یک روش خوشه بندی نیمه نظارتی افزایشی برای تشخیص نفوذ بلادرنگ

سید محمد رضا موسوی[۱۷۹] ، محمد هادی صدرالدینی[۱۸۰] ، منصور ذوالقدری جهرمی[۱۸۱]

چکیده

در مسائل دنیای واقعی مانند تشخیص نفوذ، ماهیت داده ها شناخته شده نیست و به پارامترهای مختلفی همچون زمان وابستگی پیچیده ای دارد. چالش اصلی در سیستم های تشخیص نفوذ، تغییر الگوی حملات است به گونه ای که یک سیستم خبره نمی تواند با سرعت مناسب خود را به روز کند ولی الگوریتمهای خوشه بندی می توانند به ساخت سیستمی تدریجی بهنگام شونده کمک کنند. داده های برچسب خورده و یا مجموعه های از داده ها بدون احتمال نفوذ و از قبل آماده شده برای آموزش سیستم وجود ندارند و بنابراین روشهای دسته بندی به کار نمی آیند.

در روش ارائه شده در این مقاله تنها تعداد معدودی داده برچسب خورده در نظر گرفته می شوند اما مجموعه با حجم مناسبی از ثبت ها برای آموزش سیستم وجود دارند. از آنجا که یادگیرنده ممکن است توسط یک برنامه ریزی برای تغییر تدریجی مراکز خوشه ها فریب بخورد، متغیرهای برای محدود کردن حرکت مرکز خوشه ها اضافه شده اند که به کمک آنها می توان خوشه های حملات جدید را تشخیص داد.

آزمایشات انجام شده نشان می دهند روش مطرح از نظر نرخ تشخیص و مقیاس پذیری قابل توجه است. همچنین برای استفاده در حالت بلادرنگ و بدون تحمیل بار روی خدمت دهنده، پیاده سازی انجام شده بر اساس *k-means*، به دو ماژول همروند تقسیم شده است و در عمل ماژول یادگیرنده تنها از زمان بی استفاده پردازشگر بهره می برد.

کلمات کلیدی

سیستم تشخیص نفوذ، داده کاوی، خوشه بندی، تشخیص ناهنجاری، داده برچسب خورده، *k-means*، *KDD99*

[179] بخش مهندسی و علوم کامپیوتر، دانشکده مهندسی دانشگاه شیراز mmoosavi@cse.shirazu.ac.ir

[180] بخش مهندسی و علوم کامپیوتر، دانشکده مهندسی دانشگاه شیراز sadredin@shirazu.ac.ir

[181] بخش مهندسی و علوم کامپیوتر، دانشکده مهندسی دانشگاه شیراز zjahromi@shirazu.ac.ir