Detecting Anomalous Behavior of Socially Assistive Robots in Geriatric Care Facilities

Lindsey Coffee-Johnson
Debbie Perouli

Follow this and additional works at: https://epublications.marquette.edu/comp_fac
Detecting Anomalous Behavior of Socially Assistive Robots in Geriatric Care Facilities

Lindsey Coffee-Johnson
Vassar College, Poughkeepsie, NY, USA
Debbie Perouli
Marquette University


SECTION I. Introduction
As the number of older adults who will be needing living assistance increases, the need for long term care workers increases as well [1]. Given this trend, there is concern that we will soon be unable to meet the demand for human care-givers [2]. One proposed solution to this problem is to bring in Robotic Caregivers (RCGs) to help with basic physical, social, and perhaps even emotional needs of elderly patients. Although Socially Assistive
Robotics (SAR) technology for use in elder care is still in development, there is literature that suggests increasing interest in its future use [3], [4].

As technology for using SAR in elder care advances, however, the need for effective methods of intrusion detection progresses in parallel. Despite the growing interest in this field, there is currently very little research on detecting potentially harmful behavior in caregiver robots. Without proper methods in place, elderly Care Recipients (CRs) will be at risk for manipulation, financial exploitation, psychological abuse, and neglect at the hands of hacked or accidentally misconfigured RCGs. Not only would this harm the CRs, but it could also seriously injure the reputation of the facility employing the robots or even make it vulnerable to legal action. In order for RCGs to be successful as part of a solution to the shortage of caregivers, we need to fully consider and plan for the possibility of malicious hacking.

In this paper, we propose a novel tool for the detection of abnormal RCG behavior that could harm a CR psychologically or financially. We have compiled a questionnaire building on the field of elder abuse screening. Our method can be implemented without the need for highly skilled personnel.

SECTION II. Anomaly Detection Questionnaire

We designed our method for use in a long term or geriatric care facility that employs RCGs to replace or support human caregiver employees. Our method requires the input of either older adults with the ability to remember general interactions with their RCGs or human caregivers with the ability to regularly observe the interactions of RCGs with their users.

CRs will have a high level of dependence on their RCGs for social needs such as placing calls or video conferences with friends and family and conversation with the RCG itself. Our assumption is based on the progress that is being made in developing robots with potential for applicability in elder care such as [5]–[6][7][8][9][10]. The important role of RCGs' in their user's lives places CRs at a significantly high risk for abuse and exploitation were an RCG to be hacked.

Since hacking is the result of human action, we suggest that manipulative or psychologically harmful behavior in an RCG will likely resemble manipulative or psychologically harmful behavior in a human. Furthermore, although the specific behavior of the RCG may vary by the patient it is interacting with, we can classify certain behaviors as completely out of the range of what normal RCG behavior is.

Considering the threat of psychological manipulation, neglect, and financial exploitation, we explored several elder abuse detection tools currently in use in the field of geriatric care [11]–[12][13][14][15][16]. We propose the following questions based off of our contextual requirements and current abuse screening tools. The first seven questions were adapted from an English translation of the Caregiver Psychological Elder Abuse Behavior (CPEAB) Scale [13]. The CPEAB has been featured in studies surveying validity of current tools [17], [18], and has been used as a tool of measurement in elder abuse research [19]. Questions from the CPEAB were chosen for adaptation based on applicability to our scenario and expected RCG duties. The eighth question has been added to gather information on potential financial exploitation.

1. Has your RCG ever called you names or insulted you?
2. Has your RCG ever interrupted you in a curt or impatient manner?
3. Has your RGC ever threatened you verbally?
4. Has your RCG ever interrupted your sleep during the nighttime for no clear reason?
5. Has your RCG ever failed to respond to you or remained silent when you addressed them?
6. Has your RGC ever ignored you when you have made a request?

7. Has your RCG ever denied or ignored requests to contact family or friends?

8. Has your RCG ever asked for your credit card, bank, or other financial information or means of payment?

If any of the questions result in an affirmative answer, the robot shows signs of concern and should be further inspected.

Due to the context within which this instrument would be used, we excluded several types of abuse screening tools. We determined that our Anomaly Detection Questionnaire should meet the following criteria: a) be quick to administer, as to not be overly burdensome for human employees; b) rely on easily observable changes in responses only; c) rely on recent changes in CR or RCG behavior, so that abnormal RCG behavior can be detected fast; d) questions must be closed-ended and not rely on a Likert-type scale; e) completion must result in a definitive pass or fail.

SECTION III. Discussion

In screening for human-to-human abuse, certain thresholds have to be reached for behavior to amount to abuse [20]. Humans are rarely able to achieve perfect behavior at every moment, so there must be some consideration for occasional poor interactions between the patient and human caregiver. We must ask: “Are these behaviors rare, mild occurrences or a pattern of negative behaviors that constitutes abuse?” This becomes an increasingly nuanced question when we consider that work stress or overburden have been shown to be strong correlates to elder abuse [21]. RCGs, however, are not subject to work stress or overburden making our situation one of significantly fewer grey areas. We suggest that we would still get reliable results using closed-ended questions with definitive results as opposed to scales with ranges of results.

On the other hand, our context imposes limitations on our questionnaire's applicability. We have to assume that the CR is familiar enough with the RGC and the technology to not mistake a misplaced request (like a request that does not start with the RGC's trigger word) for an ignored request. If the RCG already possesses some of the CR's financial information, e.g. in order to more easily make online purchases, the last question should be modified depending on the case.

This model could be extended in several ways. First, by using existing tools (i.e. questionnaires) to determine possible patient abuse, we leverage the fact that this is a field of study advancing in its own right. There has been some promise, for example, in finding similar elder abuse screening tools for patients with dementia [22]. As new technologies and research come out in this field, they can be readily adapted under this model to help in intrusion detection of caregiver robots.

Furthermore, after initial set-up, these methods do not require someone highly skilled in robotics or IT security to implement. This is beneficial because facilities may not have the desire or resources to employ such personnel.

References
