ارائه یک الگوریتم مناسب برای پیش‌بینی حملات سایبری مبتنی بر یادگیری

پروانه سلیمانی برایجانی[1]، علی‌جبار رشیدی[2]، کوروش داداش‌تبار احمدی[3]

۱- دانشجوی کارشناسی ارشد دانشگاه صنعتی مالک اشتر

۲- دانشیار دانشگاه صنعتی مالک اشتر

۳- استادیار دانشگاه صنعتی مالک اشتر

چکیده

امروزه حملات سایبری، به طور گسترده با استفاده از آسیب‌پذیری‌های موجود در شبکه ها با قابلیت‌ها و شیوه‌های مختلفی، با اهداف متنوع به ویژه حمله به دارایی‌های اقتصادی، سیاسی و امنیتی افراد، سازمانها و کشورها در حال افزایش هستند. طی سال‌های اخیر تحقیقات گسترده‌ای در حوزه سایبری صورت گرفته که اکثر این تحقیقات تمرکز خود را بر شناسایی و تشخیص نفوذ قرار داده‌اند. این سیستم‌ها، تشخیص خود را پس از وقوع حمله یا در حین اجرای آن صورت می‌دهند. حال آنکه برای افزایش توانایی و قابلیت سیستم‌های دفاع سایبری، نیاز به بکارگیری مدل‌های پیشرفته‌تری وجود دارد که بتوانند علاوه بر تشخیص بهنگام، راهکارهای پیش‌بینی و دفاع پیش‌دستانه را نیز فراهم و حملات را قبل از وقوع و قبل از انجام فعالیت‌های خرابکارانه در شبکه متوقف سازند. این مقاله پس از بررسی مهمترین روش‌های پیش‌بینی نفوذ موجود، به معرفی و ارائه یک سیستم کارآمد برای کمک به عملکرد و پاسخگویی به موقع و دقیق‌تر سیستم‌های سایبری مبتنی بر پیش‌بینی با برخورداری از الگوهای یادگیرنده می‌پردازد. سیستم ارائه شده قبل از آنکه شبکه در معرض خطر قرار گیرد آن را پایش کرده و از اطلاعات گذشته در راستای پیش‌بینی آینده استفاده می‌نماید. این سیستم پیش‌بینی نفوذ، می‌تواند کلاس یا گام بعدی حمله در حال اجرا را با بکارگیری تکنیک‌های یادگیری عمیق با دقت و سرعت مناسبی تعیین نماید و در مقابل حملات سایبری چند مرحله ای سطح امنیت شبکه را ارتقاء بخشد. نتایج نشان می‌دهد که به کمک این سیستم پیش‌بینی، می‌توان یک مکانیسم دفاعی فعال در مقابل حملات پیشرو را فراهم آورد و امنیت هرچه بیشتر شبکه را تضمین نمود.

کلمات کلیدی: پیش‌بینی نفوذ، حملات چندمرحله‌ای، دفاع سایبری، هشدار، شبکه

۱- مقدمه

انواع مختلفی از حملات در فضای ارتباطاتی امروز وجود دارد. در یک تعریف ساده حمله‌ی رایانه‌ای به فعالیتی گفته می‌شود که با هدف ایجاد اختلال در عملکرد تجهیزات، رایانه‌ها و سرویس‌دهنده‌ها، تغییر در نحوه‌ی کنترل فرایند پردازش، یا از بین بردن داده‌های ذخیره شده در سرورهای سازمان انجام می‌شود. امروزه سازمان‌ها دنبال راهکارهایی هستند که بتوانند در مقابل تهدیدات امنیتی، دفاع فعالانه‌ای داشته باشند. امنیت شامل سه عنصر پایه‌ای محرمانگی، یکپارچگی و

[1] P_sol69@yahoo.com
[2] aiorashid@yahoo.com
[3] dadashtabar@yahoo.com