Chronic Poisoning against Machine Learning Based IDSs Using Edge Pattern Detection

Submitted by grigby1 on Wed, 05/01/2019 - 10:33am

Title	Chronic Poisoning against Machine Learning Based IDSs Using Edge Pattern Detection
Publication Type	Conference Paper
Year of Publication	2018
Authors	Li, P., Liu, Q., Zhao, W., Wang, D., Wang, S.
Conference Name	2018 IEEE International Conference on Communications (ICC)
Date Published	may
ISBN Number	978-1-5386-3180-5
Keywords	Batch-EPD Boundary Pattern detection algorithm, big data era, chronic poisoning attack, composability, Data models, detection algorithms, edge detection, Edge Pattern Detection algorithm, edge pattern points, Image edge detection, Intrusion detection, Intrusion Detection Systems, learning (artificial intelligence), machine learning, machine learning algorithms, Metrics, pubcrawl , resilience, Resiliency, Scalability, security, security of data, security threats, Training data

Abstract

In big data era, machine learning is one of fundamental techniques in intrusion detection systems (IDSs). Poisoning attack, which is one of the most recognized security threats towards machine learning-based IDSs, injects some adversarial samples into the training phase, inducing data drifting of training data and a significant performance decrease of target IDSs over testing data. In this paper, we adopt the Edge Pattern Detection (EPD) algorithm to design a novel poisoning method that attack against several machine learning algorithms used in IDSs. Specifically, we propose a boundary pattern detection algorithm to efficiently generate the points that are near to abnormal data but considered to be normal ones by current classifiers. Then, we introduce a Batch-EPD Boundary Pattern (BEBP) detection algorithm to overcome the limitation of the number of edge pattern points generated by EPD and to obtain more useful adversarial samples. Based on BEBP, we further present a moderate but effective poisoning method called chronic poisoning attack. Extensive experiments on synthetic and three real network data sets demonstrate the performance of the proposed poisoning method against several well-known machine learning algorithms and a practical intrusion detection method named FMIFS-LSSVM-IDS.

URL https://ieeexplore.ieee.org/document/8422328

DOI 10.1109/ICC.2018.8422328

Citation Key li_chronic_2018

Batch-EPD Boundary Pattern detection algorithm big data era chronic poisoning attack composability Data models detection algorithms edge detection Edge Pattern Detection algorithm edge pattern points Image edge detection Intrusion Detection Intrusion Detection Systems learning (artificial intelligence) machine learning machine learning algorithms Metrics pubcrawl resilience Resiliency Scalability security security of data security threats Training data