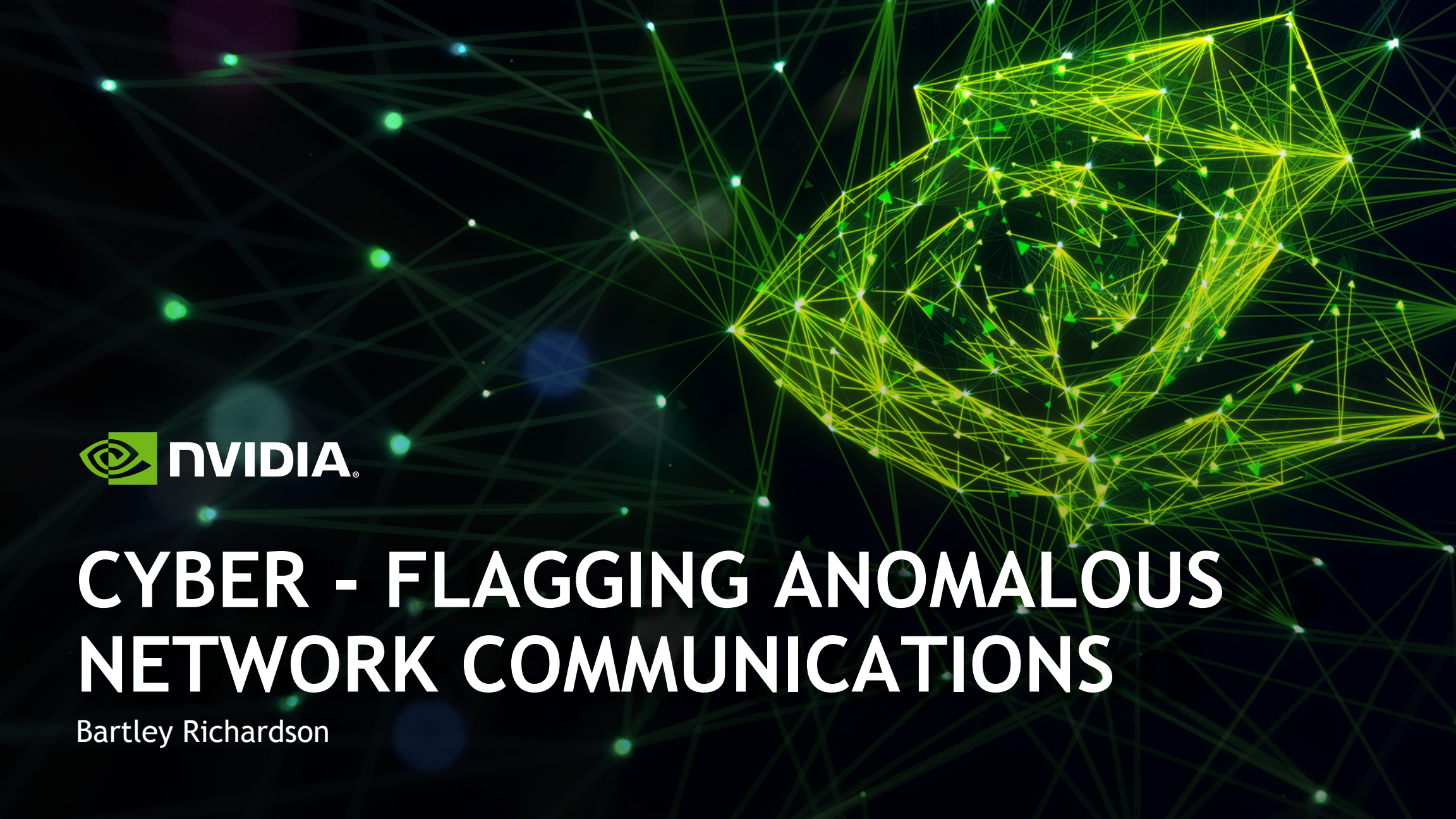

CYBER - FLAGGING ANOMALOUS NETWORK COMMUNICATIONS

Bartley Richardson

OVERVIEW

Computer networks generate massive amounts of heterogeneous data as users interact with other users, computers, and services. These interactions can be modeled as large, heterogeneous property graphs, with multidimensional characteristics of the communication embedded on an edge connecting nodes. Current techniques to identify subgraph evolution over time and extract anomalies require lengthy compute times or necessitate significant pre-filtering of the graph. In this tutorial, we showcase an approach to flagging anomalous network communications in a large graph using a combination of structural graph features and graph analytics, running end-to-end in RAPIDS.