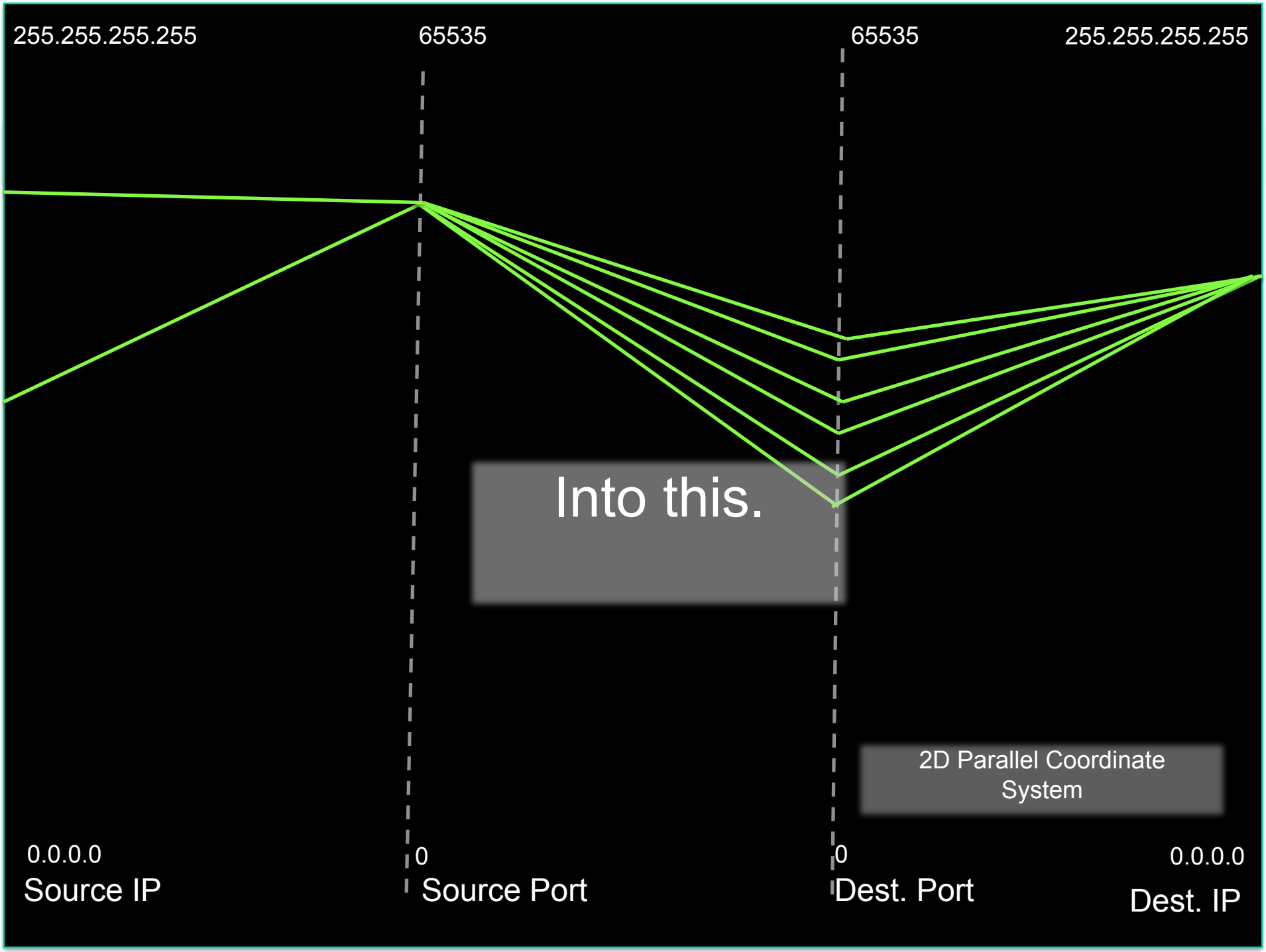
NAVSEC : A Recommender System for 3D Network Security Visualizations

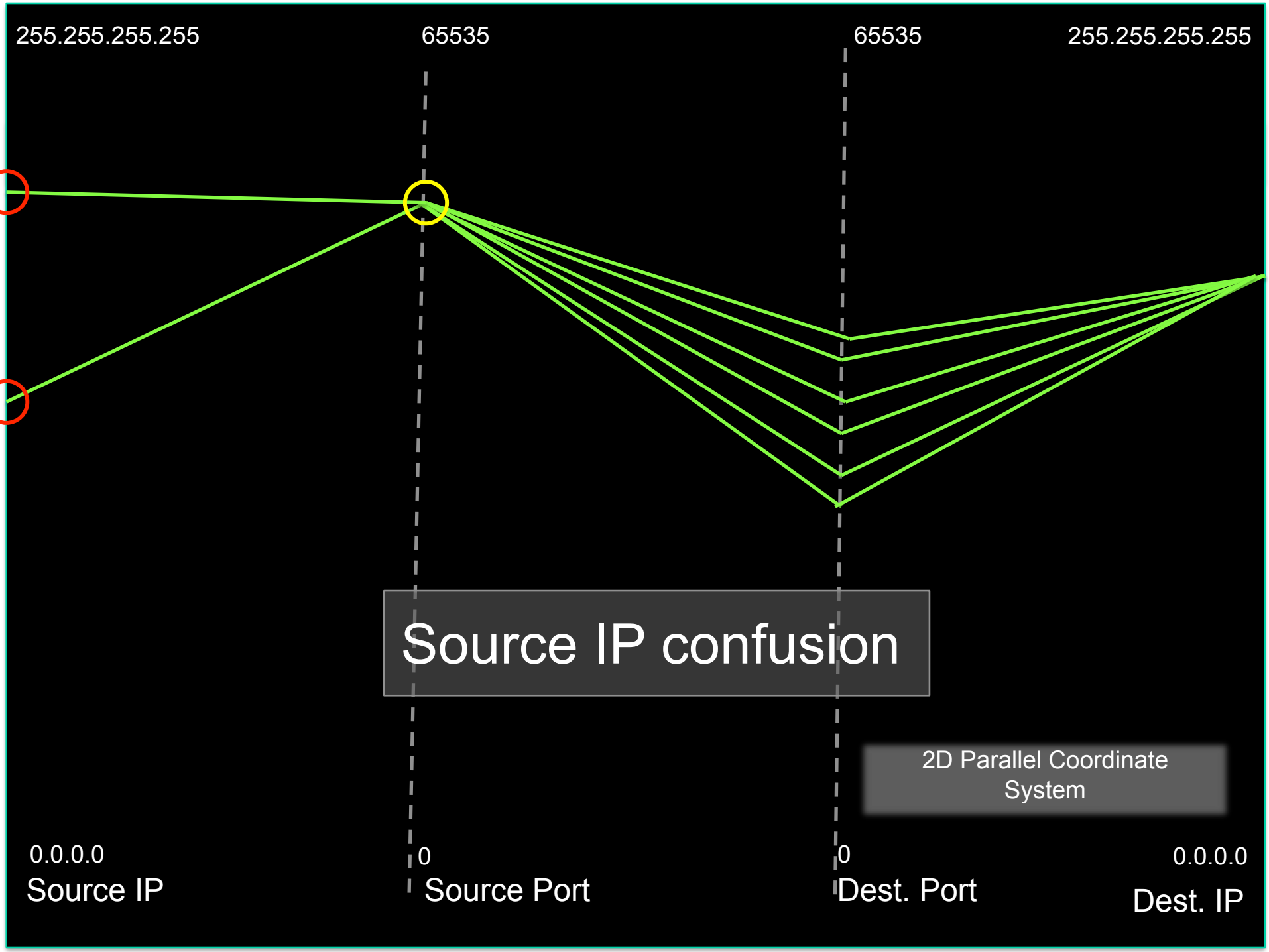
Troy Nunnally
Kulsoom Abdullah
A. Selcuk Uluagac
John A. Copeland
Raheem Beyah

October 14, 2013
CAP Group, School of ECE
VizSec 2013

Outline

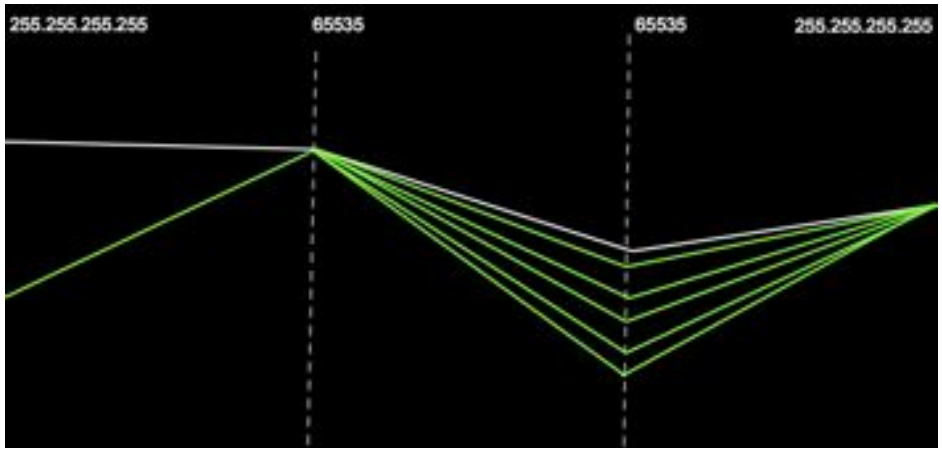

Terminal — bash — 191×51
bash
Convert this...
Textual network traffic for
Tcpdump tool.


255.255.255.255
65535
65535
255.255.255.255
Into this.
2D Parallel Coordinate System
0.0.0.0
Source IP
0
Source Port
0
Dest. Port
0.0.0.0
Dest. IP


255.255.255.255
65535
65535
255.255.255.255
Source IP confusion
2D Parallel Coordinate System
0.0.0.0
Source IP
0
Source Port
0
Dest. Port
0.0.0.0
Dest. IP

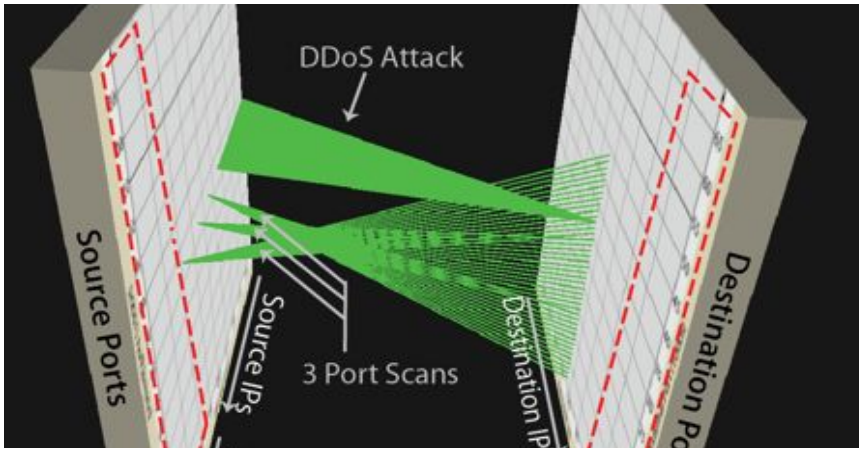
Visualization Challenges

Add Interactions to 2D visualizations



Introduce interaction techniques such as *linking and brushing*.

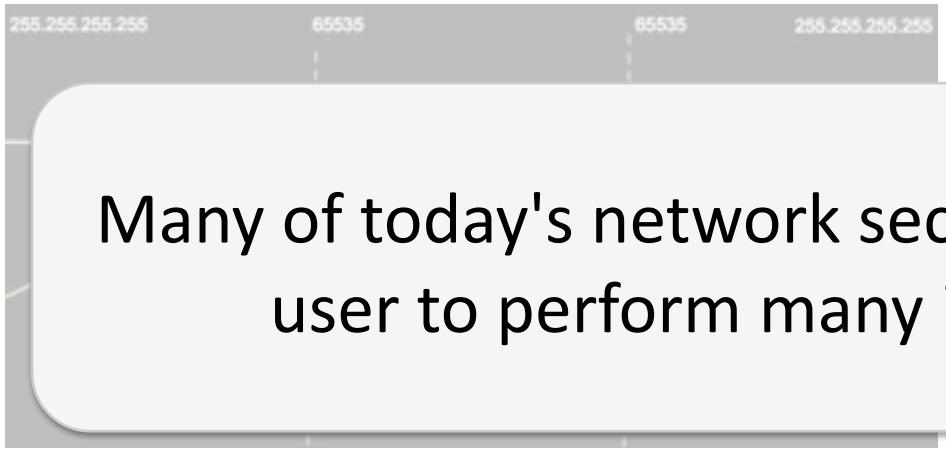
Expand the visualization space



Add the *z-direction* (i.e., 3D) to allow more information to be visualized vs. its 2D counterparts.

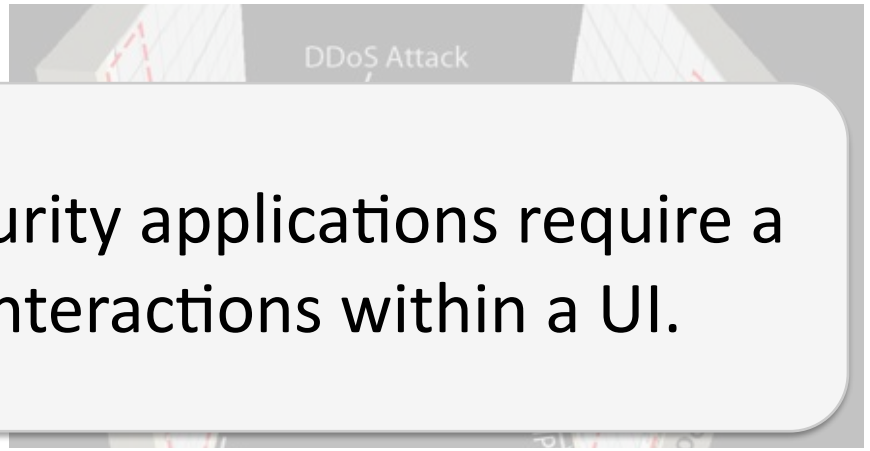
Visualization Challenges

Add Interactions to 2D visualizations



Introduce interaction techniques such as color, linking, brushing.

Expand the visualization space



Add the z-direction (i.e., 3D) to allow more information to be visualized vs. its 2D counterparts.

Many of today's network security applications require a user to perform many interactions within a UI.

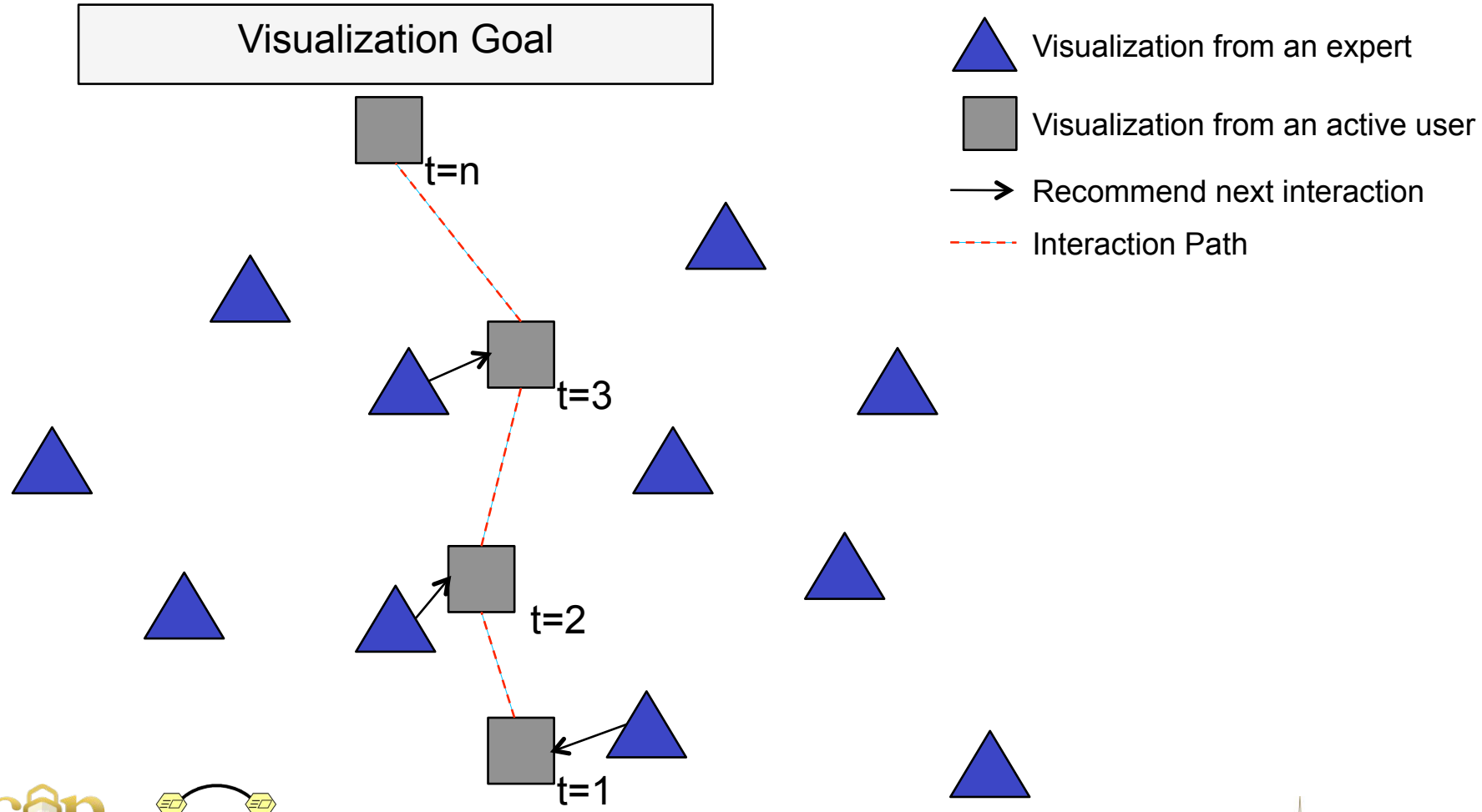
Visualization Challenges

- A large number of interactions could overwhelm or confuse a novice user.
- Finding visualization steps to complete critical tasks becomes difficult to accomplish and could take years to master.
- The more complex visualizations become, the more visualizations become difficult to navigate.

NAVSEC: A Recommender System for 3D Network Security Visualizations

The objective of this work is to help network administrators navigate through complex visualizations and assist in searching for advanced network attacks.

Motivation


Visualization Goal
t=n
t=3
t=2
t=1
Visualization from an expert
Visualization from an active user
Recommend next interaction
Interaction Path

Applications

- As a new administrator, you may need guidance to help you find existing or new attacks.
  - Network Administrator of Companies
  - Military Personnel
  - Education/Training

Outline

Related Work

Searching takes time and effort. Also, finding specific uses of visualization tool of attacks is difficult.

Ask an expert.

Experts cost time and money. Plus, he/she may not always be present.

Related Work

- Recommender systems (e.g., Netflix and Amazon) are used in recommending products and services.
- *Community Command* [16] recommend a single interaction for software applications such as AutoCAD.
- *NIMBLE* [21] calculates the similarity for given IDS alerts and historical alerts.

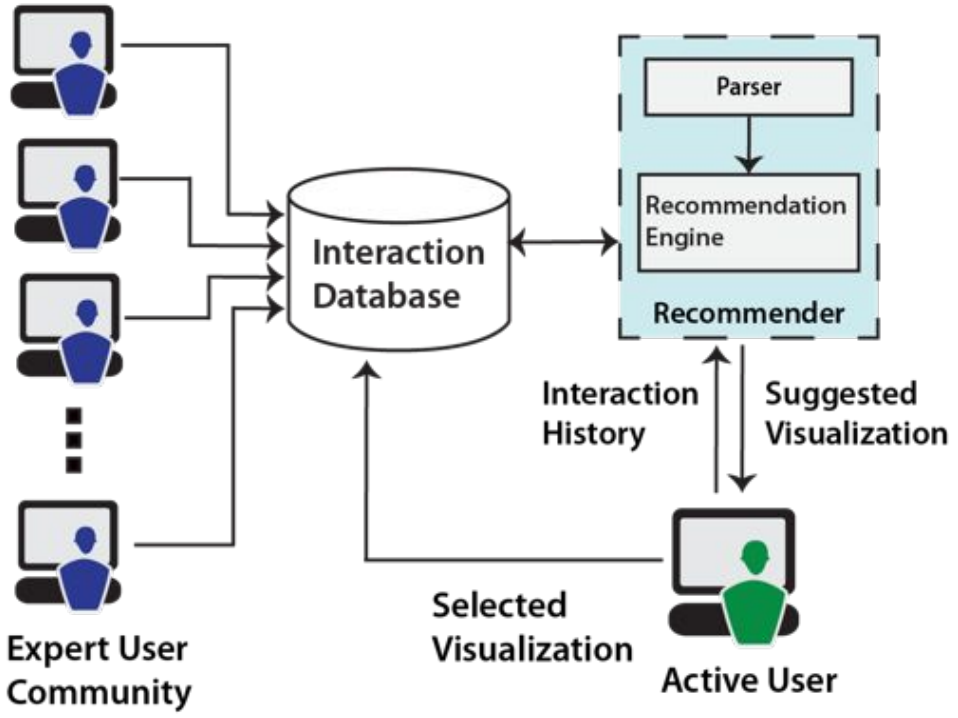
To our knowledge, no work has been done in developing a recommender system to help a novice user make intelligent decisions about network attacks in 3D visualization applications.

Outline

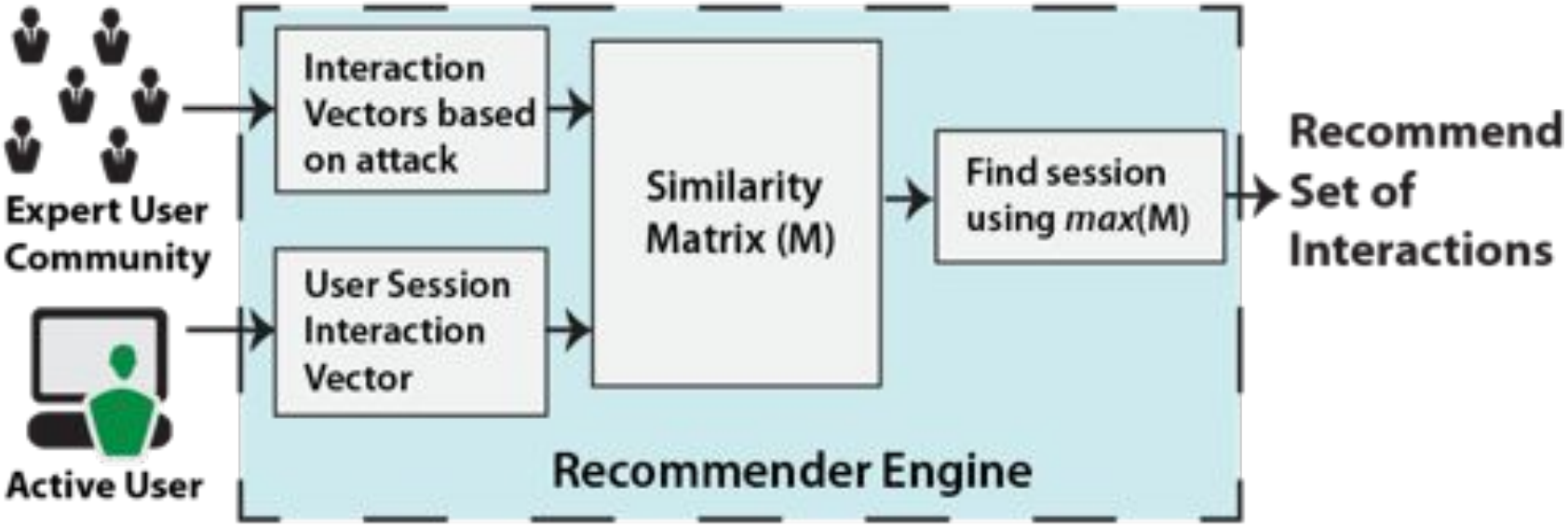
1. Introduction
2. Related Work
3. Design
4. Evaluation
5. Conclusion

System Overview

- Active User - individual navigating the visualization tool.
- Expert User Community - a set of users with significant experience in the network security and visualization fields
- Interaction Database - a collection of interaction sequences.
- Recommender - parses the data computes a set of interactions for recommendation to an active user in real-time.



Recommender Engine



We apply recommendations of interactions so that the user could navigate through the visualization more effectively.

Recommendation Engine

1 Formulate an interaction vector v_k

$$\vec{v_k} = [n_0\ n_1\ \cdots\ n_{J-1}]$$

$$where\ n_j = \sum_{i=0}^{I-1} i_j\ for\ attack\ session\ s_k.$$

V_k = interaction vector for an attack sessions s_k

n_j = interaction type (zoom, rotate, etc.) for an attack sessions s_k

2 Create a Similarity Matrix *M*

$$M_k = cos(\vec{v_k}, \vec{v_h}) = \frac{\vec{v_i} \cdot \vec{v_h}}{\|\vec{v_i}\| * \|\vec{v_h}\|}$$

v_k – *Active* users
v_h - Expert users
M_k – *similarity matrix*

3 Recommend a set of interactions

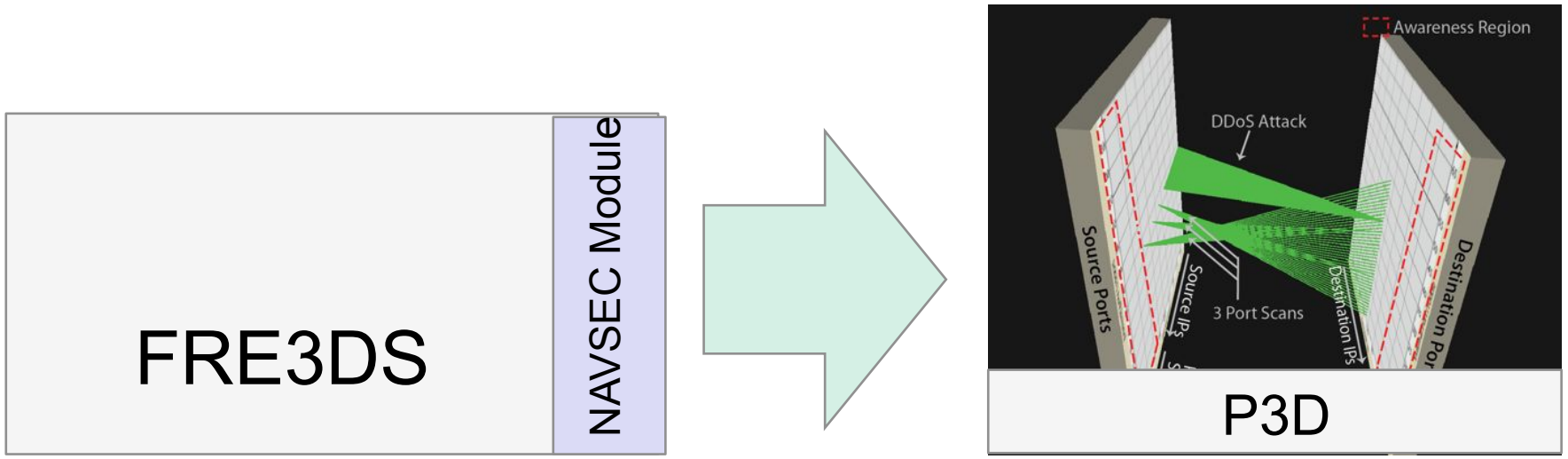
Recommend interaction sequence with the highest similarity score.

Implementation

- NAVSEC server uses an Application Programming Interface (API) to receive HTTP requests.
- NAVSEC API uses Model-View-Controller architecture design to assist in code reusability.
- NAVSEC server could act as a centralized database for multiple active user clients.

Implementation

- NAVSEC contains a client-side C++ component which is integrated as a module of FRE3DS to send GET HTTP request of interactions to the server-side application.



[19] **T. Nunnally**, A. S. Uluagac, J. Copeland, and R. Beyah, "3DSVAT: 3D Stereoscopic Vulnerability Assessment Tool for Network Security," in Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN), 2012.

1 Introduction

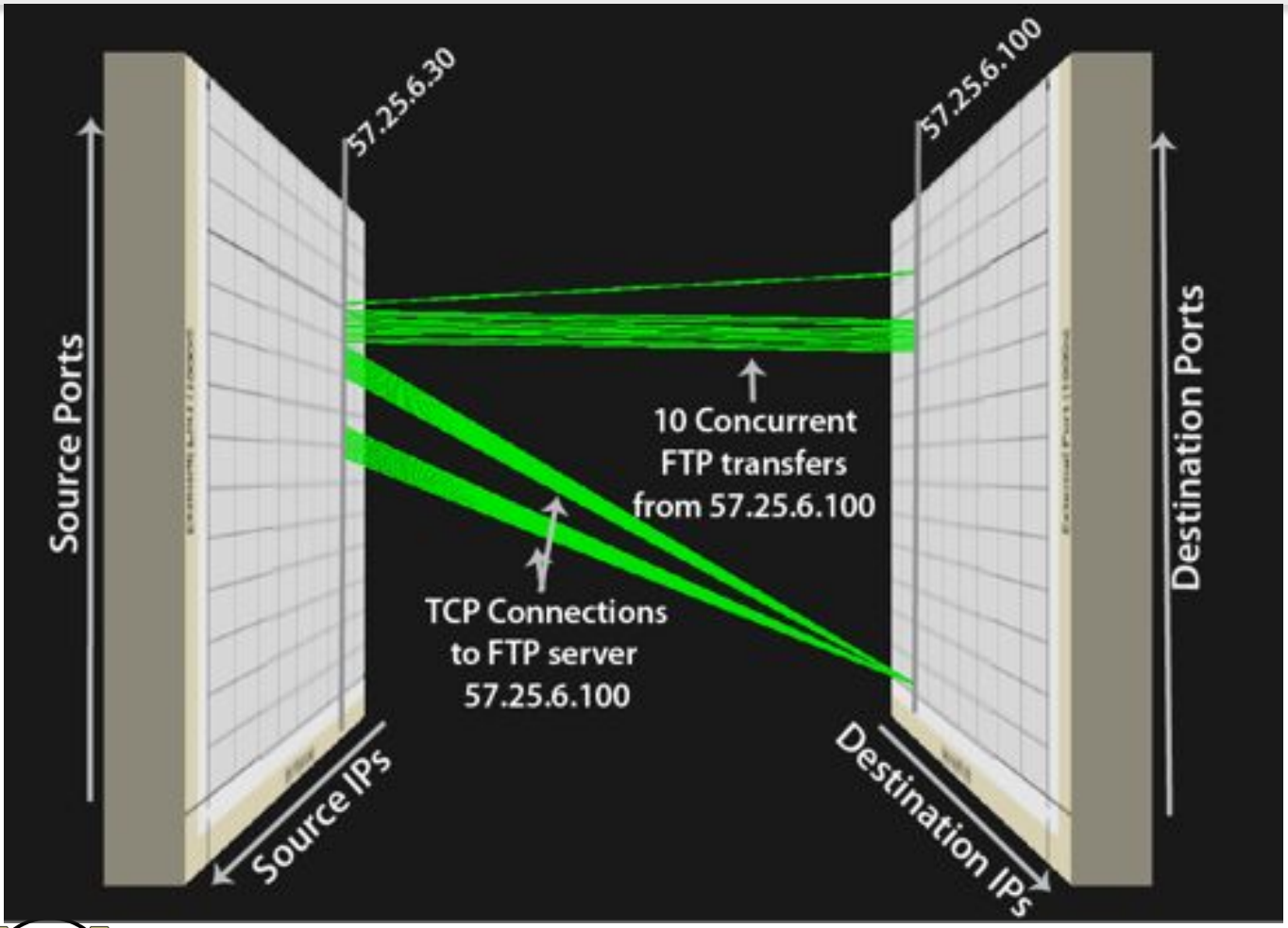
2 Related Work

3 Design

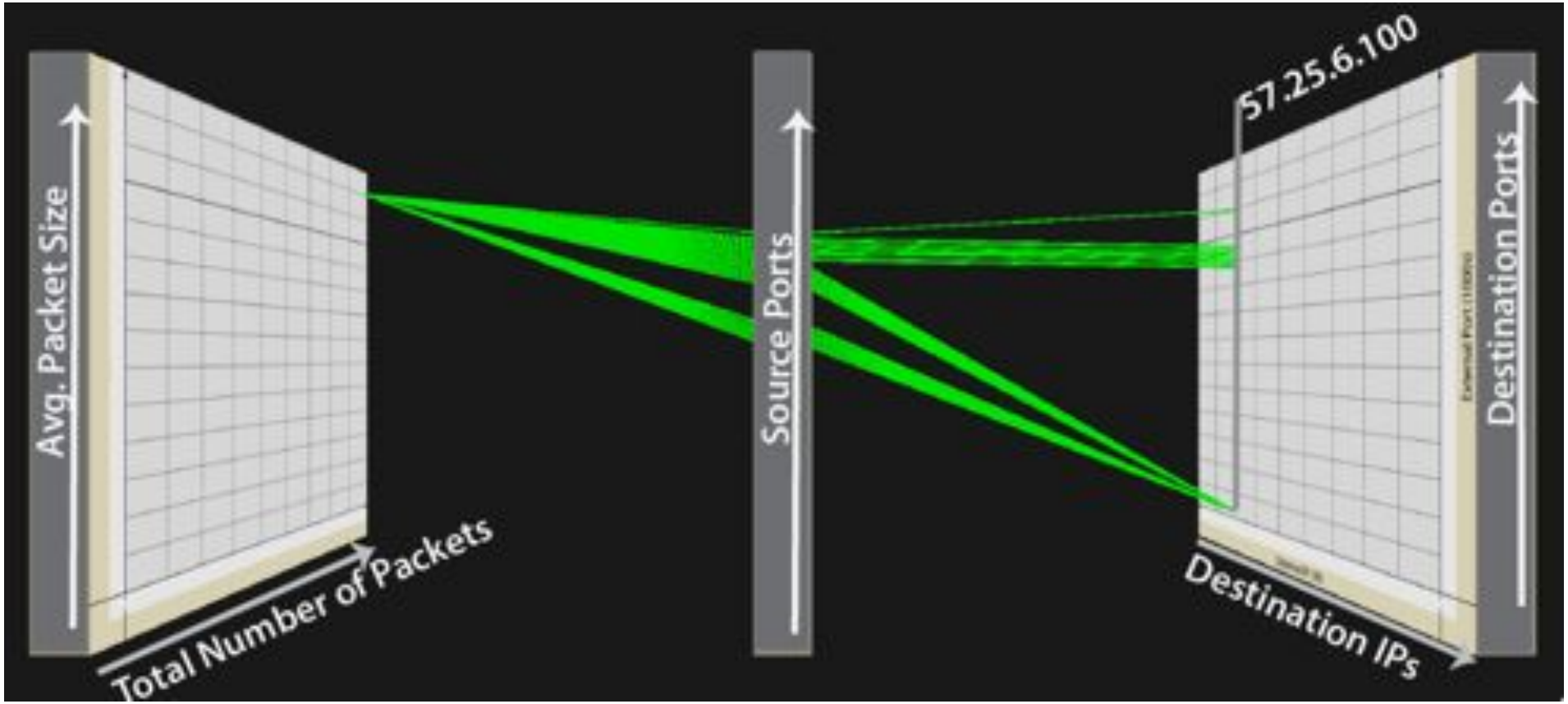
4 Evaluation

5 Conclusion

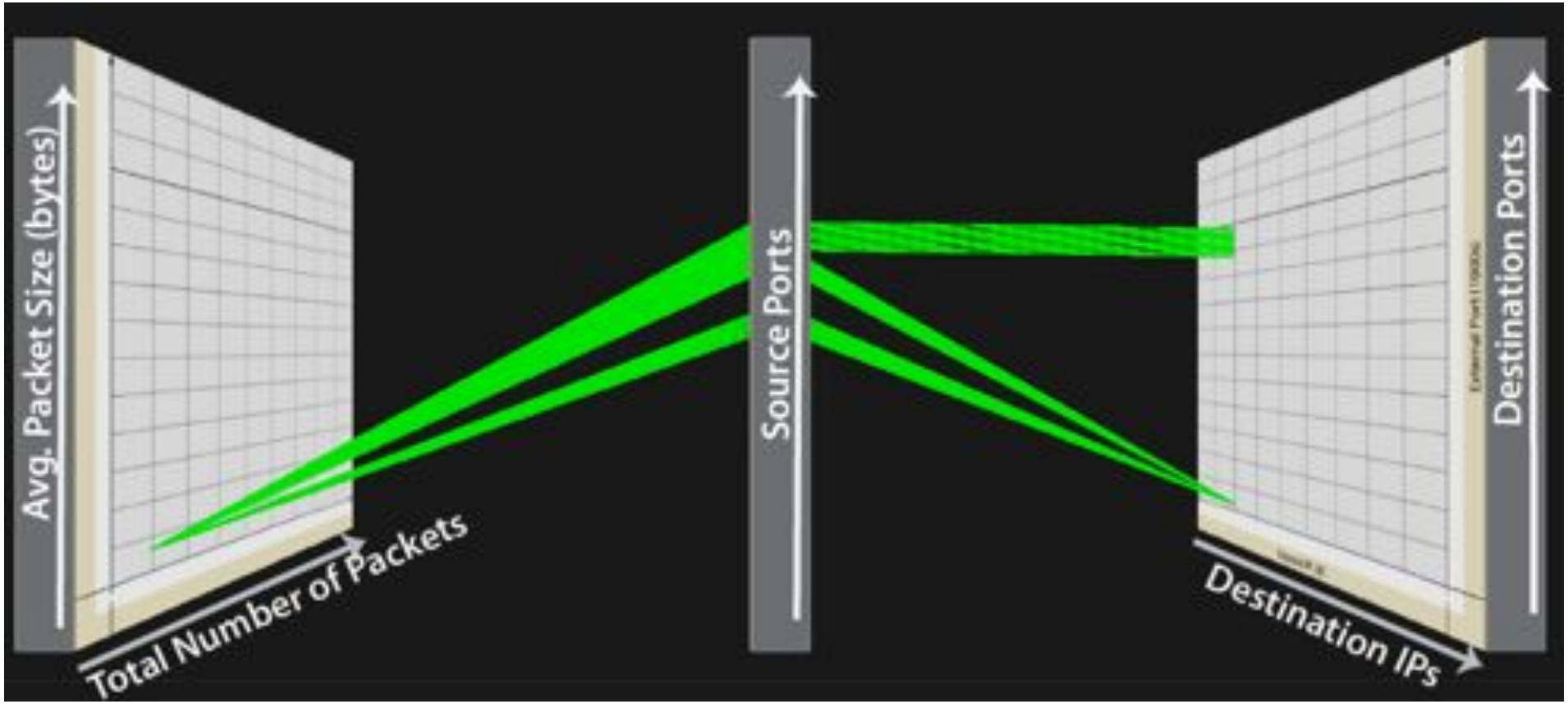
Concurrent FTP transfer



Concurrent FTP transfer

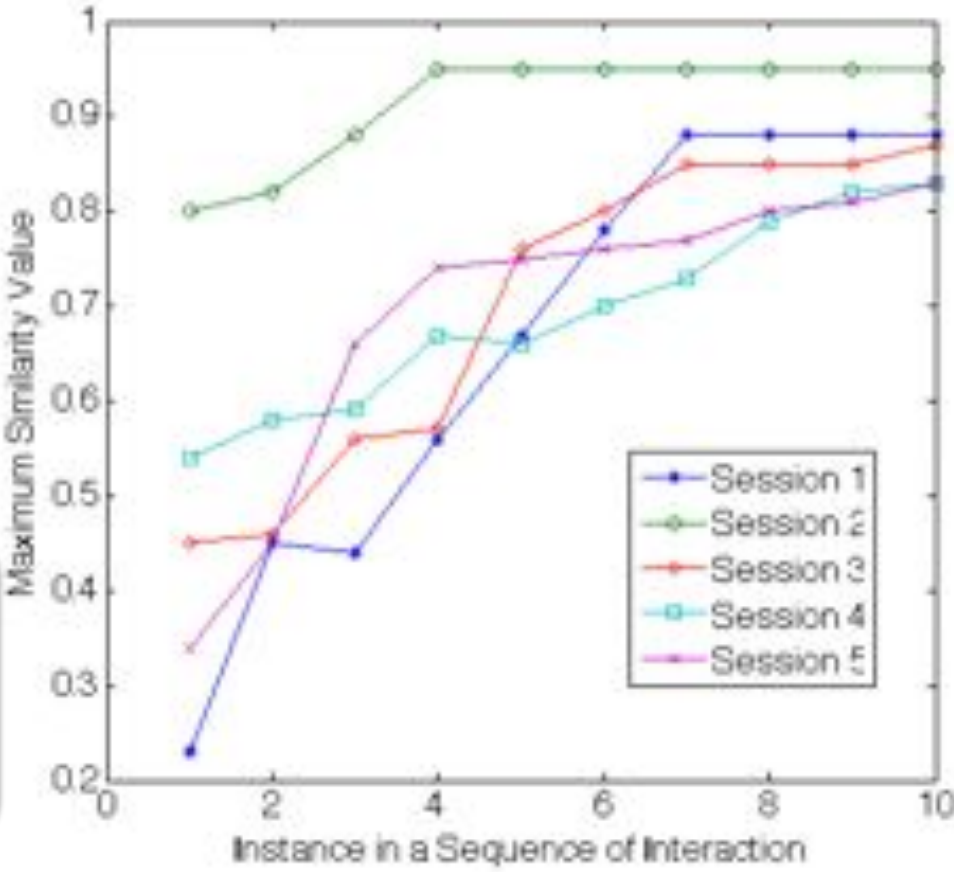


Disguised Port Scan Attack



Convergence Test

- 5 Sessions from an active user.
- 40 interaction vectors from expert users.
- 30 types of interaction types (e.g., zoom out, zoom in, rotate, add left plane, add line glyphs).



These results suggest that with the use of NAVSEC, visualizations for the P3D tool converges towards an expert user's interaction set.

Outline

Contributions and Summary

- NAVSEC uses advanced data mining techniques to recommend interactions.
- NAVSEC is useful for assisting novice users in navigating 3D visualizations.
- Our results show that NAVSEC can converge to a meaningful visualization performed by a user.

Future Work

The future work includes:

- Implementation and evaluation of more advance use-case scenarios (i.e., introduce benign traffic).
- User testing.

Thank You

Thank You

Troy Nunnally

Troy.Nunnally@gatech.edu