Detection of Deception: Collaboration Systems and Technology

Jay F. Nunamaker, Jr.
University of Arizona
Tucson, Arizona 85721
jnunamaker@cmi.arizona.edu

Deception is defined as messages and information knowingly transmitted to create a false impression or conclusion. There are many ways to deceive, such as: lies, fabrications, concealments, misdirection, bluff, fakery, mimicry, tall tales, white lies, deflections, evasions, equivocation, exaggerations, camouflage and strategic ambiguity. The above referenced methods and techniques of deception are all common, everyday occurrences we experience. We witness deception daily in our relationships. However, we are not very good at detecting deception. On the average, we are accurate approximately 50% of the time. This is not a good result given all of our personal experience with deception on a daily basis.

Since 9/11 we are all aware of the threat of terrorism and need to be vigilant in our pursuit of the detection of deception. A major risk to the success of our society in the 21st century is the failure to detect and counter deception in the world. Success depends on our society achieving information superiority. This requires safeguarding information against manipulation, infiltration, and deception by adversaries. Yet achieving high information assurance is complicated not only by the very speed, complexity, volume, and globality of communication and information exchange that society now expects and demands, but also by the fallibility of human deception detection, vulnerability exacerbated by new information technologies. Although automating deception detection is an appealing prospect, the complexity of detecting and countering deceptions that involve humans as source, conduit, or target defies a completely automated solution. A more promising approach is to integrate improved human detection with automated tools. The objectives of this minitrack are to encourage research papers that offer approaches and theories to detecting deception through one of the following: (1) synthesize applicable theories to create a model of deception and detection processes, (2) identify through experimental and longitudinal research systematic uncertainty-reduction and information-processing biases that make humans susceptible to false positives and false negatives, (3) identify reliable indicators of deceit under varying task and communication conditions, (4) develop a multi-pronged, computer-assisted training program to improve detection abilities, (5) create prototypes for automated tools to augment human detection, and (6) test integrated training program and automated tools to improve accuracy in distinguishing truthful from deceptive information and communications. To accomplish these objectives, this minitrack will bring together scientists and practitioners from the relevant fields of information systems, communication, criminology, psychology, artificial intelligence and warfare. The content of each session is as follows:

Session 1. Detection of Deception: Collaboration Systems and Technology

“Deception Detection Under Varying Electronic Media and Warning Conditions,”

“Inhibiting Deception and Its Detection,”

“Training to Detect Deception: An Experimental Investigation,”

Session 2. Detection of Deception: Collaboration Systems and Technology

“Can Online Behavior Tell a Deceiver? An Exploratory Investigation on Deception in Instant Messaging,”

“An Exploratory Study on Promising Cues in Deception Detection and Application of Decision Tree.”