****

 **دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |
| --- | --- |
| **نام استاد راهنما: جناب اقای/سرکار خانم دکتر مقصود عباسپور****نام استاد مشاور: جناب اقای/سرکار خانم دکتر** | **نام دانشجو: امیر محمودیان عکس**  |
| **مقطع: کارشناسی ارشد** | **گرایش: نرم افزار** | **رشته: مهندسی کامپیوتر** |
| **تاریخ: 21/9/1400** | **نوع دفاع:*** **دفاع پروپوزال**
 |
| **ساعت: 17 تا 19** |
| **مکان:** |
| **عنوان: ارایه یک راه­حل ترکیبی تطابق پذیر برای سیستم­های تشخیص نفوذ در اینترنت اشیا با استفاده از تکنیک­های یادگیری ماشین** |
| **داوران داخلی: جناب اقای/سرکار خانم دکتر علیرضا شاملی سندی** | **داوران خارجی: جناب اقای/سرکار خانم دکتر****احمد خونساری** |
| **چکیده:**اینترنت اشیا (IoT) یک شبکه ناهمگن از دستگاه‌هایی با منابع محدود است که هم به یکدیگر و هم به اینترنت متصل هستند. از آنجایی که اهمیت اینترنت اشیا در سال‌های اخیر به طور قابل توجهی افزایش یافته است، تحقیقات قابل توجهی در این زمینه و به ویژه در مورد مکانیسم‌ها و پروتکل‌های جدید مناسب برای چنین سیستم‌های پیچیده‌ای انجام شده است. پروتکل مسیریابی برای شبکه‌های کم مصرف و با اتلاف (RPL) یکی از پروتکل‌های مسیریابی پذیرفته شده برای اینترنت اشیا است. این پروتکل مسیریابی چند هاپ را فراهم می کند و عمدتاً برای ارتباطات "چند نقطه به یک نقطه" (MP2P) و همچنین پشتیبانی از ارتباطات "نقطه به نقطه" (P2P) و "یک به چند نقطه" (P2MP) پیشنهاد می­شود. با این حال، RPL، مانند بسیاری از پروتکل‌های پیشنهادی برای IoT، به طور هدفمند با در نظر گرفتن مسائل امنیتی طراحی نشده است؛ از این رو، راه‌حل‌های خاصی برای ایمن کردن RPL در این حوزه توسعه داده شده است. سیستم‌های تشخیص نفوذ معروف به IDS که فعالیت‌های سیستم‌ها را نظارت می‌کنند و نفوذها را شناسایی می­نمایند، به بخشی اجتناب‌ناپذیر از چنین سیستم‌های امنیتی تبدیل شده‌اند، زیرا مکانیسم‌های پیشگیری به تنهایی هرگز کافی نیستند. در مطالعه پایان نامه کنونی، یک سیستم تشخیص نفوذ جدید برای این نوع شبکه های کم مصرف و همراه با اتلفات پیشنهاد شده است. اینترنت اشیا در زمینه‌های مختلفی مانند خانه‌های هوشمند، مراقبت‌های پزشکی و وسایل نقلیه هوشمند وجود دارد و هر کدام دارای الزامات امنیتی متفاوتی هستند. دستگاه‌های موجود در اینترنت اشیا از طریق پیوندهای ارتباطی با اتلاف به یکدیگر متصل هستند، دارای منابع محدود هستند و مستعد حملات مختلف می¬باشند. علاوه بر این، از آنجایی که ارتباط چنین دستگاه هایی توسط RPL ارائه می شود، این پروتکل می تواند توسط مهاجمان داخلی نیز هدف قرار گیرد. در این پایان نامه، حملات خاص علیه RPL، یعنی «حمله شماره نسخه»، «بدترین حمله والدین» و «حمله سیل سلام» به طور عمیق مورد تجزیه و تحلیل قرار گرفته است. سپس، یک IDS مبتنی بر یادگیری ماشین به منظور شناسایی چنین حملاتی پیشنهاد گردیده. در اینجا، اثرات ویژگی‌های گرفته‌شده از تک تک گره­های شبکه بر میزان تشخیص حملات، بررسی شده است و هر دو طبقه‌بندی دو کلاسه و طبقه‌بندی چند کلاسه برای تشخیص نوع حملات انجام شده است. سپس سیستم پیشنهادی بر روی شبکه های شبیه سازی شده با استفاده از درصدهای مختلف مهاجم (5، 10 و 20 درصد) مورد ارزیابی قرار گرفته است. نتایج این پژوهش نشان می دهد که سیستم پیشنهادی قادر است حملات را با نرخ تشخیص 99.5 درصد، نرخ مثبت کاذب 0.06 درصد برای طبقه بندی دو کلاسه و نرخ دقت 99.3 درصد برای تشخیص چند کلاسه به طور موثر تشخیص دهد. به طور خاص، نرخ تشخیص برای «حمله شماره نسخه» 93.2 درصد، برای «بدترین حمله والدین» 98.17 درصد و برای «حمله سیل سلام» 99.96 درصد نشان داده شده است. |