Operator Strategy Model Development in UAV Hacking Detection

Haibei Zhu, Mary L. Cummings, *Senior Member, IEEE*, Mahmoud Elfar, Ziyao Wang, and Miroslav Pajic, *Member, IEEE*

***Abstract*—An increasingly relevant security issue for unmanned aerial vehicles (UAVs, also known as drones) is the possibility of a global positioning system (GPS) spoofing attack. Given the existing problems in current GPS spoofing detection techniques and human visual advantages in searching and localizing targets, we propose a human-autonomy collaborative approach of human geo-location to assist UAV control systems in detecting GPS spoofing attacks. An interactive testbed and experiment were designed and used to evaluate this approach, which demonstrated that human-autonomy collaborative hacking detection is a viable concept. Using the hidden Markov model (HMM) approach, operator behavior patterns and strategies from the experiment were modeled via hidden states and transitions among them. These models revealed two dominant hacking detection strategies. Statistical results and expert performer evaluations show no significant difference between different hacking detection strategies in terms of correct detection. The detection strategy model suggests areas of future research in decision support tool design for UAV hacking detection. Also, the development of HMMs presents the feasibility of quantitatively investigating operator behavior patterns and strategies in human supervisory control scenarios.**

***Index Terms*—Cyber-attack detection, hidden Markov model (HMM), human geo-location, human supervisory control, strategy classification, unmanned aerial vehicle (UAV).**

I. Introduction

UNMANNED aerial vehicles (UAVs) have significantly increasing use in commercial and military applications. The continued growth in numbers and functionalities of UAVs has been accompanied by many security, privacy, and regulatory concerns. One common security concern is UAV global positioning system (GPS) spoofing, in which attackers deceive GPS receivers by providing counterfeit GPS signals in order to override UAV navigation systems and redirect UAVs to unexpected destinations [1], [2]. One such well known incident garnered public attention in 2011 when an RQ-170 Sentinel UAV was captured using GPS spoofing attacks [3]. Therefore, successfully detecting GPS spoofing attacks is important for UAV control systems.

Understanding that human vision has advantages in complex searching and localizing tasks [4]–[6], we demonstrated a human-autonomy collaborative approach through geo-location in which humans can assist autonomous systems in the detection of possible GPS spoofing attacks on UAVs. In this study, this approach was evaluated via an experiment, which was designed and conducted using the security-aware research environment for supervisory control of heterogeneous unmanned vehicles (RESCHU-SA) platform [7], extension of the platform from [8]. Experimental sessions simulated human supervisory multiUAV control scenarios with potential UAV GPS spoofing attacks. Operators were able to successfully detect hacking events such that 65% of total experimental sessions exhibited at least 80% correct hacking identification. We also discovered that operators with significant video game experience were the best performers in hacking detection [9].

While this initial study demonstrated that human operators could successfully identify UAV GPS spoofing attacks through geo-location, given that such research has never before been conducted, our goal is to better understand what strategies emerged as novices attempted to determine if they had been hacked. To this end, it was advantageous to develop human behavior models to investigate operator behavior patterns, both in the execution of their primary task of supervising UAVs, and in attempting to thwart hacking attempts. Such models could be particularly useful as they could highlight training problems or interface design anomalies. Finally, such models could be used to develop predictive decision support tools that could assist human operators, particularly under areas of high workload and stress. The rest of this paper presents our efforts to develop strategy models of humans supervising multiple UAVs and determining whether a UAV had been hacked through human geo-location.

II. Background

A. UAV GPS Spoofing Detection

Remotely controlled UAVs typically rely on an embedded navigation system known as the GPS, which provides accurate localization information including position, velocity, and time for UAV GPS receivers. GPS receivers can calculate the precise latitude, longitude, height, and speed based on received satellite signals. However, GPS receivers are vulnerable to GPS spoofing attacks, in which GPS receivers are attacked by counterfeit

Manuscript received April 1, 2018; revised August 26, 2018; accepted November 17, 2018. Date of publication February 26, 2019; date of current version November 21, 2019. This work was supported in part by the NSF under Grant CNS-1652544 and in part by the ONR under Agreement N00014-17-1-2012 and Agreement N00014-17-1-2504. This paper was recommended by Associate Editor M. L. Bolton. *(Corresponding author: Haibei Zhu.)*

H. Zhu, M. Elfar, and M. Pajic are with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708 USA (e-mail: haibei.zhu@duke.edu; mahmoud.elfar@duke.edu; miroslav.pajic@duke.edu).

M. L. Cummings, and Z. Wang are with the Department of Mechanical Engineering and Materials Science, Duke University, Durham, NC 27708 USA (e-mail: mary.cummings@duke.edu; ziyao.wang@duke.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/THMS.2018.2888578

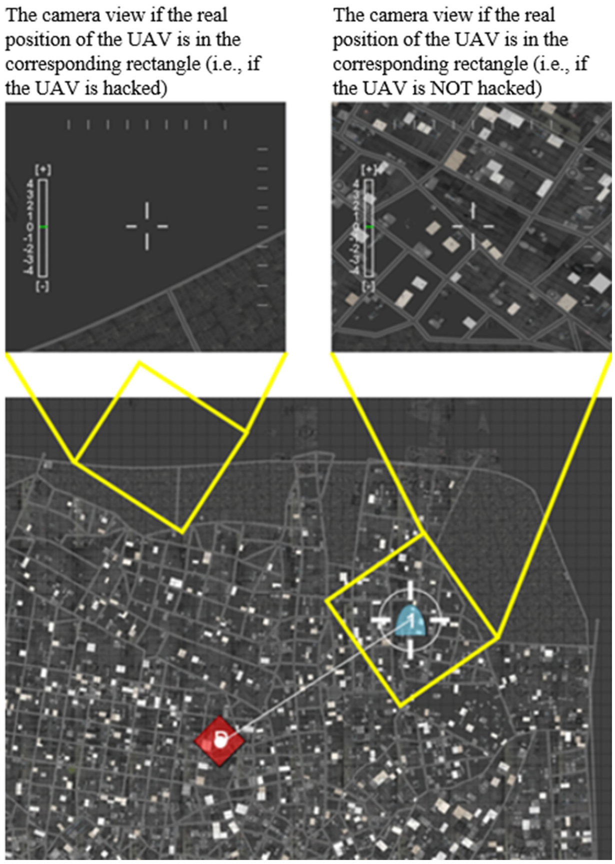

Fig. 1. Example of GPS reported locations on the map.

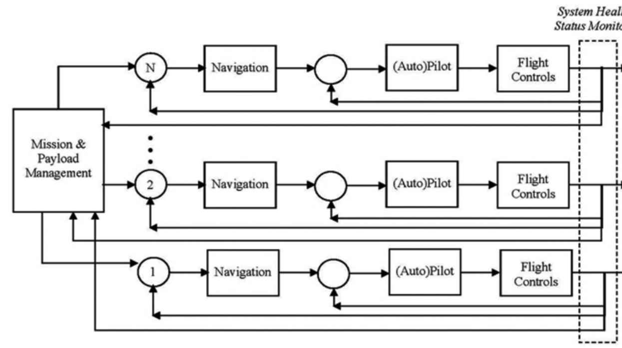

Fig. 2. Human supervisory multiple UAV control architecture [22].

signals generated from GPS spoofers [10]–[14]. Many autonomous GPS spoofing detection methods have been proposed in recent studies [11]–[17]. However, false alarms and detection failures still exist while applying autonomous GPS spoofing detection [10], [11], [15]. Therefore, more research is needed to improve autonomous detection systems.

UAVs are commonly equipped with both a GPS navigation system and payload camera, whose signal is independent of the UAV GPS signal. Thus, if these two signals are independent, the payload camera view can be used as a reference to assist autonomous detection systems in detecting UAV GPS spoofing attacks. Based on the precondition that UAV payload camera views can provide the unbiased surrounding scene of UAVs, we propose that human operators can act as supplementary sensors and assist autonomous systems to detect UAV hacking attacks through the comparative human geo-location method.

In human geo-location, an operator can compare the nontampered video feed from the UAV payload camera to the potentially falsified GPS reported location on the map. This approach allows operators to detect inconsistencies, which indicate potential hacking attacks, between the location interpreted from the camera view and the GPS location reported on the map. In theory, such cross referencing could be accomplished automatically through autonomous localization and sensor-fusion techniques (e.g., [18], [19]), but these have not been very successful [20], particularly in military applications [21].

Based on feature integration theory, the first stage of human vision obtaining information from targets is the preattentive stage, in which a human observer can gather basic information about a target even before the observer becomes conscious of it [4]. Thus, human vision can process target information efficiently in complex environments. Human observers also tend to choose areas that maximize information of the target in a salience-driven visual search strategy [5]. In addition, the direction discrimination threshold of human vision has a low average of 1.8 degrees [6], which suggests that human observers can precisely detect small changes in target movement orientation. Considering these human visual advantages, human operators can potentially assist UAV localization and detect potential UAV GPS spoofing attacks.

An example of human geo-location in UAV GPS spoofing detection is shown in Fig. 1. The GPS-reported location of the UAV is shown as the blue dome on the map in the upper right. If the UAV is under attack, the operator will observe the scene below the UAV through the camera, which would be different from the surrounding environment of the GPS-reported location on the map; e.g., as in the upper left camera-view in Fig. 1. If the UAV is not under attack, the operator will observe the scene below the UAV, as in the upper-right camera view in Fig. 1, matching the reported location. When a GPS spoofing attack is confirmed, the operator can prevent losing the hacked UAV by overriding the physical controls.

B. Modeling Operator Behavior

The human geo-location approach to hacking detection is an example of a common UAV control scheme which incorporates human supervisory control, in which a human operator monitors a multiUAV system, intermittently navigating UAVs, and conducting other higher level tasks [23]. The hierarchical architecture of a human supervisory UAV control loop of single operator with multiple UAVs is shown in Fig. 2 [22]. In this architecture, multiple parallel outermost loops represent the highest-level control of managing missions and payloads by human operators. The inner loops represent lower level navigation and flight controls by autonomous systems or operators. This architecture can be introduced with various levels of automation. The successful control of higher level operator loops depends on the success of lower level autonomous system loops. In this study, we assume that human operators keep higher level decision-making processes, and autonomous systems are in charge of lower level UAV control and navigation operations [22].

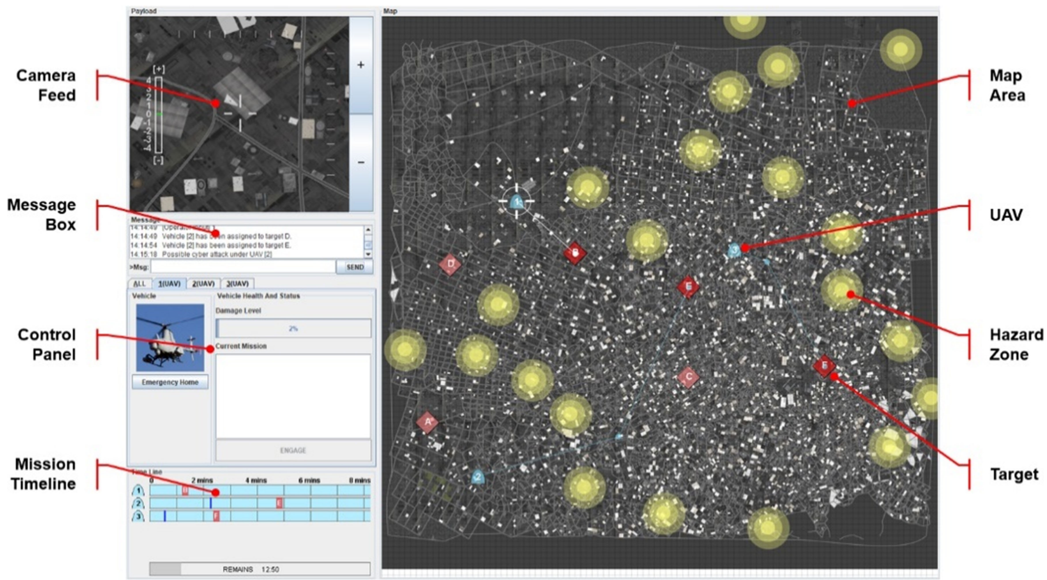

Fig. 3. RESCHU-SA experiment platform interface [7].

In supervisory control settings where humans are supervising one or more autonomous systems, human operator behavior models are needed for multiple reasons:

1) To investigate general operator behavior patterns, in order to determine if observed behaviors match the expected behaviors;
2) To investigate operators' strategies, in order to identify points of inefficiency or error;
3) Study both endogenous and exogenous factors that impact operator behavior patterns such as video game experience and task load;
4) Study how automation can improve operators' performance and success rate in task performance, including the use of predictive operator behavior models.

In terms of the hacking detection supervisory control setting we consider, we need a way to determine strategies that operators develop in their attempts to detect and mitigate hacking attempts, and how to improve upon those strategies that could include the use of automated decision support.

One problem with the generation of such models is that while interactions between a human operator and a supervisory control system can be directly observed through human physical interaction with an interface, such observations cannot be directly associated with a human thought, goal, plan, or strategy. In order to develop operator models that link actions and behaviors to plans, goals, and strategies, we need a method that abstracts low-level physical interface interactions into higher operator behavioral states and strategies. We believe that a hidden Markov modeling approach provides the foundation to do this, as described in the next section.

C. Markov Modeling Approaches

Markov models are widely used to capture stochastic evolution of state transitions in the state-space [24]. Many studies have used Markov models to investigate low-level human actions [25], [26]. However, Markov models only capture observable interactions between human operators and control systems, which may not accurately reflect operators' high-level behavioral states. Therefore, hidden Markov models (HMM), which are an extension of Markov models, could be a useful alternative in this regard.

An HMM is a two-layer stochastic model that describes a Markov process with a higher layer of indirectly observable system states and a lower layer of observable emissions from each state. The HMM formalism is widely used in machine learning, especially in speech recognition [27] and development of human operator behavior models in driving [28]. HMMs using an unsupervised approach to model training have been shown to provide more accurate operator behavior models over supervised learning approaches [29], [30]. Because an HMM can present higher level operator behavioral states using hidden system states based on lower level operator interactions with a supervisory control system like a UAV ground control station, the HMM was selected as the modeling framework for this effort.

III. Data Generation

In order to develop models of operator behavior in the UAV supervisory control environment with potential hacking events, user interactions with such a system were needed to provide the underlying training data. To this end, we developed the RESCHU-SA (now freely available to interested parties) [7], [8], [31]. RESCHU-SA is a Java-based simulation platform for a single operator with multiUAV supervisory control scenarios. It provides the flexibility to design multitasking scenarios including both navigational and imagery analysis tasks. Moreover, this platform provides the capability of simulating UAV GPS spoofing attacks, in which hacked UAVs deviate from the originally assigned paths and target unexpected destinations, along with real or false notifications that simulate autonomous GPS spoofing detection systems.

The interface of the RESCHU-SA platform is shown in Fig. 3. Five main components are featured in this interface, including the payload camera view, message box, control panel, timeline, and map area. Specifically, the camera view displays the video stream of the surrounding environment beneath the selected UAV. The primary purpose of this view is to conduct imagery analysis tasks and can be used to determine the actual location of UAVs for detecting potential hacking events. The map displays the surveillance area with real-time locations of all UAVs, hazard areas, and targets.

A. Experiment Design

To collect enough data to develop operator models, a set of experiments was conducted using RESCHU-SA. The primary objectives of operators using RESCHU-SA are to control multiple UAVs to: 1) determine whether UAVs are under GPS spoofing attacks; 2) perform reconnaissance imagery tasks of counting road intersections when UAVs reach assigned targets; and 3) ensure that UAVs do not encounter hazard areas.

Given that a previous study demonstrated that the task load can significantly impact an operator's performance, and thus strategies [8], task load was the only controlled experimental variable in this experiment. Two objective task load levels, high versus low, were introduced, and each participant had both task load scenarios in the experiment. In the low-task load scenario, operators navigate three UAVs with six targets and six hacking notifications, including three real hacking notifications and three false alarms. In the high-task load scenario, operators navigate six UAVs with nine targets and nine hacking notifications, including five real hacking notifications and four false alarms. To simplify the hacking detection, no notification miss was introduced in the experiment that all real hacking events come with notifications.

In RESCHU-SA, operators are responsible for safely navigating UAVs to targets. Hazard areas can appear and disappear randomly, which require replanning the vehicle around these threat areas. In the experiment, GPS spoofing attack events with notifications followed a predefined schedule but appeared to randomly occur while an operator navigated the UAVs. Once an operator received a notification that a certain UAV was under possible cyber-attack, the operator could then investigate the potential UAV hacking by checking the UAV camera view and matching it against the position of the UAV on the map. Although UAV position drifts may be caused by GPS degradation, we assumed that all position drifts were caused by GPS spoofing attacks to simplify the hacking detection scenarios in this experiment.

When UAVs that were not hacked reached a target, the operator engaged in an imagery task of counting the road intersections from the UAV's camera view at a prespecified zoom level. This task represents the primary purpose of the mission, which is information gathering. The imagery counting task was the participants' primary work load task, and it allowed us to assess their performance based on the number of attempted tasks and the task correctness percentage.

B. Experiment Subjects and Procedure

Thirty-six participants took part in this experiment, including 22 males and 14 females. Age ranged from 19 to 34 years with an average of 25.2 and a standard deviation of 3.8 years. Among all participants, 18 participants had little video game experience, six participants had monthly gaming experience, five participants played video game several times a week, another five participants had weekly gaming experience, and only two participants had daily gaming experience. The experimental procedure consisted of four main sections including a self-paced tutorial section, a practice section, a test section, and a debriefing section. Specifically, in the test section, each participant finished two test sessions, including a counterbalanced high- and a low-task load scenario. Thus, we had 72 test sessions and collected data from all these sessions.

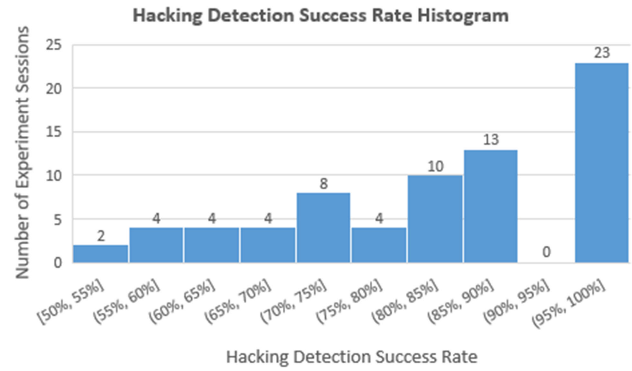

Fig. 4. Histogram of the hacking detection success rate.

TABLE I
CONFUSION MATRIX OF HACKING DETECTION DECISIONS IN DIFFERENT NOTIFICATIONS

	Real hacking notification	False alarm notification
Decision of considering UAV was hacked	224	40
Decision of considering UAV was not hacked	63	207

C. Experiment Results

In this experiment, 23 out of the total 72 test sessions (32%) resulted in 100% successful hack identifications, while another 24 (33%) reached above 80% successful attack identification. Thus, as shown in Fig. 4, 65% of total test sessions reached 80% correct hacking detection or better without having any prior formal hacking detection training.

Specifically focusing on the difference between real hacking notification and false alarms, as shown in Table I, out of all the 287 (224 + 63) real hacking notifications across all participants, the overall success rate was 78% (224 ÷ 287), and for all the 247 (40 + 207) false alarms, the success rate was 84% (207 ÷ 247). In other words, the type one error (false positive, operators considered UAV not hacked with real hacking notification) was 22% (63 ÷ 287), which was slightly higher than the type two error (false negative, operators considered UAV hacked with false alarm notification) of 16% (40 ÷ 247). Thus, operators were slightly better at detecting false alarms than identifying real hacking notifications.

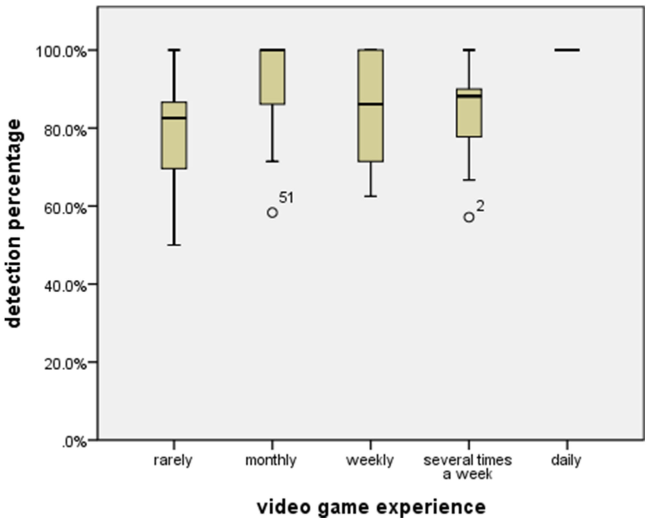

Fig. 5. Boxplot of hacking detection success rate based on different video game experience.

Task load, as a major experimental factor, only affected UAV damage level (MANOVA $F(1,31) = 32.93$, $p < 0.001$, alpha $= 0.05$), but it did not affect any other performance metric. However, the video game experience covariate had a significant effect on participants' correct hacking detections ($F(1,31) = 4.652, p = 0.039$), as shown in the boxplot in Fig. 5. This means that the more the video game experience, the higher the chance of a correct hacking detection. Not surprisingly, seven participants who lost UAVs had no video game experience, and the other five who lost UAVs ranged from little to moderate gaming experience. Participants with daily gaming experience did not lose any UAVs and were 100% correct in hacking identification.

These statistical results of our experiment provide a high-level understanding of the factors that impacted operator performance. However, we need to further investigate the underlying nature of why such factors had certain effects on performance. In addition, operators' hacking detection strategies cannot be inferred via statistical results. Therefore, human operator models are needed for further investigating operator behavior patterns and detection strategies in such UAV supervisory control scenarios.

IV. HMM Structure, Training, and Selection

As discussed previously, human operator behavior models can illustrate operator behavior patterns and strategies in high-level tasks. Considering that HMMs can infer hidden higher level operator behavioral states from observable lower level interactions between the operators and autonomous systems, HMMs were chosen for modeling the observable behaviors from the RESCHU-SA experiment.

A. HMM Structure

Based on the classic notation of HMM, the HMM can be formally defined as a tuple [32]

TABLE II
Observations (Emissions) of HMMs From RESCHU-SA Experiment Interface

Index	1	2	3	4
Observation	Add waypoint	Move waypoint	Delete waypoint	Move endpoint
Index	5	6	7	8
Observation	Switch target	Engage task	Select UAV	Confirm notification
Index	9	10	11	12
Observation	Ignore notification	Consider UAV hacked	Consider UAV not hacked	Adjust zoom level

$$H = \{S, V, A, B\}.$$

Here, $S = \{S_1, S_2, ..., S_N\}$ represents N different hidden states, $V = \{V_1, V_2, ..., V_M\}$ represents M different observations. Also, $A = \{a_{ij}\}$ is an $N \times N$ transition probability matrix, where $a_{ij} = P\{S_j^{t+1}|S_i^t\}$, $i, j = 1, 2, ..., N$, and $B = \{b_{ik}\}$ is an $N \times M$ emission probability matrix, where $b_{ik} = P\{V_k|S_i\}$, $i = 1, 2, ..., N$, $k = 1, 2, ..., M$. In addition, both $a_{ij}, b_{ik} \geq 0$. In HMMs, each hidden state can be considered as a cluster of observations with different weights, which are emission probabilities. The system states (or operator behavioral states, in this paper) transfer among hidden states based on the time sequence, and the probabilities of switching from the current state to the next state are the transition probabilities.

B. HMM Training and Selection

The first step in the HMM training process is state space reduction. In RESCHU-SA, every key stroke and mouse action were recorded in log files, along with the system status. In an HMM, the hidden higher level behavioral states are clusters of operator actions, so the interaction data should be aggregations of observations based on a predefined state reduction grammar. In this manner, there were 12 possible places for operators to click in RESCHU-SA, which yielded 12 observations, as presented in Table II.

The multisequence Baum–Welch algorithm, an unsupervised model training method, was used in model training [33]. HMM training results were then selected (number of hidden states) using the Bayesian information criterion (BIC) [27], [34] and the number of rare states (NRS) method [35] to achieve both high model likelihood values and reasonable model structures. Models with the lowest BIC values are preferred. The BIC balances the increase of model complexity, which is caused by the increase of the model features, by penalizing the number of free parameters in the model training process. The NRS method maintains the simplicity and interpretability of a descriptive model by monitoring all rare states whose occurrence frequencies are lower than a certain threshold value, which is usually 5%. Generally, HMMs without any rare state are preferred. When BIC curves are monotonically decreasing, the NRS method can suggest the model with the highest number of hidden states without any rare state.

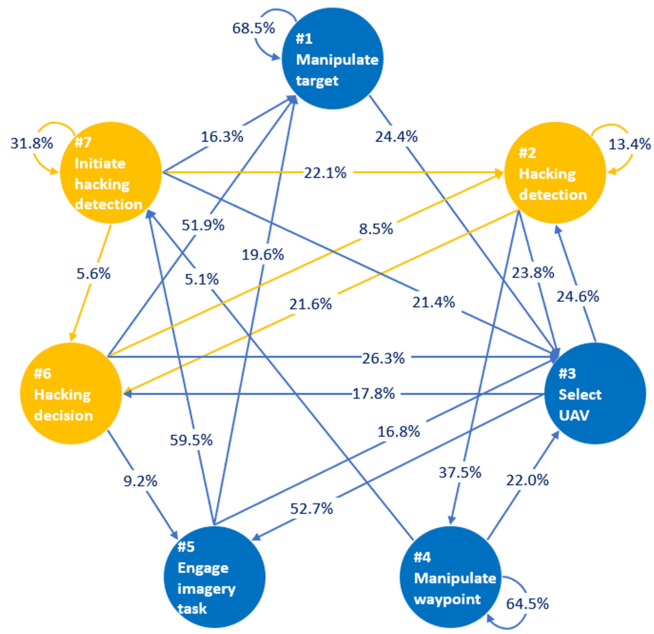

Fig. 6. General human operator behavior HMM.

Fig. 7. Emission probabilities for the HMM capturing general operator behavior.

V. General Operator Behavior Model

Understanding that task load did not affect operators' overall performance and success rate in hacking detections and imagery tasks, the general operator behavior model was trained using data from both high- and low-task load scenarios. As shown in Table II, the general operator behavior HMM was trained using observation sequences with 12 different observations. Based on the model selection process described previously, the HMM with seven states had the lowest BIC value. Also considering that the 7-state model did not have any rare states and the HMMs with eight or more states had at least one rare state, the general operator behavior model was determined to be a 7-state HMM, as shown in Fig. 6. The interpretation for each hidden state was determined by the emission probabilities, shown in Fig. 7.

The first state was interpreted as "Manipulate target" because it was mainly a cluster of observation 4 (Move endpoint), 5 (Switch target), and 7 (Select UAV), which were directly related to UAV target manipulations. The second state was interpreted as "Hacking detection" because this was the only state that had significant emission to observation 12 (Adjust zoom level), which indicated the typical operation of using a UAV's camera to compare against the map. The third state was interpreted as "Select UAV" because its only major emission was observation 7 (Select UAV). The fourth state was interpreted as "Manipulate waypoint" because it was a cluster of observation 1 (Add waypoint), 2 (Move waypoint), 3 (Delete waypoint), and 7 (Select UAV), which were directly related to waypoint management. The fifth state was interpreted as "Engage imagery task" because its only major emission was observation 6 (Engage task), indicating that people were executing the intersection counting task. The sixth state was interpreted as "Hacking decision" because it was the only state that had major emissions to observation 10 (Consider UAV hacked) and 11 (Consider UAV not hacked) which were decisions to hacking events. The seventh state was interpreted as "Initiate hacking detection" because it was the only state that had emissions to observation 8 (Confirm notification) and 9 (Ignore notification) which indicated the initiation of hacking detection.

The general operator behavior model represents the operator behavioral states in navigating UAVs, conducting imagery search, and dealing with potential hacking events. The first interesting fact shown in the model is that the UAV navigation (highlighted in blue) and hacking detection (highlighted in orange) functional groups can be distinguished clearly. The transitions between these two functional groups represent the probabilities of switching functional groups in operator behavioral states. This distinction shows that operators typically conducted tasks either in UAV navigation or hacking detection, reflecting that operators were switching between two primary objectives of navigating the UAVs and detecting hacking.

Interestingly, a previous study on the original RESCHU platform, which only dealt with the navigation of UAVs and did not have any hacking considerations [30], exhibited just four similar states to those blue states in Fig. 6. This is an important finding since it means that the addition of a new set of tasks did not dramatically change the underlying states, rather the added functionality of hacking detection simply added more states. This suggests that at least in some supervisory control environments, functions may be modeled in a modular fashion, which would reduce the workload in adapting older models as new functions are added.

In addition, the general RESCHU-SA model in Fig. 6 shows some potential inefficiencies in operator behavior patterns. In

TABLE III
OBSERVATIONS (EMISSIONS) OF THE HACKING DETECTION STRATEGY HMM FROM RESCHU-SA EXPERIMENT INTERFACE

Index	1	2	3	4
Observation	Add waypoint	Move waypoint	Delete waypoint	Move endpoint
Index	5	6	7	8
Observation	Switch target	Engage task	Select UAV	Perceive hacking
Index	9	10		
Observation	Detection decision	Adjust zoom level		

the navigation functional set of states, the first state of "Manipulate target" and the fourth state of "Manipulate waypoint" have high self-transition probabilities. These high self-transition probabilities indicate that once operators entered these two behavioral states, operators tended to conduct repeated operations. For instance, the participant who repeated manipulating targets the most (91 times compared to the average of 35 times), was enmeshed in the "Manipulate target" state and actually had a low overall performance score of 236 (compared to the average of 303). These repeated operations indicate potential inefficiencies that could be improved with future designs for the UAV supervisory control interface.

Two hidden states, "Hacking detection" and "Initiate hacking detection," in the hacking detection functional group also revealed potential problems with self-transitions. Based on statistical analyses, the time consumption in hacking detection was negatively correlated with the hacking detection success rate (Pearson $= -0.375, p = 0.001$). Thus, this fact implies that the longer the person spent investigating a potential hacking event, the less likely a successful detection would occur. This result was curious because as people gather more information, they should increase their probability of successful detection. These results then led us to develop more detailed HMMs about just operator hacking detection strategies in order to shed more light about this unexpected result. These more specific HMMs are detailed in the following section.

VI. HACKING DETECTION STRATEGY MODEL

The HMM in Fig. 6 provides an overall view into how operators approached the overall tasks of navigating the UAVs in support of their primary reconnaissance missions, while also dealing with hacking events. However, since this model does not provide enough detail about just how exactly people formed strategies for dealing with the hacking events, we elected to focus on those operator interactions from the beginning to the end of each hacking event. Overall, there were 15 such hacking events per participant. The resulting hacking detection model was trained based on ten observations instead of the original 12 observations, as shown in Table III. In the revised model training, original observations of "Confirm notification" and "Ignore notification" were combined to "Perceive hacking," and "Consider UAV hacked" and "Consider UAV not hacked" were combined to "Detection decision."

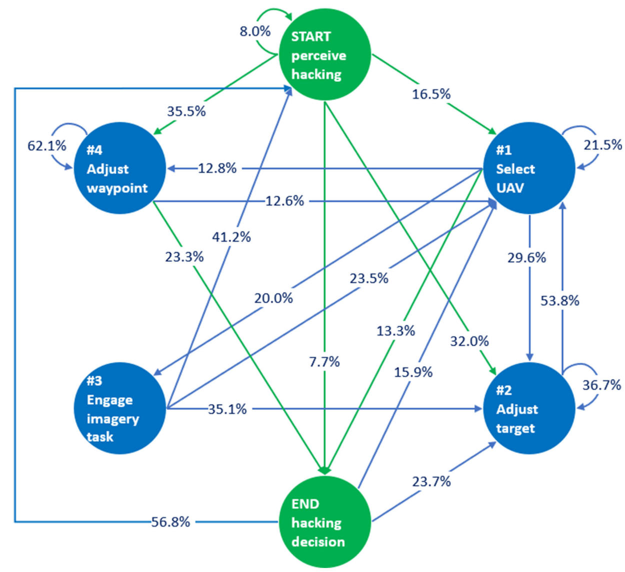

Fig. 8. Operator hacking detection strategy model.

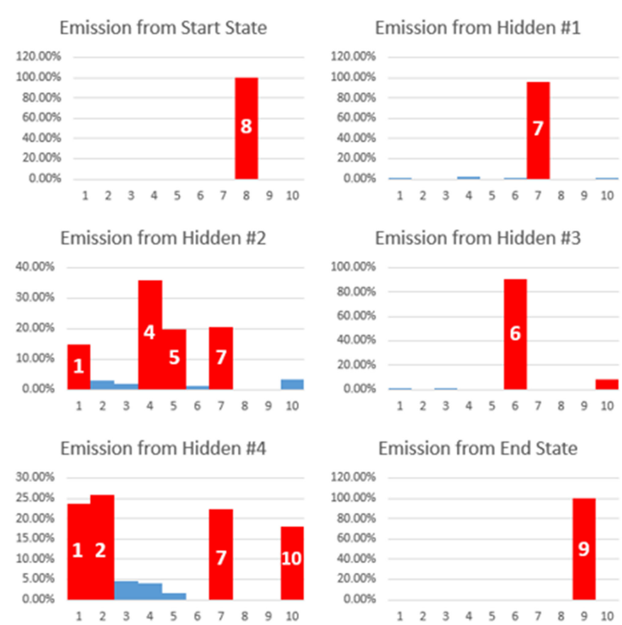

Fig. 9. Emission probabilities of the hacking detection strategy model.

As shown in Fig. 8, the obtained hacking detection strategy model is a 6-state HMM based on the similar model selection process as used for the general operator behavior model. The interpretation for each hidden state was determined by the emission probabilities shown in Fig. 9. Although the observations were slightly different, the interpretation criteria were similar to the general behavior model. The six hidden states were interpreted as: 1) the start state of "Perceive Hacking"; 2) "Select UAV"; 3) "Adjust target"; 4) "Engage imagery task"; 5) "Adjust waypoint"; and 6) the end state of "Hacking decision." The 56.8% transition from the END state to the START state represents overlapping hacking detections. This means once operators finished a hacking detection, roughly half the operators

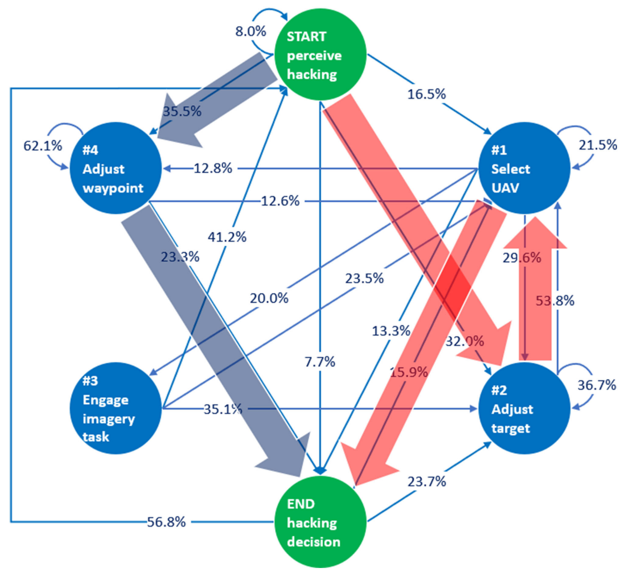

Fig. 10. Master participant strategies in hacking detection strategy model.

then went on to solve another hacking event that occurred almost coincidentally with the current event.

A. Hacking Detection Strategies

Two major behavioral state transitions (also known as operation flows) in the hacking detection HMM can be observed based on transition probabilities, as shown in Fig. 10. Such transitions are considered as detection strategies because they start from the START state, in which operators perceived hacking events, to the END state, in which operators determined detection results. The first major flow, indicated by blue arrows, has one single intermediate state of "Adjust waypoint" between the start and the end state. The second major flow, indicated by red arrows, has two intermediate states of "Adjust target" and "Select UAV" between the start and the end. These two major operation flows suggest two dominant hacking detection strategies, termed "waypoint-oriented strategy" and "target-oriented strategy."

In the waypoint-oriented strategy, operators tended to manipulate UAV waypoints, including adding and moving waypoints, to detect hacking events. In this hacking detection strategy, to investigate the potential differences in the scene between the camera view and the surrounding map area, operators typically either manipulated or introduced waypoints. Operators who used this strategy typically fixated on comparing the effects of turning the UAV and the appearance of the ground in the camera feed to that expected while turning on the map. This can be considered a dynamic strategy as motion was a key element in the determination of location.

In the target-oriented strategy, operators tended to directly switch UAV targets to detect hacking events. In this strategy, operators were typically focused more on the specific landmarks that the UAVs would fly over, such as unusual intersections or buildings. This can be considered a static strategy as operators would wait until the UAV reached a place of interest to make

TABLE IV
PARTICIPANT CLASSIFICATION BASED ON DIFFERENT HACKING DETECTION STRATEGIES

Index	Strategy	Number	Percentage
1	Waypoint strong dominant	10	27.8%
2	Waypoint weak dominant	7	19.4%
3	Target weak dominant	11	30.6%
4	Target strong dominant	8	22.2%

a hacked or not hacked decision. Both strategies revealed inefficiencies, primarily through the self-transition probabilities. For example, in the waypoint-oriented strategy, 62% of people stayed in this state, repeatedly adding, moving, and deleting waypoints. Similarly, 37% of people repeatedly redirected vehicles to other targets, suggesting an inefficient target selection process. These actions suggest inefficiencies that potentially could be made better with advanced decision support, which is an area of future work.

The occurrence frequency and percentages of the waypoint- and target-oriented strategies for each participant was obtained by applying the hacking detection HMM to each participant's data using the Viterbi algorithm [27]. Based on the occurrence percentage of the adjust waypoint and adjust target states, participants were classified into different hacking detection categories. As shown in Table IV, participants were classified into four categories: 1) waypoint strong dominant strategy; 2) waypoint weak dominant strategy; 3) target weak dominant strategy; and 4) target strong dominant strategy. The population of each strategy category was approximately one-fourth the total participant population.

Another repeated-measure multivariate ANOVA model with a significance level of 0.05 was used to analyze the impact of different hacking detection strategies on participant performance and hacking detection success rate. In this rm-MANOVA model, strategy categories were considered as a between-subject factor. The rm-MANOVA model showed that different hacking detection strategies did not affect the overall participant performance ($F(3, 27) = 0.754, p = 0.530$), their hacking detection success rate ($F(3, 27) = 0.086, p = 0.967$), and their imagery counting task success rate ($F(3, 27) = 1.528, p = 0.230$). Thus, when examining the aggregate group, no strategy dominated in terms of performance. However, given that the only operator who had perfect performance were the two operators with daily game experience, we examined their strategies in detail in the next section to shed more light on which strategies could potentially produce the best outcomes.

B. Master Participant Hacking Strategies

Developing separate HMMs for the two master participants was not possible due to the limited data; however, operator state paths can provide a map of individual strategies. As shown in Fig. 10, the two dominant hacking detection strategies are highlighted separately to represent the two master participant strategies. The red path represents the first master participant's operation flow and the blue path represents the second master participant's operation flow.

As depicted in Fig. 10, the master participants represented the two dominant strategies shown in the hacking detection model of Fig. 8. The first master participant exhibited the target-oriented strategy, spending an average of 81.1 s in each hacking detection (overall average for target-dominant people was 100.3 s). The second master participant exhibited the waypoint-adjusted strategy, spending an average of 50.5 s in each hacking detection (overall average for waypoint-dominant people was 81.8 s). The two master participants demonstrated the two dominant strategies shown in the model for all participants and both master participants achieved 100% detection, so there is no clear dominant strategy in terms of quality of final decision. However, there was a clear difference in speed with the waypoint-oriented strategy taking, on average, 30 s less to accomplish, which can be seen in the two strategies in Fig. 10 where the target-oriented strategy has an additional state. This is a practically significant number as intervening as quickly as possible in the middle of a hacking event is paramount. So, while this analysis reveals no dominant strategy in terms of detecting a hacking event, it does suggest that the waypoint-oriented strategy is likely to lead to faster results, which could be very important in prosecuting actual events.

VII. Conclusion

The human operator behavior models in this study present the feasibility of investigating operator behavior patterns and strategies in conducting supervisory control tasks through the use of HMMs. From operator behavior models, we can investigate factors that potentially impact operator behavior patterns and their higher level strategies. Observed strategies from a single HMM can provide engineers and researchers a practical approach to investigating human operators' strategies in human supervisory control scenarios.

The general behavior model, derived using RESCHU-SA-based experiments, shows seven major human operator behavioral states for supervision of UAVs that could be subject to hacking events. In this model, two functional groups emerged, including a hacking detection group with three behavioral states and a UAV navigation group with four states. Operators generally switched between functional groups as demands dictated, i.e., when a hacking event emerged, operators moved from the navigation flow to the hacking flow, indicating that such functions could be seen as modular.

A 6-state hacking detection strategy model allowed us to investigate operator hacking detection strategies in detail. Two major strategies can be observed from the model, including waypoint-oriented and target-oriented strategies. Based on statistical results, different hacking detection strategies did not affect operators' overall performance and success rate in hacking detection. Although no single best hacking detection strategy emerged in terms of quality, one strategy was superior in terms of the time to correct decision.

Although this geo-location approach for UAV hacking detection is still in an experimental stage, these initial results suggest that such an approach could enhance the security of future supervisory UAV control systems if hacking notifications are provided. Considering that no hacking notification misses were introduced in this experiment, as a future study we will investigate the potential effects on operators' performance and detection strategies if the autonomous system fails to provide notifications. In addition, certain limitations still exist in our HMM method, including limited model training data and required experimenter subjective judgment in hidden state interpretation, which is a fundamental issue for all unsupervised machine learning approaches. Current research is underway to determine how to make such model interpretation more straightforward as well as improve sensitivity analysis methods to reveal weaknesses in employed assumptions.

These descriptive operator behavior models highlight the fact that even effective strategies can be inefficient. Further work is needed to determine why people adopt different strategies and whether additional assistance can be used to improve operator strategies, either through training or a decision support system. Finally, the development and utilization of predictive behavior models can contribute to the future development of real-time guidance systems, which monitor operators constantly and provide real-time operational guidance.

References

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2008, pp. 2314–2325.

[2] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastructure Protection*, vol. 5, no. 3/4, pp. 146–153, 2012.

[3] S. Shane and D. E. Sanger, "Drone crash in Iran reveals secret US surveillance effort," *The New York Times*, vol. 7, Dec. 7, 2011.

[4] A. M. Treisman and G. Gelade, "A feature-integration theory of attention," *Cogn. Psychol.*, vol. 12, no. 1, pp. 97–136, 1980.

[5] L. Itti, C. Koch, and E. Niebur, "A model of saliency-based visual attention for rapid scene analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 11, pp. 1254–1259, Nov. 1998.

[6] B. de Bruyn and G. A. Orban, "Human velocity and direction discrimination measured with random dot patterns," *Vis. Res.*, vol. 28, no. 12, pp. 1323–1335, 1988.

[7] M. Elfar *et al.*, "Platform for security-aware design of human-on-the-loop cyber-physical systems," in *Proc. 8th Int. Conf. Cyber-Phys. Syst.*, 2017, pp. 93–94.

[8] B. Donmez, C. Nehme, and M. L. Cummings, "Modeling workload impact in multiple unmanned vehicle supervisory control," *IEEE Trans. Syst., Man, Cybern. Part A, Syst., Humans*, vol. 40, no. 6, pp. 1180–1190, Nov. 2010.

[9] H. Zhu, M. Elfar, M. Pajic, Z. Wang, and M. Cummings, "Human augmentation of UAV cyber-attack detection," in *Augmented Cognition: Users and Contexts* (Lecture Notes in Computer Science, vol 10916), D. Schmorrow, C. Fidopiastis Eds. Cham, Switzerland: Springer, 2018.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[11] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proc. IEEE/ION Position Location Navigat. Symp.*, 2012, pp. 479–487.

[12] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2011, pp. 2646–2656.

[13] K. Wesson, M. Rothlisberger, and T. Humphreys, “Practical cryptographic civil GPS signal authentication,” *Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[14] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, “Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators,” *IEEE Control Syst.*, vol. 37, no. 2, pp. 66–81, Apr. 2017.

[15] K. D. Wesson, B. L. Evans, and T. E. Humphreys, “A combined symmetric difference and power monitoring GNSS anti-spoofing technique,” in *Proc. IEEE Global Conf. Signal Inf. Process.*, 2013, pp. 217–220.

[16] T. E. Humphreys, “Detection strategy for cryptographic GNSS anti-spoofing,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[17] M. L. Psiaki, B. W. O’Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, “Civilian GPS spoofing detection based on dual-receiver correlation of military signals,” in *Proc. 24th Int. Techn. Meet. Satellite Division Inst. Navig. (ION GNSS 2011)*, Portland, OR, USA, Sep. 20–23, 2011, pp. 2619–2645.

[18] M. Pajic, I. Lee, and G. J. Pappas, “Attack-resilient state estimation for noisy dynamical systems,” *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 82–92, Mar. 2017.

[19] R. Ivanov, M. Pajic, and I. Lee, “Attack-resilient sensor fusion for safety-critical cyber-physical systems,” *ACM Trans. Embedded Comput. Syst.*, vol. 15, no. 1, Feb. 2016, Art. no. 21.

[20] R. J. Radke, S. Andra, O. Al-Kofahi, and B. Roysam, “Image change detection algorithms: A systematic survey,” *IEEE Trans. Image Process.*, vol. 14, no. 3, pp. 294–307, Mar. 2005.

[21] D. Blacknell and H. Griffiths, *Radar Automatic Target Recognition (ATR) and Non-Cooperative Target Recognition (NCTR)*. London, U.K.: Inst. Eng. Technol., 2013.

[22] M. L. Cummings, S. Bruni, S. Mercier, and P. J. Mitchell, “Automation architecture for single operator, multiple UAV command and control,” *Int. Command Control J.*, vol. 1, no. 2, pp. 1–24, 2007.

[23] T. B. Sheridan, *Telerobotics, Automation, and Human Supervisory Control*. Cambridge, MA, USA: MIT Press, 1992.

[24] S. Asmussen, *Applied Probability and Queues*, vol. 51. New York, NY, USA: Springer-Verlag, 2008.

[25] A. Pentland and A. Liu, “Modeling and prediction of human behavior,” *Neural Comput.*, vol. 11, no. 1, pp. 229–242, 1999.

[26] A. Galata, N. Johnson, and D. Hogg, “Learning variable-length Markov models of behavior,” *Comput. Vis. Image Understanding*, vol. 81, no. 3, pp. 398–413, 2001.

[27] L. R. Rabiner, “A tutorial on hidden Markov models and selected applications in speech recognition,” *Proc. IEEE*, vol. 77, no. 2, pp. 257–286, Feb. 1989.

[28] X. Meng, K. K. Lee, and Y. Xu, “Human driving behavior recognition based on hidden Markov models,” in *Proc. IEEE Int. Conf. Robot. Biomimetics*, 2006, pp. 274–279.

[29] Y. Boussemart, J. Las Fargeas, M. L. Cummings, and N. Roy, “Comparing learning techniques for hidden Markov models of human supervisory control behavior,” in *Proc. AIAA Infotech@ Aerosp. Conf. AIAA Unmanned... Unlimited Conf.*, 2009, Paper 1842.

[30] Y. Boussemart, M. L. Cummings, J. L. Fargeas, and N. Roy, “Supervised vs. unsupervised learning for operator state modeling in unmanned vehicle settings,” *J. Aerosp. Comput., Inf., Commun.*, vol. 8, no. 3, pp. 71–85, 2011.

[31] C. E. Nehme, “Modeling human supervisory control in heterogeneous unmanned vehicle systems,” Ph.D. dissertation, Dept. Aeronaut. Astronaut., Massachusetts Inst. Technol., Cambridge, MA, USA, 2009.

[32] L. Rabiner and B. Juang, “An introduction to hidden Markov models,” *IEEE ASSP Mag.*, vol. 3, no. 1, pp. 4–16, Jan. 1986.

[33] L. E. Baum and T. Petrie, “Statistical inference for probabilistic functions of finite state Markov chains,” *Ann. Math. Statist.*, vol. 37, no. 6, pp. 1554–1563, 1966.

[34] G. Schwarz *et al.*, “Estimating the dimension of a model,” *Ann. Statist.*, vol. 6, no. 2, pp. 461–464, 1978.

[35] V. Rodríguez-Fernández, A. Gonzalez-Pardo, and D. Camacho, “Finding behavioral patterns of UAV operators using multichannel hidden Markov models,” in *Proc. IEEE Symp. Ser. Comput. Intell.*, 2016, pp. 1–8.

Haibei Zhu received the B.S. degree in electrical engineering from Rensselaer Polytechnic Institute, NY, USA, in 2015. He is currently working toward the Ph.D. degree in computer engineering at Duke University, NC, USA.

He is currently a Research Assistant with the Duke Humans and Autonomy Lab. His research interests include human computer interaction, data mining, and operator strategy prediction.

Mary L. Cummings (SM’03) received the Ph.D. degree in systems engineering from the University of Virginia, Virginia, VA, USA, in 2004.

She is currently a Professor with the Duke University Department of Mechanical Engineering and Materials Science, the Duke Institute of Brain Sciences, and the Duke Electrical and Computer Engineering Department. She is the Director of the Duke Humans and Autonomy Laboratory.

Mahmoud Elfar received the B.Sc. degree in mechatronics from Ain Shams University, Cairo, Egypt. He is currently working toward the Ph.D. degree in computer engineering at Duke University, NC, USA.

His research interests are in formal methods, model checking techniques, and their applications in building human-aware cyber-physical systems.

Ziyao Wang received the B.S. degree in mechanical engineering from Jilin University, Jilin, China, in 2016, and the M.S. degree in mechanical engineering and material science from Duke University, NC, USA, in 2018.

He is currently working in the Humans and Autonomy Lab at Duke University. His current research interests include human robot interaction.

Miroslac Pajic (S’06–M’13) received the Dipl. Ing. and M.S. degrees in electrical engineering from the University of Belgrade, Belgrade, Serbia, in 2003 and 2007, and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 2010 and 2012, respectively.

He is currently the Nortel Networks Assistant Professor with the Department of Electrical and Computer Engineering at Duke University. He also holds a secondary appointment with the Computer Science Department. His research interests focus on the design and analysis of cyber-physical systems and in particular real-time and embedded systems, distributed/networked control systems, and high-confidence medical devices and systems.