A survey on the Rise of Social BOT detection techniques and Research Challenges

Dr.V.Shunmughavel
Professor, Department of CSE, SSM Institute of Engineering and Technology

Dr.A.B.Arockia Christopher
Assistant Professor Senior Grade, Department of IT, Mahalingam College of Engineering and Technology

ABSTRACT

BOTS (software robots) have been around since the early days of computers. A social bot is a computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior. Social bots have inhabited social media platforms for the past few years. Social bots populate techno-social systems: they are often benign, or even useful, but some are created to harm, by tampering with, manipulating, and deceiving social media users. Social bots have been used to infiltrate political discourse, manipulate the stock market, steal personal information, and spread misinformation. The detection of social bots is therefore an important research endeavor. A taxonomy of the different social bot detection systems proposed in the literature accounts for network-based techniques, crowd sourcing strategies, feature-based supervised learning, and hybrid systems. Therefore, this reveals the potential hazards of malicious social bots, reviews the detection techniques within a methodological categorization and proposes avenues for future research.

Keywords: Social Bot Detection, Flow based detection, Graph based detection, Feature based, Crowd sourcing.

1. INTRODUCTION

With every new technology comes abuse, and social media is no exception. A second category of social bots includes malicious entities designed specifically with the purpose to harm. These bots mislead, exploit, and manipulate social media discourse with rumors, spam, malware, slander, or even just noise. This may result in several levels of damage to society. The novel challenge brought by bots is the fact they can give the false impression that some piece of information, regardless of its accuracy, is highly popular and endorsed by many, exerting an influence. Journalists, analysts, and researchers increasingly report more examples of the potential dangers brought by social bots. These include the unwarranted consequences that the widespread diffusion of bots may have on the stability of markets.

In recent years, Twitter bots have become increasingly sophisticated, making their detection more difficult. The boundary between humanlike and bot-like behavior is now fuzzier. For example, social bots can search the Web for information and media to fill their profiles, and post collected material at predetermined times, emulating the human temporal signature of content production and consumption—including circadian patterns of daily activity and temporal spikes of information generation. They can even engage in more complex types of interactions, such as entertaining conversations with other people, commenting on their posts, and answering their questions [2]. Some bots specifically aim to achieve greater influence by gathering new followers and expanding their social circles; they can search the social network for popular and influential people and follow them or capture their attention by sending them inquiries, in the hope to be noticed [3]. To acquire visibility, they can infiltrate popular discussions, generating topically appropriate and even potentially interesting content, by identifying relevant keywords and searching online for information fitting that conversation [1].

After the appropriate content is identified, the bots can automatically produce responses through natural language algorithms, possibly including references to media or links pointing to external resources [4]. Other bots aim at tampering with the identities of legitimate people: some are identity thieves, adopting slight variants of real usernames, and stealing personal information such as pictures and links. Even more advanced mechanisms can be employed; some social bots are able to "clone" the