عنوان فارسی مقاله :

# مطالعه تطبیقی مدل مخفی مارکوف و ماشین بردار پشتیبان در تشخیص نفوذ آنومالی

عنوان انگلیسی مقاله :

# A Comparative Study of Hidden Markov Model and Support Vector Machine in Anomaly Intrusion Detection


## توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

**6. Conc sions**

This paper presents a comparative study of HMM and SVM in anomaly intrusion detection. A new method of identifying distinguishable TCP services using J48 decision tree algorithm is introduced. In the HMM based anomaly intrusion detection, each of distinguishable TCP service is associated with a decision tree that consists of features and their values presented in the KDD Cup 1999 dataset. These features are then selected for training HMM model for each TCP session of the dataset using BWT and VT algorithms. Evaluation of trained model is performed with Forward and Backward algorithms. In the SVM case, SMO algorithm of Weka is used with kernel functions at the time of training and evaluation of SVM model of each TCP service.
Both HMM and SVM methods show similar results with SVM showing marginally improved anomaly detection. However, SVM based training requires all the training data set to be applied at a time. This will preclude large training dataset. HMM based training is per TCP session and there are no such restrictions.

6
نتایج
در تشخیص نفوذ SVM و HMM مقاله حاضر مطالعه تطبیقی TCP آنومالی را مطرح می کند. روش جدید شناسایی سرویس های معرفی شده است. J48 تمیز دادنی با استفاده از الگوریتم درخت تصمیم هر یک از سرویس های HMM، در تشخیص نفوذ آنومالی مبتنی بر تمیزدادنی با یک درخت تصمیم ارتباط دارند که از ویژگیها و TCP مقادیر مطرح شده در مجموعه داده تشکیل می شود. سپس این مجموعه TCP برای هر نشست HMM ویژگیها برای آموزش مدل انتخاب می شوند. VT و BWT داده با استفاده از الگوریتم های ارزیابی مدل آموزش دیده با الگوریتم های پیشرو و پسرو انجام می با توابع کرنل در SMO Weka از الگوریتم SVM، شود. در مورد استفاده می TCP هر سرویس SVM زمان آموزش و ارزیابی مدل شود.
نشان می دهند که SVM نتایجی مشابه با SVM و HMM روشهای تشخیص آنومالی بهبود یافته در حاشیه را نشان می دهد.اما آموزش مستلزم کاربرد کل مجموعه داده های آموزشی به SVM مبتنی بر یکباره می باشد. این مسئله جلوی کار مجموعه داده آموزشی بزرگ را انجام شده و TCP در هر نشست HMM می گیرد.آموزش مبتنی بر چنین محدودیت هایی وجود ندارد.