Proceedings of the International Conference on Augmented Intelligence and Sustainable Systems (ICAISS-2022)
DVD Part Number: CFP22CB2-DVD; ISBN: 978-1-6654-8961-4

93_A Comprehensive Review on Social Botnet Detection Techniques

A Comprehensive Review on Social Botnet Detection Techniques

Anagha Jayesh Patil
Research Scholar,
TSEC, Bandra
anagha.patil@vcet.edu.in

Arti Deshpande
Computer Engineering Department
TSEC, Bandra
arti.deshpande@thadomal.org

Abstract— **In modern era, social bots have become more prevalent as automated social actors as a result of the growth of services on web and fame of online social networks (OSN). Social media sites such as Facebook, YouTube, Twitter, Telegram, LinkedIn, etc. are populated with enormous numbers of "social bots". "Social bots" can be typically believed of as artificial social media accounts used by bad actors to sway public opinion. They are praised for having the capacity to connect with human users and create content on their own. These players can take on a variety of harmful activities, such as eavesdroppers on people's conversations, con artists, spoofers, disseminators of false information, manipulators of the stock market, astroturfers, and content scavengers (spammers, spreaders of malware, etc.). Therefore, the study describes the possible risks posed by harmful social bots, evaluates detection methods using a methodological classification, various available data sources and suggests directions for future study. The findings can assist OSN managers and researchers in comprehending the potentially harmful effects of harmful social bots and can strengthen the current countermeasures.**

Keywords— Social bot, Online Social Networks, social bot detection, Machine learning, Deep Learning, Crowdsourcing.

I. INTRODUCTION

In the modern world, the study of security apprehensions is ongoing, and the subject of information and computer security is expanding quickly. When a new piece of software or product enters the market, a new vulnerability is revealed and used by attackers for a variety of purposes. Click fraud, DDoS (Distributed Denial of Service) attacks, email spamming, intrusive advertisements, virtual deceit, information and identity theft, and distributed resource utilization for mining of cryptocurrency are just a few of the distributed attacks that are carried out by botnets that widely disrupt network activity. Use of at least of one online social network (OSN) such as Facebook, YouTube, Twitter, Instagram and LinkedIn is common among today's population. Their fascinating features have increased their popularity and in turn give rise to the existence of social bots. In the present day, botnet accounts are responsible for 80% of internet attacks.

A social bot is an application that pretends the actions of a genuine user on social media and are managed by spam accounts. Social bots can be good as well as bad. Good bots can be Chatbots; assisting users of social media platforms and applications like Facebook Messenger. Siri, Google Assistant and Alexa are also bots which are used for improving customer engagement. A Twitch bot that handles requests for song for gamers and other live-streaming content creators on the network. They can perform the tasks much faster than humans. Some bad bots can make fake Instagram comments and followers, register phoney YouTube views, spread false information on Twitter, falsely report views on live game. Instances of automatons appropriating Covid-19 hashtags with false information and conspiracy hashtags, such as #qanon and #greatawakening, are undoubtedly present. In paper, Millions of messages among various articles on Twitter around year 2016, related to presidential drive and election in United States were analyzed. Social bots had uneven role in magnifying low-credibility content was proved. Even during course of pandemic, many of bots were discussing about COVID-19 which led to misinformation and crack the social media platforms. Anti-Amber Heard hashtags were frequently made popular by a group of Twitter trolls using manipulative platform techniques. Trolls commonly used copypasta methods to promote positive Johnny Depp articles while spreading false information about Amber Heard [1] make spam accounts.

This misinformation or rumors can be spread with the help of online social bots. Using astroturfing the malicious bots can create a fake impression on real users to access personal and private information. More than two million artificial accounts, or bots, were recently shut down by Twitter in an effort to stop the spread of misinformation on its site. Social media influencers having Instagram accounts with hundreds of millions of followers can grasp huge amount of money. For example, Christiano Ronaldo, a great footballer has almost 475-million followers on Instagram. Having a stunning number of followers or subscribers to your Instagram account indicates that you can also ask huge sums of money for a post as well as re-post. For example, Christiano Ronaldo's post on Instagram can cost up to INR 12cr and for Virat Kohli, it is upto INR 5cr.

The introduction to the social botnet is briefly discussed in section I. Analysis of social botnets such as representation of social network and review of social botnet detection techniques are covered in section II. Social botnet detection techniques can be based on structure, feature and crowdsourcing. Latest research work for social botnet detection is covered in this paper. Section III contains datasets and data sources for social botnet detection. Comparison of available tools for social botnet detection is covered in section IV. Section V concludes the paper and provides research direction for researchers.

HEAD
Dept. of Information Technology
Vidyavardhini's College of Engineering and Technology.

978-1-6654-8962-1/22/$31.00 ©2022 IEEE

A Comprehensive Review on Social Botnet Detection Techniques

Publisher: IEEE

Anagha Jayesh Patil ; Arti Deshpande All Authors

Abstract:
In modern era, social bots have become more prevalent as automated social actors as a result of the growth of services on web and fame of online social networks (OSN). Social media sites such as Facebook, YouTube, Twitter, Telegram, LinkedIn, etc. are populated with enormous numbers of "social bots". "Social bots" can be typically believed of as artificial social media accounts used by bad actors to sway public opinion. They are praised for having the capacity to connect with human users and create content on their own. These players can take on a variety of harmful activities, such as eavesdroppers on people's conversations, con

for future study. The findings can assist OSN managers and researchers in comprehending the potentially harmful effects of harmful social bots and can strengthen the current countermeasures.

Published in: 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)

Date of Conference: 24-26 November 2022 **INSPEC Accession Number:** 22540402

Date Added to IEEE *Xplore*: 16 January 2023 **DOI:** 10.1109/ICAISS55157.2022.10010877

ISBN Information:

Publisher: IEEE

Conference Location: Trichy, India

I. Introduction

In the modern world, the study of security apprehensions is ongoing, and the subject of information and computer security is expanding quickly. When a new piece of software or product enters the market, a new vulnerability is revealed and used by attackers for a variety of purposes. Click fraud, DDoS (Distributed Denial of Service) attacks, email spamming,

P.T Lanjewar

HEAD
Dept. of Information Technology
Vidyavardhini's College of
Engineering and Technology.
Vasai Road 401 202.