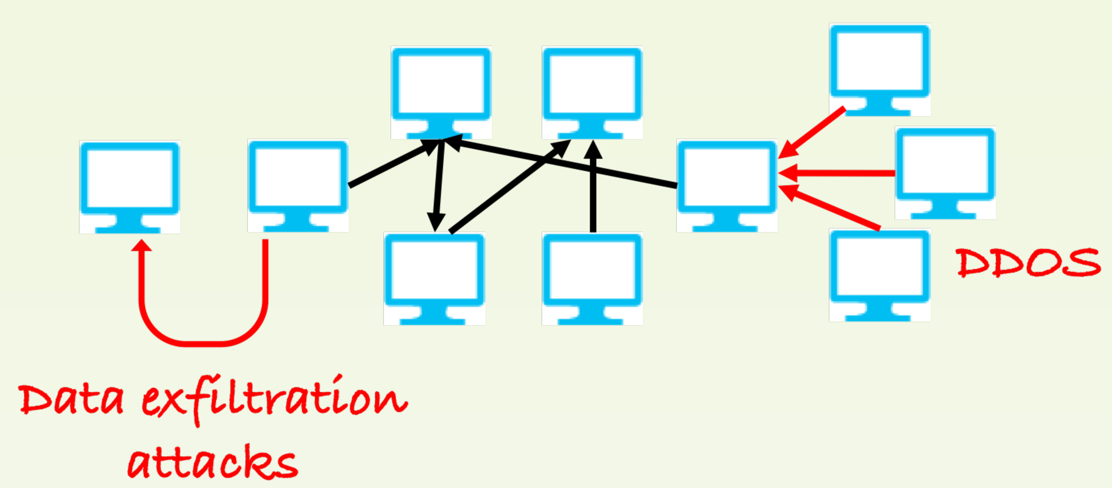
Fast and Accurate Anomaly Detection in Dynamic Graphs with a Two-Pronged Approach

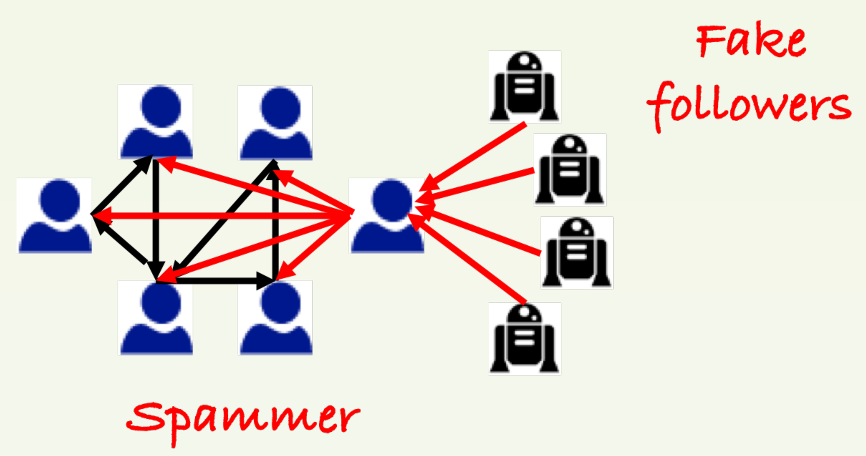
Minji Yoon, Bryan Hooi, Kijung Shin, and Christos Faloutsos

Carnegie Mellon University

Introduction

Many network-based systems including computer networks and social networks services have been a focus of various attacks.





Various approaches have focused on static graphs. But graphs are dynamic with node/edge insertion/deletion.
Then how can we detect anomalies on dynamic graphs?

Anomalies in Dynamic Graphs

Definition 1 (Structure Change)
If a node u changes the destination of Δm of its out-edges from previous neighbors $v_1, \ldots, v_{\Delta m}$ to new neighbors $v'_1, \ldots, v'_{\Delta m}$, we call the change a structure change of size Δm.

With abnormally large Δm, a structure change becomes an **AnomalyS**. To detect AnomalyS, we need to focus on the existence of edges between two nodes, rather than the number of occurrences of edges between two nodes.

Definition 2 (Edge Weight Change)
If a node u adds/subtracts Δm out-edges to neighbor node v, we call the change an edge weight change of size Δm.

With abnormally large Δm, an edge weight change becomes an **AnomalyW**. In contrast to AnomalyS, we focus on the number of occurrences of each edge, rather than only the presence or absence of an edge.

Node Score Functions for Detecting AnomalyS and AnomalyW

Define the row-normalized unweighted adjacency matrix A_s, a starting vector b_s which is an all-$\frac{1}{n}$ vector of length n and the damping factor c.
(n denotes the number of nodes)

Definition 3 (ScoreS)
ScoreS node score vector p_s is defined by the following iterative equation:
$$p_s = cA_s^T p_s + (1-c)b_s$$

To deal with edge weight in AnomalyW, we use the weighted adjacency matrix A_w instead of A_s.
We introduce an out-degree proportional starting vector b_w, (i.e. setting the initial scores of each node proportional to its outdegree).

Definition 4 (ScoreW)
ScoreW node score vector p_w is defined by the following iterative equation:
$$p_w = cA_w^T p_w + (1-c)b_w$$

$A_w(i,j)$ is the edge weight from node i to node j.
$b_w(i)$ is m_i/m, where m_i denotes the total edge weight of out-edges of node i, and m denotes the total edge weight of the graph.

We estimate changes in ScoreS/W induced by a structure change/an edge change (Definition 1,2). Then we compare the changes with those in ScoreS/W to prove **the suitability of ScoreS for detecting AnomalyS and ScoreW for detecting AnomalyW**, respectively.

Metrics for AnomalyS and AnomalyW

We discretize the first and second order derivatives of ScoreS vector p_s as follows:
$$p'_s = [p_s(t+\Delta t) - p_s(t)] / \Delta t$$
$$p''_s = [(p_s(t+\Delta t) - p_s(t)) - (p_s(t) - p_s(t-\Delta t))] / \Delta t^2$$

Definition 5 (AnomRankS)
Given ScoreS vector p_s, AnomRankS a_s is an $(n \times 2)$ matrix $[p'_s\ p''_s]$, concatenating 1st and 2nd derivatives of p_s.
The AnomRankS score is $\|a_s\|_1$.

We discretize the first and second order derivatives ScoreW vector p_w as follows:
$$p'_w = [p_w(t+\Delta t) - p_w(t)] / \Delta t$$
$$p''_w = [(p_w(t+\Delta t) - p_w(t)) - (p_w(t) - p_w(t-\Delta t))] / \Delta t^2$$

Definition 6 (AnomRankW)
Given ScoreW vector p_w, AnomRankW a_w is a $(n \times 2)$ matrix $[p'_w\ p''_w]$, concatenating 1st and 2nd derivatives of p_w.
The AnomRankW score is $\|a_w\|_1$.

Dataset

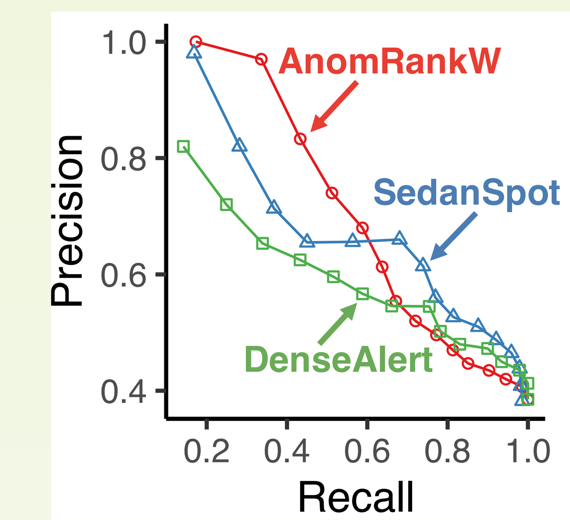
DARPA has 4.5M IP-IP communications between 9.4K source IP and 2.3K destination IP over 87.7K minutes. Each communication is a directed edge (srcIP, dstIP, timestamp, attack).

ENRON contains 50K emails from 151 employees over 3 years in the ENRON Corporation. Each email is a directed edge (sender, receiver, timestamp).

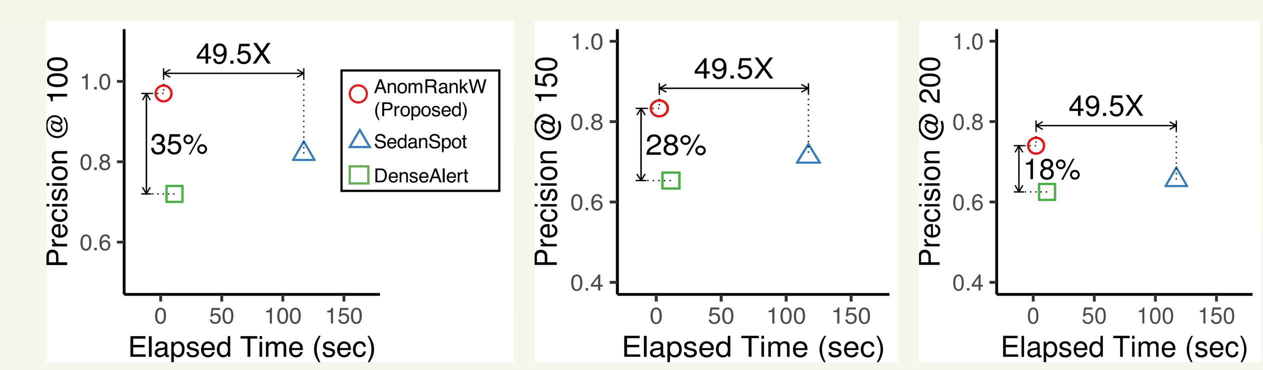
See paper for more: online approach, theoretical guarantees, experiments on synthetic dataset
Code: *https://github.com/minjiyoon/anomrank*

Experiments

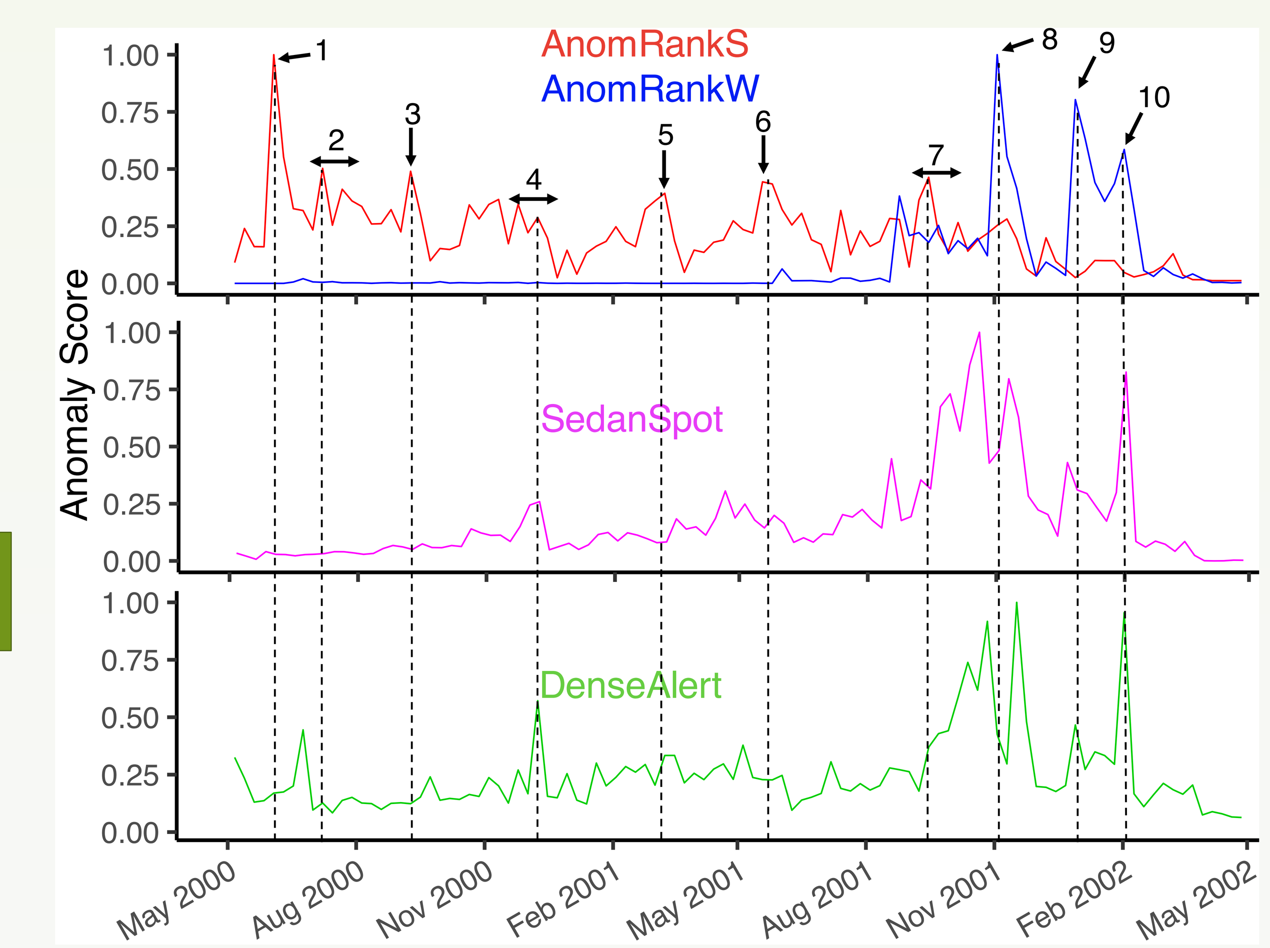
Precision vs. Recall on DARPA



Accuracy vs. Speed on DARPA



Two-Pronged Approach pays off on ENRON



AnomRank localizes the culprits of anomalous events in DARPA