دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: مرتضی رضائی		**نام استاد راهنما: آقای دکتر مقصود عباسپور**
مقطع: کارشناسی ارشد	**رشته: مهندسی کامپیوتر**	**گرایش: معماری سیستم‌های کامپیوتری**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ■ • **دفاع رساله دکترا** □		**تاریخ: ۱۴۰۲/۰۶/۲۸** **ساعت: ۰۹:۰۰ الی ۱۱:۰۰** **مکان: کلاس ۲۰۰**

عنوان: ارائه یک روش دفاعی جهت مقابله با حملات مبتنی بر یادگیری ماشین خصمانه در شبکه‌های کامپیوتری

داوران خارجی: آقای دکتر محمد صیاد حقیقی	**داوران داخلی: آقای دکتر علیرضا شاملی**

چکیده:

با پیشرفت‌های فراوانی که در زمینه شبکه‌های کامپیوتری، استفاده از اینترنت در زندگی روزمره و به‌کارگیری نرم‌افزارها و ابزارهای مختلف توسط انسان انجام شده است، اینترنت بخش مهم و بزرگی از زندگی انسان‌ها را تشکیل می‌دهد. لذا حفظ امنیت آن یک امر حیاتی است، به همین منظور واحدهای امنیتی مختلفی ایجاد شده‌اند که یکی از مهم‌ترین آن‌ها سیستم‌های تشخیص نفوذ شبکه هستند. با پیشرفت‌های انجام شده در زمینه یادگیری ماشین، استفاده از آن‌ها در طراحی ساختار سیستم‌های تشخیص نفوذ شبکه افزایش‌یافته و در نتیجه موفق شده‌ایم که حملات مهاجمان را بادقت خوبی شناسایی نماییم. هم‌زمان با استفاده پژوهشگران از یادگیری ماشین در طراحی سیستم‌های تشخیص نفوذ شبکه، مهاجمان نیز حملات جدیدی را تحت عنوان حملات خصمانه یادگیری ماشین ایجاد کرده‌اند، که در آن‌ها شخص مهاجم با اصلاح مشخصه‌هایی از داده‌های ورودی که بیشترین تأثیر را در طبقه‌بندی سیستم‌های تشخیص نفوذ شبکه دارند حملات خود را انجام می‌دهد. برای انجام یک حمله خصمانه مهاجم نیاز به تولید ورودی‌هایی دارد که قابلیت دورزدن مدل یادگیری ماشین سیستم‌های تشخیص نفوذ شبکه را داشته باشند که به آن‌ها نمونه‌های خصمانه گفته می‌شود.

برای مقابله با حملات خصمانه روش‌های دفاعی مختلفی در گذشته پیشنهاد شده‌اند و اگرچه عملکرد قابل قبولی از خود نشان داده‌اند، اما با افزایش حجم ترافیک شبکه دیگر پاسخگو نیستند. لذا روش دفاع خود را با استفاده از سیستم‌های تشخیص نفوذ شبکه ارائه خواهیم کرد. روش پیشنهادی در این پژوهش دو بخش اصلی دارد که بخش اول مسئول پیش‌گیری از انجام حمله است و هنگامی که ترافیک ورودی دریافت می‌شود با پردازش آن بخشی از داده‌های شامل حمله را شناسایی و معرفی می‌کند. بخش دوم مسئول مقاوم‌سازی سیستم‌های تشخیص نفوذ شبکه می‌باشد و در ساختار آن به جای مدل‌های یادگیری ماشین عادی از مدل‌های یادگیری عمیق استفاده شده است که قادر به شناسایی الگوی داده‌ها با دقت بیشتر هستند.

در این پژوهش موفق شدیم مدل‌های دفاع پیشنهاد شده در کارهای پیشین را پیاده‌سازی کرده و دقت آن‌ها را از ۹۹٪ به مقادیر کمتر از ۶۰٪ کاهش دهیم. سپس با استفاده از مدل پیشنهادی خود موفق شدیم یک سیستم تشخیص نفوذ شبکه ایجاد نماییم که حملات خصمانه را شناسایی نموده و با استفاده از آن، در این پژوهش موفق شده‌ایم دقت مدل را به مقادیری بالاتر از ۹۰٪ افزایش دهیم.

واژگان کلیدی: یادگیری ماشین خصمانه – یادگیری عمیق – نمونه‌های خصمانه – سیستم‌های تشخیص نفوذ شبکه