

## عنوان مقاله:

شناسایی بات نت در شهرهای هوشمند با یادگیری ماشین و انتخاب ویژگی با الگوریتم بهینه سازی آموزش گروهی

## محل انتشار:

هشتمین همایش ملی مطالعات و تحقیقات نوین در حوزه علوم کامپیوتر، برق و مکانیک ایران (سال: 1401)

تعداد صفحات اصل مقاله: 22

## نویسندگان:

محمدرضا جمشیدپورترابی - کارشناسی ارشد، گروه کامپیوتر دانشگاه آزاد اسلامی، واحد ورامین پیشوا مهندسی فناوری و اطلاعات گرایش

محمد مهدی پناهی - دکتری کامپیوتر و دانشگاه آزاد اسلامی، واحد ورامین پیشوا

اکبر مرشداسکی - دکتری کامپیوتر و استاد دانشگاه آزاد اسلامی، واحد ورامین پیشوا

## خلاصه مقاله:

اینترنت اشیاء یک شبکه بزرگ با تعدادی شی هوشمند با قابلیت اتصال به اینترنت است. در این شبکه گره ها در لایه حسگر قرار دارند و برای انجام خدمات ترافیکی را برای لایه مه یا لایه ابر محاسباتی ارسال می کنند. برخی از گره های موجود در اینترنت اشیاء می توانند در معرض بدافزار و ویروس قرار گرفته و به عنوان یک بات نت به فعالیت پردازند. بات نتها در واقع گره های آلوده به بدافزار بوده و می توانند حملاتی نظیر DDoS را بر علیه سرویس های لایه کاربردی اجرا کنند. برای تشخیص حملات به شبکه می توان از سیستم های تشخیص نفوذ به شبکه استفاده نمود اما متأسفانه در بیشتر موارد این سیستم ها به صورت متمرکز تشخیص نفوذ را انجام می دهند و توانایی آنها برای تحلیل ترافیک بزرگ اینترنت اشیاء محدود است. در روش پیشنهادی در این مقاله، یک روش تشخیص حملات بر پایه لایه مه ارایه شده است و سیستم تشخیص نفوذ به صورت غیر متمرکز در گره های مه استقرار پیدا کرده است. روش پیشنهادی برای تشخیص حملات در گره های مه دو فاز دارد. در فاز اول انتخاب ویژگی بر اساس الگوریتم یادگیری گروهی انسان و در فاز طبقه بندی از رای گیری اکثریت استفاده می شود. آزمایشات روی مجموعه داده (NSL-KDD) نشان می دهد روش پیشنهادی در تشخیص حملات بات نت و DDoS دارای دقت، حساسیت و صحتی به ترتیب برابر ۹۹.۵۶٪، ۹۹.۳۴٪ و ۹۹.۲۸٪ است. ارزیابی ها نشان داد روش پیشنهادی در تشخیص بات نت ها از شبکه عصبی چند لایه، درخت تصمیم گیری و ماشین بردار پشتیبان دقت بیشتری در تشخیص حملات دارد. روش پیشنهادی نسبت به الگوریتم ژنتیک بهینه سازی ذرات و روش PBC در تشخیص حملات دارای دقت بیشتری است.

## کلمات کلیدی:

سیستم تشخیص نفوذ اینترنت اشیاء، بات نت، انتخاب ویژگی، رای گیری اکثریت

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1621083>

