

## عنوان مقاله:

شناسایی جریان های مخرب در شبکه با به کارگیری اجماع

## محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری، دوره 6، شماره 2 (سال: 1397)

تعداد صفحات اصل مقاله: 16

## نویسندگان:

حمید پروین - استادیار دانشگاه آزاد اسلامی یاسوج

وحیده رضایی - دانشگاه آزاد اسلامی یاسوج

صمد نجاتیان - دانشگاه آزاد اسلامی یاسوج

روح اله امیدوار - باشگاه پژوهشگران جوان و نخبگان دانشگاه آزاد اسلامی یاسوج

## خلاصه مقاله:

مقوله امنیت در شرایط جدید جهانی ابعاد متفاوتی پیدا کرده است. یکی از حوزه های امنیتی که در شرایط جدید جهانی بسیار مورد اهمیت قرار گرفته است، حوزه امنیت سایبری است. در این تحقیق برای مطالعه بر روی حملات ناشناخته دو هانی نت آزمایشگاهی مجازی در دو مکان مختلف طراحی شده و همچنین از سایر مجموعه داده های علمی استفاده گردیده است. در داده های شبکه ای، مشکل داده های نامتوازن اغلب اتفاق می افتد و موجب کاهش کارایی در پیش بینی برای رده هایی که در اقلیت هستند، می گردد. در این مقاله برای حل این مشکل، از روش های یادگیری جمعی استفاده گردیده است تا بتوان مدلی خودکار ارائه نمود که با استفاده از فنون مختلف و با استفاده از یادگیری مدل، حملات شبکه به ویژه حملات ناشناخته را شناسایی نماید. روش های جمعی، بسیار مناسب برای توصیف مشکلات امنیتی رایانه ای می باشند زیرا هر فعالیتی که در سیستم های رایانه ای انجام می گیرد را می توان در سطوح چند انتزاعی مشاهده کرد و اطلاعات مرتبط را می توان از منابع اطلاعاتی چندگانه جمع آوری نمود. روش تحقیق بر اساس تحلیل های آماری جهت بررسی میزان صحت و درستی نتایج و میزان اتکاپذیری آن ها صورت گرفته است. در این مرحله به کمک فنون و آزمایش های آماری نشان داده شده که عملکرد الگوریتم طراحی شده با رای گیری وزنی پیشنهادی بر اساس الگوریتم ژنتیک نسبت به دوازده طبقه بند دیگر بهتر می باشد.

## کلمات کلیدی:

هانی نت، حملات ناشناخته، یادگیری جمعی، داده های نامتوازن، رای گیری وزنی، آزمایش های آماری

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1008931>

