Modeling Flash Mobs in Cybernetic Space

Evaluating Threats of Emerging Socio-Technical Behaviors to Human Security

Samer Al-khateeb
Department of Applied Science
University of Arkansas at Little Rock
Email: sxalkhateeb@ualr.edu

Nitin Agarwal
Department of Information Science
University of Arkansas at Little Rock
Email: nxagarwal@ualr.edu

Since the occurrence of the first 'Flash Mob' organized by Bill Wasik in Manhattan in 2003; flash mob phenomenon has become widespread. Recent journalistic accounts have reported that this form of public engagement has the potential to pose considerable amounts of risks to civil, political, social, and economic stability of a region. This raises the importance of systematically studying such behaviors. Modern Information and Communication Technologies (ICTs) provide affordable and easy to use means of communications (such as social network platforms, viral emails, and SMS) that facilitates the process of recruiting, training, and looking for a specific sector of the society (specific gender, age, political affiliation, interest, and cultural background) easier than it was before. This in turn has led to an increase in the occurrences of emerging socio-technical behaviors [1], including parkour, flash mobs, campaigns, and social or mass movements. This research is an attempt to bridge social and computational sciences that would help analyze and explain manifestations of emerging socio-technical behaviors, especially the flash mobs.

Flash mob is a form of public engagement, which according to Oxford Dictionaries, is defined as "A large public gathering at which people perform an unusual or seemingly random act and then quickly disperse". Recent observations pertaining to the deviant aspect of the flash mobs has insisted to add a highly debated perspective, which is *the nature* of the flash mob (whether it is for entertainment, satire, and artistic expression or it is a deviant act that can lead to robberies and thefts, a.k.a., criminal flash mobs. A flash mob could be entertaining such as *Happy Birthday for a bus driver* [2] or it can be the new face of Transnational Crime Organizations (TCOs) [3], such as the "Bash Mob" that happened in Long Beach, California in July 9, 2013 [4].

In this ongoing research, we focus on the flash mob behavior that takes place in the cyberspace but could possibly extend to the physical space, or "Cybernetic Space" [5]. In this study, we seek answers to, (i) what are the factors that motivate an individual to participate in a flash mob?, (ii) what are the choices an individual has regarding acting (or not) in a flash mob?, and (iii) can we develop a conceptual framework capable of predictive modeling of a flash mob?

Toward this direction, we explore the choices flash mob practitioners have and its influence over determining their decision with regard to acting or not in a flash mob. The decision can then be parameterized over an individuals *interest* in the flash mob and his/her *control* over it. The interest is defined as the difference between the utilities associated with the choices available to the individual. Control can be measured using authoritativeness of an individual or access to network resources, where the network refers to the social network of individuals used for recruiting, mobilizing, and coordinating the flash mob. The flash mob practitioner (a node in the network) faces one of the following four scenarios: (1) node *has interest* and *has control* over the event, then it will **act**, (2) node *has interest* but *does not have control*, then most likely it will **act**, (3) node *does not have interest* but *has control*, then the node will have two choices - either **withdraw** or execute **power exchange** (to gain control over other flash mob events or to gain social capital), and (4) node has *no interest* and *no control* then the node will have two choices either **withdraw** or **defect (act against)** the group. Categorizing the individuals according to the four scenarios helps conduct a targeted analysis. Individuals belonging to scenarios 1 and 2 pose the most imminent threat. For a long term monitoring of the groups behavior, individuals belonging to scenario 3 are relevant as they could lead us to identify other flash mob events. Individuals belonging to scenario 4 can be eliminated from the analysis, as they may just be lurkers in the group and become relevant if their tendencies shift towards defecting.

Acknowledgments: This material is based upon work supported by the U.S. Office of Naval Research under Grant No. N000141410489.

References

[1] Y. S. Mohilever, "Taking over the city: Developing a cybernetic geographical imagination-flash mobs & parkour," *Theatre Space After 20 TH Century*, p. 188.

[2] C. Kirkland, "12 great examples of flash mobs," Econsultancy, 2014. [Online]. Available: http://econsultancy.com/blog/8548-12-great-examples-of-flash-mobs

[3] G. Ackerman *et al.*, "The "new" face of transnational crime organizations (tcos): A geopolitical perspective and implications to us national security," 2013.

[4] B. Holbrook, "Lbpd prepared for potential bash mob event," Everything Long Beach, 2014. [Online]. Available: http://www.everythinglongbeach.com/lbpd-prepared-for-potential-bash-mob-event/

[5] A. Mitra and R. L. Schwartz, "From cyber space to cybernetic space: Rethinking the relationship between real and virtual spaces," *J. Computer-Mediated Communication*, vol. 7, no. 1, 2001.