In this paper, we study mimicking attacks and detections from both sides, as attackers and defenders, which is a significant extension based on our preliminary work in [23]. From the botnet programmers' perspective, in order to simulate the legitimate behavior of a web browser, we need three key pieces of information: web page popularity of the target website, web page requesting time interval for a user, and number of pages a user usually browses for one browsing session (referred to as browsing length). Based on the research on web browsing dynamics, there are three distributions in place for the three key pieces of information. Namely, the web page popularity follows the Zifp-Mandelbrot distribution [24], the page requesting time interval follows the Pareto distribution [25], and the browsing length follows the inverse Gaussian distribution [26]. Furthermore, Borgnat et al. [27] observed a backbone of the Internet for 7 years (2001 to 2008), and compared their observation with previous ones (1998-2003) [28]. They concluded that the Internet is consistent in terms of traffic although the Internet has developed significantly. Therefore, the properties of the Internet we use in this paper are reliable. If botmasters have a sufficient number of active bots (here we mean the number of active bots is no fewer than the number of active users of a genuine flash crowd, which we will refer to as the sufficient number condition), then each bot can simulate one legitimate user using the three statistical distributions. As a result, it is impossible to differentiate mimicking attacks from the legitimate web browsing of a large number of browsers. We will analyze and prove this as the first goal of this paper.

REF: S. Yu, S. Guo and I. Stojmenovic, "Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace," in *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 139-151, Jan. 2015.