Leader Member Exchange: An Interactive Framework to Uncover a Deceptive Insider as Revealed by Human Sensors

Shuyuan Mary Ho
School of Information
College of Communication and Information
Florida State University
smho@fsu.edu

Abstract

This study intends to provide a theoretical ground that conceptualizes the prospect of detecting insider threats based on leader-member exchange. This framework specifically corresponds to two propositions raised by Ho, Kaarst-Brown et al. [42]. Team members that are geographically co-located or dispersed are analogized as human sensors in social networks with the ability to collectively "react" to deception, even when the act of deception itself is not obvious to any one member. Close interactive relationships are the key to afford a network of human sensors an opportunity to formulate baseline knowledge of a deceptive insider. The research hypothesizes that groups unknowingly impacted by a deceptive leader are likely to use certain language-action cues when interacting with each other after a leader violates group trust.

Keywords: *computer-mediated deception*, *human computer interaction*, *insider threat*, *language-action cues*, *leader member exchange*

1. Introduction

Insider threat has been a complex and prolonged problem in the history of governments. Early espionage cases such as CIA agent Aldrich Ames and FBI agent Robert Hanssen provide examples of insiders that successfully deceived their colleagues. Both betrayed their organizations to sell national intelligence for personal profit, demonstrating the prolonged investigative challenges presented by a deceptive insider [1]. Studies have resulted in significant findings on illicit cyber activities within government sectors, as identified by the U.S. Secret Services and CERT/SEI [48], but insider threat incidents continue—and may be on the increase. After the 911 attacks, information-sharing across the governments was mandated, and easy access to information may have paved the way for Edward Snowden; a junior NSA contractor with elevated system administrator's privileges who compromised and disclosed thousands of classified documents without authorization in 2013. Soon after, CIA hacking tools were leaked by intelligence agents and contractors [72, 73], setting intelligence operations back many years. While digital innovation works to improve the public sector's ability to deliver value, and e-Government venues allow for novel systems capabilities and collaborative resources, the problem of insider threats increases by allowing the deceptive insider easy access to information (i.e., supported by the cloud computing services). The benefits of this innovation cannot be ignored, but the threat presented by rogue and deceptive insiders must also be addressed. Traditional case analysis approaches (e.g., [1, 48, 65]) do not allow for early threat identification of computer-mediated deception. New theoretical frameworks for understanding potential deceptive insider are urgently needed to balance the need for information sharing against the dangers of deceptive insiders accessing secrets and national intelligence within the government.

The pervasive adoption of computer-mediated technologies has created new opportunities for communication and online self-expression, enabling collaboration that transcends our physical space. However, computer-mediated technologies also present challenges in the establishment and maintenance of trusting relationships among members in virtual teams. Trust, irrespective of communication mode (computer-mediated or face-to-face), can be easily undermined by an act of deception [10, 11]. Ironically, when one communicating partner attempts to deceive another, s/he often will leverage the trust that has already been established with that partner to conceal the deception. When one group member attempts to deceive an entire group, particularly in a virtual team context, the deception unwittingly affects every interacting member

URI: https://hdl.handle.net/10125/59757
ISBN: 978-0-9981331-2-6

of the group, and can negatively impact the effectiveness of group communication as well as functional efficiency and operations.

Identifying deception has been explored in a wide range of facets and contexts. For example, Ekman and Friesen [18], [19] suggested deception leakage through facial expression and body gesture. Deception occurs frequently from everyday white lies [13, 67], to serious lies [16]. Verbal [15, 75], nonverbal [7, 8, 14, 83-85], and text-based [81] cues in deceivers' interpersonal communication have been effective clues for deception detection. Research on deception strategies [5, 6, 79], beneficiary [78], perceived credibility [24, 25], as well as cultural influences and media choice [23, 49] have collectively informed our understanding of "how" and "why" people deceive. Physiological and behavioral reactions, cognitive effort and stress can serve as indicators of deception [17, 59]. Moreover, automated credibility screening and assessment systems have been designed to evaluate the frequency of exposure to highly concealed information [20, 69, 70], and to conduct automated interviews that can detect deception [71] in face-to-face (FtF) settings. As rich as this deception research is, it has largely focused on the context of interpersonal communication. Several research efforts have been exploring the group's ability to detect deception in virtual teams settings. Marett and George [54], for example, suggested that interaction, diverse knowledgebase and distinct perspectives in a group will positively influence the deception detection. Moreover, a deceiver will typically strategize to establish credibility by presenting truthful information at first, followed by false information. Marett and George [55] later explored the motivation, characteristics and intrinsic factors of deceivers in relations with the group members, and found support for the idea that deceivers devise strategies to confuse with false information, and that groups in this situation detect deception better when they are collocated. Giordano and George [27] further suggested the correlation of task complexity with a group's ability to detect deception. That is, groups performing low-complexity tasks can detect deception better than groups performing high-complexity tasks. Groups with baseline knowledge of each other can detect deception better than groups without baseline knowledge of each other. These studies suggest that the more familiar and experienced the deceiver is with the group, the less likely the deceiver will succeed in deception. Because the impact of leader deception [31] in group-level communication can be significant, and could result in loss of organizational commitment, reputation or revenue, the present study furthers this inquiry by bolstering literature in leader deception within a group context, with specific reference to the impact exhibited by group dynamics when a leader becomes deceptive.

Unfortunately, effectively detecting insider threat presents great challenges. First, an insider's deception generally occurs subtly, and there are rarely detectable early warning signs. Second, detection of insider's deception requires acute observation and discernment. Inaccurate observations generate false positive alarms, and create a low trust atmosphere in the workplace. Third, although an insider refers to anyone in the organization, the present study specifically defines that an insider could be any individual with authorized access to information, that once betrayed, could inflict significant damage (e.g., reputational, or financial loss) against his or her own organization [42]. In this study, the term "leader" is metaphorically adopted to refer to those individuals who control critical information resources and whose access to certain essential information is granted. Thus, the leader's deception becomes the focus of this theoretical inquiry. Based on the above challenges, this study adopts a new theoretical framework that aims to review and evaluate the communications between a deceptive insider and group dynamics, while proposing to explore group dynamics objectively, rather than through group members' subjective cognitive perceptions as collected by survey instruments. More specifically, communication logs of virtual teams that include a deceptive leader are compared to those of control groups that do not. Moreover, the groups' collective reactions before and after a leader becomes deceptive are also hypothesized as being capable of indicating a possible insider threat occurrence.

This paper discusses an inquiry into the influences of deceptive leaders' behaviors on the collective perspectives of virtual teams, and intends to address the research question: *How is communication in a virtual team collectively impacted to reflect the presence of a deceptive leader*? To answer this question, leader-member exchange (LMX) and deception literature are reviewed and discussed. Ho, Kaarst-Brown *et al.* [42] boldly postulated that "humans as smart sensors can understand and interpret subtle communication signals associated with reduced trustworthiness" (p. 276). Based on this proposition, the present study framework further develops the rationale for observing patterns of language-action cues in a virtual group's interactive communication behavior that can collectively "react" and change after a leader has taken covert actions to deceive.

2. Group Trust in Leader Member Exchange

Trust influences and impacts interpersonal relationships, as well as the relationships within, between, and among groups [45]. In a group context, trust is essentially necessitated by the interdependence of the group members. Each member of the group is expected to fulfill a designated role and perform certain responsibilities that contribute to the group's collective goal(s). As such, each member's ability to perform their own tasks to some extent depends upon others also performing their respective designated responsibilities. Group trust depends on the interaction and relationships between leaders and their group members. Team leaders play an essential role in establishing and maintaining trust among members of a team, and members develop exchange relationships with their leaders [76]. Group trust can be influenced by a leader's behavior and leadership style. Dansereau, Graen *et al.* [12], Liden and Graen [50] and many colleagues proposed the dyadic exchange between leader and subordinates concerning organizational behavior. Liden, Wayne *et al.* [51] suggested that leaders tend to develop different leadership styles, relationships or exchange with different subordinates. Moreover, Bauer, Green *et al.* [2] suggested that "leader-member exchange is intertwined with the concept of mutual trust" (p. 1541). The importance of the interaction between the leader and members was emphasized, especially when building group trust [26, 52]. Different leadership styles engender different group communication patterns and performance outcomes [53]. On the other hand, members of a group can also develop different types of social exchange relationships both with other group members as well as with their immediate supervisors. As leaders represent organizational support, LMX social exchange can influence and mediate members' perception of the overall organizational support [76]. The differences in leader-member exchanges within a group will impact the group members' work attitudes, as well as coworkers' relationships with each other. Erdogan and Bauer [22] noted that while low-quality leader/ member exchanges typically put less favored employees/ members at a disadvantage in terms of resource distribution and promotion; high-quality leader/member exchanges often result in faster advancement and productivity for a favored employee/ member. LMX differentiation is the extent to which a leader's behavior affects (encourages or undermines) group trust and performance outcomes [35, 53]. That is, perceived injustices by a group leader against certain group members can negatively affect the attitudes, interactions, sense of loyalty and commitment of all group members [21, 22]. Moreover, group members may withdraw (i.e., reduce interactivity/ participation) when they perceive an imbalance in fairness or justice.

One's trust towards an individual can be impacted (i.e., reduced or lost) as a result of the violation of competence in the performance of obligations, or the violation of integrity [42]. Competence-based trust violations occur when group members feel betrayed because a member does not fulfill obligations or expectations. This breach of trust occurs as a result of "incongruence" [57] arising from a violation against the reciprocal exchanged agreements (often referred to as a "psychological contract") by and among group members [63, 66]. Integrity-based trust violations, on the other hand, occur when a member behaves against the interests of the group in an illegal or unethical manner [36, 40, 42]. This violation of integrity-based trust, often triggered by a leader's ethical dilemma, constitutes an act of deception [40]. When this leader violates group trust, not only does the violation significantly impact the functions and effectiveness of a group, but his/her intimate knowledge of the group's activities and privileged access to relevant information may also jeopardize intellectual property and information assets. Jones and Marsh [46] stated that in some cases, the cause(s) of a loss of group trust may be superficial and relatively minor (e.g., personality clashes between individual group members), having only a small overall impact on group efficacy. However, the loss of group trust can also result in the loss of a leader's credibility within the group, which can further impact his/her leadership [c.f., 66]. The group's perception of the leader's credibility is a primary source of influence leveraged by the leader to manage the group and its members. George, Giordano *et al.* [25] pointed out that credibility assessments/perceptions can change over time. Individuals with higher perceived credibility are more likely to be trusted than those with lower credibility [c.f., 24]. In turn, loss of credibility within the group can trigger suspicion and motivate other members to detect deception. That is, those group members are apt to be more sensitive toward the leader's behavior vis-à-vis group interaction. Motivation as one of the antecedents can be essential in successful deception detection. The more motivated members are to identifying deception, the easier it is to find a communicator that is not creditable; however, the number of false alarms accompany the detection may also increase [24].

When the leader breaches a psychological contract by deceiving (or attempting to deceive) fellow members of a group, the dynamics of deception in group communication becomes more complex than deception in one-on-one interpersonal communication. The deceptive leader's persuasive strategy must

account for multiple, interactive perspectives, which often requires a deceiver to leverage and combine cognitive and affective processes. That is, regardless of whether trust within a group is built on cognitive factors, affective factors or a combination, when trust is observed as being violated by a deceptive leader, subordinates' perception and commitment to the organization may be negatively influenced [31]. Furthermore, the group's collective view and assessment of the deceptive leader's behavior will be impacted, and overall group trust may be undermined. This, in turn, results in less effective group interactions, and ultimately (negatively) affects the group's overall performance.

3. Close Relationships

Close relationships and interaction within the group allows an opportunity for group members to construct baseline expectations and build trust with each other [43, 44, 62]. As group size and task characteristics would necessitate differences in ways people interact in groups, Hackman and Vidmar [32] empirically proved that optimal satisfaction is found with groups having four to five members (pp. 48-49). Wheelan [77] also confirmed that groups containing 3 to 6 members were significantly more productive and developmental than larger groups. The present study thus suggests designing experiments to facilitate small group situations where members are given opportunities to interact closely [41], which also follows the proposition postulated by Ho, Kaarst-Brown *et al.* [42] that "close relationships" are required to afford groups the opportunities to unknowingly observe subtle language-action cues that may indicate a lowering of trustworthiness (p. 276).

Highly controlled and structured research design can allow researchers to collect a large dataset of parsed language-action cues as repeated measures, which represent the objective perspectives of virtual teams' interaction.

4. Language-Action Cues in Deception

Ekman and Friesen [18] characterized deception as the purposeful concealment of the truth, either by omission or commission. Deception typically involves a persuasive, strategic process by which a deceiver transmits messages that have been deliberately distorted and/or manipulated, with the intention of misleading or misdirecting a receiver into reaching a wrong conclusion, or otherwise fostering a false belief, often for the deceiver's own benefit [6]. Buller and Burgoon [6] proposed Interpersonal Deception Theory (IDT), which explores the chess-like "move/counter-move" aspect of deception. Vrij [74] referred to deception as an intentional and volitional act. It would be an act of deception to convey a message knowing it to be false. However, it would not be an act of deception to convey a false message while believing it to be true [74, p. 5]. Gneezy [28] suggested that deception is often motivated by self-interest, and just as often results in an outcome that is detrimental to the other party(ies) involved. Deception occurs not only in face-to-face interactions, but also frequently occurs within computer-mediated communication (i.e., e-mail, instant-message, or group chat).

4.1. Language-Action Cues

Computer-mediated communication enables information to be transferred to a message receiver through words and a pattern of communication cues. These cues can reveal both the overt and covert intent of a message sender. However, in this cue-lean environment, the availability of such cues is effectively limited to the text itself without the physical cues in FtF communication. Nonetheless, even in 'cue lean' text-based communication, there can be linguistic and syntactical cues of deception. For example, Newman, Pennebaker *et al.* [58] suggested that the overuse of sensory or spatiotemporal words, and changes in the diversity and complexity of language have been shown to be suggestive of deception. Zhou, Burgoon *et al.* [80] noted that deceivers tend to be more casual and expressive in their linguistic style. Level of detail (too much or too little) may also be indicative of deception in both FtF and CMC communication. Deceivers in CMC particularly tend to be wordier than truth-tellers, but the additional words (i.e., detail) provided are not necessarily relevant or meaningful in context [82]. Not only so, Hancock, Curry *et al.* [33] discovered that deceivers tend to use more sense-based words (e.g., seeing, touching), few self-oriented but more other-oriented pronouns in text-based CMC. Enabled with multiple cues and immediate feedbacks, richer media can increase the ability of message receivers to perceive and thus facilitate the deception detection [47]. However, simply knowing these linguistic cues does not help conversational partners to improve deception detection. Hancock, Birnholtz *et al.* [34] suggested that certain language-action cues (e.g., first-person references, words of emotion or inhibition, etc.) have been shown to be effective indicators to differentiate deceivers from truth tellers. While, in general, humans are poor at detecting deception, Ho, Hancock *et al.* [39] computationally identified deceivers' strategies through the use of salient language-action cues, which include the use of words associated with affective processes, cognitive

processes, self- and other- references, as well as the use of peripheral expressions and overall wordiness.

The importance of immediacy cues and the representation of these cues illustrate psychological elements of communication [7-9]. A message sender may employ cues to associate (or distance) him/herself physically or psychologically from the content of a message [56, p. 203]. Buller and Burgoon [5] noted that deceivers often use both verbal and nonverbal means to "distance [him/herself] from others, to disaffiliate, and to close off scrutiny or probing communication" (p. 204). These include cues of (1) uncertainty and vagueness, (2) nonimmediacy, reticence, and withdrawal, (3) disassociation, and (4) image- and relationship-protecting behavior [5, p.204]. Similarly, social distance theorists [c.f., 13] suggested that a deceptive actor will try to minimize potential cues to minimize the cognitive load associated with deception, by adopting a cue-lean communication mode or style and thereby limiting opportunities for others to question or engage him/her in conversation. In FtF communication, a deceiver can create psychological distance by exhibiting literal (physical) distance (e.g., standing/ sitting remotely from the conversational party), or perhaps by choosing to interact via the telephone rather than meeting in physical space [56]. Likewise, in CMC communication, psychological distance can be created through word choice and phraseology—that is, minimizing immediacy [5]. Word choice and overall tone that suggest negative feelings (such as disappointment, frustration, or even anger) may be a sign of distancing, while word choice and tone suggesting a positive relationship—perhaps conveying humor or praise—can foster a positive, trusting relationship between communicating actors.

4.2. Deceptive Leader's Language-Action Cues

Several studies have been conducted to illustrate how a deceptive insider's behavior can be uncovered. Schultz [64], for example, speculated on a set of behavioral cues that can be used to predict deceptive insider attacks, including deliberate markers, meaningful errors, preparatory behavior, correlated use patterns, verbal behavior, and personality traits. Greitzer, Kangas *et al.* [29], [30] attempted to create a behavioral/ psychological model that can identify deceptive insiders with a view towards preemptive intervention. The focus in these models involves categorizing and modeling behaviors and psycholinguistic cues [3, 4, 68]. Brown, Watkins *et al.* [4] focused on linguistics—specifically, translating observed linguistic cues into behavioral categories identified as corresponding to behaviors significantly associated with deceptive insiders. Ho, Hancock *et al.* [40] further the investigation by setting up insider threat experiments with the complexity of objectives and tasks as controlled variables, and identifying that deceptive leaders can successfully conceal their deceptive intent in leader-member exchange. In other words, no statistical significant differences were found in deceptive leaders' language-action cues after they were influenced to betray. No statistical significant differences were found in a deceptive leader's language-action cues when compared with those of non-deceptive leaders. However, these findings only examine CMC deception from the perspective of the leaders' communication.

4.3. Language-Action Cues in Group Dynamics

Taylor, Dando *et al.* [68] on the other hand examined the use of language-action cues (specifically, personal pronouns, as well as words conveying negative emotions and cognitive processes) in the context of deception through (asynchronous) e-mail exchanges, within and between teams in a common physical location. An insider threat experiment was conducted in which 25% of the participants were incentivized to "act" (i.e., pretend) to be deceptive insiders. Their study discovered that insiders who were told to pass information—without authorization—to a provocateur seemed to be more self-focused, and used more linguistic features associated with negative emotion and cognitive processes than non-deceptive insiders in the same group. Specifically, Taylor, Dando *et al*.'s [68] findings indicate that the deceptive insiders used more personal pronouns than others in their group. Additionally, Taylor, Dando *et al.* [68] found that the designated deceivers also used more words associated with cognitive processes (particularly discrepancy and tentative).

5. Hypotheses Development

Previous studies suggest that although no statistical significance was found when comparing a deceptive leader's language-action cues with those of non-deceptive leaders, and when comparing a deceptive leader's language-action cues after they are incentivized to betray, it is possible to learn insights about the deceptive leaders from the interaction, as well as the reaction of the group members. That is, the language-action cues including wordiness and expressiveness (i.e., overall word count), as well as cognitive processes (i.e., words associated with insight, causation, discrepancy, certainty, inclusivity and exclusivity) and affective processes (i.e., words associated with positive and negative emotion) [60, 61]

can be indicative of deceptive insider's intent from the perspective of the group dynamics. Building on these research insights, the current study hypothesizes on each of these cue-types, and presents three sets of hypotheses with respect to each.

5.1. Expressiveness and Wordiness

First, we consider overall word counts of the communication within groups that include a deceptive leader, and expect to observe the leader's deception through wordiness and expressiveness that stimulates group communication. Ho, Hancock *et al.* [38], [40] suggested that group members will often sense this, resulting in more conversations as a whole. Thus, we attempt to aggregate and parse out word counts of all group members (including the deceptive leader), and we hypothesize that groups including deceptive leaders will likewise exhibit a higher overall word count than groups without a deceptive leader. That is, we would expect the overall word count of the groups that include deceptive leaders to be higher, because a deceptive leader stimulates more expression and words overall. Second, we would expect that the overall word counts of groups that include a deceptive leader will increase after the leader acts with deceptive intent. In this hypothesis, the deceptive leader is influenced to betray the organization for personal gain, rather than merely acting (i.e., pretending) to betray. Thus, the groups' overall word counts are hypothesized to increase after the betrayal influence in a natural setting. Accordingly, the following hypotheses are proposed:

H1(a). *Communication within groups that include a deceptive leader (treatment groups) will display more words overall than communication within groups consisting only of non-deceptive leaders (control groups) in a synchronous CMC group environment*.

H1(b). *Groups that include a deceptive leader will display an increase of total word count after this leader has initiated a process of deception*.

5.2. Cognitive Process

As the most prominent insider threat cases are often committed by those who are in power positions and betray inherent trust [37, 38], we note that certain influences can be found in the deceptive leader's exchange with the subordinates, and further impact the subordinates commitment to the organization [31]. Griffith, Connelly *et al.* [31] validated the deceptive leader's influences on leader-member exchange using survey instruments, while Ho, Hancock *et al*. [37, 38] simulated experiments to investigate the differences in language-action cues between deceptive leaders and non-deceptive leaders in group interaction, and specifically how language-action cues from groups that include a deceptive leader differed from those of groups that did not include a deceptive leader.

Ho, Hancock *et al*.'s [37, 38] findings are consistent with Taylor, Dando *et al*.'s [68] findings, suggesting that, in both asynchronous and synchronous communication, deceptive leaders can be expected to use more words associated with cognitive processes in their communication than other members from the same group. In a different set of hypotheses, Ho, Hancock *et al.* [40] further identified differences in language-action cues—not only between deceptive leaders and non-deceptive leaders—but also between groups with a deceptive leader and groups without one. Ho, Hancock *et al.* [40] acknowledged that the cues to a leader's deceptive behavior tend to be subtle, and may be hidden or even unnoticeable. The results also support the proposition that a statistically significant difference can be found in language-action cues between groups with a deceptive leader and groups without one. Our present study, thus, takes a further step to examine the group's collective use of words associated with cognitive processes i.e., words connoting inclusion, exclusion, certainty and insight, and how these types of language-action cues are manifested in patterns of group communication.

As a deceptive leader will influence the LMX [31], the study further posits that, as a result of a deceptive leader distancing him-/ herself from other team members, the group as a whole will sense a change—specifically, a difference in the leader's communication (e.g., use of more cue-lean communication modes, and distancing behaviors) [40]. As the deceptive leader attempts to disguise his/her deceptive intent, groups may collectively interact with the deceptive leader in ways that display less cognitive process (i.e., certainty, inclusion, suggestions, or insight). Accordingly, the following two hypotheses are proposed:

H2(a). *Communication within groups that include a deceptive leader (treatment groups) will display fewer words relating to cognitive process than communication within groups consisting of only non-deceptive leaders (control groups) in a synchronous CMC group environment*.

H2(b). *Groups that include a deceptive leader will display an increase of cognitive process after this leader has initiated a process of deception*.

5.3. Affective Process

Moreover, as a deceptive leader will influence LMX [31], the study further proposes that a deceptive leader's changed behavior can influence and infect an associated group with negative emotions. While the changed behavior of a deceptive leader may initially prompt analytical discussion amongst team members (i.e., the use of cognitive-process words reflecting uncertainty, discrepancy, insight, causation, question, etc.), the interaction within groups having a deceptive leader will quickly reflect affective processing (e.g., confusion, concern, emotion, frustration, or even apathy) [40]. Thus, the group's collective use of words after deception has been initiated could have been more associated with affective processes, and the study suggests that groups including a deceptive leader are likely to show more emotion (i.e., affect) in their discussions, using more words reflecting affective processes (i.e., confusion, concern, frustration, or even apathy). Accordingly, the study proposes the following hypotheses on these cues in group dynamics:

H3(a). *Communication within groups that include a deceptive leader (treatment groups) will display more words of affect than communication within groups consisting only of non-deceptive leaders (control groups) in a synchronous CMC group environment*.

H3(b). *Groups that include a deceptive leader will display an increase of affect after this leader has initiated a process of deception*.

6. Recommendations and Future Work

This proposed framework can be empirically tested through simulating insider threat scenario-based experiments [42]. Data of group interaction can be collected to provide insight by comparing groups with vs. without incentives used to lure individuals to betray or to deceive the members of the same group. Experiments can also be set up to compare groups whose individuals are lured, but do not accept the incentive.

Future analysis should focus on how group members collectively react and respond in situations where a leader becomes deceptive (i.e., "active" versus "passive" deception), not on the activities carried out during the deception. Future research may benefit from a revised design that manipulates this variable by offering different incentives for active versus passive deception.

7. Conclusion and Contributions

Insider threat detection and analysis involve multiple factors, and a better understanding of the leader's trustworthiness dynamic in context. The framework illustrated in this paper supports the two propositions raised by Ho, Kaarst-Brown *et al.* [42] that group members work as smart sensors in close relationships to objectively reflect in their communication the subtle changes of the deceptive insider's reduced trustworthiness (p. 276). This framework provides a base for insider threat detection through understanding of the group dynamics.

Trust is essential for any group and organization to function. When a team leader violates trust, the leader's deceptive behavior can influence the group's communication and performance. Moreover, the collective language-action cues can be observed and collected as repeated measures during group interaction. To emphasize, the collective language-action cues can be indicative when deception is present, and especially when the interaction within a team provides context for members to unknowingly become a network of sensors. Deceptive intent can be identified through the analysis of group interaction, and the analysis of a multilevel model can be an effective means in outing a deceptive leader. Organizations may consider the analysis of group interaction as one potential way to understand and identify leader deception.

8. References

[1] Band, S.R., D.M. Capelli, L.F. Fischer, A.P. Moore, E.D. Shaw, and R.F. Trzeciak. *Comparing insider IT sabotage and espionage: A model-based analysis*, in *Technical Report*, 2006. Software Engineering Institute (SEI): Carnegie Mellon University. 1-91.

[2] Bauer, T.N., S.G. Green, and T.N. Bauer. *Development of leader-member exchange: A longitudinal test.* The Academy of Management Journal, 1996. **39**(6): 1538-1567. doi:10.2307/257068.

[3] Brown, C.R., F.L. Greitzer, and A. Watkins. *Toward the development of a psycholinguistic-based measure of insider threat risk focusing on core word categories used in social media*. in *2013 Americas Conference on Information Systems*. 2013. Chicago, Illinois: AIS, 1-8.

[4] Brown, C.R., A. Watkins, and F.L. Greitzer. *Predicting insider threat risks through linguistic analysis of electronic communication*. in *2013 46th Hawaii International Conference on System Sciences*. 2013. Wailea, Hawaii: IEEE, 1849-1858. doi:10.1109/HICSS.2013.453.

[5] Buller, D.B. and J.K. Burgoon. *Deception: Strategic and nonstrategic communication.* Strategic Interpersonal Communication, 1994: 191-223.

[6] Buller, D.B. and J.K. Burgoon. *Interpersonal deception theory.* Communication Theory, 1996. **6**(3): 203-242.

[7] Burgoon, J.K. and D.B. Buller. *Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics.* Journal of Nonverbal Behavior, 1994. **18**(2): 155-184. doi:10.1007/BF02170076.
[8] Burgoon, J.K., D.B. Buller, L. Dillman, and J.B. Walther. *Interpersonal deception. IV. Effects of suspicion on perceived communication and nonverbal behavior dynamics.* Human Communication Research, 1995. **22**(2): 163-196.
[9] Burgoon, J.K., J.P. Blair, T. Qin, and J.F. Nunamaker. *Detecting deception through linguistic analysis.* Intelligence and Security Informatics, 2003. **2665**: 91-101.
[10] Burgoon, J.K., G.M. Stoner, J.A. Bonito, and N.E. Dunbar. *Trust and deception in mediated communication*. in *Proceedings of the 2003 Hawaii International Conference on System Sciences (HICSS-36)*. 2003. Big Island, Hawaii: IEEE. doi:10.1109/HICSS.2003.1173792.
[11] Castelfranchi, C. and Y.-H. Tan, ***Trust and deception in virtual societies***. 2001: Springer Netherlands.
[12] Dansereau, F., G. Graen, and W.J. Haga. *A vertical dyad linkage approach to leadership within formal organizations: A longitudinal investigation of the role making process.* Organizational Behavior and Human Performance, 1975. **13**(1): 46-78. doi:10.1016/0030-5073(75)90005-7.
[13] DePaulo, B.M., D.A. Kashy, S.E. Kirkendol, M.M. Wyer, and J.A. Epstein. *Lying in everyday life.* Journal of Personality and Social Pyschology, 1996. **70**(5): 979-995. doi:0022-3514/96.
[14] DePaulo, B.M. and H.S. Friedman. *Nonverbal communication*, in *The Handbook of Social Psychology*, Gilbert, D.T., S.T. Fiske, and G. Lindzey. 1998. The McGraw-Hill Companies, Inc.: New York. 3-40.
[15] DePaulo, B.M., J.J. Lindsay, B.E. Malone, L. Muhlenbruck, K. Charlton, and H. Cooper. *Cues to deception.* Pyschological Bulletin, 2003. **129**: 74-112.
[16] DePaulo, B.M., M.E. Ansfield, S.E. Kirkendol, and J.M. Boden. *Serious lies.* Basic and applied social psychology, 2004. **26**(2&3): 147-167.
[17] Derrick, D.C., A.C. Elkins, J.K. Burgoon, J.F. Nunamaker Jr., and D.D. Zheng. *Border security credibility assessments via heterogeneous sensor fusion.* IEEE Intelligent Systems, 2010. **25**(3): 41-49. doi:10.1109/MIS.2010.79.
[18] Ekman, P. and W.B. Friesen. *Nonverbal leakage and clues to deception.* Psychiatry, 1969. **32**: 88-106.
[19] Ekman, P. and W.V. Friesen. *Detecting deception from the body or face.* Journal of Personality and Social Pyschology, 1974. **29**(3): 288-298. doi:10.1037/h0036006.
[20] Elkins, A.C., N.E. Dunbar, B. Adame, and J.F. Nunamaker Jr. *Are users threatened by credibility assessment systems?* Journal of Management Information Systems, 2013. **29**(4): 249-261. doi:10.2753/MIS0742-1222290409.
[21] Erdogan, B., R.C. Liden, and M.L. Kraimer. *Justice and leader-member exchange: The moderating role of organizational culture.* The Academy of Management Journal, 2006. **49**(2): 395-406.
[22] Erdogan, B. and T.N. Bauer. *Differentiated leader-member exchanges: The buffering role of justice climate.* Journal of Applied Psychology, 2010. **95**(6): 1104-1120. doi:10.1037/a0020578.
[23] Furner, C.P. and J.F. George. *Cultural determinants fo media choice for deception.* Computers in Human Behavior, 2012. **28**(4): 1427-1438. doi:10.1016/j.chb.2012.03.005.
[24] George, J.F., P.A. Tilley, and G. Giordano. *Sender credibility and deception detection.* Computers in Human Behavior, 2014. **35**: 1-11. doi:10.1016/j.chb.2014.02.027.
[25] George, J.F., G. Giordano, and P.A. Tilley. *Website credibility and deceiver credibility: Expanding prominence-Interpretation Theory.* Computers in Human Behavior, 2016. **54**: 83-93. doi:10.1016/j.chb.2015.07.065.
[26] Gerstner, C.R. and D.V. Day. *Meta-analytic review of leader-member exchange theory: Correlates and construct issues.* Journal of Applied Psychology, 1997. **82**(6): 827-844. doi:10.1037/0021-9010.82.6.827.
[27] Giordano, G. and J.F. George. *The effects of task complexity and group member experience on computer-mediated groups facing deception.* IEEE Transactions on Professional Communication, 2013. **56**(3): 210-225. doi:10.1109/TPC.2013.2273817.
[28] Gneezy, U. *Deception: The role of consequences.* The American Economic Review, 2005. **95**(1): 384-394. doi:10.1257/0002828053828662.
[29] Greitzer, F.L., L.J. Kangas, C.F. Noonan, A.C. Dalton, and R.E. Hohimer. *Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats*. in *2012 45th Hawaii International Conference on System Sciences*. 2012. Maui, Hawaii: IEEE, 2392-2401. doi:10.1109/HICSS.2012.309.
[30] Greitzer, F.L., L.J. Kangas, C.F. Noonan, C.R. Brown, and T. Ferryman. *Psychosocial modeling of insider threat risk based on behavioral and word use analysis.* e-Service Journal, 2013. **9**(1): 106-138. doi:10.2979/eservicej.9.1.106.
[31] Griffith, J.A., S. Connelly, and c.E. Thiel. *Leader deception influences on leader-member exchange and suborginate organizational commitment.* Journal of Leadership & Organizational Studies, 2011. **18**(4): 508-521. doi:10.1177/1548051811403765.
[32] Hackman, J.R. and N. Vidmar. *Effects of size and task type on group performance and member reactions.* Sociometry, 1970. **33**(1): 37-54. doi:10.2307/2786271.
[33] Hancock, J., L.E. Curry, S. Goorha, and M. Woodworth. *On lying and being lied to: A linguistic analysis of deception in computer-medicated communication.* Discourse Process, 2008. **45**(1): 1-23. doi:10.1080/01638530701739181.
[34] Hancock, J., J. Birnholtz, N. Bazarova, J. Guillory, J. Perlin, and B. Amos. *Butler lies: Awareness, deception and design*. in *CHI'09*. 2009. Boston, MA: ACM.
[35] Henderson, D.J., R.C. Liden, B.C. Glibkowski, and A. Chaudhry. *LMX differentiation: A multilevel review and examination of its antecedents and outcomes.* The Leadership Quarterly, 2009. **20**(4): 517-534. doi:10.1016/j.leaqua.2009.04.003.
[36] Ho, S.M. and I. Benbasat. *Dyadic attribution model: A mechanism to assess trustworthiness in virtual organizations.* Journal of the Association for Information Science and Technology, 2014. **65**(8): 1555-1576. doi:10.1002/asi.23074.
[37] Ho, S.M., H. Fu, S.S. Timmarajus, C. Booth, J.H. Baeg, and M. Liu. *Insider threat: Language-action cues in group dynamics*. in *SIGMIS-CPR'15*. 2015. Newport Beach, CA: ACM, 101-104. doi:10.1145/2751957.2751978.

[38] Ho, S.M., J.T. Hancock, C. Booth, M. Burmester, X. Liu, and S.S. Timmarajus. *Demystifying insider threat: Language-action cues in group dynamics*. in *HICSS-49*. 2016. Kauai, Hawaii: IEEE Computer Society, 2729-2738. doi:10.1109/HICSS.2016.343.

[39] Ho, S.M., J.T. Hancock, C. Booth, and X. Liu. *Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication.* Journal of Management Information Systems, 2016. **33**(2): 393-420. doi:10.1080/07421222.2016.1205924.

[40] Ho, S.M., J. Hancock, and C. Booth. *Ethical dilemma: Deception dynamics in computer-mediated group communication.* Journal of the Association for Information Science and Technology, 2017. **68**(12): 2729-2742. doi:10.1002/asi.23849.

[41] Ho, S.M. and M. Wartentin. *Leader's dilemma game: An experimental design for cyber insider threat research.* Information Systems Frontiers, 2017. **19**(2): 377-396. doi:10.1007/s10796-015-9599-5.

[42] Ho, S.M., M. Kaarst-Brown, and I. Benbasat. *Trustworthiness attribution: Inquiry into insider threat detection.* Journal of the Association for Information Science and Technology, 2018. **69**(2): 271-280. doi:10.1002/asi.23938.

[43] Holmes, J.G. and J.K. Rempel. *Trust in close relationships*, in *Review of Personality and Social Psychology*, Hendrick, C. 1989a. Sage: Beverly Hills, CA.

[44] Holmes, J.G. and J.K. Rempel. *Trust in close relationships*, in *Close Relationship*, Hendrick, C. 1989b. Sage: Newbury Park, CA. 187-220.

[45] Hosmer, L.T. *Trust: The connecting link between organizational theory and philosophical ethics.* Academy of Management Review, 1995. **20**(2): 379-403.

[46] Jones, S. and S. Marsh. *Human-computer-homan interaction: Trust in CSCW*. ACM SIGCHI Bulletin, 1997. **29**(3): 36-40. doi:10.1145/264853.264872.

[47] Kahai, S.S. and R.B. Cooper. *Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality.* Journal of Management Information Systems, 2003. **20**(1): 263-299.

[48] Kowalski, E., T. Conway, S. Keverline, M. Williams, D. Cappelli, B. Willke, and A. Moore. *Insider threat study: Illicit cyber activity in the government sector*, edited by Service, U.S.S., 2008. National Threat Assessment Center & CERT Program.

[49] Lewis, C.C. and J.F. George. *Cross-cultural deception in social networking sites and face-to-face communication.* Computers in Human Behavior, 2008. **24**(6): 2945-2964. doi:10.1016/j.chb.2008.05.002.

[50] Liden, R.C. and G. Graen. *Generalizability of hte vertical dyad linkage model of leadership.* Academy of Management Review, 1980. **23**(3): 451-465. doi:10.2307/255511.

[51] Liden, R.C., S.J. Wayne, and D. Stilwell. *A longitudinal study on the early development of leader-member exchanges.* Journal of Applied Psychology, 1993. **78**(4): 662-674. doi:10.1037/0021-9010.78.4.662.

[52] Liden, R.C., R.T. Sparrowe, and S.J. Wayne. *Leader-member exchange theory: The past and potential for the future.* Research in Personnel and Human Resources, 1997. **15**: 47-119.

[53] Liden, R.C., B. Erdogan, S.J. Wayne, and R.T. Sparrowe. *Leader-member exchange, differentiation, and task interdependence: Implications for individual and group performance.* Journal of Organizational Behavior, 2006. **27**(6): 723-746. doi:10.1002/job.409.

[54] Marett, L.K. and J.F. George. *Deception in the case of one sender and multiple receivers.* Group Decision and Negotiation, 2004. **13**(1): 29-44. doi:10.1023/B:GRUP.0000011943.73672.9b.

[55] Marett, L.K. and J.F. George. *Barriers to deceiving other group members in virtual settings.* Group Decision and Negotiation, 2013. **22**(1): 89-115. doi:10.1007/s10726-012-9297-3.

[56] Mehrabian, A. *Methods & designs: Some referents and measures of nonverbal behavior.* Behavior Research Methods & Instrumentation, 1968. **1**(6): 203-207.

[57] Morrison, E.W. and S.L. Robinson. *When employees feel betrayed: A model of how psychological contract violation develops.* Academy of Management Review, 1997. **22**(1): 226-256.

[58] Newman, M.L., J.W. Pennebaker, D.S. Berry, and J.M. Richards. *Lying words: Predicting deception from linguistic styles.* Personality and social psychology bulletin, 2003. **29**(5): 665-675.

[59] Nunamaker Jr., J.F., D.C. Derrick, A.C. Elkins, J.K. Burgoon, and M.W. Patton. *Embodied conversational agent-based kiosk for automated interviewing.* Journal of Management Information Systems, 2011. **28**(1): 17-48. doi:10.2753/MIS0742-1222280102.

[60] Pennebaker, J.W. and L.A. King. *Linguistic styles: Language use as an individual difference.* Journal of Personality and Social Pyschology, 1999. **77**(6): 1296-1312. doi:10.1037/0022-3514.77.6.1296.

[61] Pennebaker, J.W., M.R. Mehl, and K.G. Niederhoffer. *Psychological aspects of natural language use: Our words, our selves.* Annual Review of Psychology, 2003. **54**: 547-577. doi:10.1146/annurev.psych.54.101601.145041.

[62] Remple, J.K., J.G. Holmes, and M.P. Zanba. *Trust in close relationships.* Journal of Personality and Social Pyschology, 1985. **49**(1): 95-112. doi:10.1037/0022-3514.49.1.95.

[63] Robinson, S.L. *Trust and breach of the psychological contract.* Administrative Science Quarterly, 1996. **41**(4): 574-599. doi:10.2307/2393868.

[64] Schultz, E.E. *A framework for understanding and predicting insider attacks.* Computers & Security, 2002. **21**(6): 526-531.

[65] Shaw, E. and L. Sellers. *Application of the critical-path method to evaluate insider risks.* Studies in Intelligence, 2015. **59**(2): 1-8.

[66] Simons, T. *Behavioral integrity: The perceived alignment between managers' words and deeds as a research focus.* Organization Science, 2002. **13**(1): 18-35. doi:10.1287/orsc.13.1.18.543.

[67] Smith, M.E., J.T. Hancock, L. Reynolds, and J. Birnholtz. *Everyday deception or a few prolific liars? The prevalence of lies in text messaging.* Computers in Human Behavior, 2014. **41**: 220-227. doi:10.1016/j.chb.2014.05.032.

[68] Taylor, P.J., C.J. Dando, T.C. Ormerod, L.J. Ball, M.C. Jenkins, A. Sandham, and T. Menacere. *Detecting insider threats through language change.* Law and Human Behavior, 2013. **37**(4): 267-275. doi:10.1037/lhb0000032.

[69] Twyman, N.W., A.C. Elkins, J.K. Burgoon, and J.F. Nunamaker Jr. *A rigidity detection system for automated credibility assessment.* Journal of Management Information Systems, 2014. **31**(1): 173-202. doi:10.2753/MIS0742-1222310108.

[70] Twyman, N.W., P.B. Lowry, J.K. Burgoon, and J.F. Nunamaker Jr. *Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals.* Journal of Management Information Systems, 2014. **31**(3): 106-137. doi:10.1080/07421222.2014.995535.

[71] Twyman, N.W., J.G. Proudfoot, R.M. Schuetzler, A.C. Elkins, and D.C. Derrick. *Robustness of multiple indicators in automated screening systems for deception detection.* Journal of Management Information Systems, 2015. **32**(4): 215-245. doi:10.1080/07421222.2015.1138569.

[72] Vault 7. CIA Hacking tools revealed, WikiLeaks, March 23, 2017.

[73] Vault 8. CIA Hacking tools revealed, WikiLeaks, November 9, 2017.

[74] Vrij, A., ***Detecting lies and deceit: The Psychology of lying and the implications for professional practice***. 2000. New York, NY: John Wiley & Sons Ltd.

[75] Vrij, A. *Verbal lie detection tools: Statement validity analysis, reality monitoring and scientific content analysis*, in *Detecting deception: Current challenges and cognitive approaches*, edited by Granhag, P.A., A. Vrij, and B.e. Verschuere, 2015. Wiley-Blackwell: Malden, MA. 3-35.

[76] Wayne, S.J., L.M. Shore, and R.C. Liden. *Perceived organizational support and leader-member exchange: A social exchange perspective.* The Academy of Management Journal, 1997. **40**(1): 82-111.

[77] Wheelan, S.A. *Group size, group development and group productivity.* Small Group Research, 2009. **40**(2): 247-262. doi:10.1177/1046496408328703.

[78] Whitty, M.T. and S.E. Carville. *Would I lie to you? Self-serving lies and other-oriented lies told across different media.* Computers in Human Behavior, 2008. **24**(3): 1021-1031. doi:10.1016/j.chb.2007.03.004.

[79] Whitty, M.T., T. Buchanan, A.N. Joinson, and A. Meredith. *Not all lies are spontaneous: An examination of deception across different modes of communication.* Journal of the American Society for Information Science and Technology, 2012. **63**(1): 208-216. doi:10.1002/asi.21648.

[80] Zhou, L., J.K. Burgoon, J.F. Nunamaker Jr., and D.P. Twitchell. *Automating linguistics-based cues for detecting deception in text-based asynchronous computer-mediated communication.* Group Decision and Negotiation, 2004. **13**(1): 81-106. doi:10.1023/B:GRUP.0000011944.62889.6f.

[81] Zhou, L., J.K. Burgoon, D.P. Twitchell, T. Qin, and J.F. Nunamaker Jr. *A comparison of classification methods for predicting deception in computer-mediated communication.* Journal of Management Information Systems, 2004. **20**(4): 139-165.

[82] Zhou, L. and D. Zhang. *Can online behavior unveil a deceiver?* in *Proceedings of the 2004 Hawaii International Conference on System Sciences (HICSS-37)*. 2004. Hilton Waikoloa Village Big Island, Hawaii: IEEE Press.

[83] Zuckerman, M., B.M. DePaulo, and R. Rosenthal. *Verbal and nonverbal communication of deception.* Advances in Experimental Social Psychology, 1981. **14**: 1-59. doi:10.1016/S0065-2601(08)60369-X.

[84] Zuckerman, M., R.E. Driver, and R. Koestner. *Discrepancy as a cue to actual and perceived deception.* Journal of Nonverbal Behavior, 1982. **7**(2): 95-100.

[85] Zuckerman, M. and R.E. Driver. *Telling lies: Verbal and nonverbal correlates of deception*, in *Multichannel integrations of nonverbal behavior*, Siegman, A.W. and S. Feldstein. 1985. Erlbaum: Hillsdale, NY. 129-147.