تشخیص نفوذ و شناسایی حملات در اینترنت اشیاء مبتنی بر پروتکل مسیریابی RPL

مؤلفان:

کمیل قنبری، علی احمدی رشادت، سعید جمشیدی

سرشناسه: قنبری، کمیل، ۱۳۶۷ـ
عنوان و نام پدیدآور: تشخیص نفوذ و شناسایی حملات در اینترنت اشیا مبتنی بر پروتکل مسیریابی PRL مؤلفان کمیل قنبری، علی احمدی رشادت، سعید جمشیدی
مشخصات نشر: همدان، روزاندیش، ۱۴۰۰
مشخصات ظاهری: ۷۳ ص، مصور (بخش رنگی)، جدول (بخش رنگی) نمودار (بخش رنگی)
شابک: ۷-۲۹۷-۴۳۸-۶۰۰-۹۷۸
وضعیت فهرست‌نویسی: فیپا
یادداشت: واژنامه
یادداشت: کتابنامه
موضوع: اینترنت اشیاء ـ ـ تدابیر ایمنی
موضوع: Internet of things – Security measures
موضوع: پروتکل‌های مسیریابی (پروتکل‌های شبکه کامپیوتری)
موضوع: Routing protocols (Computer network protocols)
شناسه افزوده: احمدی رشادت، علی، ۱۳۶۶ـ
شناسه افزوده: جمشیدی، سعید، ۱۳۶۵ـ
رده‌بندی کنگره: TK۵۱۰۵/۸۸۵۷
رده‌بندی دیویی: ۰۰۴/۶۷۸
شماره کتابشناسی ملی: ۷۶۷۰۲۳۱

انتشارات روز اندیش

مدیرمسئول: رضا قمریان ـ همدان، ابتدای خیابان جهاد (جهان نما) طبقه زیرین ساختمان خجسته
تلفن:۰۸۱-۳۸۲۲۱۰۲۸ همراه: ۰۹۱۸۱۱۱۱۸۷۶
پست الکترونیکی: RoozBook578@gmail.com

عنوان: تشخیص نفوذ و شناسایی حملات در اینترنت اشیاء مبتنی بر پروتکل مسیریابی RPL
مؤلفان: کمیل قنبری، علی احمدی‌رشادت، سعید جمشیدی
ناشر: روزاندیش
نوبت چاپ: اول ۱۴۰۰
شابک: ۷-۲۹۷-۴۳۸-۶۰۰-۹۷۸
قیمت: ۴۰۰۰۰ تومان

مقدمه:

تأثیر اقتصادی اینترنت اشیا در محدوده تریلیون دلار ارزیابی می‌شود و منافع حاصل از یک جامعه متصل، قابل توجه و متحول کننده است. اگر چه مزایای اینترنت اشیا غیرقابل انکار است، ولی با این وجود حملات پرمخاطب، همراه با عدم اطمینان در مورد بهترین روشهای امنیتی و هزینه‌های مربوط به آنها، بسیاری از مشاغل را از پذیرش این فناوری باز می‌دارد. علاوه بر این، کاربران نهایی از عواقب نقض امنیت اینترنت اشیا واهمه دارند. تحقیقات اخیر نشان می‌دهد که ۹۰٪ از مصرف‌کنندگان از امنیت دستگاه اینترنت اشیا اطمینان ندارند. اکوسیستم‌های IoT مدرن پیچیده هستند. ماشین‌ها و اشیا تقریباً در هر صنعتی می‌توانند متصل شده و پیکربندی شوند تا داده‌ها را از طریق شبکه‌های تلفن همراه به برنامه‌های ابری ارسال کنند. خطر امنیت دیجیتال در هر مرحله از سفر اینترنت اشیا وجود دارد و گروهی از هکرها هستند که از آسیب‌پذیری سیستم استفاده می‌کنند. متأسفانه، انواع مختلف داده‌ها و قدرت محاسبات در میان دستگاه‌های اینترنت اشیا به این معنی است که هیچ راه حلی برای امنیت سایبری "یک اندازه و متناسب با همه" وجود ندارد که بتواند از کاربر هنگام استفاده از اینترنت اشیا محافظت کند.

امنیت اینترنت اشیا عملیاتی است برای ایمن‌سازی دستگاه‌های اینترنت اشیا و شبکه‌هایی که به آنها متصل هستند. دستگاه‌های اینترنت اشیا با توجه به امنیت ساخته نشده‌اند. در اکثر موارد، هیچ راهی برای نصب امنیت روی خود دستگاه وجود ندارد. علاوه بر این، آنها گاهی اوقات بدافزار روی خود حمل می‌کنند، و سپس شبکه‌ای را که به آن متصل شده‌اند آلوده می‌کند. اهداف معمول امنیتی در اینترنت اشیا شامل رازداری، یکپارچگی و در دسترس بودن می‌باشد. با این حال، اینترنت اشیا از نظر اجزا و دستگاه‌ها، منابع محاسباتی و توان و حتی ماهیت ناهمگون و همه جا حاضر اینترنت اشیا محدودیت‌ها و محدودیت‌های زیادی دارد که نگرانی‌های دیگری را ایجاد می‌کند.

فهرست مطالب

اینترنت اشیاءIOT ۱۱

پروتکل‌های ارتباطی اینترنت اشیاء ۱۷

معماری اینترنت اشیاء ۲۰

شبکه‌های کمتوان و پراتلاف ۲۲

استانداردLOWPAN6 ..... ۲۳

تهدیدات امنیتی در اینترنت اشیاء ۲۵

حملات محرومیت از سرویس ۲۶

استراق سمع ۲۷

تجزیه و تحلیل ترافیک ۲۷

اختلال ۲۸

سرقت ۲۸

حملات فیزیکی ۲۸

حملات منجلاب /سیاه چاله ۲۹

حملات HELLO FLOOD ۳۰

تشخیص حملات در اینترنت اشیاء ۳۰

مسیریابی در اینترنت اشیاء ۳۳

روش‌های کلاسیک ۳۹

پروتکل مسیریابی چند مسیره مبتنی بر تقاضای موردی در اینترنت اشیاء ۳۹

پروتکل مسیریابی چندگامی امنSMRP ۴۰

الگوریتم آگاه از انرژی مسیریابی مورچگان ۴۰

مسیریابی اینترنت اشیاء انطباقی هرس شده ۴۱

پروتکل مسیریابی مبتنی بر انرژی و کیفیت پیوند ۴۲

روش‌های استانداردشده توسطIETF ۴۴

پروتکل مسیریابیRPL ۴۴