APJ 6 (4):66-75, Winter 2025

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Security Enhancement Solution in Home Networks, based on the Internet of Things

H. Ganjkhanloo [1]

[1] *Department of Computer Engineering, Khod.C., Islamic Azad University, Khodabandeh , Iran*

ABSTRACT

RESEARCH PAPER

The explosive growth of Internet of Things (IoT) devices in home environments, coupled with the inherent limitations of these devices in terms of computing power, memory, and energy consumption, has increased the level of cyberattacks to an unprecedented level. Traditional home networks lack adequate security mechanisms to deal with emerging IoT-specific threats. This paper presents a comprehensive and multi-layered solution to enhance security in IoT-based home networks. The proposed approach, titled "SecHome-IoT", is composed of three main layers: (1) a deep learning-based anomaly detection layer (automated preprocessing and 1D convolutional neural network with long-term short-term memory), (2) a secure virtualization layer based on lightweight microservices (using hardware containers and critical path isolation), and (3) Dynamic and adaptive policy management layer (using adaptive-neural fuzzy inference system). Best hardware-software simulation on real-world datasets CICIDS2017, Bot-IoT and UNSW-NB15 along with implementation on Raspberry Pi platform and OpenWrt smart switches shows that the proposed method is superior to the previous ones (such as IoT-IDSA and Deep-STM) with an attack detection rate of 98.6% and a false positive rate of 1.4%. It has an improvement of 25% in security and performance metrics. This paper provides a roadmap for the security of IoT home networks by providing a comprehensive threat analysis, real-world and similar implementations.

Received: 2025-7-13
Accepted: 2025-11-2

KEYWORDS:
Home Network Security,
Internet of Things,
Intrusion Detection,
Network Isolation,

[1] Corresponding author:
hn.ganjkhanloo@gmail.com

نشریه تخصصی آرمان پردازش، دوره ۶، شماره ۴، سال ۱۴۰۴

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

راهکار افزایش امنیت در شبکه‌های خانگی مبتنی بر اینترنت اشیا

حسین گنج‌خانلو

گروه مهندسی برق و کامپیوتر ، واحد خدابنده، دانشگاه آزاد اسلامی، خدابنده، ایران

چکیده

مقاله پژوهشی

رشد انفجاری دستگاه‌های اینترنت اشیا (IoT) در محیط‌های خانگی، همراه با محدودیت‌های ذاتی این دستگاه‌ها از نظر توان محاسباتی، حافظه و مصرف انرژی، سطح حملات سایبری را به طور بی‌سابقه‌ای افزایش داده است. شبکه‌های خانگی سنتی فاقد مکانیسم‌های امنیتی مناسب برای مقابله با تهدیدات نوظهور اختصاصی IoT هستند. این مقاله یک راهکار جامع و چندلایه برای افزایش امنیت در شبکه‌های خانگی مبتنی بر IoT ارائه می‌دهد. رویکرد پیشنهادی با عنوان "SecHome-IoT" از ترکیب سه لایه اصلی تشکیل شده است: اول لایه تشخیص ناهنجاری مبتنی بر یادگیری عمیق (پیش‌پردازش خودکار و شبکه عصبی کانولوشن یک‌بعدی به همراه حافظه کوتاه‌مدت طویل‌مدت)، دوم لایه مجازی‌سازی امن مبتنی بر میکروسرویس‌های سبک (با استفاده از کانتینرهای سخت‌افزاری و جداسازی مسیر بحرانی) و سومین لایه مدیریت خط‌مشی پویا و تطبیقی (با استفاده از سیستم استنتاج فازی تطبیقی-عصبی) انجام می‌دهد. ارزیابی سخت‌افزاری-نرم‌افزاری بر روی مجموعه داده‌های واقعی CICIDS2017 ، Bot-IoT و UNSW-NB15 به همراه پیاده‌سازی بر روی پلتفرم Raspberry Pi و سوییچ‌های هوشمند OpenWrt نشان می‌دهد که روش پیشنهادی با نرخ تشخیص حمله ۹۸,۷٪، نرخ هشدار اشتباه ۱,۴٪، و تأخیر پردازش میانگین ۴۲,۶ میلی‌ثانیه نسبت به بهترین روش‌های پیشین مانند IoT-IDSA و Deep-STM بهبودی بین ۱۲ تا ۲۵ درصدی در معیارهای امنیتی و کارایی دارد. این مقاله با ارائه تحلیل جامع تهدیدها، پیاده‌سازی واقعی و مقایسه کمی گسترده، نقشه راهی عملی برای تأمین امنیت شبکه‌های خانگی IoT فراهم می‌آورد.

واژگان کلیدی:

امنیت شبکه خانگی،
اینترنت اشیا،
تشخیص نفوذ،
یادگیری عمیق،
جداسازی شبکه،

مقدمه

انقلاب صنعتی چهارم و گسترش همه‌گیر اینترنت پُرشتاب، مفهوم "خانه هوشمند" را از یک رویای علمی-تخیلی به واقعیتی روزمره تبدیل کرده است. اینترنت اشیا به عنوان ستون فناورانه خانه‌های هوشمند، امکان اتصال ده‌ها تا صدها دستگاه (از جمله دوربین‌های مداربسته، قفل‌های هوشمند، دستیارهای صوتی، لوازم خانگی، سنسورهای دما و رطوبت، روشنایی هوشمند و کنتورهای هوشمند انرژی) را به شبکه خانگی و متعاقباً به اینترنت فراهم می‌آورد [۱, ۲]. بر اساس گزارش‌های معتبر، تعداد دستگاه‌های IoT فعال در سراسر جهان تا پایان سال ۲۰۲۵ از مرز ۳۰ میلیارد عبور کرده است که بیش از ۴۰ درصد آن‌ها در بخش مسکونی (شبکه‌های خانگی) مستقر هستند [۳].

با این حال، این رشد شتابان همراه با یک حقیقت تلخ است :اکثر دستگاه‌های IoT مصرفی با حداقل ملاحظات امنیتی طراحی و تولید می‌شوند [۴و۵]. محدودیت‌های ذاتی این دستگاه‌ها از جمله حافظه محدود (اغلب کمتر از ۵۱۲ کیلوبایت رم)، پردازنده‌های کُند (کمتر از ۲۰۰ مگاهرتز)، مصرف انرژی بسیار پایین (اغلب باتری‌خور) و عدم قابلیت به‌روزرسانی امنیتی منظم، پیاده‌سازی مکانیسم‌های امنیتی پیشرفته روی خود دستگاه را غیرممکن یا حداقل بسیار چالش‌برانگیز می‌سازد [۶, ۷]. این محدودیت‌ها در کنار تنوع فوق‌العاده بالا در پروتکل‌های ارتباطی(MQTT ، CoAP، AMQP، HTTPو پروتکل‌های اختصاصی) و معماری‌های ناهمگن، شبکه خانگی را به محیطی بسیار جذاب برای مهاجمان سایبری تبدیل کرده است [۸]. شبکه‌های خانگی مبتنی بر IoT با طیف گسترده‌ای از تهدیدات امنیتی روبرو هستند که برخی از مهمترین آن‌ها عبارتند از:

– **تهدیدات لایه فیزیکی و دسترسی :** مهاجم با دسترسی فیزیکی به دستگاه مثلاً از طریق پورت USB یا JTAG می‌تواند میان‌افزار دستگاه را استخراج، تحلیل معکوس کرده و بدافزار تزریق کند [۹]. همچنین حمله کلونینگ (Cloning) دستگاه‌های IoT ارزان‌قیمت به منظور دور زدن احراز هویت مبتنی بر MAC address امکان‌پذیر است.

– **تهدیدات لایه شبکه :** حملات متداول لایه شبکه در IoT خانگی شامل حمله مرد میانی با جعل گیت‌وے پیش‌فرض، حمله انکار سرویس (DDoS) با استفاده از بات‌نت‌های متشکل از دستگاه‌های IoT آلوده)مانند Mirai و انواع تکامل‌یافته آن، حمله بازپخش برای تکرار فرمان‌های معتبر (مثلاً باز کردن قفل هوشمند) و حمله تکه‌تکه شدن پروتکل ۶ LoWPANبرای سرریز بافر و اختلال در عملکرد [۱۰و۱۱].

– **تهدیدات لایه برنامه کاربردی :** از آنجا که بسیاری از دستگاه‌های IoTاز پروتکل MQTT بدون رمزنگاری یا با رمزنگاری ضعیف استفاده می‌کنند، مهاجم می‌تواند با اشتراک در توپیک‌های عمومی تمام ترافیک را شنود کند. همچنین حملات تزریق پیام و فرمان‌های مخرب از طریق واسط‌های ابری ضعیف امنیت‌شده بسیار رایج است [۱۲].

– **تهدیدات نرم‌افزاری و میان‌افزاری :** آسیب‌پذیری‌های شناخته‌شده در کتابخانه‌های شخص ثالث و عدم به‌روزرسانی خودکار میان‌افزار، دستگاه‌های IoT را در معرض بهره‌برداری از آسیب‌پذیری‌های روز صفر قرار می‌دهد [۱۳]. همچنین بسیاری از دستگاه‌ها دارای رمزهای عبور پیش‌فرض بدون تغییر مانند admin/admin یا root/123456 هستند که مهاجم به راحتی می‌تواند از طریق اسکن اینترنتی) مثلاً با Shodan آن‌ها را شناسایی و کنترل کند.

– **چالش‌های خاص شبکه خانگی :** فراتر از تهدیدات فنی، چالش‌های زیر نیز وجود دارند:

– **عدم وجود مدیر امنیتی حرفه‌ای :** بر خلاف شبکه‌های سازمانی، در خانه‌ها کاربران عادی (اغلب بدون دانش فنی) مسئول تأمین امنیت هستند.

– **ماهیت پویا و موقتی دستگاه‌ها :** دستگاه‌های IoT در شبکه خانگی دائماً اضافه، حذف و جابجا می‌شوند که پیکربندی دستی خط‌مشی‌های امنیتی را عملاً غیرممکن می‌سازد.

– **محدودیت هزینه :** راهکارهای امنیتی پیشرفته سازمانی از نظر اقتصادی و پیچیدگی برای شبکه خانگی قابل قبول نیستند.

– **مسائل حریم خصوصی :** ترافیک شبکه خانگی حاوی داده‌های حساس است که هر راهکار باید حریم خصوصی را حفظ کند [۱۴].

جدول ۱: دسته‌بندی حملات رایج در شبکه‌های خانگی IoT و شدت تأثیر آن‌ها

دسته حمله	نمونه حمله	لایه هدف	قابلیت تشخیص توسط راهکارهای سنتی	شدت تأثیر(۵-۱)
مخرب شبکه	DDoS (Mirai)	شبکه	متوسط	۵
نفوذ به دستگاه	آپلود میان‌افزار مخرب	فیزیکی/برنامه	ضعیف	۵
شناسایی و اسکن	پورت اسکن گسترده	شبکه	خوب	۲
بدافزار باج‌افزار	رمزگذاری فایل‌هایNAS	برنامه	ضعیف	۴
مرد میانی	ARP Spoofing + SSL Strip	شبکه	متوسط) نیازمند(TLS	۴
احراز هویت	حدس رمز(Credential Stuffing)	برنامه	متوسط	۳
نشت اطلاعات	اکسترود کردن ویدئوی دوربین	برنامه/شبکه	ضعیف	۵

شکاف تحقیقاتی و سوالات اصلی

علیرغم تحقیقات گسترده در زمینه امنیتIoT ، تمرکز عمده پژوهش‌ها بر روی شبکه‌های صنعتی(IIoT) ، شهرهای هوشمند یا شبکه‌های حسگر بی‌سیم (WSN) بوده است و شبکه‌های خانگی به عنوان محیطی منحصربه‌فرد با محدودیت‌های خاص خود کمتر مورد توجه قرار گرفته است [۱۵]. راهکارهای موجود عمدتاً از سه دسته هستند: اول اهکارهای مبتنی بر رمزنگاری سبک که روی خود دستگاه اجرا می‌شوند اما با سخت‌افزار ضعیف برخی دستگاه‌ها ناسازگارند، دوم راهکارهای مبتنی بر فایروال و جداسازی که نیازمند پیکربندی دستی و حرفه‌ای هستند و (۳) راهکارهای مبتنی بر تشخیص نفوذ مرکزی که با چالش تأخیر و نرخ هشدار اشتباه بالا مواجه‌اند [۱۶].

این مقاله به دنبال پاسخ به سه سؤال تحقیقاتی اصلی است:

- چگونه می‌توان یک سامانه تشخیص نفوذ با دقت بالا و تأخیر کم برای ترافیک ناهمگن IoT در شبکه خانگی طراحی کرد که قادر به شناسایی حملات روز صفر و نیز حملات رمزنگاری‌شده باشد؟
- چگونه می‌توان با ترکیب مجازی‌سازی سبک و مدیریت پویای خط‌مشی، جداسازی مؤثر دستگاه‌های IoT با حداقل مداخله کاربر عادی ایجاد کرد؟
- آیا ترکیب یادگیری عمیق با سیستم فازی تطبیقی (ANFIS) و جداسازی میکروسرویس می‌تواند ضمن حفظ حریم خصوصی، امنیت شبکه خانگی را به سطح قابل قبولی برساند؟

در ادامه ادبیات پژوهش و تحقیقات مرتبط را بررسی خواهیم نمود.

تحقیقات مرتبط

پژوهش‌های پیشین در زمینه امنیت شبکه‌های خانگی IoT را می‌توان در چهار دسته کلی تقسیم‌بندی کرد:

دسته اول: راهکارهای مبتنی بر رمزنگاری سبک و احراز هویت : این دسته بر روی طراحی پروتکل‌های رمزنگاری با نیاز پردازشی پایین مانندPRESENT ، SPECK، SIMON و ASCON و پروتکل‌های احراز هویت کارا مانند DTLS با پروفایل‌های IoT متمرکز هستند [۱۹-۱۷]. اگرچه این روش‌ها امنیت انتها به انتها را افزایش می‌دهند، اما اجرای آن‌ها بر روی دستگاه‌های بسیار ضعیف (مثلاً حسگرهای دما با مانند ۸ بیتی) عملاً غیرممکن است. همچنین این روش‌ها در برابر حملات سمت سرور ابری و حملات لایه دوم شبکه مثلاً حملات ARP ناتوان هستند.

دسته دوم: راهکارهای مبتنی بر فایروال و جداسازی شبکه : استفاده ازVLAN های مبتنی بر پورت سوییچ و قوانین ACL (Access Control List)برای جداسازی دستگاه‌های IoT از شبکه اصلی و از یکدیگر [۲۱,۲۰]. نقاط قوت این روش سادگی و کارایی بالا است، اما نقاط ضعف آن عبارتند از :نیاز به سخت‌افزار شبکه هوشمند (سوییچ لایه ۳) که در اکثر شبکه‌های خانگی وجود ندارد، عدم پویایی و پاسخ به تهدیدات لحظه‌ای و ناتوانی در مسدودسازی حملاتی که از طریق کانال‌های مجاز اتفاق می‌افتند مثلاً دستگاه آلوده به باتنت.

دسته سوم: راهکارهای مبتنی بر تشخیص ناهنجاری با یادگیری ماشین :پرکاربردترین رویکرد در پژوهش‌های اخیر که از الگوریتم‌های مختلف یادگیری نظارت‌شده مانندRandom Forest ، XGBoost، SVM، بدون نظارت (مانند خوشه‌بندی خودسازمانده) و نیمه‌نظارت‌شده برای مدلسازی ترافیک نرمال و تشخیص انحراف استفاده می‌کنند [۲۵-۲۲]. مطالعات جامع نشان می‌دهد که روش‌های مبتنی بر جنگل تصادفی و بوستینگ روی مجموعه داده‌های استاندارد IoT دقت بالای ۹۵٪ قابل دستیابی هستند. با این حال چالش اصلی این روش‌ها، نرخ مثبت کاذب بالا در محیط‌های پویا و ناهمگن (به دلیل تغییر رفتار کاربران و دستگاه‌ها) و همچنین عدم توانایی در تشخیص حملات بسیار کند است.

دسته چهارم: راهکارهای مبتنی بر یادگیری عمیق : استفاده از شبکه‌های عصبی عمیق از جملهCNN ، RNN، LSTM، GRUو ترکیب آن‌ها برای استخراج خودکار ویژگی از ترافیک خام و یادگیری الگوهای زمانی-مکانی پیچیده [۲۹-۲۶]. نتایج این روش‌ها بر روی مجموعه داده‌های جدیدی مانند Bot-IoT و CSE-CIC-IDS2018 نشان‌دهنده دقت بالای ۹۷-۹۹٪ است، اما چالش‌های اصلی آن شامل نیاز به توان محاسباتی بالا برای آموزش (مناسب نبودن برای اجرای روی روتر خانگی ضعیف) و تأخیر بالا در استنتاج در زمان واقعی است. همچنین این روش‌ها به حجم زیادی داده برچسب‌گذاری‌شده نیاز دارند که در عمل تأمین آن دشوار است.

۲,۲ .تحلیل شکاف‌های تحقیقاتی و جدول مقایسه

بررسی عمیق تحقیقات مرتبط نشان می‌دهد که علیرغم پیشرفت‌های قابل توجه، شکاف‌های زیر همچنان پابرجا هستند:

عدم ارائه راهکار یکپارچه و چندلایه : اکثر پژوهش‌ها تنها بر یک جنبه امنیتی (مثلاً تشخیص نفوذ یا جداسازی شبکه) تمرکز کرده‌اند و راهکاری که تشخیص ناهنجاری، جداسازی پاسخ تطبیقی و مدیریت متمرکز را در یک بسته یکپارچه ارائه دهد، وجود ندارد.

مقیاس‌پذیری و محدودیت سخت‌افزاری : دقت بالای مدل‌های عمیق با تأخیر و مصرف حافظه بالا همراه است که اغلب با توان پردازشی روترهای خانگی(معمولاً ARM Cortex-A با ۵۱۲ مگابایت رم) سازگار نیست.

عدم ارزیابی عملی بر روی سخت‌افزار واقعی : بسیاری از مقالات صرفاً ارزیابی شبیه‌سازی یا مبتنی بر مجموعه داده‌های قدیمی انجام داده‌اند و اثربخشی روش خود را در یک شبکه خانگی واقعی با تداخل ترافیک مثل استریم ویدئو، بازی آنلاین و تماس نشان نداده‌اند.

ضعف در تشخیص حملات رمزنگاری‌شده : با گسترش استفاده از TLSدر IoT (حتی نسخه‌های ضعیف)، اکثر روش‌های تشخیص ناهنجاری مبتنی بر محتوای بسته به دلیل رمز بودن ترافیک کارایی خود

را از دست می‌دهند. روش‌های مبتنی فقط بر ویژگی‌های جریان نیز از دقت کمتری برخوردارند.

عدم تعبیه حریم خصوصی در طراحی : بسیاری از روش‌های تشخیص نفوذ برای دقت بیشتر نیاز به بازرسی عمیق بسته (DPI) دارند که با حریم خصوصی کاربران در شبکه خانگی در تعارض است.

جدول ۲: مقایسه تحقیقات مرتبط با رویکرد پیشنهادی(SecHome-IoT)

معیار / روش	IoT-IDSA [۲۲]	Deep-STM [۲۶]	LightSec [۱۸]	HomeGuard [۲۰]	رویکرد پیشنهادی
نوع رویکرد	تشخیص ناهنجاری (ML)	یادگیری عمیق (LSTM)	رمزنگاری سبک	جداسازیVLAN	یکپارچه (تشخیص + جداسازی + پاسخ)
لایه‌های امنیتی	۱ لایه (تشخیص)	۱ لایه (تشخیص)	۱ لایه (رمز)	۱ لایه (فایروال)	۳ لایه (DL + ANFIS) مجازی‌سازی +
حالت اجرا	مبتنی بر سرور ابری	روی گیت‌وے لبه	روی دستگاه IoT	روی سوییچ مرکزی	روی گیت‌وے خانگی (محلی)
نیاز به اینترنت	بله (اتصال ابر)	خیر	خیر	خیر	خیر (مستقل)
تشخیص حملات رمز	متوسط	خوب	نه	نه	خوب (ویژگی‌های آماری جریان)
نرخ تشخیص(DR)	٪۹۴,۲	٪۹۶,۸	N/A	N/A	٪۹۸,۷
نرخ هشدار اشتباه (FAR)	٪۴,۷	٪۳,۲	N/A	N/A	٪۱,۴
تأخیر پردازش (میلی‌ثانیه)	~۱۸۵ ارسال به ابر	~۶۸	<۱	~۵ فقط فیلتر	۴۲,۶
مصرف رم میانی (مگابایت)	نامشخص	~۴۲۰ بدون بهینه‌سازی	<۱	~۳۲	۱۶۸
مدیریت پویای خط‌مشی	خیر	خیر	خیر	خیر	بله(ANFIS)
ارزیابی سخت‌افزاری واقعی	خیر (شبیه‌سازی)	خیر	بله (ESP32)	بله (Raspberry Pi)	بله

در جدول ۲،روش‌های IoT-IDSA و Deep-STM علیرغم دقت قابل قبول، یا به ابر متکی هستند (که تأخیر بالا و قطعی اینترنت مشکل‌ساز است) یا نیاز به سخت‌افزار قدرتمند دارند. روش LightSec امنیت را به دستگاه IoTانتقال می‌دهد اما در برابر حملات شبکه ناتوان است HomeGuard . جداسازی خوبی ارائه می‌دهد اما فاقد تشخیص ناهنجاری پیشگیرانه است. رویکرد پیشنهادی با ترکیب سه لایه، دقت و تأخیر متوازن را با امکان اجرا روی سخت‌افزار خانگی معمولی ارائه می‌دهد.

راه‌حل پیشنهادی

در این بخش، جزئیات معماری پیشنهادی با عنوان SecHome-IoT (Secure Home IoT Architecture) ارائه می‌شود. این معماری بر اساس تحلیل شکاف‌های بخش قبل و با سه اصل کلیدی طراحی شده است : اول، چندلایگی و تدافعی عمیق، دوم، تعادل میان امنیت و سوم، خودمختاری و حداقل نیاز به کاربر.

معماری SecHome-IoT از سه لایه‌ی اصلی تشکیل شده است که به صورت هماهنگ عمل می‌کنند و دارای اجزاء و شرح وظایف زیر است:

– **لایه تشخیص ناهنجاری مبتنی بر یادگیری عمیق** : مسئولیت نظارت بر کل ترافیک شبکه خانگی، استخراج ویژگی‌های رفتاری (فقط ویژگی‌های جریان و آماری بدون نیاز به بازرسی محتوا) و تشخیص هرگونه الگوی غیرعادی و حمله را بر عهده دارد.

– **لایه مجازی‌سازی امن مبتنی بر میکروسرویس‌های سبک :** پس از تشخیص حمله یا به صورت پیشگیرانه، دستگاه‌های IoT را در کانتینرهای مجازی شبکه و میکروسرویس‌های امنیتی جداسازی می‌کند و مسیرهای بحرانی را ایزوله می‌نماید.

– **لایه مدیریت خط‌مشی پویا و تطبیقی :** با استفاده از سیستم استنتاج فازی-عصبی تطبیقی، با در نظر گرفتن چندین معیار (شامل سطح ریسک تشخیص‌داده‌شده، نوع دستگاه، بازه زمانی، و نرخ خطاهای

گذشته)، تصمیم‌گیری می‌کند که آیا یک اتصال را مسدود، محدود یا به مسیریاب مجازی هدایت کند.

جمع‌آوری و پیش‌پردازش داده

در این لایه، ترافیک ورودی/خروجی گیت‌وے خانگی (روتر) با استفاده از کتابخانه‌های DPDKو PF_RING به صورت صفر-کپی (Zero-copy) جمع‌آوری می‌شود تا تأخیر کاهش یابد. برای هر جریان (Flow) که با تپل ۵گانه (آدرس مبدأ، پورت مبدأ، آدرس مقصد، پورت مقصد، پروتکل) تعریف می‌شود، ویژگی‌های زیر در بازه زمانی ۵ ثانیه (پنجره اسلایدی) محاسبه می‌شوند:

- ویژگی‌های پایه :طول مدت جریان، تعداد بسته‌های رفت/برگشت، تعداد بایت رفت/برگشت، نرخ بسته در ثانیه.
- ویژگی‌های آماری پیشرفته :میانگین و انحراف معیار طول بسته‌ها، میانگین و واریانس فاصله بین بسته‌ها (Inter-arrival time)، درصد بسته‌های با علامت(FIN) TCP ، SYN، RST، PSH، ACK، URG).
- ویژگی‌های رفتاری دامنه (سطح جریان) :نسبت بایت به بسته، شاخص جریان‌شدگی(Flow duration entropy) ، تعداد جریان‌های همزمان از یک IP مبدأ به مقصدهای گوناگون.
- ویژگی‌های بدون محتوا :DNS برای ترافیک DNS (بدون رمزگشایی)، طول نام دامنه، تنوع کاراکترها، روزمرگی (Entropy)، نسبت اعداد به حروف و وقوع کلمات کلیدی مشکوک (مثل'update' ، 'cdn'، 'api' اما با رویکرد آماری) به عنوان ویژگی استفاده می‌شود – این کار به شناسایی کانال‌های فرماندهی و کنترل (C2) باتنت‌ها که از الگوریتم‌های تولید دامنه (DGAs) استفاده می‌کنند، کمک می‌کند.

مدل ترکیبی CNN-1D + LSTM با مکانیزم توجه

برای طبقه‌بندی جریان‌ها به دو دسته "عادی" و "ناهنجار" (و در نسخه پیشرفته، نوع حمله شامل DDoS ، Scan، MITM، Malwareو غیره)، یک معماری یادگیری عمیق سفارشی طراحی شده است:

لایه ورودی و نرمال‌سازی :۱۲۸ ویژگی استخراج‌شده) پس از کاهش ابعاد با PCA برای حفظ ۹۹٪ واریانس (وارد شبکه می‌شوند.

لایه تبدیل توالی :ابتدا با یک لایهReshape ، بردار ویژگی به توالی‌هایی به طول ۱۶ (۸ بلوک زمانی) تبدیل می‌شود.

لایه کانولوشن یک‌بعدی :(Conv1D) سه لایه کانولوشن موازی با اندازه هسته‌های ۳، ۵ و ۷ (برای استخراج الگوهای محلی در مقیاس‌های متفاوت) و هر کدام با ۶۴ فیلتر و فعال‌سازی ReLU و سپس MaxPooling.خروجی این لایه‌ها الحاق (Concatenate) می‌شود.

لایه LSTM دوطرفه :(BiLSTM) دو لایه LSTM دوطرفه با ۱۲۸ سلول حافظه و میزان Dropout 0.4 برای یادگیری وابستگی‌های طولانی‌مدت در ترافیک) مثلاً رفتار تدریجی حمله.(Low-and-Slow

مکانیزم توجه :(Attention) لایه توجه وزنی (Weighted Attentionکه به مدل اجازه می‌دهد بر مهم‌ترین بازه‌های زمانی (بازه‌هایی که حاوی رفتار حمله هستند) تمرکز بیشتری داشته باشد.

این مکانیزم با استفاده از فرمول زیر وزن‌دهی می‌کند:

$$\text{Attention}(Q,K,V) = \text{softmax}((Q \cdot K^T)/\sqrt{(d\_k)}) \cdot V$$

که در آن Q ، K، Vاز خروجی لایه BiLSTM استخراج می‌شوند.

لایه خروجی :دو لایه کاملاً متصل با ۶۴ و ۳۲ نرون و سپس لایه Softmax با ۲ نورون (کلاس‌های عادی/ناهنجار).

آموزش با یادگیری نیمه‌نظارت‌شده (Semi-supervised) و افزایش داده

برای حل مشکل کمبود داده‌های برچسب‌گذاری‌شده برای حملات جدید، یک رویکرد آموزشی دومرحله‌ای استفاده می‌شود: (۱) پیش‌آموزش (Pre-training) بر روی مجموعه داده‌های عمومی CICIDS2017)و UNSW-NB15) با برچسب کامل، (۲) تنظیم دقیق (Fine-tuning)روی ترافیک واقعی شبکه خانگی که بخش کوچکی از آن توسط متخصص (هشدارهای اولیه) برچسب زده شده و بقیه با استفاده از روش Pseudo-labeling توسط مدل آموزش‌دیده قبلی برچسب فرضی می‌خورند. همچنین برای افزایش مقاومت در برابر حملاتadversarial ، از تکنیک افزایش داده مانند افزودن نویز گوسی به ویژگی‌ها و جابجایی موقتی پنجره اسلایدی استفاده می‌شود.

لایه مجازی‌سازی امن مبتنی بر میکروسرویس‌های سبک

پس از شناسایی ترافیک مشکوک توسط لایه تشخیص، لایه مجازی‌سازی وارد عمل می‌شود. برخلاف روش‌های سنتی که به سادگی کل IP مهاجم را مسدود می‌کنند، رویکرد ما جراحی دقیق‌تری روی ارتباطات انجام می‌دهد.

کانتینرهای شبکه سبک باLinux Network Namespaces

در هسته سیستم‌عامل گیت‌وے OpenWrt) یا شاخه اختصاصی آن(، برای هر دستگاه IoT یا گروهی از دستگاه‌ها، یک Namespace شبکه مجزا ایجاد می‌شود که دارای جدول مسیریابی، قوانینiptables ، و رابط شبکه مجازی اختصاصی است. مزایای این روش نسبت به VLAN سخت‌افزاری: (الف) پیاده‌سازی روی هر سخت‌افزاری با هسته لینوکس ≤ ۴,۱۹ ممکن است، (ب) هزینه محاسباتی ناچیز (~۲٪ مصرف CPU اضافی)، (ج) امکان ایجاد و حذف پویا در پاسخ به تهدیدات.

هر میکروسرویس امنیتی (مانند فایروال تخصصی برایMQTT ، سنسور تشخیص ناهنجاری دامنه، یا محافظ (DNS درون یک کانتینر Docker جداگانه با حداقل تصویر Alpine Linux)، حجم کمتر از ۵۰ مگابایت (اجرا می‌شود و با دیگر مؤلفه‌ها از طریق سوکت‌های UNIX یا صف‌های پیام (ZeroMQ) ارتباط برقرار می‌کند.

جداسازی مبتنی بر نقش

برخلاف جداسازی سخت همهIoT ها از یکدیگر که ممکن است عملکرد عادی (مثلاً ارتباط دستیار صوتی با لامپ هوشمند را مختل کند)، جداسازی پروفایل-محور انجام می‌شود:

- پروفایل عمومی :(Public) دستگاه‌هایی که فقط به اینترنت نیاز دارند (مثل دستیار صوتی، تلویزیون هوشمند) – دسترسی به داخل شبکه خانگی ممنوع.
- پروفایل حسگر :(Sensor) دستگاه‌هایی که فقط داده تولید می‌کنند (دماسنج، حسگر در) – امکان ارسال به Gateway مرکزی، نه ارتباط مستقیم با یکدیگر.
- پروفایل کنترلی :(Controller) دستگاه‌هایی که فرمان می‌دهند (برنامه موبایل کاربر، صفحه کلید هوشمند) – دسترسی محدود به دستگاه‌های مشخص با پروتکل خاص.
- پروفایل دوربین :(Camera) دستگاه‌های استریم تصویر – مسیر اختصاصی با QoS تضمینی و جداسازی کامل از سایر دستگاه‌ها.

لایه مدیریت خط‌مشی پویا با ANFIS (ANFIS-PPM)

لایه سوم، مغز تصمیم‌گیرنده است که با استفاده از سیستم استنتاج فازی-عصبی تطبیقی (ANFIS) رفتار پویای شبکه را مدل کرده و خط‌مشی‌های کنترلی را به روز می‌کند .ANFIS با توجه به مزایای زیر انتخاب شده است: (۱) قابلیت استفاده از دانش خبرگی انسانی در قالب قوانین فازی(If-Then) ، ۲ قابلیت یادگیری و تنظیم توابع عضویت از داده‌ها، (۳) تفسیرپذیری بالا برای کاربر عادی (امکان ارائه علت تصمیم‌گیری.

ورودی‌های سیستمANFIS

پنج متغیر ورودی به ANFIS تغذیه می‌شوند:

- :(Risk Index) RIشاخص ریسک خروجی از لایه DL عدد بین ۰ تا ۱، هرچه به ۱ نزدیکتر باشد حمله محتمل‌تر است :(Device Type) DT.نوع دستگاه (با کدگذاری ۰ تا ۵: حسگر، دوربین، کنترلی، صوتی، ذخیره‌سازی، سایر.
- :(Time Importance) TIضریب اهمیت زمانی (برای مثال شب هنگام، حساسیت امنیتی بالاتر است؛ مقدار ۰ تا ۱).
- :(Historical Rate) HRنرخ خطای هشدار اشتباه (False Positive Rate)مدل تشخیص در ۲۴ ساعت گذشته – برای تنظیم حساسیت.
- :(Traffic Rate) TRنرخ ترافیک لحظه‌ای بر حسب بسته بر ثانیه برای آن دستگاه خاص (به عنوان عامل زمینه‌ای).

خروجی‌های سیستمANFIS

خروجی ANFIS یک بردار تصمیم با چهار مؤلفه است با تابع عضویت گوسی بهینه‌شده توسط الگوریتم بهینه‌سازی ازدحام ذرات:(PSO)

- Action اقدام "Allow" :مجاز، "Log-only"فقط ثبت وقوع "Limit-bandwidth"کاهش پهنای باند به ۵۰٪، "Isolate"انتقال به Namespace قرنطینه، "Block" مسدودسازی کامل.
- Duration مدت زمان اعمال بر حسب دقیقه :۵، ۱۵، ۶۰، ۲۸۸۰ (دو روز)، یا نامحدود.
- Priority اولویت در اعمال :بالا، متوسط، پایین.
- Log-level سطح لاگ‌گذاری :جزئی، خلاصه، فقط خلاصه هشدار.

قوانین فازی نمونه

چند قانون از بانک قوانین ANFIS شامل ۳۶ قانون ابتدایی که به ۱۱۸ قانون بعد از یادگیری ارتقا یافت:

- قانون ۱ : اگر RI بالا (بیش از ۰,۸) و DT برابر "دوربین" و TRخیلی بالا (بیش از ۱۰۰۰ بسته در ثانیه) آنگاه Action "Isolate" =، مدت = ۶۰ دقیقه.
- قانون ۲ : اگر RI متوسط (۰,۳ تا ۰,۷) و DT برابر "کنترلی" و TI خیلی پایین (شب هنگام) آنگاه."Log-only" = Action
- قانون ۳ : اگر RI پایین (کمتر از ۰,۲) و HR خیلی بالا (بیش از ۰,۱۵) آنگاه "Allow" = Action برای جلوگیری از قفل شدن سرویس‌های عادی.(قانون ۴ : اگر RI بسیار بالا (بیش از ۰,۹۵) و صرف نظر از نوع دستگاه وTR ، = Action "Immediate Block".

ارزیابی

برای اثبات کارایی عملی راهکار پیشنهادی، یک نمونه آزمایشگاهی کامل پیاده‌سازی و بر روی سناریوهای واقعی ارزیابی شده است.

محیط پیاده‌سازی سخت‌افزاری و نرم‌افزاری در پیاده سازی به شرح زیر می باشد:

یک برد Raspberry Pi 4 Model B با مشخصات: پردازنده چهار هسته ARM Cortex-A72فرکانس ۱,۵ گیگاهرتز، ۸ گیگابایت رمLPDDR4 ، کارت حافظه ۶۴ گیگابایت کلاس ۱۰، و دو رابط شبکه (Ethernet onboardو یک USB-to-Ethernet Realtek) به عنوان روتر دو پورت. گیت‌وے در مقابل مودم اینترنت و سوییچ داخلی قرار گرفت.

شش دستگاه واقعی) :IoT ۱ (دوربین مداربسته Xiaomi 360 ،)۲ (لامپ هوشمند Philips Hue،)۳ (پریز هوشمندTP-Link Kasa ،)۴ (دستیار صوتیGoogle Home Mini ،)۵ (سنسور دمایAqara ،)۶ (یک تبلت اندروید شبیه‌ساز دستگاه کنترل مرکزی. سیستمعامل گیت‌وے : OpenWrt 23.05(هسته لینوکس ۵,۱۵) با پچ‌های اختصاصی برای .PF_RING

پیاده‌سازی لایه DL: TensorFlow Lite 2.15 با کامپایل اختصاصی برای) ARM با استفاده از بهینه‌سازی NEON و.(TFLite Delegate

پیاده‌سازی لایه مجازی‌سازی Bash scripts + iptables + netns :)توکار لینوکس) Docker 25.0 + موتور کانتینر.
پیاده‌سازی لایه :ANFIS کتابخانه‌های Python–anfis و تطبیق آن برای اجرا به عنوان سرویس سیستمی.(systemd)
ذخیره‌سازی لاگ و آمار SQLite3 :(مصرف حافظه کم) و ارسال انبوه آمار به MQTT broker محلی.
برای ارزیابی جامع، از سه منبع داده استفاده شد:
CICIDS2017: مجموعه داده استاندارد حملات شبکه) شاملDDoS ، Brute Force، Web Attack، (Infiltrationکه به عنوان پایه آموزش اولیه استفاده شد.
Bot-IoT: شامل سناریوهای باتنت اختصاصی) IoT ترافیکMirai ، (Bashliteکه برای ارزیابی حملات خاص IoT استفاده شد.
ShIoT (Self-collected): داده‌های ضبط‌شده از شبکه آزمایشگاهی با اجرای ۱۵ سناریوی حمله واقعی شامل DDoS :بهLAN ، ARP Spoofingبین دوربین و اپلیکیشن، تزریق فرمان MQTT به لامپ هوم، اسکن پورت باnmap ، حمله بازپخش فرمان باز کردن قفل (با اسکریپت سفارشی)، و پنج سناریوی ترکیبی.
پارامترهای ارزیابی : معیارهای استاندارد طبقه‌بندی: دقت (Accuracy - ACC)، نرخ تشخیص (Detection Rate - DR = Recall)، نرخ هشدار اشتباه(False Alarm Rate - FAR = FP/(FP+TN)) ، معیار F1، سطح زیر منحنی(AUC) ROC ، و نیز معیارهای کارایی: تأخیر پردازش هر بسته(Latency) ، مصرف حافظه(RAM usage) ، مصرف CPUو پهنای باند شبکه اشغال‌شده توسط فرایند نظارت.
نتایج حاصل از پیاده‌سازی روی سخت‌افزار واقعی در جدول ۳ و نمودارهای ۱ تا ۳ (شرح در متن) ارائه شده است.

جدول ۳: نتایج کمی پیاده‌سازی در مقایسه با روش‌های پیشین (میانگین ۱۰ اجرا)

روش/معیار	دقت (ACC)	تشخیص (DR)	نرخ هشدار (FAR)	F1-Score	تأخیر (ms)	مصرف RAM (MB)	مصرف CPU (%)
IoT-IDSA [22] (Cloud)	٪۹۱٫۴	٪۹۴٫۲	٪۴٫۷	۰٫۹۱	۱۸۵ ارسال	-	-
Deep-STM [26] (GPU)	٪۹۵٫۹	٪۹۶٫۸	٪۳٫۲	۰٫۹۶	۷۳٫۴	۴۲۱	٪۳۴
Light-HomeGuardتطبیق ([20])	٪۸۲٫۳	٪۷۹٫۱	٪۱۲٫۶	۰٫۸۱	۴٫۲	۴۳	٪۸
CNN-LSTMبدون توجه	٪۹۵٫۲	٪۹۴٫۳	٪۴٫۱	۰٫۹۴	۵۶٫۲	۲۴۶	٪۲۶
دیدگاه پیشنهادی	٪۹۷٫۹	٪۹۸٫۷	٪۱٫۴	۰٫۹۸	۴۲٫۶	۱۶۸	٪۱۹

نتایج به دست آمده نشان می‌دهد که رویکرد SecHome-IoT توانسته است به طور معناداری از روش‌های پیشین بهتر عمل کند. در این بخش، این نتایج را از چند منظر تحلیل می‌کنیم.
دقت و نرخ هشدار اشتباه (FAR) : دستیابی به نرخ تشخیص ٪۹۸٫۷ با نرخ هشدار اشتباه تنها ٪۱٫۴ یک دستاورد قابل توجه است. این بهبود را مدیون استفاده از مکانیزم توجه هستیم که به مدل اجازه می‌دهد بر بخش‌های مهم جریان متمرکز شود. در Deep-STMکه فاقد توجه است، مدل گاهی اوقات انحرافات طبیعی و نوسانات غیرعادی) مثل fluctuationsترافیک ویدئو (را با حمله اشتباه می‌گیرد و نرخ FAR بالاتری دارد. همچنین استفاده از ویژگی‌های آماری جریان به جای محتوای بسته، مقاومت در برابر حملات رمزنگاری‌شده ارائه می‌دهد.
کارایی محاسباتی و مناسب بودن برای شبکه خانگی : با مصرف حافظه ۱۶۸ مگابایت و ٪۱۹ مصرف CPU روی Raspberry Pi که یک گیت‌وے میان‌رده خانگی است، راهکار پیشنهادی به راحتی در کنار وظایف مسیریابی اصلی NAT)، DHCP، (DNS قابل اجراست. این عدد در مقایسه با مصرف ۴۲۱ مگابایتی) Deep-STMکه اساساً برای اجرا روی GPU طراحی شده و روی ARM نیاز به Swap حافظه دارد که تأخیر را افزایش می‌دهد) بسیار بهتر است. همچنین تأخیر ناچیز ۴۲ میلی‌ثانیه)که عمدتاً ناشی از استخراج ویژگی و اجرای TFLite است (تأثیر محسوسی بر کیفیت تجربه کاربر (QoE) در سناریوهایی مانند تماس ویدئویی یا بازی آنلاین ندارد.
تطبیق‌پذیری و مدیریت پویا : لایه ANFIS-PPM نشان داده که در طول ۳۰ روز آزمایش مداوم، توانسته با تغییر الگوی رفتاری خانواده (مثلاً افزایش استفاده از دستگاه‌ها در تعطیلات آخر هفته) خود را تطبیق دهد و نرخ مثبت کاذب را با افزایش RI تنظیم کند .رفتار "خودآموزی" ANFISاز طریق به‌روزرسانی پارامترهای توابع عضویت نیز مشاهده شد. یک مورد جالب: در هفته دوم آزمایش، یک برنامه اندرویدی مخرب (که کاربر آگاهانه نصب کرد) شروع به ارسال پکت‌های ICMP با قالب غیرعادی کرد .مدل تشخیص اولیه نتوانست آن را بخوبی شناسایی کند، اما پس از سه روز، داده‌های جدید جمع‌آوری و Fine-tune شد و دقت تشخیص از ٪۶۲ به ٪۹۶ افزایش یافت.
محدودیت‌ها و چالش‌های مشاهده‌شده :علیرغم موفقیت‌ها، محدودیت‌هایی نیز مشاهده شد: (۱) مدل تشخیص برای حمله بازپخش (Replay)به دلیل شباهت بسیار زیاد به ترافیک اصلی، دقت نسبتاً

پایین‌تری داشت. یک راهکار بالقوه استفاده از timestamp و nonce است که نیاز به تغییر در سمت دستگاه دارد. (۲) راهکار پیشنهادی به یک گیت‌وے مرکزی متکی است؛ اگر مهاجم بتواند گیت‌وے را فریب دهد یا از کار بیندازد، کل حفاظت مختل می‌شود. به عنوان راه‌حل موقتی، یک سرویس Watchdog برای راه‌اندازی مجدد خودکار لایه تشخیص در نظر گرفته شده است. (۳) پیاده‌سازی فعلی فقط برای شبکه‌های با مقیاس کمتر از ۵۰ دستگاه IoT آزموده شده است؛ برای شبکه‌های بزرگتر کارایی احتمالی کاهش می‌یابد.

نتیجه‌گیری و راهکارهای آتی

این مقاله معماری SecHome-IoT را به عنوان یک راهکار جامع، چندلایه، کارا و تفسیرپذیر برای افزایش امنیت شبکه‌های خانگی مبتنی بر اینترنت اشیا ارائه داد. مهم‌ترین دستاوردهای این پژوهش عبارتند از:

- **ارائه یک معماری ترکیبی نوین** که برای اولین بار لایه تشخیص ناهنجاری مبتنی بر یادگیری عمیق با مکانیزم توجه) را با لایه مجازی‌سازی سبک و لایه تصمیم‌گیری فازی-عصبی ادغام کرده است. این ترکیب نقاط قوت هر روش را جذب و نقاط ضعف را پوشش می‌دهد.

- **طراحی مدل تشخیص ناهنجاری سبک و کارآمد** که با دقت ۹۸,۷٪ و نرخ هشدار اشتباه ۱,۴٪ روی سخت‌افزار) Raspberry Pi با مصرف ۱۹٪ CPU و ۱۶۸ مگابایت رم) عملکردی قابل قبول برای محیط خانگی ارائه می‌دهد. انتخاب ویژگی‌های مبتنی بر جریان-Flow) (basedو عدم نیاز به بازرسی محتوا، حریم خصوصی کاربران را حفظ و قابلیت تشخیص ترافیک رمزنگاری‌شده را فراهم می‌کند.

- **ارزیابی عملی و واقعی:** بر روی سخت‌افزار خانگی معمولی با ترکیبی از دستگاه‌های واقعی IoT و سناریوهای حمله متنوع، که اعتبار علمی نتایج را در مقایسه با تحقیقات صرفاً شبیه‌سازی‌شده افزایش می‌دهد. نتایج ما به طراحان سیستم‌های امنیتی خانگی نشان می‌دهد که با هزینه زیر ۱۰۰ دلار (قیمت یک Raspberry Pi و یک سوییچ ساده) می‌توان امنیت خانه هوشمند را به سطح سازمانی نزدیک کرد.

علی‌رغم جامعیت، تحقیق حاضر دارای محدودیت‌هایی است که باید توسط پژوهشگران آتی در نظر گرفته شود: (الف) مجموعه داده جمع‌آوری‌شده ShIoT مربوط به یک خانواده چهارنفره در یک بازه ۹۰ روزه است و ممکن است نماینده تمام الگوهای رفتاری جامعه نباشد. (ب) آزمایش‌ها بر روی یک پیکربندی سخت‌افزاری خاص (RPi4) انجام شده و نتایج در گیت‌وے‌های ضعیف‌تر) مثل RPi3 یا روترهای ارزان (MIPSمی‌تواند متفاوت باشد. (ج) پیاده‌سازی فعلی از پروتکل‌های بی‌سیم اختصاصی) IoTمانند Zigbee و (Z-Wave که مستقیماً به درگاه USBمتصل می‌شوند و ترافیک آن‌ها از گیت‌وے عبور نمی‌کند، صرف نظر کرده است. (د) حملات فیزیکی (مانند دستکاری سنسور یا نویز الکترومغناطیسی) در حیطه این پژوهش نبوده است. پیشرفت امنیت در شبکه‌های خانگی IoT یک زمینه تحقیقاتی باز و امیدوارکننده است. مسیرهای آتی پیشنهادی عبارتند از:

-**تشخیص نفوذ توزیع‌شده و همکاری چند-گیت‌وے (Federated Learning for IoT)**: با توجه به نگرانی‌های حریم خصوصی و تمایل کاربران به اشتراک نگذاشتن ترافیک خانگی خود، رویکرد یادگیری فدرال می‌تواند مدل‌های تشخیص ناهنجاری را بدون نیاز به جمع‌آوری داده خام در یک سرور مرکزی، با همکاری هزاران گیت‌وے خانگی ارتقا دهد. هر گیت‌وے فقط به‌روزرسانی گرادیان را ارسال می‌کند نه داده اصلی.

- **استفاده از بلاک‌چین سبک برای مدیریت اعتماد و یکپارچگی خط‌مشی‌ها (Blockchain-based Policy Management):** در معماری فعلی، گیت‌وے مرکزی یک تک‌نقطه تصمیم‌گیری است. استفاده از یک بلاک‌چین خصوصی) مانند Hyperledger Fabric روی گیت‌وهای همسایه (می‌تواند برای ثبت تغییرات خط‌مشی و ایجاد اجماع در مورد قرنطینه یک دستگاه آلوده، امنیت را افزایش دهد.

- **پیش‌بینی زودهنگام حملات با استفاده از مدل‌های مولد (Generative Models for Early Warning)**: استفاده از شبکه‌های مولد مانند VAE (Variational Autoencoders) یا GANs برای تولید سناریوهای حمله واقع‌بینانه و آموزش مدل تشخیص در فضاهای با داده کم .(Few-shot learning) همچنین می‌توان از این روش‌ها برای شبیه‌سازی "مسیرهای پیشرفت حمله (Attack kill chain) "استفاده کرد و قبل از وقوع خسارت جبران‌ناپذیر، اخطار صادر کرد.

- **یکپارچه‌سازی با استانداردهای در حال ظهور خانه هوشمند :** با تکامل استاندارد) Matter اتصال‌پذیری یکپارچه (IoT و پروتکل Thread، راهکار امنیتی پیشنهادی باید برای کار با این لایه‌های جدید منطبق شود. به طور خاص، الگوریتم‌های تشخیص ناهنجاری باید ویژگی‌های مربوط به مش (Mesh) و مسیریابی درختوار (Tree routing) Threadرا استخراج کنند.

- **توسعه سخت‌افزار امنیتی اختصاصی و کم‌مصرف :** طراحی یک شتاب‌دهنده سخت‌افزاری ASIC) یا (FPGA با هزینه کمتر از ۲۰ دلار که بتواند عملیات استخراج ویژگی و اجرای TFLite را با مصرف انرژی کمتر از ۲ وات انجام دهد، می‌تواند تحولی در امنیت شبکه خانگی ایجاد کند.

منابع

[1] Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer Networks. 2010 Oct 28;54(15):2787-805.

[2] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013 Sep 1;29(7):1645-60.

[3] Statista Research Department. Number of connected IoT devices worldwide 2020-2030 [Internet]. New York: Statista; 2025 [cited 2026 Apr 25]. Available from: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[4] Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017 Jun 1;88:10-28.

internet of things (IoT) security. IEEE Communications Surveys & Tutorials. 2020 Apr 3;22(3):1646-85.
[23] Hasan M, Islam MM, Zarif MII, Hashem MMA. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things. 2019 Sep 1;7:100059.
[24] Anthi E, Williams L, Słowińska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal. 2019 May 23;6(5):9042-53.
[25] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 2018 May 1;82:761-8.
[26] Ullah I, Mahmoud QH. A two-level flow-based anomalous activity detection system for IoT networks using deep learning. Journal of Network and Systems Management. 2021 Apr;29(2):1-27.
[27] Khan MA, Khan MA, Jan SU, Ahmad J, Jamal SS, Shah AA, Pitropakis N, Buchanan WJ. A deep learning-based intrusion detection system for MQTT enabled IoT. Sensors. 2021 Oct 18;21(20):7016.
[28] Roopak M, Tian GY, Chambers J. Deep learning models for cyber security in IoT networks. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC); 2019 Jan 7-9; Las Vegas, NV, USA. IEEE; 2019. p. 452-7.
[29] Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications. 2020 Feb 1;50:102419.
[30] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS); 2015 Nov 10-12; Canberra, ACT, Australia. IEEE; 2015. p. 1-6.
[31] Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018); 2018 Jan 22-24; Funchal, Portugal. p. 108-16.
[32] Koroniotis N, Moustafa N, Sitnikova E, Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems. 2019 Nov 1;100:779-96.
[5] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal. 2018 Nov 1;6(2):1606-16.
[6] Trappe W, Howard R, Moore RS. Low-energy security: Limits and opportunities in the internet of things. IEEE Security & Privacy. 2015 Jan 22;13(1):14-21.
[7] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015 Jan 15;76:146-64.
[8] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE Communications Surveys & Tutorials. 2018 Jul 16;21(2):1636-75.
[9] Bertino E, Islam N. Botnets and internet of things security. Computer. 2017 Feb 21;50(2):76-9.
[10] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017 Jul 6;50(7):80-4.
[11] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, et al. Understanding the mirai botnet. In: 26th USENIX Security Symposium (USENIX Security 17); 2017 Aug 16-18; Vancouver, BC. p. 1093-110.
[12] Andy S, Rahardjo B, Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. In: 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI); 2017 Sep 19-21; Yogyakarta, Indonesia. IEEE; 2017. p. 1-6.
[13] Chen Y, Zhang Y, Wang S. Vulnerability assessment and mitigation for IoT firmware: A survey. Computers & Security. 2024 Mar 1;138:103674.
[14] Ziegeldorf JH, Morchon OG, Wehrle K. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks. 2014 Dec;7(12):2728-42.
[15] Mohanty SN, Ramya KC, Rani SS, Gupta D, Shankar K, Lakshmanaprabu SK, Khanna A. An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems. 2020 Jan 1;102:1027-37.
[16] HaddadPajouh H, Dehghantanha A, Khayami R, Choo KKR. A deep recurrent neural network based approach for internet of things malware threat hunting. Future Generation Computer Systems. 2018 Aug 1;85:88-96.
[17] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things using RC4 and LFSR lightweight hybrid algorithm (RLHA). Wireless Personal Communications. 2020 Dec;115(4):2953-67.
[18] McKay KA, Bassham LE, Sonmez Turan M, Mouha N. Report on lightweight cryptography (NIST IR 8114). Gaithersburg (MD): National Institute of Standards and Technology; 2017 Apr. 34 p.
[19] Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors. 2019 Jan 18;19(2):326.
[20] Sivanathan A, Sherratt D, Gharakheili HH, Sivaraman V, Vishwanath A. Low-cost flow-based security for home IoT networks. In: 2019 IEEE 44th Conference on Local Computer Networks (LCN); 2019 Oct 14-17; Osnabrück, Germany. IEEE; 2019. p. 360-7.
[21] Sivanathan A, Gharakheili HH, Sivaraman V. Managing IoT cyber-security using programmable telemetry and data plane filtering. In: 2020 IEEE 28th International Conference on Network Protocols (ICNP); 2020 Oct 13-16; Madrid, Spain. IEEE; 2020. p. 1-6.
[22] Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for