Poster: Extracting Human Behavioral Biometrics From Robot Motions

Long Huang
Louisiana State University
Baton Rouge, LA, USA
lhuan45@lsu.edu

Zhen Meng
University of Glasgow
Glasgow, Scotland
2227311M@student.gla.ac.uk

Zeyu Deng
Louisiana State University
Baton Rouge, LA, USA
zdeng6@lsu.edu

Chen Wang
Louisiana State University
Baton Rouge, LA, USA
chenwang1@lsu.edu

Liying Li
Northumbria University
Newcastle, United Kingdom
emma.li@northumbria.ac.uk

Guodong Zhao
University of Glasgow
Glasgow, Scotland
guodong.zhao@glasgow.ac.uk

Abstract

Motion-controlled robots allow a user to interact with a remote real world without physically reaching it. By connecting cyberspace to the physical world, such interactive teleoperations are promising to improve remote education, virtual social interactions and online participatory activities. This work builds up a motion-controlled robotic arm framework and proposes to verify who is controlling the robotic arm by examining the robotic arm's behavior. We show that a robotic arm's motion inherits its human controller's behavioral biometric in interactive control scenarios. Furthermore, we derive the unique robotic motion features to capture the user's behavioral biometric embedded in the robot motions and develop learning-based algorithms to verify the robotic arm user. Extensive experiments show that our system achieves high accuracy to distinguish users while using the robot's behaviors.

ACM Reference Format:
Long Huang, Zhen Meng, Zeyu Deng, Chen Wang, Liying Li, and Guodong Zhao. 2022. Poster: Extracting Human Behavioral Biometrics From Robot Motions . In *The 27th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '21), January 31–February 4, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3447993.3482860

1 Introduction

Consumer robotic arms have been increasingly used for a multitude of applications for providing augmented interactions, including remote education, health care, research, industrial control and social network [2]. By controlling a robotic arm, the user is able to conduct mission-critical and high-risk applications in the real world remotely without physically reaching it. However, because a motion-controlled robot system involves sensors, actuators, networks and computing devices at two ends, it suffers from more severe security threats from both cyberspace and the physical world. More specifically, an adversary might intrude and gain the system access by exploiting any of the above interfaces, which makes the defense hard. Current access control of the robot system is achieved through traditional user-end authentications, but these methods are independent of robot control, and could not guarantee that the robotic arm is consistently under the control of the enrolled user(s). The adversary might also fool the authentication at the user end by forging the user's authentication entry. To secure the robot system access, we propose to continue verifying the user after the robot system is logged in, and the verification is done by examining the robot's behavior.

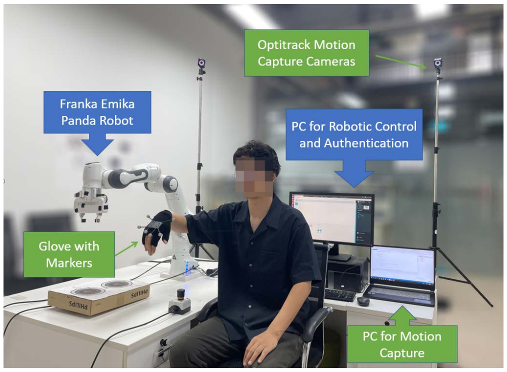
Optitrack Motion Capture Cameras
Franka Emika Panda Robot
PC for Robotic Control and Authentication
Glove with Markers
PC for Motion Capture

Figure 1. The motion-controlled robotic arm platform to facilitate interactive control.

A motion-controlled robotic arm system comprises two ends, which are connected by a local or wide area network. We build up a real motion-controlled robot system as shown in Figure 1. The user end is responsible for tracking the user's motions and issuing the corresponding control commands. The robotic arm end receives and executes the commands

ACM MobiCom '21, January 31–February 4, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-8342-4/22/01...$15.00
https://doi.org/10.1145/3447993.3482860

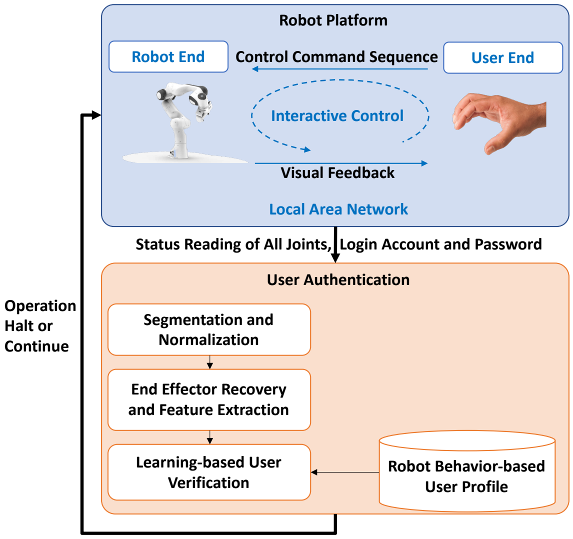
Robot Platform
Robot End
Control Command Sequence
User End
Interactive Control
Visual Feedback
Local Area Network
Status Reading of All Joints, Login Account and Password
User Authentication
Operation Halt or Continue
Segmentation and Normalization
End Effector Recovery and Feature Extraction
Learning-based User Verification
Robot Behavior-based User Profile

Figure 2. The motion-controlled robotic arm framework with the robot behavior authentication at the robot end.

to perform tasks. In the meanwhile, the user observes the robotic arm's movement feedback and adjusts his/her hand motion accordingly for the interactive control, which facilitates performing fine tasks. Due to the individually unique human arm structures, strengths and motion behaviors, the robotic arm exhibits the behaviors highly correlated with the user. We thus design the robotic arm-end user authentication approach, which tracks the robotic arm's movements to verify the robot-inherited human behavior. This work, for the first time, demonstrates that the robotic arm could inherit much of its controller's behavioral information in the interactive control environment. In particular, we derive unique robotic motion features to capture the user's behavioral characteristics that are embedded in the robotic arm's motions. Our contributions are summarized as follows:

- We develop a user authentication approach for motion-controlled robotic arm systems based on examining the robotic arm's movement behavior.
- This work demonstrates that people's motion behaviors in interactive control scenarios are individually unique. Moreover, the robotic arm under control inherits such behaviors to show the per-user distinctive robot behaviors.
- We build up a real motion-controlled robotic arm platform and design learning-based algorithms to both recognize the type of task the robot is performing and verify the identity of the robot's user.

2 System Design

Figure 2 shows the framework of our system, which consists of a user end for the real-time motion capture and a robotic arm end for executing control commands.

Robot Platform. Our motion-controlled robotic arm platform maps human motion to robotics movements in real-time. At the user end, six motion capture cameras (OptiTrack Prime 13) are deployed in a 5m by 5m circular area to capture the user's hand movements. The user is required to wear a glove attached with passive reflective markers, which allows the motion capture system to obtain high precision of tracking the position and orientation of the human's hands in 6-DOF, with positional errors less than +/-0.20mm and rotational errors less than 0.5 degrees [3]. The captured hand motions are further transformed into control command sequences, which are sent to the robot end to execute.

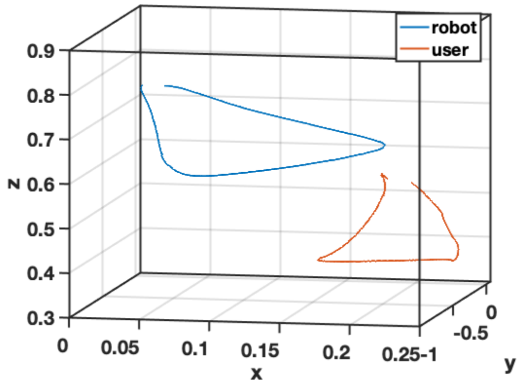

Figure 3. Comparison of the user's hand and the robotic arm end-effector raw trajectories of drawing a "triangle". Both are obtained by OptiTrack cameras.

An industrial robot (Franka Emika Panda) is used at the robotic arm end [1]. The robotic arm has 7 DOF achieving up to 2 m/s end-effector speed and +/- 0.1 mm repeatability, which ensures the accurate replication of human hand movements. Consider the significant differences of the physiologies, kinematic characters, joint numbers and arm lengths between robotic arms and human arms, we design a PID-based path planning algorithm to relax the mapping constraints between the human hand and end-effector of robots to generate smoothly, continuously mimicry-based control trajectories, which converts the received joint angle values into a series of angular velocity commands within the trajectory limitations. In addition, to enable the robotic arm to follow hand movements, we set the robotic arm and the motion capture system in the same coordination system, as illustrated in Figure 3. In the meanwhile, the user receives the visual feedback of the robotic arm's movement to perform the interactive control, which forms a control loop.

A commercial Ethernet is used to connect the two ends and facilitate the data transmission. We utilize the User Datagram Protocol (UDP) to support the high packet delivery rate. This protocol also reduces the queuing delay at the transmitter side and improves real-time tracking performance.

User Authentication. When accessing the robotic arm, the user enters the login account and password at the user end. Once the credentials are accepted, the user can manipulate the robotic arm with hand motions in real-time. Our authentication approach runs once the login is successful. Unique

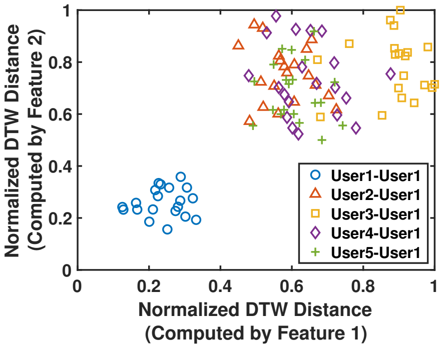

Figure 4. The DTW distances of the robotic arm motion features (e.g., trajectory and acceleration) between users.

robotic motion features are derived to capture the robotic arm's unique behavior associated with the user's behavioral biometric, which are fed into our Dynamic Time Warping (DTW) based algorithms, where task recognition and user identification are performed successively. When registering the system and using the robotic arm for the first time, the user's profile is created based on the robotic arm's motion behavior. When the user accesses the robotic arm later, the current robotic arm behavior is compared with the user's profile to verify whether the user's identity is as claimed. Based on the verification result, the robotic arm would continue to operate or reject the access and halt. If the access is rejected, the framework requires the re-login, and challenge/security questions and message authentication codes could be further required. The traditional login credentials and robot-behavior verification form the two security layers for the motion-controlled robotic arm framework.

3 Preliminary Results

Feasibility. We conduct a feasibility study to investigate if a robotic arm can inherit the user's behavioral information. The participants are asked to operate the robotic arm to repeatedly draw an "Δ" in the air 40 times using our platform. As shown in Figure 3, the robotic arm follows the path of the user's hand and draws a similar "triangle" curve. Figure 4 presents the DTW distances of two motion features (i.e., trajectory and acceleration) between *user 1* and five users (*user 1* to *5*). We find that the DTW distances of *user 1*'s own robotic arm motions are much smaller than the cross-user DTW distances. The behavioral consistency and uniqueness demonstrated above confirm that the robotic arm carries a portion of the user's behavioral biometrics, which can be used to distinguish users.

Experiment. Then we recruit 10 participants for the interactive control experiments, who are all first-time users of the platform. Before experiments, the users have 5 minutes to be familiar with the platform by operating the robotic arm. During data collection, the participants are asked to control the robotic arm to write letters, draw curves in the air and perform some basic operations. Each participant repeats 40 times per task.

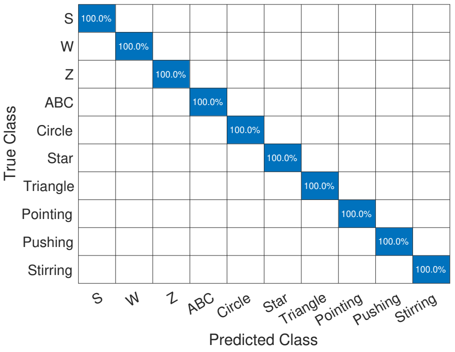

Figure 5. Confusion matrix of recognizing robot tasks.

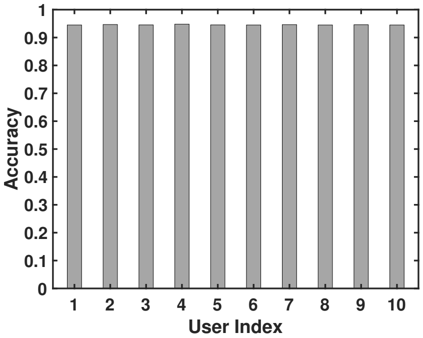

Figure 6. Performance of user verification.

Authentication. Figure 5 shows the confusion matrix of the task classification. Our approach achieves 100% task recognition accuracy, this result indicates that our robotic motion features capture the differences among tasks well and the weighted DTW-based classifier tolerates the network delays and the user's varying hand movement speeds when recognizing a task. We alternatively select each participant to be the target legitimate user and use the corresponding user template for verification. Figure 6 presents the average accuracy for each of the 10 participants, all the participants achieve over 94% accuracy, while the median accuracy is 94.5%. Some participants reach around 95% accuracy. The results confirm the effectiveness of our approach to verify users via the robot behaviors.

Acknowledgment. This work was partially supported by LEQSF(2020-23)-RD-A-11 and EPSRC IAA (EP/R511705/1).

References

[1] Franka Emika GmbH. Franka Control Interface Documentation, Dec 2020. https://frankaemika.github.io/docs/overview.html.

[2] Grau, A., Indri, M., Bello, L. L., and Sauter, T. Industrial robotics in factory automation: From the early stage to the internet of things. In *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society* (2017), IEEE, pp. 6159–6164.

[3] NaturalPoint, Inc. DBA OptiTrack. Optitrack prime 13, Last visited: May 2020. https://www.optitrack.com/cameras/primex-13/.