9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

# تشخیص نفوذ در شبکه های کامپیوتری با استفاده از تکنیکهای ترکیبی یادگیری ماشین

**محمد خدایار و علیرضا عصاره**

**۱- دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، گروه کامپیوتر، فارس، ایران**

**۲-دانشکده مهندسی، دانشگاه شهید چمران اهواز، خوزستان، ایران**

Khodayar_Mohammad@yahoo.com

نام ارائه‌دهنده: محمد خدایار

## خلاصه

با توجه به رشد فوق العاده خدمات مبتنی بر شبکه، تشخیص نفوذ به عنوان یک روش مهم جهت ارتقاء امنیت شبکه معرفی شده است. در سیستم های تشخیص نفوذ، نفوذهای غیرمجاز به شبکه با توجه به الگوریتم‌های خاص تشخیص داده‌شده و آن‌ها را به کاربر اطلاع می‌دهد. بطورکلی این الگوریتم‌ها به دو دسته تشخیص سوءاستفاده و آنومالی تقسیم می شود. در این مقاله به ارائه یک روش ترکیبی یادگیری ماشین به منظور تشخیص نفوذ در شبکه می‌پردازد. روش ترکیبی ارائه شده در این مقاله مبتنی بر مفهوم کاهش ابعاد و الگوریتم های درخت تصمیم و روشهای ترکیبی بوده و از دقت ۹۷,۱۹ درصدی برخوردار است. همچنین مجموعه داده به کار گرفته شده در این مقاله مجموعه داده NSL-KDD می باشد که نسبت به مجموعه داده های دیگر که برای سیستم های تشخیص نفوذ استفاده می‌شود از رکوردهای واقعی تری برخوردار است.

**کلمات کلیدی: الگوریتم های یادگیری ماشین، سیستم های تشخیص نفوذ، داده کاوی، درخت تصمیم**

## ۱. مقدمه

نفوذ با انگیزه های متفاوتی سیاسی، مالی، نظامی و حتی نشان دادن مهارت با توجه به نقاط ضعف موجود در برنامه های کاربردی و عیوب نرم‌افزاری ضعف طراحی پروتکل و طراحی سیستم عامل در طی مراحل شناسایی، یافتن نقاط ضعف و بدست آوردن سناریوی نفوذ از جانب نفوذی صورت می‌گیرد. به منظور مقابله با نفوذکنندگان به سیستم ها و شبکه های کامپیوتری، روش های متعددی تدوین شده است که روش‌های تشخیص نفوذ نامیده می‌شود. هدف از تشخیص نفوذ این است که استفاده غیرمجاز، سوءاستفاده و آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری توسط هر دو دسته کاربران داخلی و حمله‌کنندگان خارجی شناسایی شود. سیستم های تشخیص نفوذ[1] به عنوان یکی از عناصر اصلی زیرساخت‌های امنیت در بسیاری از سازمان ها می‌باشد. این سیستم ها، مدل ها و الگوهای سخت افزاری و نرم افزاری می باشند که به خودکار کردن فرایندهایی می‌پردازد که این فرایندها به پایش وقایع رخ داده‌شده در شبکه یا سیستم های کامپیوتری می پردازد. سیستم های تشخیص نفوذ به بررسی و تحلیل این وقایع رخ داده‌شده برای

[1] Intrusion detection systems