THE RISE OF SOCIAL BOTS

Stephanie Bae

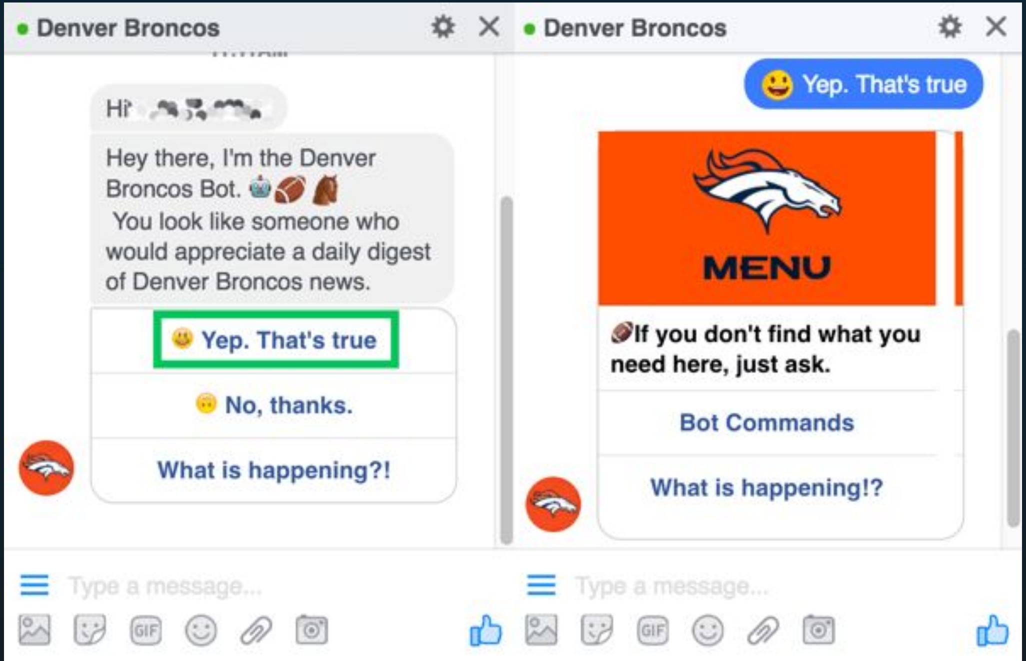
WHAT ARE SOFTWARE BOTS?

(a.k.a. ‘bots’)
are a simple or complex
computer program designed
to execute specific actions

WHAT ARE SOCIAL BOTS?

Use a computer algorithm that automatically produces content and interacts with humans on social media

Example: Chatbots designed to hold a conversation with a human



Hi [redacted]

Hey there, I'm the Denver Broncos Bot. 🤖🏈🐴
You look like someone who would appreciate a daily digest of Denver Broncos news.

🏈If you don't find what you need here, just ask.

Social bots can be split into two categories:

HARMLESS

automatically aggregate content from social sources (like news feeds)

Example: bots designed to provide good customer service

HARMFUL

Exploit and manipulate spam, malware, etc.

Example: bots artificially inflate support for a political candidate

(a.k.a astrosurf or Twitter bombs)

The biggest challenge is being able to understand what social bots are able to do.

How many of you have read
something on the internet and
believed it without checking for facts?

Humans are vulnerable.
Bots can easily infiltrate and
manipulate
our perception of reality.

"THE BOT EFFECT"

Went from one task, like posting content automatically

↓

Taking a piece of information, regardless of validity, and exerting influence over society

"THE HONEYPOT TRAP"

In 2011, James Caverlee + team created a trap that detected thousands of social bots.

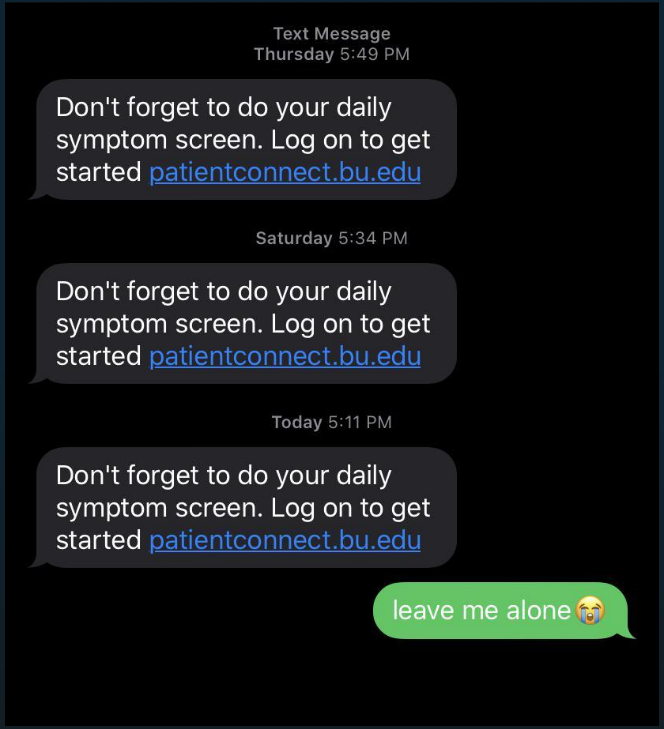
How? They created twitter accounts that posted gibberish tweets regularly.

The suspicious followers were social bots trying to increase their circles by following random accounts.

WHY IS THIS RELEVANT?

Have you ever received those DMs on social media that say “Click here!” or “You won a prize”?

Super annoying!



Text Message
Thursday 5:49 PM

Don't forget to do your daily symptom screen. Log on to get started patientconnect.bu.edu

Saturday 5:34 PM

Don't forget to do your daily symptom screen. Log on to get started patientconnect.bu.edu

Today 5:11 PM

Don't forget to do your daily symptom screen. Log on to get started patientconnect.bu.edu

leave me alone😭

Bots are more sophisticated and harder to find.

They have the ability to…

- search the web for information
- post content at anytime
- imitate patterns of daily activities by humans.

Other bots aim at tampering with the identities of legitimate people

Some are stealing information and using our pictures!

Social bots are “cloning” users.

WHAT IS BEING DONE?

The computing community is designing methods to automatically detect social bots or to discriminate between humans and robots.

The methods that are currently employed are inadequate.

The authors propose 3 strategies for bot detections.

01

Bot detection systems based on social network information

02

Systems based on crowdsourcing and leveraging human intelligence

03

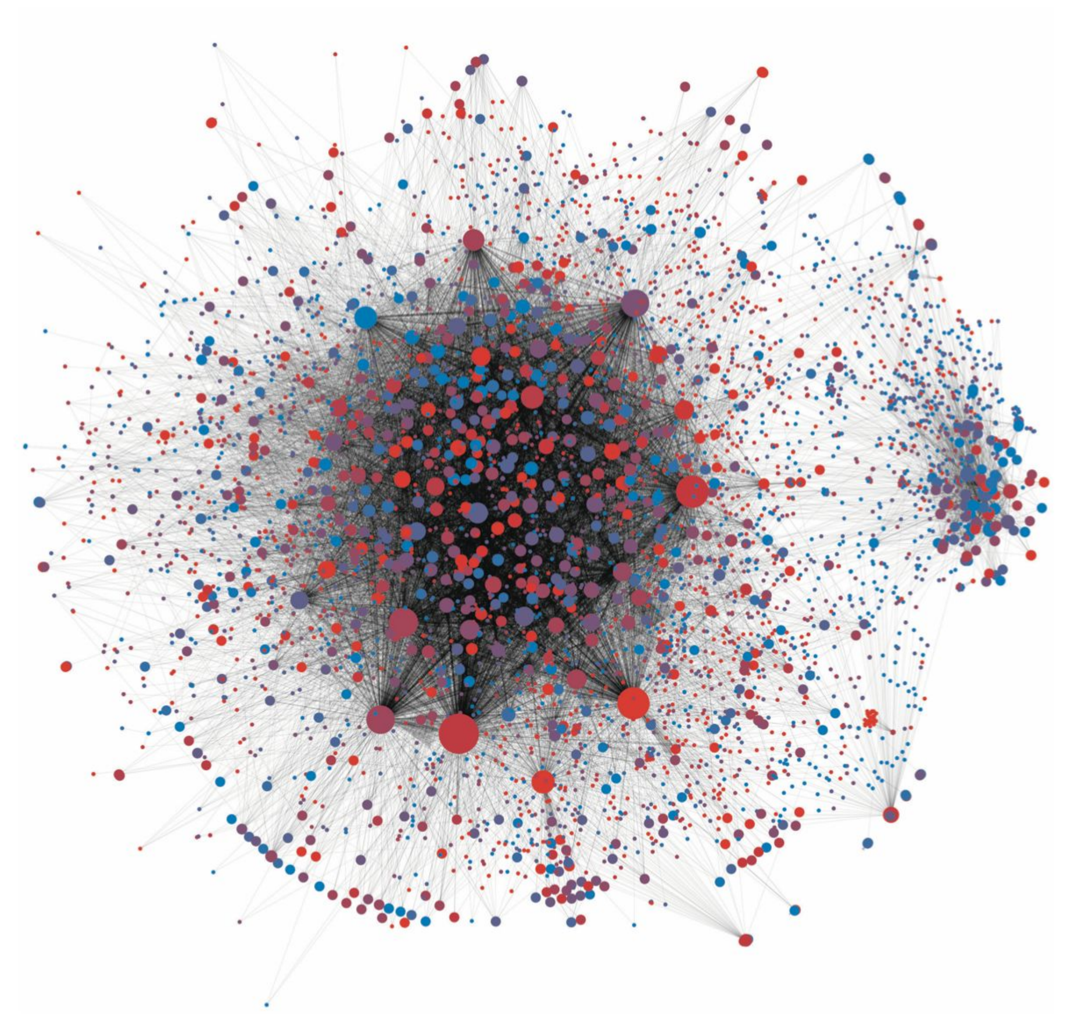
Machine learning methods that discriminate between bots and humans

01

Graph-based Social Bot Detection

Graph-based detection (a.k.a "graption")

- relies on examining the structure of a social graph
- features mainly exploit the spatial relationships in communication traffic
- focuses on analyzing the social relationships that are modeled as graph of nodes



Illustrates the retweet network for the #SB277 online debate about a California law on vaccination requirements

Nodes = Twitter users
Node size = influence (times a user is retweeted)

Links = how information spreads among users

Red nodes = bot accounts
Blue nodes = humans

PROS

- Detection rate is accurate and efficient
- Framework is independent of the software architecture of the malware infecting the hosts

CONS

- The amount of data that needs to be investigated is large
- Computational expense is high
- Accuracy can be disputed if other types need to be detected

02

Crowdsourcing Social Bot Detection

: the process where work is outsourced to an undefined group of people.

The web simplifies the task of gathering virtual information in one place (like Wikipedia)

The goal is to explore a scalable and systematic approach of applying human effort

There are 3 drawbacks with this approach:

1) crowdsourcing might work if implemented in the early stage, but not for large pre-existing user bases

2) “expert” workers are still needed since the “average” worker does not perform well individually. Large companies are forced to hire a team of experts, but small social networks cannot.

3) exposing personal information to external works for validation raises privacy issues.

03

Feature-based Social Bot Detection

Can you identify the difference between a bot and human?

Feature-based detection: machine- and deep-learning algorithms are used to identify social bots based on account features (profile pics, age, etc)

We can train machine learning algorithms on a data set with labelled bot and non-bot accounts.

Pro: Feature-based classifiers yield high accuracies

Con: They are unable to detect new classes of bots that have not been represented in the training data.

IN CONCLUSION...

Bots are continuously changing and evolving. They can build realistic social networks and produce credible content with human-like patterns.

There is a race to detect new threats.

It’s important to reverse engineer the strategies of social bots:
WHO they target
WHAT topics they talk about
WHEN they take action
HOW they generate content

With this, we can identify its puppet masters!

THANK YOU

DISCUSSION

- Do you think social bots are ethical or unethical? Why?
- The author suggests three methods of detecting social bots:
  (1) Graph-based
  (2) Crowdsourcing
  (3) Feature-based

  Which do you feel will work best?
- Could social bots pose a threat to public health?