



SNAPSKETCH: Network Representation Approach for Anomaly Detection in Dynamic Network

- Identify denial of service attacks, port scans, and other cyber-attacks using network graphs.
- Unique approach that identifies anomalous hotspots by tracking sudden increases/decreases edges connecting to a vertex; or the sudden (dis)appearance of edges with high weight
- The proposed **SNAPSKETCH** approach is fully unsupervised, has constant memory space usage, and can be used for real-time anomaly detection.

Problem Statement and Goals

Problem Statement

Given a graph stream $G_s = \{G_1, G_2, \dots, G_t, \dots\}$, our goal is to learn a graph representation function f for each graph $G_t \in \mathbb{R}^{|V|^2}$ such that $f : G_t \rightarrow v_{G_t} \in \mathbb{Z}^d$ and $d \ll |V|^2$ and using v_{G_t} detect whether a graph G_t at any time t contain an anomalous hotspot.

Goals

- Generate a fixed-size feature vector (**SNAPSKETCH**) to represent a graph in a graph stream.
- Detect DoS attack (a type of anomalous hotspot) in network traffic using a **SNAPSKETCH**.

Approach

- Perform node2vec [1] random walk and construct n-shingles.
- Project discriminative shingles into a d-dimensional projection.
- Sketch graphs using a simplified hashing of projection vector and the cost of shingles.
- Detect anomalous hotspot using RRCF [2] in sketch vector.

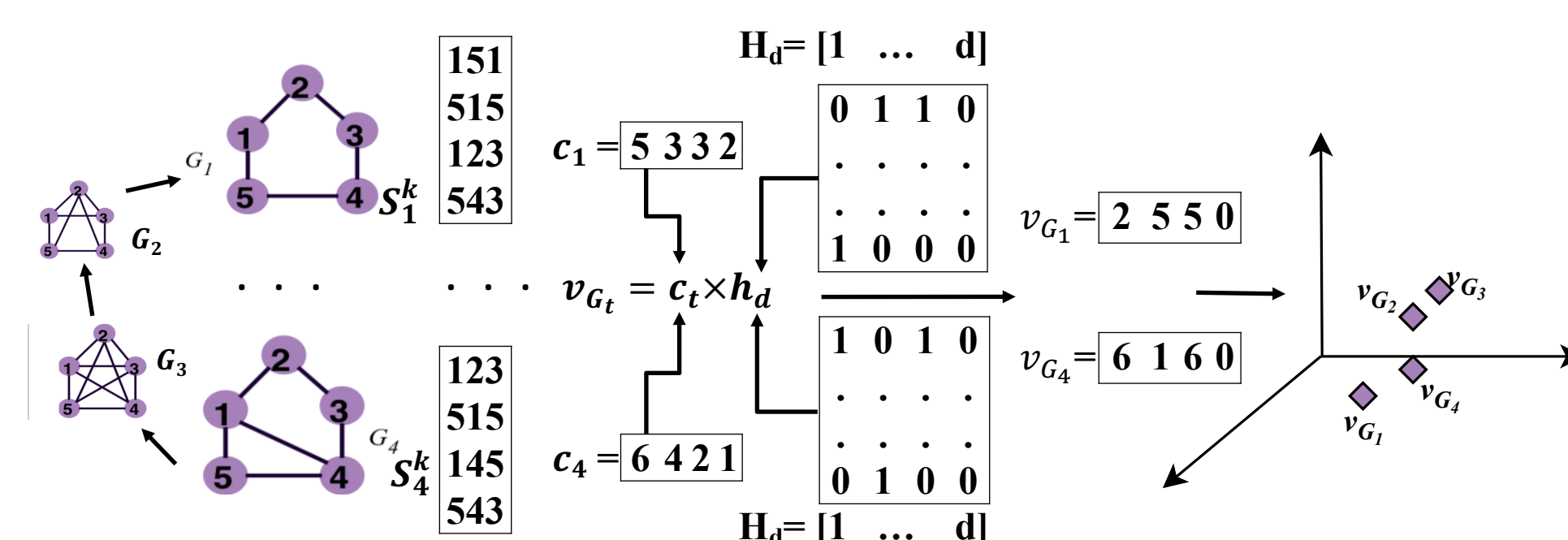


Fig 1: **SNAPSKETCH** Framework

Results

DoS Attack Detection Result:

- Smart Home IoT Traffic Data** - 95% precision and 93% recall (in 100 most severe DoS attack graphs).
- DARPA 1998 Data**- 83% precision and 82% recall (in 100 most severe DoS attack graphs).

Future Work:

Integrate structural information into **SNAPSKETCH** for better representation.

Acknowledgement:

Advisor Dr. William Eberle

References:

- Grover, Aditya and Leskovec, Jure. "node2vec: Scalable feature learning for networks." In "Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining," pages 855-864. ACM, 2016.
- Guha, Sudipto, Mishra, Nina, Roy, Gourav, and Schrijvers, Okke. "Robust random cut forest based anomaly detection on streams." In International conference on machine learning," pages 2712-2721, 2016.

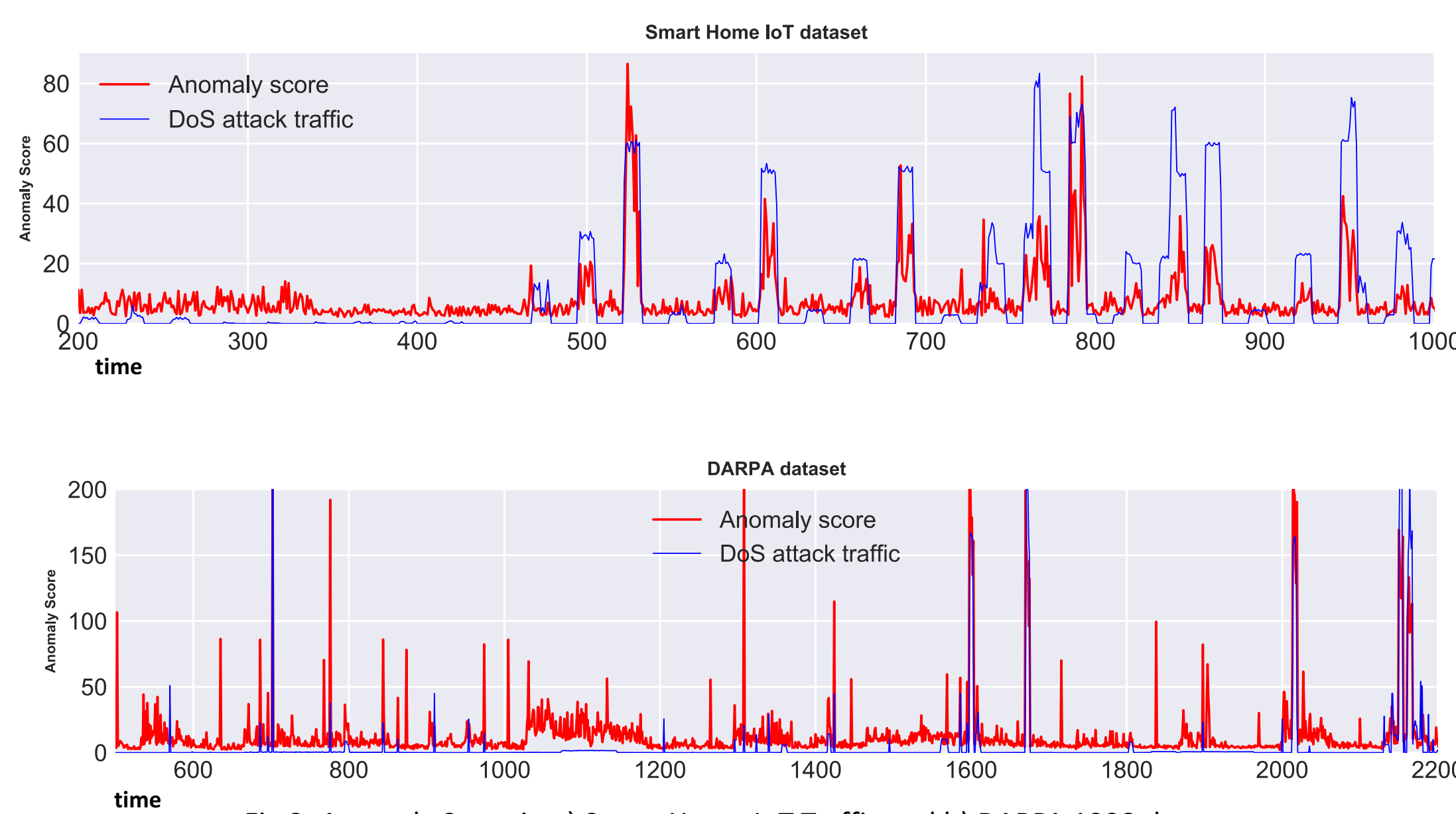


Fig 2: Anomaly Score in a) Smart Home IoT Traffic and b) DARPA 1998 dataset.