Abstract 98 – Paper ID: 123

Detection of Attacks in Wireless Sensor Networks Using Unsupervised Learning Approach

Hanjabam Saratchandra Sharma[1], Moirangthem Marjit Singh[1], Arindam Sarkar[1]

[1]Manipur Technical University, Imphal, Manipur, India
[2]North Eastern Regional Institute of Science and Technology, Itanagar, Arunachal Pradesh, India
[3]Ramakrishna Mission Vidyamandira, Belur Math, West Bengal, India

Email: sarat.hanjabam@gmail.com

Abstract

This paper presents an unsupervised machine learning based attack detection approach for wireless sensor networks (WSNs). Two unsupervised methods, namely Fuzzy–c–means (FCM) and K–means clustering, are employed. Principal Component Analysis (PCA) is implemented in both methods as a feature selection technique. The models are trained and tested on the WSN–DS and KDD Cup 99 datasets. These datasets are originally labeled, and by removing the labels they are transformed into unlabeled datasets. The proposed unsupervised learning approach is then applied to these unlabeled datasets, and the number of clusters is finally validated using the original labeled datasets. The attack types considered include blackhole, grayhole, flooding, TDMA, probe, U2R, and R2L.

Unsupervised learning methods present several constraints when compared with attack detection models based on supervised learning paradigms. These limitations include explicit reliance on label–free techniques such as FCM and K–means, making comprehensive performance evaluation challenging. The lack of labeled data reduces accuracy and other critical performance metrics. In addition, the K–means clustering algorithm exhibits high sensitivity to initial conditions, where different initializations may lead to varying and unstable clustering results. Despite these limitations, unsupervised learning methods such as clustering algorithms can identify anomalies without labeled data, which is particularly important in WSNs where obtaining labeled data for all possible attack scenarios may not be feasible. The proposed models are evaluated using metrics such as TPR, NPV, PPV, TNR, FPR, FDR, and FNR. The results indicate that the model employing Fuzzy–c–means clustering outperforms the model based on K–means clustering.

Keywords: Wireless sensor networks, Unsupervised learning, Attack detection, Fuzzy–c–means, K–means clustering

ISBN: 978-81-989164-2-6; DOI: 10.21467/abstracts.8.1