Fake Chatroom Profile Detection

Patrick Bours[1]*, Parisa Rezaee Borj[2], and Guoqiang Li[3]

[1] NTNU, patrick.bours@ntnu.no
[2] NTNU, parisa.rezaee@ntnu.no
[3] NTNU, guoqiang.li@ntnu.no

Abstract

People communicate more and more online in various manners, from posting status updates on Facebook, and sharing videos on YouTube, to direct chatting with friends while playing games and making new (international) friends in online chatrooms. The online society provides a million opportunities for those interested in engaging in harmless activities, but equally well it provides an environment for those with less honorable intentions. Online identities are hard to link directly to physical identities and anonymity and privacy are available to all, independent of the actual intentions of the person.

In our research, we focus on using biometric (keystroke dynamics) and textual (stylometry) features to determine both the correctness of the profile of chatter, as well as ongoing harassment activity. Biometric Keystroke Dynamics (KD) is generally used for authentication purposes to verify the identity of a user while he/she types the (fixed) password. Stylometry is used frequently for Authorship Attribution on long texts (or even books) to establish the identity of the author. In our research, we combine both factors but apply them on short texts that are sent in a chat. From this minimal amount of information, we first want to determine age group (adult vs. adolescent) and gender (female vs. male) of a chatter. This will prevent a 41-year-old male from pretending to be a 14-year-old girl in a chatroom.

Our initial focus in on chat data collected from students and staff of NTNU and we have used SVM to detect gender based on KD data only with an accuracy of approximately 80% per message. Even though this number might not be that high, we noticed for example that correct decision often had a high confidence level, while incorrect decisions were made with a lower confidence level. Even if we take the binary decision of the SVM, then simple majority voting will boost the probability of an error to about 10% with 5 chat messages and less than 1% in 13 chat messages.

In this presentation, we will describe a framework that can be used for creating a safer cyber society by detecting online grooming in chatrooms. We will focus on how this can make a safer online society.

Future work will be to include the stylometry features besides the KD features

*The author presented the paper at the NISK 2018 conference.