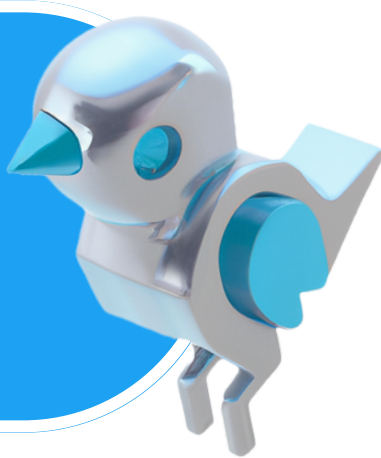


# Interactive Twitter Bot Detection through Network Graph Analysis



**Jonathan Womack,**  
(MSCS)



**Anirudh Prabakaran,**  
(MSCS)



**Madelyn Scandlen,**  
(MSCS)



**Albert Chen,**  
(MSCS)



**Shannon Isaacs**  
(MSA)

## Summary

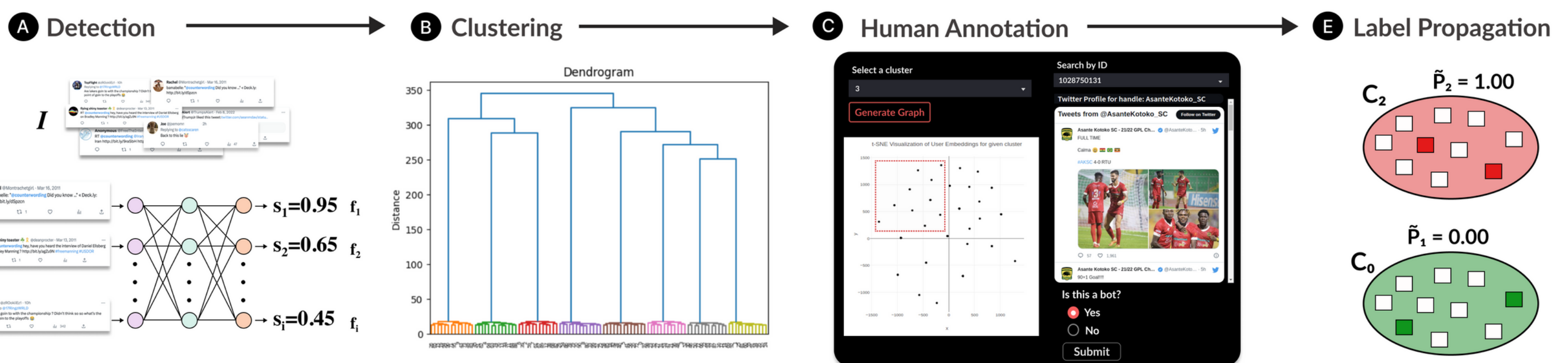
We developed an interactive, multi-pronged method for detecting Twitter bots that combines network graph analysis with expert human input.

## Bot Likelihood from User Tweets

A bi-LSTM was trained on user tweets, embedded with GloVe, to generate bot-scores, the probability that an account is a bot, which were thresholds for which accounts to show.

## Embeddings & Clustering

GraphWave was used to produce high-dimensional embeddings for accounts that were then clustered via FastCluster. Clusters are shown to the human interface user.



## What are Twitter Bots?

Bots are Twitter accounts that mimic human behavior & can be used for malicious activity like spam, phishing, spreading propaganda & more, undermining the purpose of the platform.

## Twibot-20 & Twibot-22

Graph-based twitter bot detection datasets developed by Feng et al. Twibot-22 is the largest to date, with 1 million users.

## Interactive Interface

Streamlit was used to create our user interface. Our interface allows users to select a cluster, perform a t-SNE reduction, investigate user accounts, and label profiles.

## Evaluation

5-person user study using the bot-scores, graph embeddings, and clusters of the Twibot-20 dataset was performed. Each user rated at least 5 accounts in a cluster and the majority label was propagated to other accounts in the cluster. The accounts were then compared to the ground truth label to evaluate the success of the model, with overall accuracy of 0.7897 and a best accuracy of 0.8829.

