چکیده

شبکه های کامپیوتری در سال های اخیر گسترش چشم گیری داشته اند و به این ترتیب هدف نفوذگران و هکر های مختلف قرار گرفته اند. در زمینه امنیت شبکه، روشهایی برای بر خورد و یا تشخیص نفوذ وجود دارد که از آن جمله می توان به سیستم های تشخیص نفوذ اشاره کرد. مهمترین وظیفه یک سیستم تشخیص نفوذ طبقه بندی فعالیتهای سیستم به دو گروه فعالیتهای نرمال و فعالیتهای نفوذی (مشکوک) است. سیستم های تشخیص نفوذ به طور معمول نوع حملات را مشخص می کنند و یا آنها را در گروه های خاص طبقه بندی می کنند. هدف اصلی در ارائه این پایان نامه ترکیب چند روش محاسبات نرم به عنوان یک سیستم طبقه بندی کننده می باشد که نفوذ ها را در سطح شبکه بر اساس نوع حمله از فعالیتهای عادی تشخیص داده و گزارش می کند. در میان روش های مختلف محاسبات نرم روشهایی مانند شبکه های فازی- عصبی، سیستم های استنتاج فازی و الگوریتم ژنتیک در این پایان نامه به کار گرفته شده اند. یک مجموعه از طبقه بندی کننده های فازی-عصبی که به صورت موازی عمل می کنند، برای انجام طبقه بندی اولیه مورد استفاده قرار می گیرند. سپس ماژول تصمیم گیری فازی بر اساس خروجی های طبقه بندی کننده های فازی– عصبی یک تصمیم گیری نهایی در مورد اینکه آیا فعالیت جاری نفوذی است یا یک فعالیت عادی انجام می دهد. در نهایت برای رسیدن به بهترین نتایج، الگوریتم ژنتیک ساختار موتور تصمیم گیری فازی را بهنیه سازی می کند. آزمایشات و ارزیابی سیستم ارائه شده بر اساس مجموعه داده های ارزیابی KDD cup 99 انجام گرفته است. نتایج نشان می دهد که روش ارائه شده در مقایسه با دیگر روش ها می تواند در تشخیص نفوذ موثر باشد و نرخ تشخیص حملات را افزایش دهد. این افزایش نرخ تشخیص در حالی است که نرخ هشدار های غلط در سطح مناسبی می باشد. توانایی اصلی این سیستم در تطبیق پذیری برای شرایط مورد نظر طراح سیستم است که در آن می تواند با تعاریف و تنظیم های مختلف، سیستم را برای شرایط گوناگون آماده سازد. علاوه بر این سیستم ارائه شده این قابلیت را دارد که با داده های که توزیع الگو ها در آنها یکنواخت نیست به خوبی آموزش ببیند.

تقدیر و تشکر

خدایا تو را شکر که در راهی که می رفتم کسانی و نشانه هایی را در راهم نهادی که مرا به سوی آنچه هدفم بود، هدایت کردند. در اینجا لازم می دانم از اساتید صبور و مهربانم، جناب آقای دکتر کاهانی و جناب آقای دکتر منصفی که همواره مرا با راهنمایی ها و نظرات دلسوزانه، در انجام این پایان نامه همراهی و حمایت کردند و همینطور از کلیه اساتید محترم گروه که در پرورش و آموزش من تلاش بی دریغی داشته اند، صمیمانه تشکر و قدردانی کنم.

تشکر ویژه ای از پدر و مادر عزیز و مهربانم دارم که دست یاریشان همواره همراهم بوده و هست و از هیچ تلاشی در راه ترقی و پیشرفت من فروگذار نبوده اند. از همسر مهربانم که با نیروی عظیم عشق خود، سختی راهی که در بهار زندگی مشترک پیش رویمان بود، هموار نمود و آنچه گمان می رفت سد راهی باشد را به ابزاری امید بخش و یاری رسان بدل نمود، نیز با تمام وجود متشکرم. همچنین از کلیه کسانی که در طی این مسیر مرا از راهنمایی خود بهره مند نمودند ، به ویژه دوستان خوبم آقایان مهندس محسن امینی صالحی و مهندس ابراهیم باقری تشکر و قدردانی می نمایم.

این پایان نامه با پشتیبانی مالی مرکز تحقیقات مخابرات ایران به انجام رسیده است که در همین جا لازم می دانم از همکاری آنها نیز تشکر نمایم. در انتها دست کلیه کسانی که در مرکز تحقیقات مخابرات و کامپیوتر دانشگاه مرا همراهی و همیاری نمودند و با فراهم آوردن امکانات مناسب راهگشای من بودند، را به گرمی می فشارم و از ایشان کمال تشکر را دارم.