وزارت علوم تحقیقات و فناوری
دانشگاه صنعتی سجاد
FEBRUARY 24 ,2018
چهارمین کنفرانس بین المللی
مطالعات نوین درعلوم کامپیوتر و فناوری اطلاعات
4th International Conference
On New studies Of Computer And IT
ISC
Islamic World Science Citation Center
مشهـــــــد
۰۵ اسفند ماه ۱۳۹۶

بررسی و ارزیابی رویکردهای دفاعی سیستم های تشخیص نفوذ الهام گرفته شده از ایمنی بیولوژیک

احسان فرزادنیا [۱]، حسین شیرازی [۲] ، علیرضا نوروزی [۳]

۱-دانشجوی کارشناسی ارشد رایانش امن ، دانشگاه صنعتی مالک اشتر

۲- دانشیار ، دانشگاه صنعتی مالک اشتر

۳- استادیار ، دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف

چکیده

در سالهای اخیر جهت گیری کارهای پژوهشی در زمینه امنیت شبکه به سمت الهام گرفتن از ایده های ناب در طبیعت به منظور حل مسائل پیچیده این حوزه بوده است. در این پژوهش الگوریتم های ایمنی مصنوعی با هدف تحلیل و ارزیابی عملکرد سیستم ایمنی مصنوعی با روشهای مختلف تشخیص نفوذ مبتنی بر داده کاوی ، یادگیری ماشین و الگوریتمهای فراابتکاری الهام گرفته شده از طبیعت مقایسه و ارزیابی شده اند. ارزیابی در نرم افزار استاندارد Weka۳.۶ و دادگان نفوذ NSL-KDD انجام شده است. نتایج آزمایشات نشان می دهند که الگوریتم های الهام گرفته شده از ایمنی مصنوعی علیرغم زمان بالایی که در فاز یادگیری اوّلیه نیاز دارند وابستگی زیادی به تعیین پارامترهای بهینه ورودی داشته و تاثیر کاربرد یک الگوریتم انتخاب ویژگی موثّر به عنوان فاز پیش پردازش ، تغییر محسوسی را در نرخ های عملکردی نشان می دهد. از نتایج آزمایشات اینگونه استنباط می شود که برخی از ضعفهای مهمّ متدهای ایمنی مصنوعی؛ از جمله تعیین حدود آستانه تولید و تکثیر تشخیص دهنده های بالغ و بطور کلّی بحث پارامتردهی بهینه می تواند ضمن ایده ترکیب با سایر رویکردهای یادگیری ماشین نتیجه مطلوب تری را از لحاظ نرخ های خطا و تشخیص ارائه دهد.

کلیدواژه : سیستم تشخیص نفوذ[۱] ، انتخاب ویژگی ، الگوریتمهای فراابتکاری ، سیستم ایمنی مصنوعی ، بهره اطلاعات[۲].

[۱] *intrusion detection system (IDS)*
[۲] *information gain (IG)*