Guess Who? An Empirical Study of Gender Deception and Detection in Computer-Mediated Communication

#53

Shuyuan Mary Ho & Jonathan M. Hollister
School of Library & Information Studies, College of Communication and Information, Florida State University

Introduction

- Theories addressing deceptive communications are primarily focused on face-to-face (FtF), synchronous interactions. (Ekman & O'Sullivan, 1991)
- Without the synchronous visual cues, a user may face difficulties in assessing the truthfulness of their identity attributes (e.g., gender, etc.) of those whom they are communicating with in computer-mediated communication. Users are vulnerable to online deception, and identity theft. (Hancock 2007)
- Buller & Burgoon (1996) suggests that both speakers and receivers of deceptive messages dynamically adjust and use strategic communicative behaviors to deceive and detect, respectively. Deceivers may divulge intent via nonstrategic cues.
- Deceptions, at the base, are behaviors that are affected by self-efficacy (Bandura, 1977). The belief of a speaker may affect the level of effort or even the decision to attempt deception.
- Herring and Martinson (2004) suggest that intentional deceivers would still use stylistic features characteristic of their actual gender in the language they speak.
- Elangovan (1998) states that betrayal in interpersonal relationship is a type of violation of trust expectation, and suggests a process model of opportunistic betrayal of trust in organization.
- Ho (2013) empirically tested that betrayal initiates the downward shift of speaker's trustworthiness, which can be observed through information and communication behavior by a recipient who is in close relationship with the speaker. Only through a recipient's internal attribution can trustworthiness of a sender be accurately attributed.

Research Question

What factors enable gender deception and detection in CMC environments?

Hypotheses

H1a: **Gender of the speaker** is associated with the success of deception of gender deceptive messages.

H1b: **Perceived gender of the speaker** is associated with the success of detection of gender deceptive messages.

H2: **Perceived trustworthiness of the speaker** is positively associated with the recipient's ability to detect correct gender.

H3: **Trustfulness of the recipient** is negatively associated with their ability to detect deceptive messages.

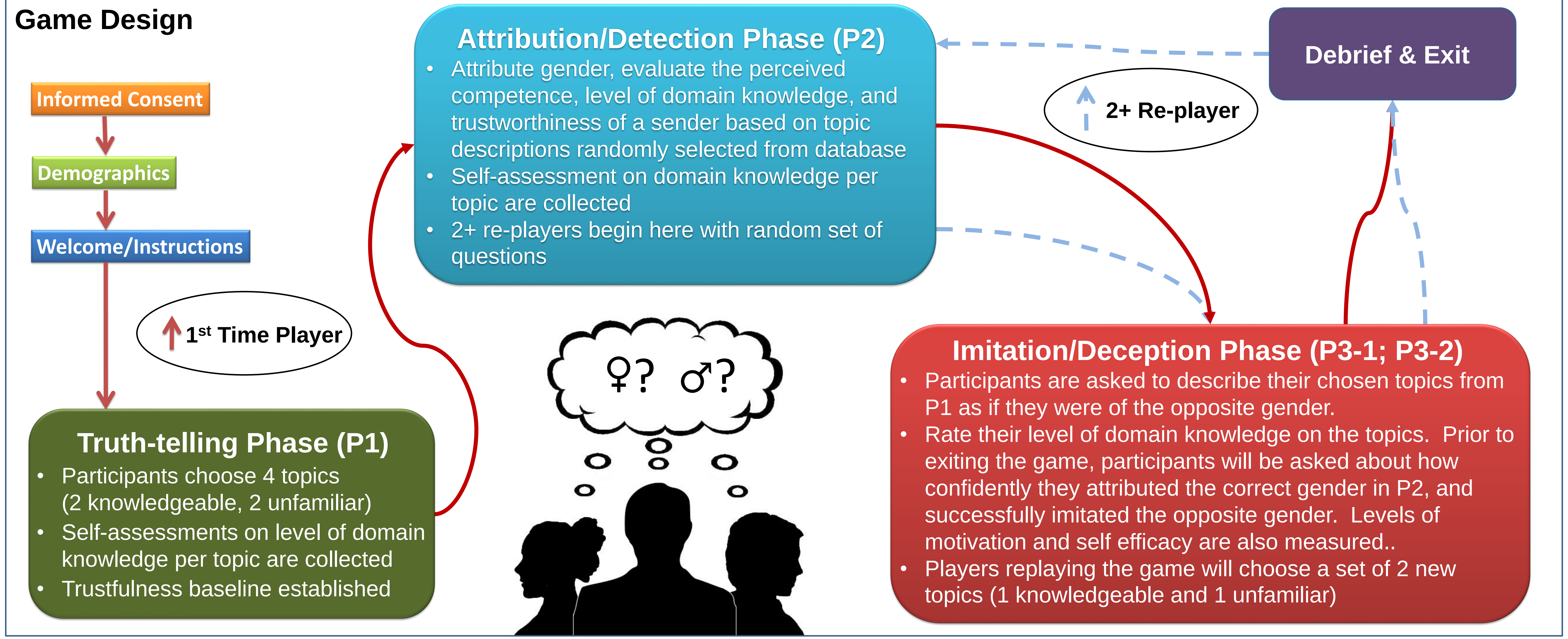
H4: **Domain knowledge** is positively associated with the speaker's ability to send successful deceptive messages.

H5: Speakers with higher **self-efficacy** can deceive better.

Method

- Quasi-experiment using asynchronous, text-based game, Guess Who?, facilitated through Facebook to authenticate users and verify gender information and ported to the Virtual Funhouse, a sociotechnical research game portal.
- Participants recruited from November 2012 through January 2013 via Facebook, Twitter, and email listservs.
- Number of participants was 26; 11 females (42.3%) and 15 males (57.7%)
- 26 participants generated and evaluated 98 records (n=98) usable for analysis creating 3 data sets: overall, truthful, and deceptive.

Game Design



Truth-telling Phase (P1)

- Participants choose 4 topics (2 knowledgeable, 2 unfamiliar)
- Self-assessments on level of domain knowledge per topic are collected
- Trustfulness baseline established

Attribution/Detection Phase (P2)

- Attribute gender, evaluate the perceived competence, level of domain knowledge, and trustworthiness of a sender based on topic descriptions randomly selected from database
- Self-assessment on domain knowledge per topic are collected
- 2+ re-players begin here with random set of questions

Imitation/Deception Phase (P3-1; P3-2)

- Participants are asked to describe their chosen topics from P1 as if they were of the opposite gender.
- Rate their level of domain knowledge on the topics. Prior to exiting the game, participants will be asked about how confidently they attributed the correct gender in P2, and successfully imitated the opposite gender. Levels of motivation and self efficacy are also measured..
- Players replaying the game will choose a set of 2 new topics (1 knowledgeable and 1 unfamiliar)

Pilot Study Findings

Hypothesis	Results	Relevant Statistics			Significance	Notes
H1a (Gender of Speaker)	Not Supported	N/A			*p*>.05	In the overall sample, 46.95% of participants were successful in gender attribution; 47.4% in the truthful; 46.7% in the deceptive state. No significance difference in success rate between genders.
H1b (Perceived Gender)	Partially Supported	59.6% Female	32.6% Male	*n*=98 overall	χ2=7.148; *df*=1 *p*<.01	Receivers that perceived speakers to be female were more accurate in their attributions. However, receivers that perceived speakers as male were less likely successful. In the overall sample, speakers perceived to be men were significantly (*t*=2.239, *df*=96, *p*<.05) perceived as less trustworthy (*m*=2.7391, *SD*=.72064, *n*=46) than those who perceived as women (*m*=3.0753, *SD*=.76024, *n*=52).
		63.6% Female	25% Male	*n*=38 natural	χ2=5.546; *df*=1 *p*<.05	
H2 (Trustworthiness)	Supported	*m*=.59	*SD*=.50	*n*=29	*t*=3.278 *df*=20.309† p<.01	Receivers that perceived speakers more trustworthy were more successful in gender detection and receivers that perceived speakers less trustworthy were less successful in gender detection. *α* of trustworthiness index=.898
		m=.11	*SD*=.33	*n*=9		
H3 (Trustfulness)	NS	N/A			N/A	Non testable, α of trustfulness index was less than .60
H4 (Domain Knowledge)	Partially Supported	*m*=2.55	*SD*=2.32	*n*=20	*t=5.597; df=28* *p<.001*	Successful deceivers had lower domain knowledge in the natural group and higher domain knowledge in the deceptive group; this suggests an influence of the game. No significant difference in domain knowledge level of successful deceivers in overall sample.
		m=6.17	*SD*=3.48	*n*=29		
H5 (Self-efficacy)	Supported	*m*=4.92	*SD*=1.79	*n*=24	*t*=2.161 *df*=47 *p*<.05	Successful gender deceptive message speakers were significantly more confident that their messages would be successful at gender deception than unsuccessful speakers.
		m=3.88	*SD*=1.56	*n*=25		

*Outcome coded as: 1=successful gender attribution/failed gender deception; 0=failed gender attribution/successful gender imitation. †Equal variances not assumed.

Limitations

- Quasi-experimental design may threaten contextual realism; randomized participant selection and statement display improve generalizability.
- Unequal, yet statistically insignificant gender distribution of sample; gender bias may be inherent in list of topics.
- Asynchronous, text-based design does not facilitate an understanding of other factors, such as historical, relational, physical, or visual factors.

Conclusions & Future Research

- Our findings will assist both practitioners and researchers in understanding the role of gender, as an attribute of identity, in trust and deception within CMC environments.
- Future research will utilize Structural Equation Modeling to develop a theoretical framework of gender attribution and qualitative content analysis of strategic and nonstrategic behaviors that both detectors and intentional deceivers deploy in a/synchronous and synchronous CMC environments.

PO Box 3062100, Tallahassee, FL 32306-2100 | smho@fsu.edu | jmh09k@my.fsu.edu | apps.facebook.com/isensor | isensorlab.com

The authors thank the National Science Foundation for the support of Secure and Trustworthy Cyberspace EAGER award #1347113.