Development of Operator Behavior Model in Hacking Detection of UAVs

Haibei Zhu
Department of Electrical & Computer Engineering
Email: haibei.zhu@duke.edu

Mahmoud Elfar
Department of Electrical & Computer Engineering
Email: mahmoud.elfar@duke.edu

Miroslav Pajic
Department of Electrical & Computer Engineering
Email: miroslav.pajic@duke.edu

M. L. Cummings
Department of Mechanical Engineering & Materials Science
Email: mary.cummings@duke.edu

Supported by the ONR

DUKE ROBOTICS

HAL
Humans and Autonomy Lab

Summary

Unmanned aerial vehicles (UAVs) have extensive applications in both civilian and military, and its rapid development has been accompanied by many security concerns. One common attack is GPS spoofing [1], in which attackers navigate hacked UAVs to unexpected destinations. To improve the success rate of hacking detection and the design of human supervisory UAV control system are significant in UAV development. In this study, we proposed a human-autonomy collaborative approach of human geo-location for single-operator with multiple-UAV supervisory control systems to detect potential UAV GPS spoofing attacks. We also developed human operator behavior models to investigate operators' hacking detection strategies.

Questions: 1) can human operator successfully detect cyber-attacks on UAVs via human geo-location, 2) what factors would affect operators' performance and behavior patterns, 3) what are the common strategies in hacking detections, and 4) what are the general operator behavior patterns in detecting UAV cyber-attacks

Methods: 1) design and conduct experiment with UAV hacking events, 2) investigate operators' performance via statistical analysis, and 3) develop human operator behavior models through unsupervised Hidden Markov Model

Results: 1) human operators can detect UAV hackings with an average success rate of 83%, 2) video game experience affected operators' performance, 3) taskload affected operator behavior models, and 4) operators' UAV control and hacking detection strategies are different under different taskload, and strategies can be interpreted from the operator behavior models

Experiment Design

The experiment was designed and conducted on the platform of RESCHU-SA [2]. Each participant completed two experiment scenarios with different taskload (low and high). The performance of all 36 participants was determined by their final scores.

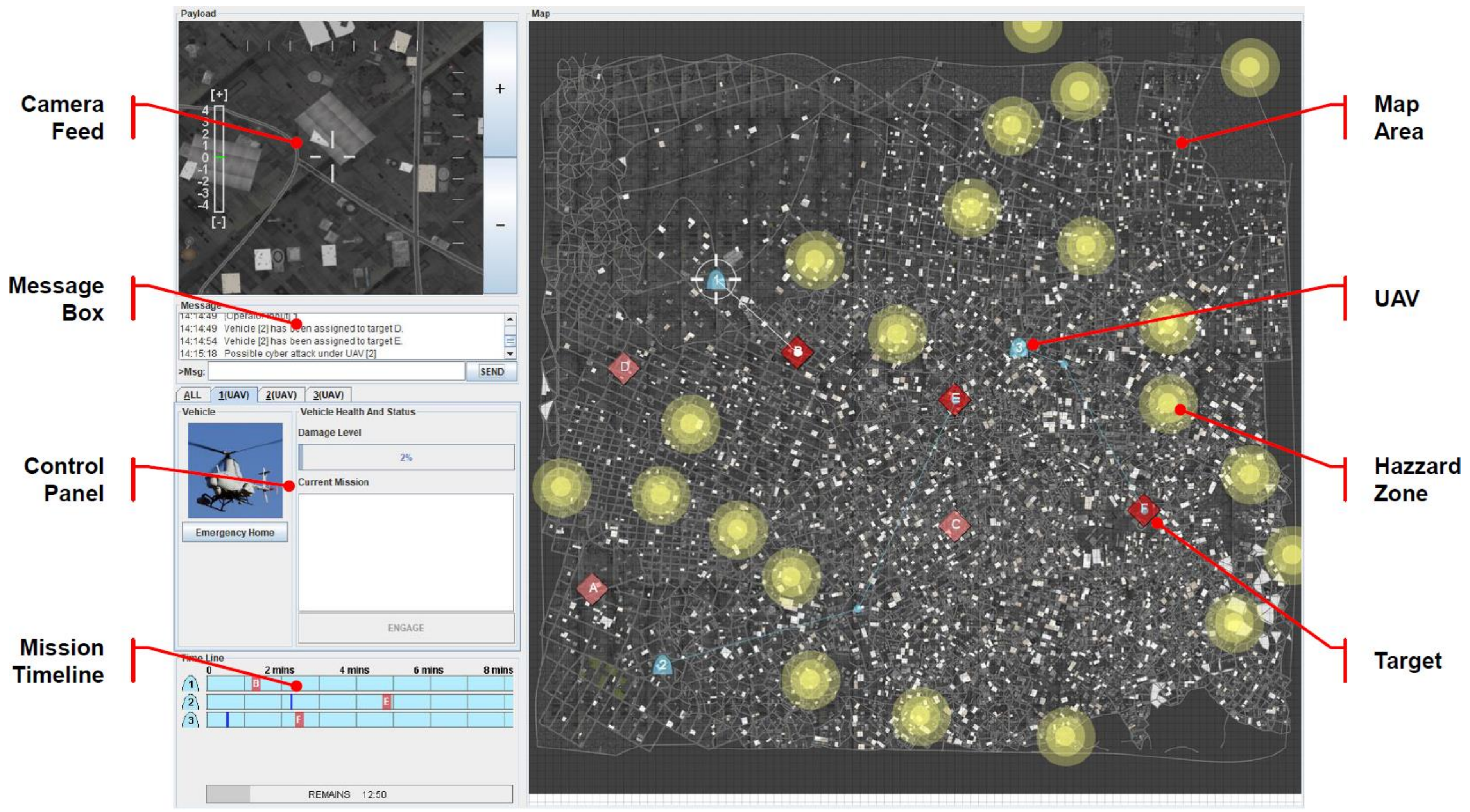

Figure 1. An example of RESCHU-SA interface in low taskload scenario

Experiment Statistical Results

- Both taskload and gender did not affect participants' performance scores
- Video game experience was moderately correlated with participants' performance (Pearson = .254, p = .031) and percentage of correct hacking identification (Pearson = .30, p = .011)
- Operators with the most gaming experience performed the best with 100% success rate in hacking detection
- The average time participants controlled UAVs was significantly negatively correlated with the time UAVs stayed in hazard areas (Pearson = -.345, p = .003)
- The time participants spent in imagery tasks was also negatively correlated with correct hacking detection percentage (Pearson = -.275, p = .019)
- The average hacking detection time and correct hacking detection were significantly negatively correlated (Pearson = -.375, p = .001)
- Comparing to high taskload, operators had much less UAV damage and spent less time in hazard areas in low taskload

Human Operator Behavior Models

Human operator behavior models are trained through unsupervised Hidden Markov Model (HMM), which is a data-driven machine learning approach. HMMs allow the inference of hidden human cognitive states from observable operator interactions with RESCHU system [3] [4]. Both models for high and low taskload scenarios are selected mainly based on both Bayesian Information Criterion (BIC) and the number of rare state (NRS).

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

Figure 2. Observations (emissions) of HMM models

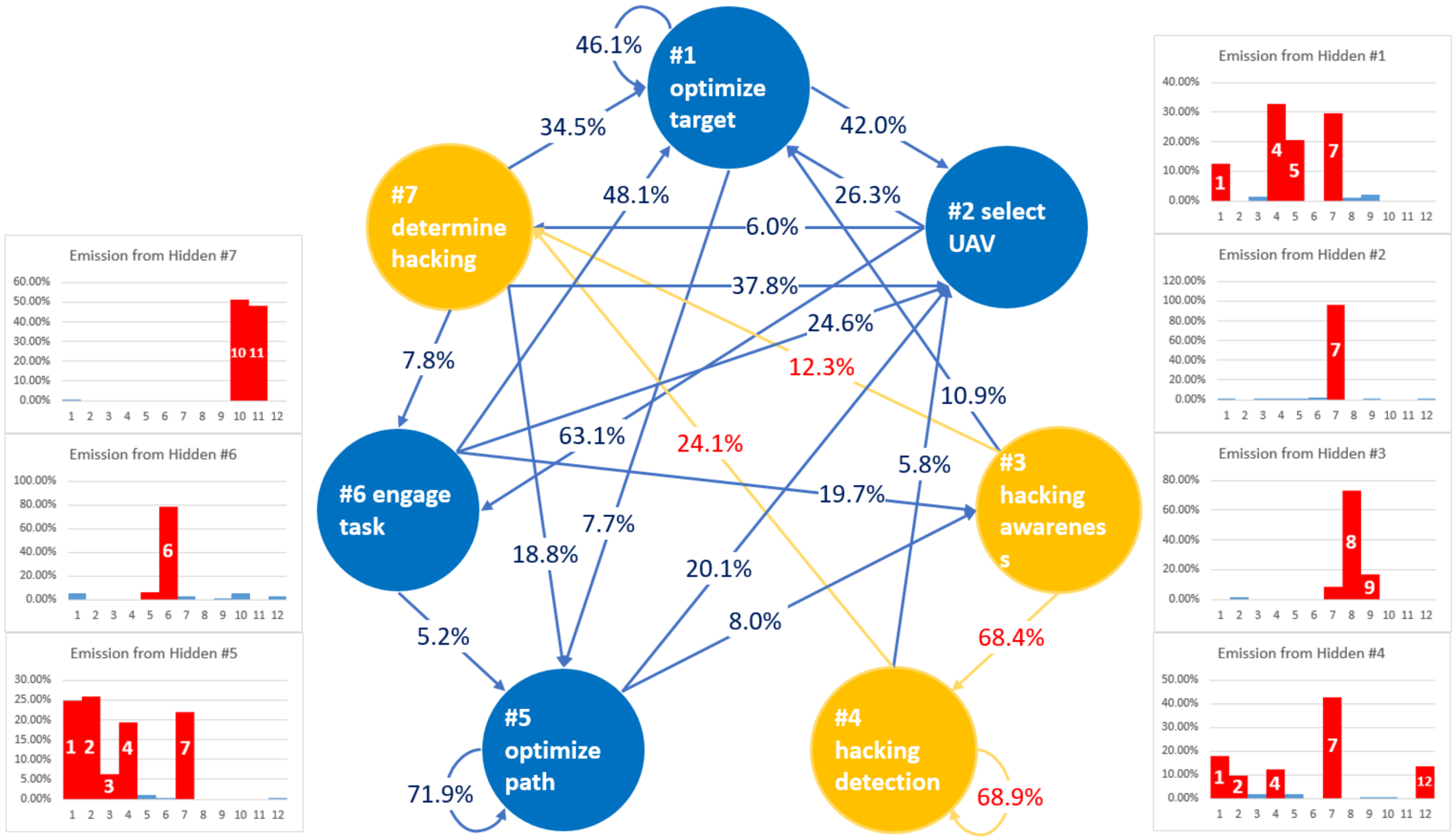

Figure 3. The HMM model of high taskload scenario with state emissions

In the high taskload HMM model, the hacking detection related states (state #3, 4 and 7) and UAV navigation related states (state #1, 2, 5 and 6) can be separated clearly.

- Detection flow is clear – from perceiving hacking to detection to decision
- As an add-on task, hacking detection brings additional states to core UAV navigation model

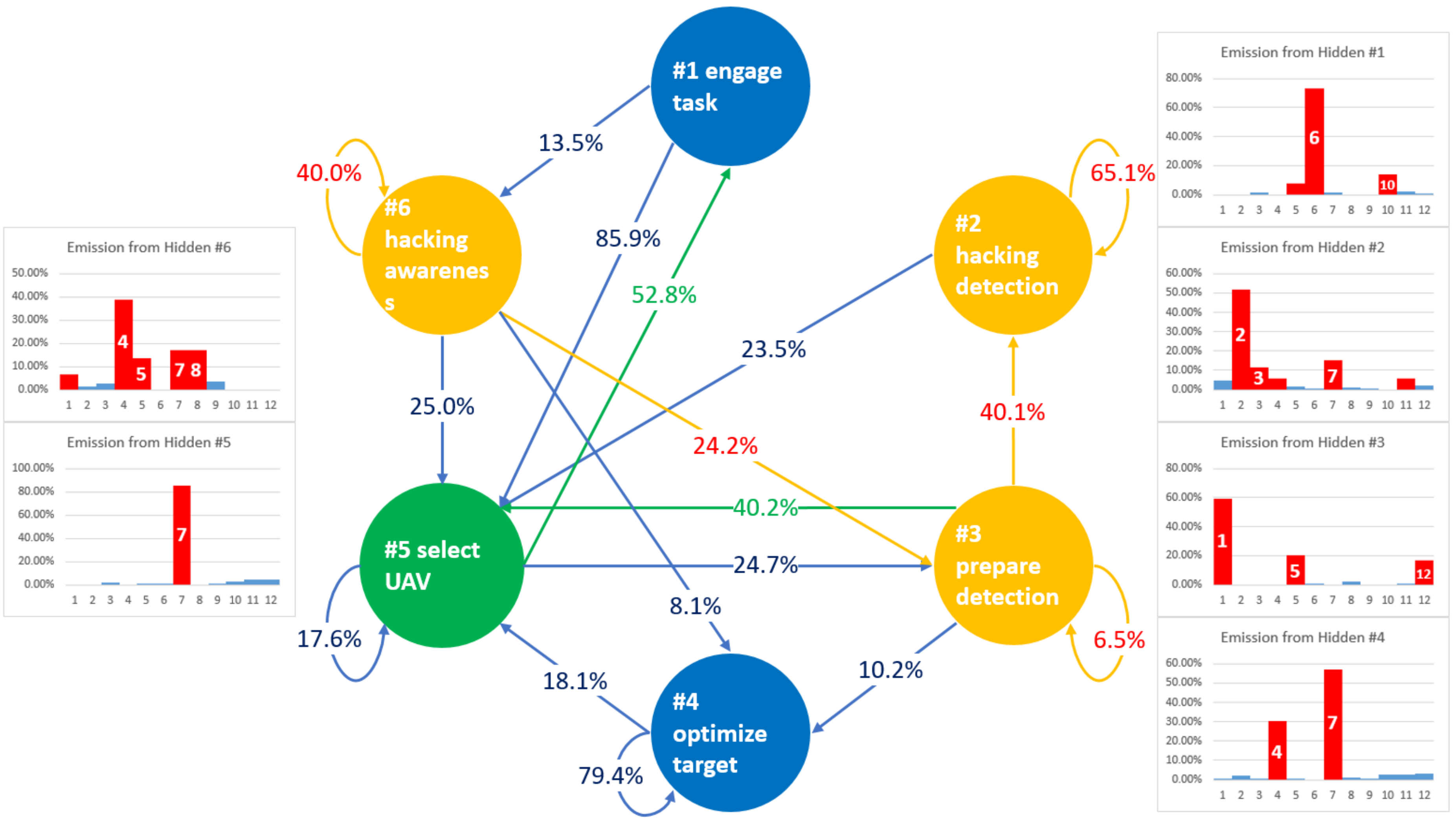

Figure 4. The HMM model of low taskload scenario with state emissions

The low taskload model presents the different hacking detection strategies via different states transition paths – also shows operators' multi-tasking.

- Proactive – operators made decision while the notified UAV was still moving (green path)
- Reactive – operators made decision after notified UAV's arrival (green path)

Possible improvement of utilizing automation to assist human in hacking detection

- Increase transition probability from "hacking awareness" to "hacking detection"
- Reduce redundant self transition in "hacking detection"

Conclusion and Future Work

In this work, we have shown that human operators can assist autonomous systems in UAV GPS spoofing detection via human geo-location. Operators' performance and behavior patterns are affected by many factors. Operators' hacking detection strategies can be clearly interpreted from HMM models. Future work will include 1) development of general operator behavior models in human supervisory UAV control system, 2) investigation of advanced hacking detection strategies, and 3) investigation of HMM selection criteria and HMM model stability.

Reference

[1]. Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 31(4), 617-636.

[2]. Nehme, C. E. (2009). Modeling human supervisory control in heterogeneous unmanned vehicle systems. MASSACHUSETTS INST OF TECH CAMBRIDGE DEPT OF AERONAUTICS AND ASTRONAUTICS.

[3]. Baum, L. E., & Petrie, T. (1966). Statistical inference for probabilistic functions of finite state Markov chains. The annals of mathematical statistics, 37(6), 1554-1563.

[4]. Rabiner, L., & Juang, B. (1986). An introduction to hidden Markov models. ieee assp magazine, 3(1), 4-16.