Anomaly Detection for Mobile Devices in Industrial Internet

Ge Ma, Weixi Gu, Qiyang Huang, Guowei Zhu, Kan Lv and Yujia Li
China Academy of Industrial Internet, Beijing, China

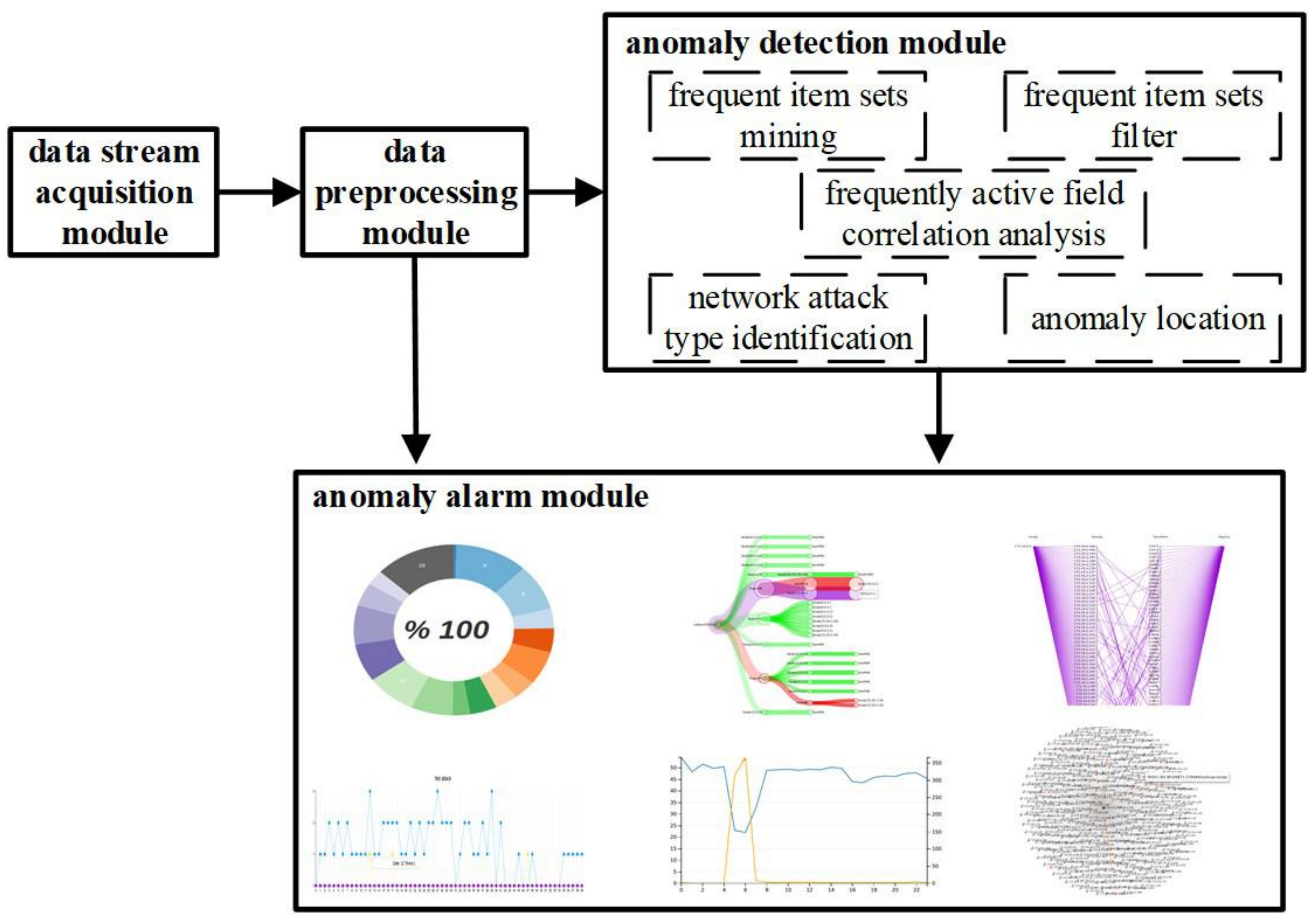
Abstract

With the development of the Industrial Internet, some criminals launch attacks on industrial control terminals (such as computers and mobile devices), causing the failure of industrial control terminals or wrong instructions, which resulting in factory losses. Therefore, there is an immediate need to extract valuable information from mobile network streaming, accurately detect abnormal behaviors and timely raise the alarm. We propose a method of anomaly detection for mobile devices in Industrial Internet based on knowledge graph and demonstrate the results by using visualization technology.

Introduction

- Background
  - The Industrial Internet, as a product of the deep integration of new-generation information technology and manufacturing, results in expanding the boundaries of cyberspace and function.
  - The Industrial Internet breaks the traditional structure of industrial control systems by using mobile networks, exposing a large number of security issues.
  - Reports on industrial information security issued by various countries show that the current network security risks are constantly shifting to the industrial field.
  - Content providers are pushing content to the edge networks, by using edge-network access points for content delivery.
- Solution
  - We propose a method of anomaly detection for mobile devices based on frequent item sets. This method uses a data mining algorithm based on knowledge graph to analyze the obtained mobile network data stream and detect anomalies. To demonstrate the effectiveness of our method, we design an anomaly detection system.

System



data stream acquisition module → data preprocessing module → anomaly detection module

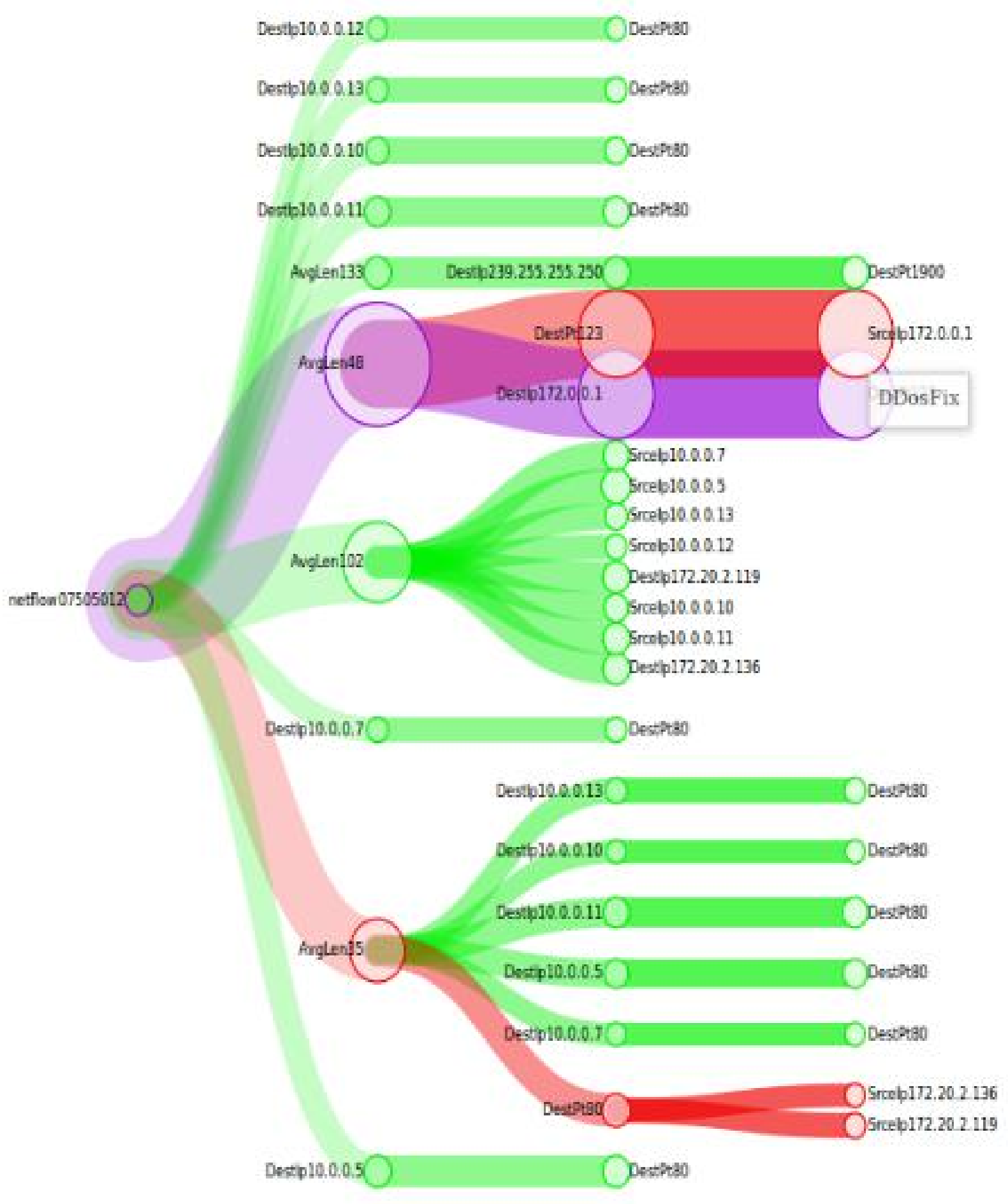
anomaly detection module: frequent item sets mining; frequent item sets filter; frequently active field correlation analysis; network attack type identification; anomaly location

anomaly alarm module

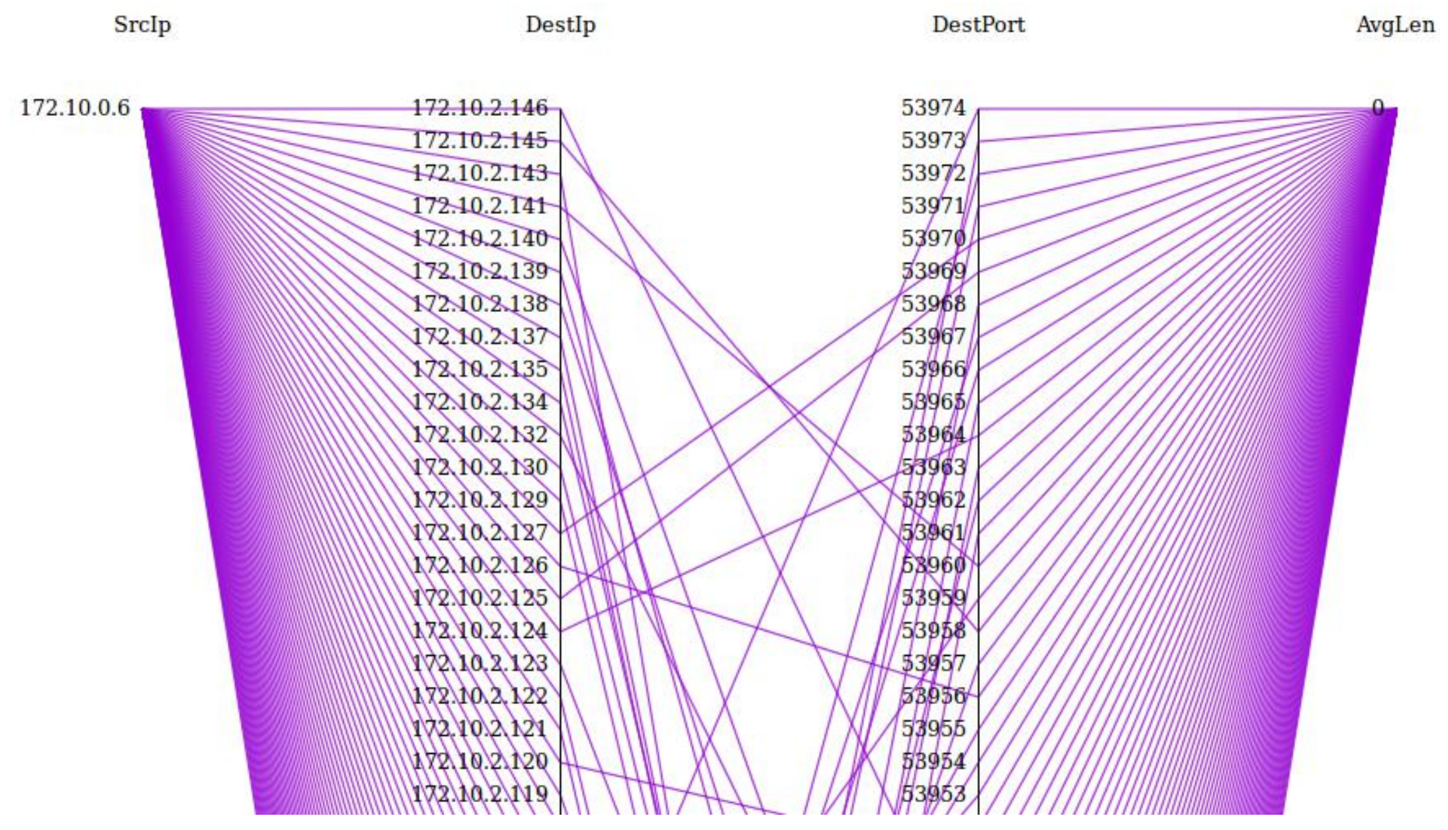
- The anomaly detection system consists of four components: mobile network data stream acquisition module, data preprocessing module, mobile network anomaly detection module based on frequent item sets and anomaly alarm module.
  - The mobile network data flow acquisition module is responsible for fetching network packets from the server where DPDK has been deployed.
  - The data preprocessing module is responsible for the string segmentation of the data set obtained from the server according to the separators (such as space, comma) to obtain the data format of a specific format.
  - The mobile network anomaly detection module based on frequent item sets investigate valuable information to detect the anomaly, identify the type of attack, and locate the attacker and victim. The module is mainly composed of five sub-modules: (i) mining submodule; (ii) filter submodule; (iii) correlation analysis module; (iv) network attack type identification submodule; (v) anomaly location submodule.
  - The anomaly alarm module displays the preprocessed data and the results of anomaly detection to the user in the form of dynamic charts.

Contact: Ge Ma, mage@china-aii.com

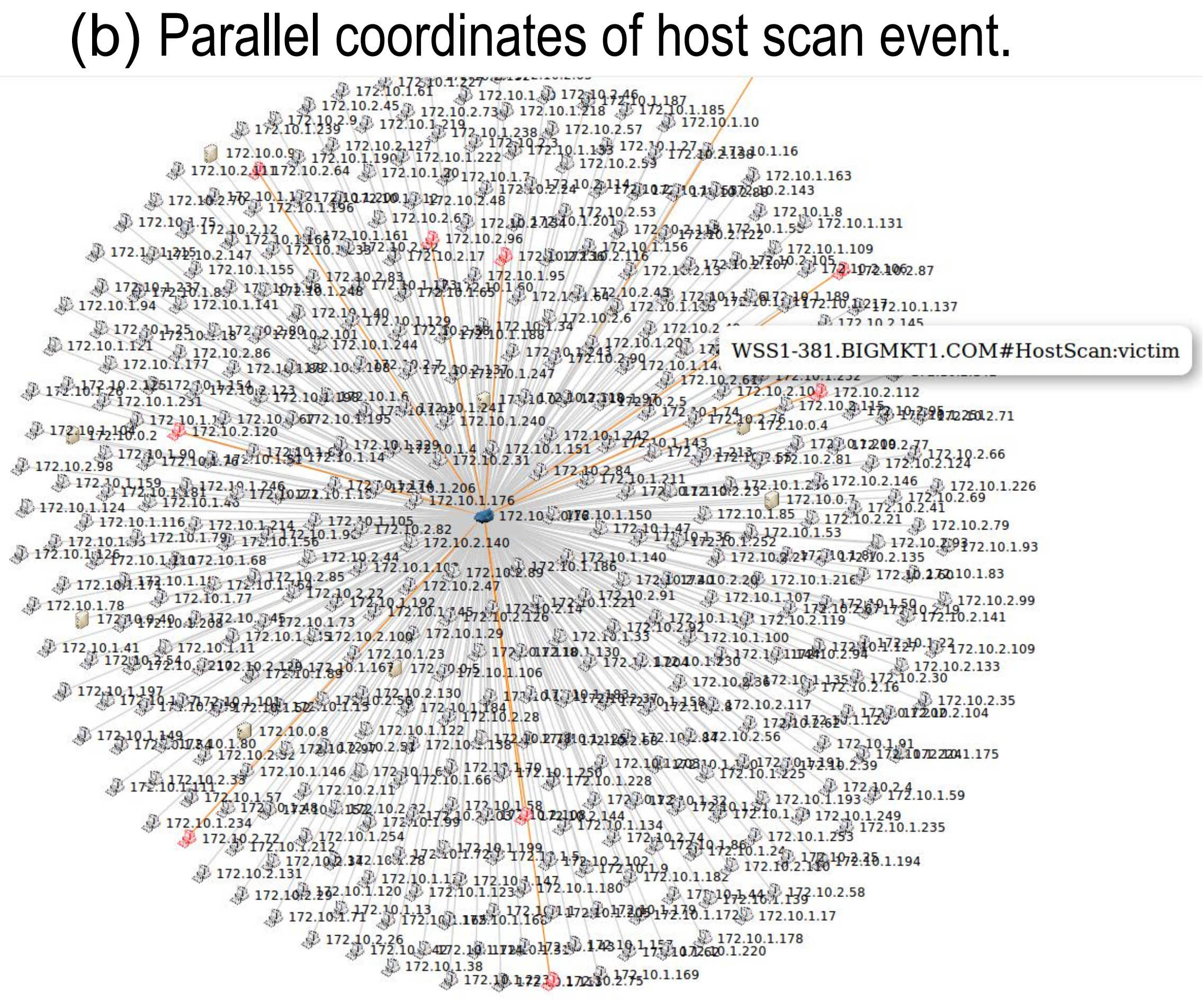
Results



(a) The concurrency of attack events within one second. The green branches indicate a secure network data flow, and the red branches indicate that an abnormal condition (usually information collection) has occurred in the network. This activity usually occurs in the early stages of a network attack. The purple branches indicate that serious network attacks such as DDoS and worms have occurred.



(b) Parallel coordinates of host scan event.



(c) Network topology with anomalous locations (red point indicates the IP of the victim).

The number of host scanning attacks, worm attacks, backscatter attacks, port-fixed DDoS attacks, and port-variable DDoS attacks detected by our method are 158, 3, 133, 2, 0, respectively. The number of the above anomalies detected by the traditional algorithm PCAV is 149, 3, 132, 1 and 0, respectively. Experiments show that our method can detect more attacks.

Conclusion & Future Work

We propose a new method to alarm network attacks for mobile networks in Industrial Internet. Our experiments have shown the promising avenue of anomaly detection in mobile network. For future work, we plan to optimize the speed of data collection and anomaly detection to achieve real-time detection. In addition, we plan to combine machine learning to increase the number of types of network attacks that can be detected by our method.