1208

استفاده از سیستم دسته‌بندی فازی مبتنی بر جستجوی ممنوعه به منظور تشخیص نفوذ در شبکه‌های کامپیوتری

عبدالحمید مومن‌زاده[۱۳۷]، حمید حاج سید جوادی[۱۳۸]

چکیده

توانایی سیستم‌های فازی در حل مسائل مختلف در تحقیقات گذشته مورد اثبات قرار گرفته است. سیستم فازی مبتنی بر الگوریتم جستجوی ممنوعه روش استدلال تقریبی سیستم‌های فازی را با قابلیت یادگیری روش‌های جستجوی مکاشفه‌ای ترکیب می‌کند. هدف این مقاله اثبات توانایی سیستم فازی مبتنی بر الگوریتم جستجوی ممنوعه به منظور ایجاد یک سیستم تشخیص نفوذ می‌باشد که در کارهای گذشته مورد بررسی قرار نگرفته است. سیستم تشخیص نفوذ فازی مبتنی بر الگوریتم جستجوی ممنوعه ارائه شده قادر خواهد بود تا قوانین دسته‌بندی فازی دقیقی را از داده‌های ترافیک شبکه استخراج نموده و آنها را به منظور تشخیص رفتارهای عادی و نفوذی در شبکه‌های کامپیوتری مورد استفاده قرار دهد. مجموعه داده مورد استفاده قرار گرفته به منظور ارزیابی روش پیشنهادی، **KDD-Cup99** می‌باشد که اطلاعاتی مربوط به رفتارهای عادی و نفوذی شبکه‌های کامپیوتری را در بر دارد. نتایج به دست آمده نشان می‌دهد که روش پیشنهادی، سیستم تشخیص نفوذ کارامدتری نسبت به روش‌های معروف در این زمینه و الگوریتم‌های دسته‌بندی جدید دیگر ایجاد می‌نماید.

کلمات کلیدی

جستجوی ممنوعه، استخراج قوانین فازی، تشخیص نفوذ، دسته‌بندی الگو.

[۱۳۷] momenzadeh.hamid@gmail.com

[۱۳۸] h.s.javadi@cic.aut.ac.ir