Multi-layer Filtering for the Management of Alerts in Intrusion Detection Systems

Mahboobeh Soleimani and Ali A. Ghorbani
Faculty of Computer Science
University of New Brunswick

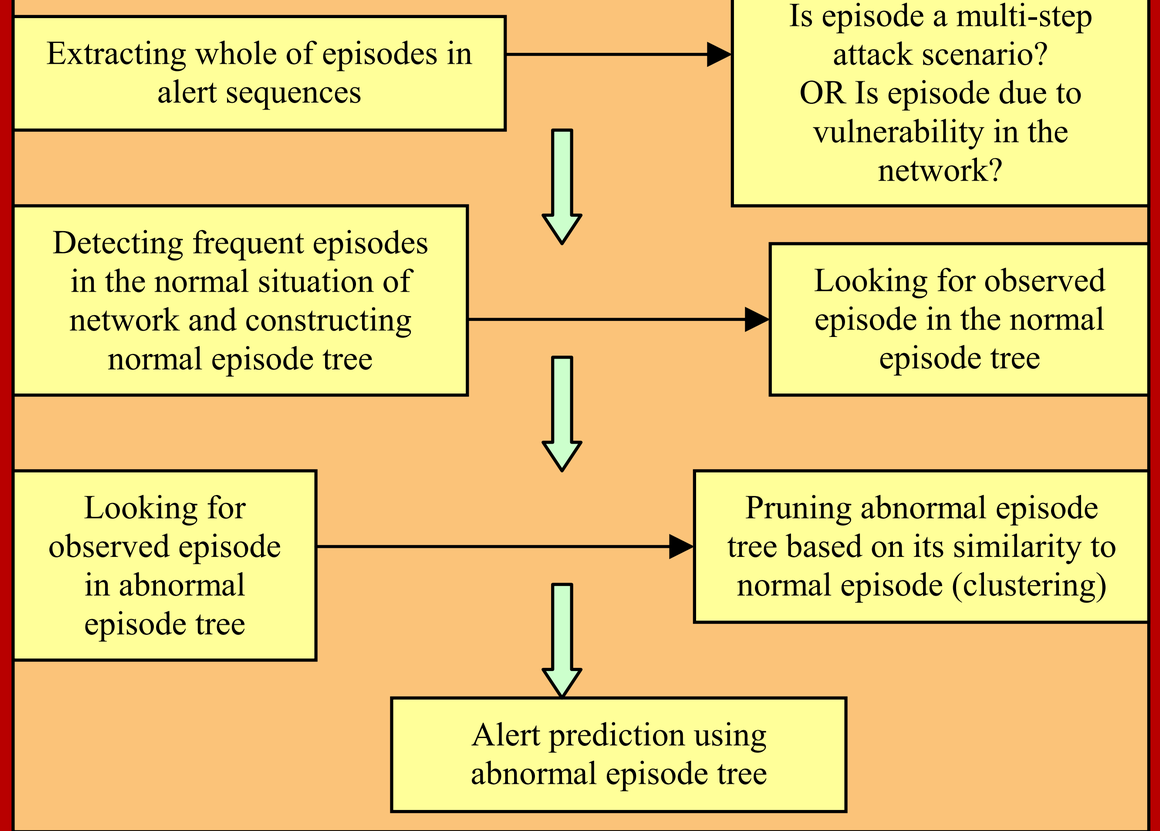
Motivation

Often Intrusion Detection Systems (IDSs) generate too many alerts in a typical network. Managing this huge amount of alerts and finding the important ones are the main goals of this research.

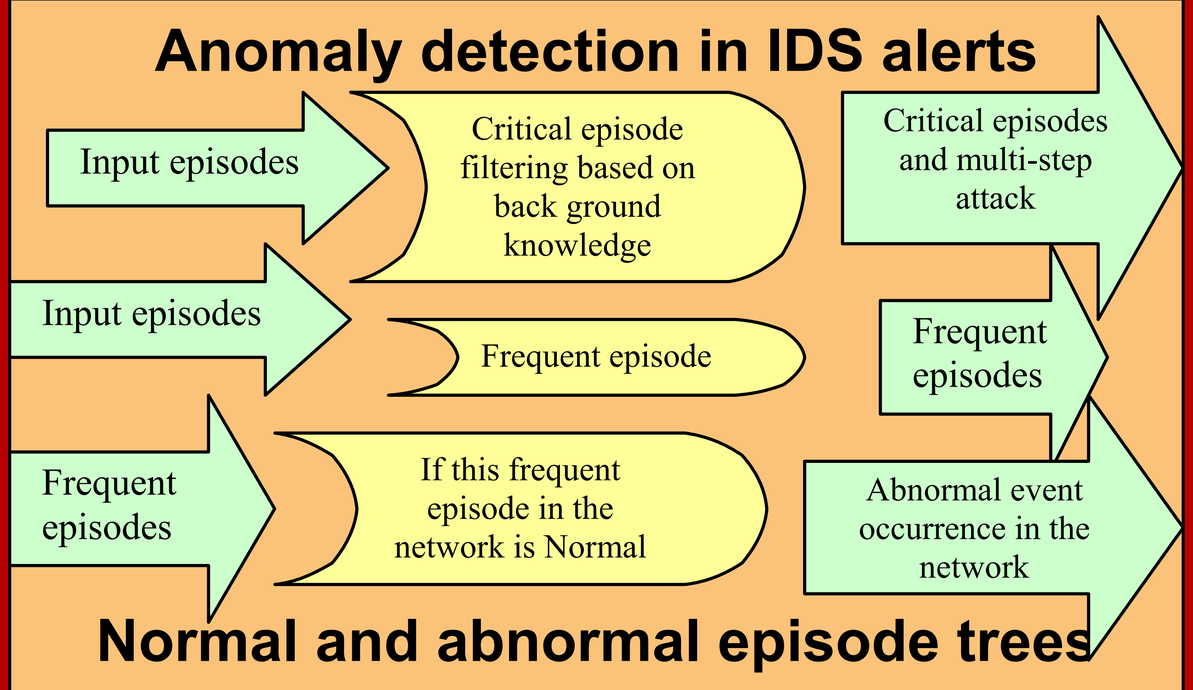
Methodology

- Multi-filtering approach for identifying critical alerts in a network, based on expert knowledge and machine learning methods.
- Determining normal behaviour of security devices and consequently normal alerts that are triggered frequently by an IDS in a particular network.
- Comparing normal behaviour with current frequent alerts that are generated by an IDS in the network to identify those alerts in the network which are more interesting for administrator.
- Using a combination of signature based IDS and an anomaly-based framework in our framework.
- Applying “Discovery of frequent episodes in event Sequences” algorithm for alert mining.

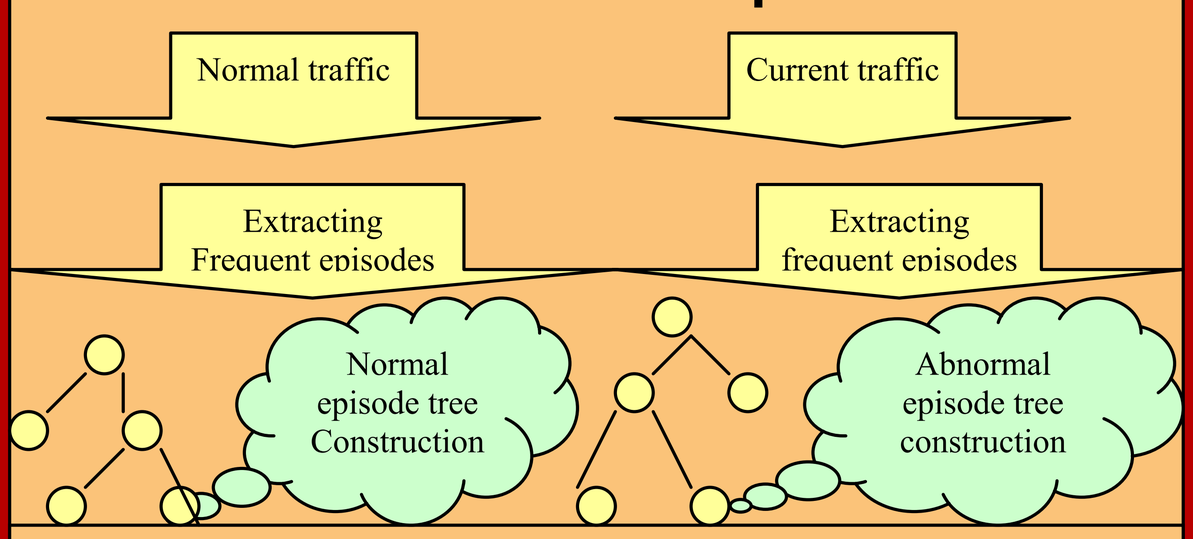
Multi-step filtering for alert reduction



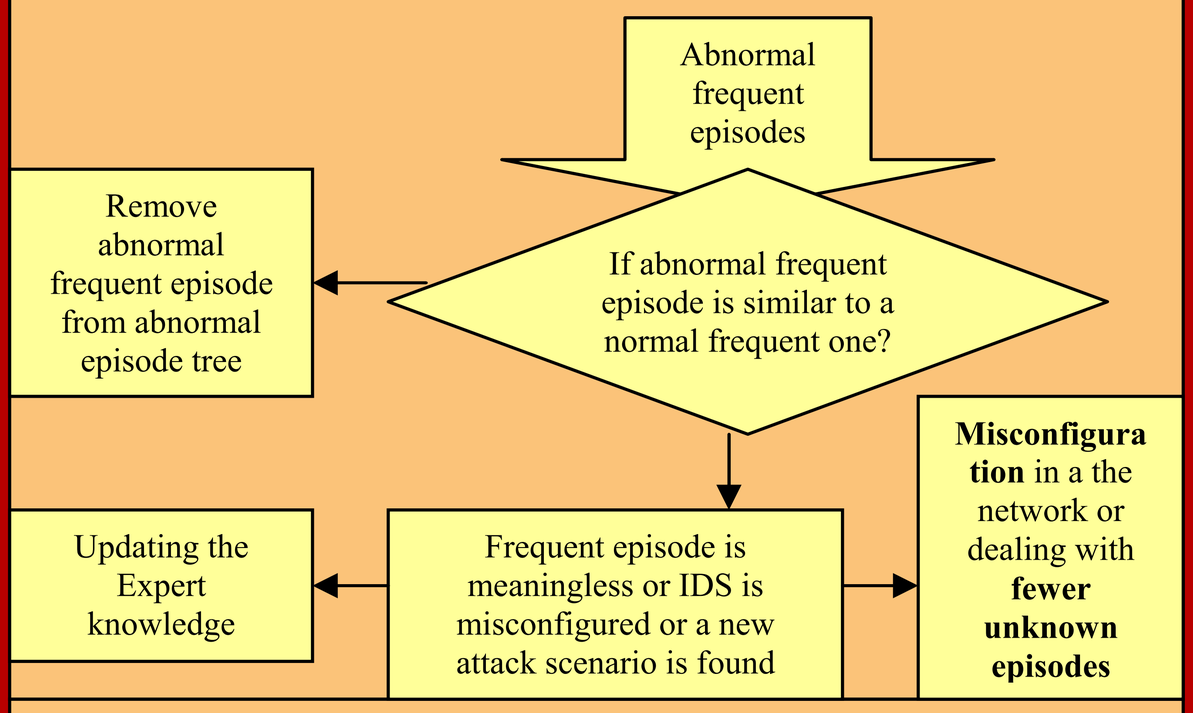
Anomaly detection in IDS alerts



Normal and abnormal episode trees



Clustering and pruning abnormal episodes tree



Episode rule extraction for attack prediction

Support (X) *= Percentage of alert sequences that contain alert X.*

Rule: X→ Y (s, c)

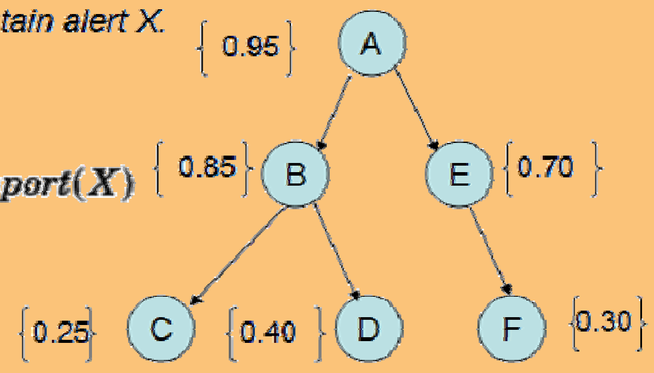
$$s = support(X \cup Y)$$

$$c = support(X \cup Y)/support(X)$$

Support , Confidence

A → B, [0.85, 0.89]

AE → F, [0.30, 0.42]



Results

Our method could extract all of critical and multi-step attacks in LL DDoS 1.0 data set while we had almost 90% reduction in number of alerts.