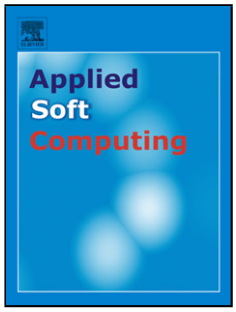

Title: Incorporating unsupervised learning into intrusion detection for wireless sensor networks with structural co-evolvability

Authors: Hongchun Qu, Zeliang Qiu, Xiaoming Tang, Min Xiang, Ping Wang

PII: S1568-4946(18)30432-0
DOI: https://doi.org/10.1016/j.asoc.2018.07.044
Reference: ASOC 5012

To appear in: *Applied Soft Computing*

Received date: 17-7-2017
Revised date: 18-7-2018
Accepted date: 20-7-2018

Please cite this article as: Qu H, Qiu Z, Tang X, Xiang M, Wang P, Incorporating unsupervised learning into intrusion detection for wireless sensor networks with structural co-evolvability, *Applied Soft Computing Journal* (2018), https://doi.org/10.1016/j.asoc.2018.07.044

Incorporating unsupervised learning into intrusion detection for wireless sensor networks with structural co-evolvability

Hongchun Qu*, Zeliang Qiu, Xiaoming Tang, Min Xiang, Ping Wang
Key Laboratory of Industrial Internet of Things & Networked Control, Ministry of Education, College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

* Corresponding author: Hongchun Qu, ORCIDID: orcid.org/0000-0001-7623-2383
Email: hcchyu@gmail.com

Highlights

- Unknown attacks detection for wireless sensor networks without any prior knowledge
- Better balance between detection rate and false alarm rate
- Detection process and result are not sensitive to network structures
- The ability to co-evolve with network dynamics

Abstract: Wireless sensor networks (WSNs) are vulnerable to many security threats because of the open and unreliable communication channels, the highly dynamic network structure as well as the decentralized management scheme. It is therefore, quite challenging to build an intrusion detection system that can detect various unknown attacks, reach better balance between detection rate and false alarm rate and increase the adaptivity to network dynamics, particularly for a resource-constraint WSN. In this paper, we proposed a knowledge-based intrusion detection strategy (KBIDS) to bridge the gap. We firstly used the Mean Shift Clustering Algorithm (MSCA), an unsupervised learning scheme to distinguish undefined abnormal patterns which reflect the abnormal behavior of a WSN being attacked from the normal context; then we employed a support vector machine to maximize the margin between abnormal and normal features so that the classification error can be minimized, which in turn to effectively enhance the detection accuracy; finally, we adopted a feature updating strategy to reflect network dynamics so that the system can co-evolve with the network change. Then, the validation of KBIDS in both network emulator and the real environment were conducted and analyzed. Results showed that KBIDS had achieved the highest detection rate and the lowest false alarm rate among several state-of-the-art intrusion models. In addition to that, we also conducted some parameter sensitivity analyses to help identifying the optimal configuration which can be used to parameterize KBIDS in real applications.

Keywords: wireless sensor network, machine learning, intrusion detection, clustering, support vector machine

1. Introduction

Wireless Sensor Networks (WSNs) have been widely used in many critical fields, such as control and surveillance in manufactory and power grid, military and intelligence deployment [1]. However, they are vulnerable to many security threats [2] because of their open and unreliable communication channels, highly dynamic network structure due to node mobility as well as decentralized management scheme.