad (6)$$

دروازه هوشمند می‌تواند با سایر دروازه‌ها ارتباط برقرار کند و همچنین دارای یک پایگاه داده محلی است که در آن تمام اطلاعاتی که دائم توسط شبکه خانگی و دستگاه‌های موجود در آن استفاده می‌شود را ذخیره می‌کند. دروازه هوشمند اطلاعات محلی را به‌طور بازه‌ای و متناوب در ابر به‌روزرسانی می‌کند. بدین ترتیب ابر اطلاعات تمام شبکه‌های خانگی و دستگاه‌های متصل را، و دروازه اطلاعات دستگاه‌های متصل در شبکه خانگی خود را دارند. شکل (۴) نحوه ارتباط موارد یادشده را به‌طور یکجا نمایش می‌دهد.

۳-۳- مرحله عملکرد

هنگام عملیات در شبکه خانگی، کاربر از یک دستگاه شخصی مثل تلفن همراه برای درخواست یک عمل خاص از D_1 استفاده می‌کند. برای این کار دستگاه D_1 می‌بایست با دستگاه دیگری در شبکه خانگی یعنی D_2 ارتباط برقرار



(شکل-۵): مرحله عملکرد
(Figure-5): Operation part

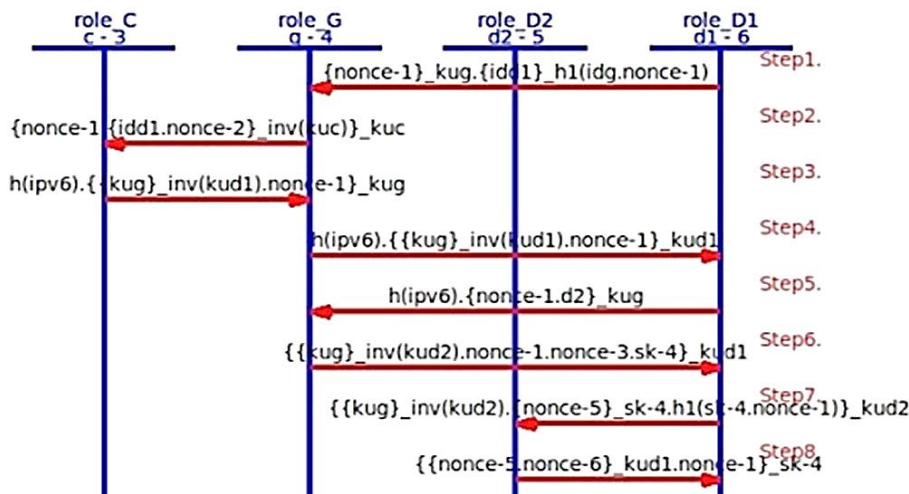
پروتکل ناامن باشد، ردپای حمله نشان داده می‌شود. نتیجه شبیه‌سازی طرح پیشنهادی بر اساس پشتیبان‌های مورد قبولی نظیر OFMC و CL-AtSe می‌باشد. همچنین با توسعه مدل AVISPA با استفاده از HLPSL، از یک انیماتور پروتکل امنیتی (SPAN) برای اجرای نمادین پروتکل پیشنهادی استفاده شده است. SPAN درک بهتری از پروتکل را در اختیار قرار داده و در صورت قابل اجرا بودن تشریح آن را تأیید می‌کند. شکل (۶) توالی پیام‌ها در پروتکل پیشنهادی را نشان می‌دهد.

شکل (۵) نحوه ارتباط موارد یادشده را به‌طور یک‌جا نمایش می‌دهد.

۴- راستی‌آزمایی و نتایج شبیه‌سازی

۴-۱- محیط شبیه‌سازی

برای شبیه‌سازی از ابزار AVISPA [25]، بر روی ماشین مجازی با ۲ گیگ حافظه و سیستم‌عامل Ubuntu 10 استفاده شده است. ابزار AVISPA بررسی می‌کند که آیا پروتکل پیشنهادی ویژگی‌های امنیتی نظیر تأیید، جامعیت و محرمانه‌بودن را برآورده می‌سازد یا خیر. اگر



(شکل-۶): شبیه‌سازی پروتکل پیشنهادی در AVISPA و توالی پیام‌ها
(Figure-6): Protocol simulation in AVISPA and sequence of messages

نتایج بررسی با استفاده از پشتیبان‌های OFMC و CL-AtSe به‌ترتیب در شکل‌های (۷ و ۸) نشان داده شده‌اند. دو پشتیبان دیگر یعنی SATMC و TA4SP، گزارش NOT SUPPORTED را ارائه کرده و نتیجه بررسی را بدون نتیجه اعلام کرده‌اند.

۴-۲- بررسی‌های امنیتی

شبیه‌سازی شامل مدل‌سازی پروتکل با استفاده از HLPSL در AVISPA و ایجاد MSCها با استفاده از SPAN است. برای این منظور یک مهاجم فعال را معرفی کرده و مدل را با استفاده از پشتیبان‌های ارائه‌شده در ابزار بررسی می‌کنیم.

۳-۴- تحلیل نظری امنیت پروتکل

همان‌طور که در بخش قبل ملاحظه شد، برای تشخیص حملاتی مانند تکرار، نشست موازی و جلوگیری از سرویس از ابزار CL-AtSe استفاده شد که حملات احتمالی را تشخیص می‌دهد و ردپای حملات را نشان می‌دهد. پشتیبان CL-AtSe تأیید کرد که پروتکل پیشنهادی از حملات بالا مصون است.

۱. **حمله تکرار:** مهرهای زمانی به‌طورعمومی برای مقاومت در برابر حمله تکرار استفاده می‌شوند. در برخی موارد، این شیوه ممکن است، تحت تأثیر مسأله همگام‌سازی پالس ساعت در هر نقطه از زمان قرار گیرد. پروتکل پیشنهادی از شماره‌های تصادفی علاوه بر مهرهای زمانی به‌منظور تضمین تازگی پیام استفاده می‌کند.

۲. **حمله حدس‌زدن رمز عبور:** کلمات رمز عبور یک‌بارمصرف با استفاده از سازوکار ساخت رمز عبور تصادفی در سمت تولیدکننده ایجاد می‌شود. از آنجایی که رمز عبور به هیچ‌گونه اعتبارنامه‌ای وابسته نبوده تا متجاوز بتواند از طریق پروتکل به آن برسد، احتمال حدس‌زدن رمز عبور قابل‌چشم‌پوشی است و متجاوز از حدس زدن رمز عبور صحیح بازمی‌ماند.

۳. **حمله انعکاسی:** یک موجودیت متقلب را در نظر بگیرید که تلاش می‌کند D_1 را به جای D_2 جا بزند. مثالی از حمله انعکاسی بر یک پروتکل ساده مطابق زیر است:

$$1: iD_1 \rightarrow D_2 : D_1, ND_1 \quad (12)$$

$$2: D_2 \rightarrow iD_1 : D_2, ND_2, \{ND_1\}K_{I2} \quad (13)$$

در این مرحله، متجاوز گیر افتاده است؛ چون نمی‌تواند ND_2 را برای ارسال به D_2 رمزگذاری کند، اما متجاوز می‌تواند وهله دومی از پروتکل را آغاز کند و D_2 را وادار سازد تا ND_2 را رمزگذاری کند.

$$3: iD_1 \rightarrow D_2 : D_1, ND_2 \quad (14)$$

$$4: D_2 \rightarrow iD_1 : D_2, ND_2, \{ND_2\}K_{I2} \quad (15)$$

متجاوز وهله دوم را رها می‌کند و وهله نخست را ادامه می‌دهد.

$$5: iD_1 \rightarrow D_2 : \{ND_2\}K_{I2} \quad (16)$$

حمله انعکاسی بر روی این پروتکل ممکن است؛ زیرا آغازکننده نیازی ندارد هویت خود را اثبات کند و

شکل‌های (۷ و ۸) تأیید می‌کنند که پروتکل پیشنهادی تحت هر دو ابزار ایمن شناخته شده‌اند. نتایج شبیه‌سازی AVISPA تضمین می‌کنند که طرح پیشنهادی در مقابل حملاتی از جمله حملات بازپخش و مردِ میانی ایمن است. این نشان می‌دهد که هیچ حمله‌ای متوجه شناسایی و محرمانه‌بودن پروتکل نیست. شناسایی طرف‌های دخیل با تبادل شماره‌های تصادفی متناظر ایجادشده توسط آنها انجام می‌شود. هیچ حمله‌ای به کلید نشست توسط متجاوز یافت نشد. همچنین محرمانه‌بودن کلید نشست و پیام‌های انتقال‌یافته بین طرف‌ها حفظ شده است. از طرف دیگر تابع درهم‌ساز در مدل‌سازی پروتکل باعث حفظ جامعیت نیز شده است. از آنجایی که ابزار AVISPA انواع حملات را بررسی می‌کند و اطلاعاتی در مورد حمله احتمالی اعلام نکرده است؛ لذا می‌توان گفت پروتکل امن است. باتوجه به ارزیابی‌های انجام‌شده به‌وسیله ابزار AVISPA، جدول (۵) امنیت روش پیشنهادی را در مقایسه با کارهای پیشین نمایش می‌دهد.

SUMMARY

SAFE

DETAILS

BOUNDERD_NUMBER_OF_SESSIONS

TIME_MODEL

PROTOCOL

Home / span / span / testsuite / results / htpsIGenFile .

if

GOAL

As_Specified

BACKEND

Cl-AtSe

STATISTICS

Analysed : 22 states

Reachable : 8 states

Translation : 0.01 seconds

(شکل-۷): آزمون تست پروتکل پیشنهادی با ابزار CL-AtSe

(Figure-7): Protocol verication with CL-AtSe.

% OFMC

% Version of 2006/02/13

SUMMAER

SAFE

DETAILS

BOUNDED_NUMBER_OF_SESSIONSPROTOCOL

/home / span / span / testsuite / results / htpsIGenFile .

if

GOAL

as specified

BACKEND

OFMC

COMMENTS

STATISTICS

parseTime: 0.00s

searchTime: 0.02s

visitNodes: 11 nodes

(شکل-۸): آزمون تست پروتکل پیشنهادی توسط

ابزار OFMC

(Figure-8): Protocol verication with OFMC

$$M2: D_1 \rightarrow D_2: \{N_4, D_2\}K_{u1}^J \quad (20)$$

پیغام ۱ در پروتکل ایجاد شده به طور دقیق قالب مشابه گام ۱ در پروتکل پیشنهادی است. حمله کننده از پیغام های پروتکل های مختلف به منظور حمله به پروتکل شناسایی استفاده می کند که به صورت زیر است:

$$\text{Step 1: } iD_1 \rightarrow D_2 : \{ \{K_{uG}, K_{12}\}K_{u2}^J, \{N_3\}K_{12}, H_1(K_{12}, T_c)\}K_{u2} \quad (21)$$

$$\text{Step 2: } D_2 \rightarrow iD_1 : \{ \{N_3, N_4\}K_{u1}, T_c\}K_{12} \quad (22)$$

$$M1: iD_2 \rightarrow D_1: \{ \{M, N_4\}K_{u1}, T_c\}K_{12} \quad (23)$$

$$M2: D_1 \rightarrow iD_2: \{N_4, D_2\}K_{u1}^J \quad (24)$$

حمله به صورت زیر ادامه می یابد:

۱. متجاوز iD_1 با تغییر شکل به D_1 پیامی را در گام ۱ به D_2 می فرستد. پروتکل ایجاد شده به N_3 و M برای داشتن قالب مشابه نیاز دارد.

۲. متجاوز پیغام پاسخ را در گام ۲ از D_2 دریافت می کند.

۳. متجاوز با تغییر شکل به D_2 ، این پیغام را به عنوان پیغام ۱ به D_1 ارسال می کند.

۴. D_1 به پیغام ۲ از پروتکل ایجاد شده پاسخ می دهد، که این پاسخ شامل یک رونوشت عمومی از شماره تصادفی N_4 است.

۵. متجاوز این مقدار N_4 را برای ارسال آن به D_2 به منظور شناساندن خود دریافت می کند.

گیرنده هر پیامی را که دریافت می کند، بدون تأیید هویت صادرکننده آن رمزگذاری و رمزگشایی می کند.

پروتکل پیشنهادی در این مورد از حمله انعکاسی جلوگیری می کند. تلاش برای حمله به صورت زیر است:

$$1: iD_1 \rightarrow D_2 : \{ \{K_{uG}, K_{12}\}K_{u2}^J, \{N_3\}K_{12}, H_1(K_{12}, T_c)\}K_{u2} \quad (17)$$

$$2: D_2 \rightarrow iD_1 : \{ \{N_3, N_4\}K_{u1}, T_c\}K_{12} \quad (18)$$

حتی اگر متجاوز تلاش کند تا وهله دوم پروتکل پیشنهادی را اجرا کند، حمله به دو دلیل صورت نمی گیرد:

۱. متجاوز نمی تواند هیچ گونه اطلاعاتی را در مورد شماره تصادفی N_4 از گام ۲ دریافت کند. علت آن است که پیام ارسال شده توسط D_2 در گام ۲ طوری است که شماره های تصادفی می تواند تنها توسط D_1 رمزگشایی شوند.

۲. ماهیت چالش های ایجاد شده توسط D_1 و D_2 به واسطه وجود اطلاعات مختلف در پیام رمز شده و ارسال شده بین دو موجودیت متفاوت است. این امر تضمین می کند که ارسال کورکورانه یک پیام از نقطه دیگر به متجاوز اجازه شناساندن خود را نمی دهد.

۴. **حمله چند پروتکلی:** حمله ای ضد پروتکل شناسایی با استفاده از پیغام های ایجاد شده از طرف یک پروتکل مجزا به منظور منحرف ساختن هر دو طرف. پروتکل زیر را در نظر بگیرید:

$$M1: D_2 \rightarrow D_1: \{ \{M, N_4\}K_{u1}, T_c\}K_{12} \quad (19)$$

(جدول-۵): مقایسه امنیتی روش پیشنهادی نسبت به کارهای پیشین

(Table-5): Security comparison of the proposed method

پروتکل پیشنهادی	[3]	[18]	[23]	[19]	[8]	[21]	[7]	[6]	[20]	[5]	[17]	
*	*			*	*	*	*	*	*	*	*	مرد میانی
												زمان سنجی
									*			عامل داخلی
	*			*				*	*			جعل هویت
*	*			*		*	*	*	*		*	بازپخش
*			*					*	*	*		تعویض / حدس رمز عبور
*					*	*		*				جعل
						*	*					شنود
*		*										منع سرویس
*									*	*		کارت هوشمند دزدیده شده
									*	*		جدول رنگین کمائی
									*	*		جستجوی فراگیر

این حمله ناموفق است؛ زیرا اگرچه متجاوز قادر به وادار کردن D_1 به رمز گشایی N_4 از گام ۲ و ارسال آن به یک متجاوز در قالبی قابل خواندن توسط آن است، اما نمی تواند آن را با همان قالب مورد انتظار D_2 رمزگذاری و به D_2 ارسال کند. علت این است که پیغام در گام ۳ توسط K_{12} رمزگذاری می شود که برای متجاوز نا آشناست. بنابراین، تلاش های متجاوز برای شناساندن خود بدون آگاهی موجودیت میزبان بیهوده است.

۴-۴- نتایج ارزیابی

جامعیت

جامعیت به این معناست که اطلاعات توسط یک متجاوز/موجودیت/ فرایند در طول ارتباط بین موجودیت های شناخته شده به شیوه ای نامعمول تغییر نیافته و یا از بین نرفته اند. علاوه بر استفاده از کلید نشست به منظور تضمین جامعیت، درهم سازی داده ها توسط فرستنده صورت می گیرد.

محرمانگی

این ویژگی تضمین می کند که اطلاعات قابل کشف نیستند و در اختیار موجودیت دیگری قرار نمی گیرند. پروتکل این امر را با رمزگذاری مقادیر تصادفی یک بار مصرف انجام می دهد، طوری که تنها دریافت کننده مورد نظر می تواند پیام را رمزگشایی کند. کلید مشترک K_{12} نیز بین دو طرف ارتباط محرمانه باقی می ماند.

تأیید

تأیید، فرایند اعتبارسنجی هویت دستگاه به وسیله دیگر دستگاه های در ارتباط و تضمین اعتماد پذیری مبدأ ارتباط و اطمینان از ارتباط با یک طرف مطلوب است. تأیید دوطرفه به واسطه کلید نشست مشترک ایجاد شده به وسیله دروازه انجام می شود و این کلید بین دو دستگاه مورد نظر یعنی D_1 و D_2 محرمانه می ماند. D_1 و D_2 خود را به واسطه تبادل شماره های تصادفی N_3 و N_4 به یکدیگر می شناسانند. استفاده از کلید نشست محرمانه به منظور رمزگشایی پیام ها تضمین می کند که داده ها نمی توانند توسط یک عامل واسطه دست کاری شوند.

۵-۴- محدودیت ها

در ادامه محدودیت هایی با توجه به پژوهش های انجام گرفته در اینترنت اشیا بر روی کنترل دسترسی و احراز هویت خلاصه شده است:

۱. فقدان یک معماری کامل برای کنترل دسترسی مانند AAA (احراز هویت، بررسی مجوز، و حسابرسی) در سناریوهای اینترنت اشیا برای سیستم های M2M.

۲. نیاز است که مسائل قابلیت همکاری در روش های کنترل دسترسی برای شبکه ها/ وسایل ناهمگن در سناریوهای اینترنت اشیا مورد بررسی قرار گیرند.

۳. در سال های اخیر، روش های جالب زیادی برای احراز هویت غیر مبتنی بر گواهی نامه ارائه شده است. ولی همچنان روش های احراز هویت دیگری برای محیط های محاسباتی معمولی وجود دارند که نیاز است تا در محیط هایی با احراز هویت ناشناس مانند اینترنت اشیا آزمایش و پیاده سازی شوند.

۵- نتیجه گیری و کارهای آینده

در این مقاله یک الگوریتم احراز هویت دوطرفه دستگاه به دستگاه در اینترنت اشیا ارائه شد که قابلیت استفاده شدن به وسیله دستگاه های مختلف در شبکه IoT را دارد و برای استفاده شبکه هوشمند خانگی ساده سازی شده است. پروتکل پیشنهادی، انتقال داده امن بین نهادهای ارتباطی را با استفاده از اصول رمزنگاری تضمین می کند. در ابتدا پروتکل با نشان گذاری A-B برنامه نویسی و یک شبیه ساز پروتکل نیز پروتکل را به طور دقیق به همان صورتی که در ابزار AVISPA برنامه نویسی شد، شبیه سازی کرد؛ سپس یک اعتبارسنجی از پروتکل، با استفاده از ابزارهای OFMC و CL-AtSe به همراه تحلیل نظری انجام شد. نتایج بررسی نشان داد که پروتکل پیشنهادی امن است.

جنبه های متفاوتی برای ادامه کار در آینده می توان پیشنهاد کرد که از جمله به موارد زیر می توان اشاره کرد:

۱. گسترش پروتکل برای مواردی که دستگاه IoT یک شبکه خانگی مشخص را ترک کرده و به شبکه دیگری می پیوندد.

۲. در نظر گرفتن احتمال متفاوت بودن پروتکل ارتباطی شبکه های خانگی دو دستگاه IoT.

6- References

۶- مراجع

- [1] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) Authentication schemes," *Sensors*, vol. 19, pp. 1141, 2019.
- [2] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and

- challenges for enterprises," *Business Horizons*, vol. 58, pp. 431-440, 2015.
- [14] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721-82743, 2019.
- [15] N. Moustafa, "A Systemic IoT-Fog-Cloud Architecture for Big-Data Analytics and Cyber Security Systems: A Review of Fog Computing," *arXiv preprint arXiv:1906.01055*, 2019.
- [16] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.
- [17] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," in *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, 2015, pp. 1-6.
- [18] W.-T. Su, W.-M. Wong, and W.-C. Chen, "A survey of performance improvement by group-based authentication in IoT," in *2016 International Conference on Applied System Innovation (ICASI)*, 2016, pp. 1-4.
- [19] F. Chu, R. Zhang, R. Ni, and W. Dai, "An improved identity authentication scheme for internet of things in heterogeneous networking environments," in *2013 16th International Conference on Network-Based Information Systems*, 2013, pp. 589-593.
- [20] X. Yao, X. Han, X. Du, and X. Zhou, "A lightweight multicast authentication mechanism for small scale IoT applications," *IEEE Sensors Journal*, vol. 13, pp. 3693-3701, 2013.
- [21] N. Shone, C. Dobbins, W. Hurst, and Q. Shi, "Digital memories based mobile user authentication for IoT," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1796-1802.
- [22] H. Tschofenig, "Fixing user authentication for the internet of things (iot)," *Datenschutz und Datensicherheit-DuD*, vol. 40, pp. 222-224, 2016.
- [23] L. Takkinen, "Analysing security protocols with AVISPA," in *TKK T-110.7290 research seminar on network security*, 2006.
- [24] S. Emerson, Y.-K. Choi, D.-Y. Hwang, K.-S. Kim, and K.-H. Kim, "An OAuth based authentication mechanism for IoT networks," outlook," *Journal of Systems Architecture*, vol. 97, pp. 185-196, 2019.
- [3] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: A survey," in *2016 cybersecurity and cyberforensics conference (CCC)*, 2016, pp. 28-34.
- [4] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210-223, 2015.
- [5] M. A. Crossman and H. Liu, "Study of authentication with IoT testbed," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2015, pp. 1-7.
- [6] H. Ren, Y. Song, S. Yang, and F. Situ, "Secure smart home: A voiceprint and internet based authentication system for remote accessing," in *2016 11th International Conference on Computer Science & Education (ICCSE)*, 2016, pp. 247-251.
- [7] A. Ukil, S. Bandyopadhyay, A. Bhattacharyya, and A. Pal, "Lightweight security scheme for vehicle tracking system using CoAP," in *Proceedings of the International Workshop on Adaptive Security*, 2013, pp. 1-8.
- [8] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, "An authentication model for IoT clouds," in *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2015, pp. 1032-1035.
- [9] S. Janbabaei, H. Gharaee, and N. Mohammadzadeh, "The Lightweight Authentication Scheme with Capabilities of Anonymity and Trust in Internet of Things (IoT)," *Signal and Data Processing*, vol. 15, no. 4, pp. 111-122, 2019.
- [10] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019: IEEE, pp. 1-4.
- [11] K. Park et al., "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification Table in Medical Internet of Things," *IEEE Access*, vol. 8, pp. 119387-119404, 2020.
- [12] V. Plantevin, A. Bouzouane, B. Bouchard, and S. Gaboury, "Towards a more reliable and scalable architecture for smart home environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 2645-2656, 2019.
- [13] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and



پیام محمودی نصر تحصیلات خود را

در مقاطع کارشناسی و کارشناسی ارشد

مهندسی رایانه به ترتیب در سال‌های

۱۳۷۳ و ۱۳۷۵ از دانشگاه صنعتی

امیرکبیر و در مقطع دکترای مهندسی

قدرت در سال ۱۳۹۵ از دانشگاه تربیت مدرس به پایان

رسانده و هم‌اکنون استادیار دانشکده مهندسی و فناوری

دانشگاه مازندران است. زمینه‌های پژوهشی موردعلاقه

ایشان عبارت‌اند از: امنیت شبکه‌های صنعتی و رایانه‌ای،

امنیت داده‌ها و شبکه‌های رایانه‌ای.

نشانی رایانامه ایشان عبارت است از:

P.mahmoudi@umz.ac.ir



حسین کیمیا متولد ۱۳۶۶ تحصیلات

خود را در مقطع کارشناسی مهندسی

کامپیوتر - نرم‌افزار در سال ۱۳۹۰ از

دانشگاه غیردولتی شما آمل و در مقطع

کارشناسی ارشد فناوری اطلاعات گرایش

شبکه‌های رایانه‌ای در سال ۱۳۹۸ از مؤسسه غیردولتی

صنعتی مازندران به پایان رسانده است. زمینه‌های

موردعلاقه ایشان امنیت شبکه‌های رایانه‌ای است.

نشانی رایانامه ایشان عبارت است از:

hosseinkimia@gmail.com