HMMs for Anomaly Detection in Autonomous Robots

Davide Azzalini
Politecnico di Milano
Milano, Italy
davide.azzalini@polimi.it

Alberto Castellini
University of Verona
Verona, Italy
alberto.castellini@univr.it

Matteo Luperto
Università degli Studi di Milano
Milano, Italy
matteo.luperto@unimi.it

Alessandro Farinelli
University of Verona
Verona, Italy
alessandro.farinelli@univr.it

Francesco Amigoni
Politecnico di Milano
Milano, Italy
francesco.amigoni@polimi.it

ABSTRACT

Detection of anomalies and faults is a key element for long-term robot autonomy, because, together with subsequent diagnosis and recovery, allows to reach the required levels of robustness and persistency. In this paper, we propose an approach for detecting anomalous behaviors in autonomous robots starting from data collected during their routine operations. The main idea is to model the nominal (expected) behavior of a robot system using Hidden Markov Models (HMMs) and to evaluate how far the observed behavior is from the nominal one using variants of the Hellinger distance adopted for our purposes. We present a method for online anomaly detection that computes the Hellinger distance between the probability distribution of observations made in a sliding window and the corresponding nominal emission probability distribution. We also present a method for offline anomaly detection that computes a variant of the Hellinger distance between two HMMs representing nominal and observed behaviors. The use of the Hellinger distance positively impacts on both detection performance and interpretability of detected anomalies, as shown by results of experiments performed in two real-world application domains, namely, water monitoring with aquatic drones and socially assistive robots for elders living at home. In particular, our approach improves by 6% the area under the ROC curve of standard online anomaly detection methods. The capabilities of our offline method to discriminate anomalous behaviors in real-world applications are statistically proved.

KEYWORDS

long-term autonomy; anomaly detection; hidden Markov models; autonomous robots

ACM Reference Format:
Davide Azzalini, Alberto Castellini, Matteo Luperto, Alessandro Farinelli, and Francesco Amigoni. 2020. HMMs for Anomaly Detection in Autonomous Robots. In *Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), Auckland, New Zealand, May 9–13, 2020,* IFAAMAS, 9 pages.

1 INTRODUCTION

Autonomous robots are increasingly becoming part of human everyday life. From driverless cars to assistive robots for elderly people, these systems are leaving the factories and entering unconstrained scenarios with close interaction with humans. Complex and dynamic environments are characterized by large degrees of uncertainty and pose big challenges to robot designers. One of the key competences required to newly conceived robots is to reliably operate over long periods of time under changing and unpredictable environmental conditions, which is referred to as *long-term autonomy* (LTA) [26]. Exhibiting LTA means that robots are persistent, robust, and able to adapt to changes in their operational environments. Fault Detection and Diagnosis (FDD) approaches [22] are a fundamental ingredient of LTA in order to identify anomalies and recover a robot system in time for continuing its operations.

Hidden Markov Models (HMMs) [33] have been successfully used for learning robot behaviors, especially in the context of Learning from Demonstration (LfD) for manipulators and humanoid robots [2, 5]. An HMM is a statistical model in which the system being modeled is assumed to be a Markov process with unobservable (hidden) states, each characterized by an emission distribution governing the probability of producing any of the observable system outputs and a transition distribution indicating which are the likely next states. Because of their robustness to spatiotemporal variations of sequential data, HMMs are also commonly used for encoding and abstracting noisy time series [7–9]. We advocate that HMMs can provide good representations also of robot behaviors in LTA contexts, where similar sequences of actions (tasks) are typically repeated multiple times. Representing robot behaviors in these domains is still wildly unexplored because of the difficulty to predict the diverse situations in which the robot may have to deal with.

In this paper, we propose an approach for detecting anomalous behaviors of robot systems involved in complex LTA scenarios, both online, while robots are operating, and offline, after robots have completed a run of their tasks. The behavior of robots is modeled using HMMs and, originally, the Hellinger distance [16] is used to compute *(i)* the dissimilarity between the probability distribution of subsequences of observations in a sliding window and the emission probability of related HMM hidden states (online approach) and *(ii)* the distance between pairs of HMMs representing nominal and actual behaviors (offline approach). The advantage of using such a distance measure instead of standard measures (such as the likelihood of observation subsequences for online approaches) is

twofold:fi rst, the Hellinger distance is bounded and thus lends itself to simpler interpretation and thresholding; second, it is less noisy and hence more informative and discriminative.

Experiments on two robot systems operating in real-world settings show that the proposed online and offline approaches outperform standard fault detection methods. The online approach allows to discover both trajectory and speed anomalies of aquatic drones performing water monitoring. In the same application, the offline approach significantly discriminates regular and anomalous behaviors observed in different runs of the same task. Anomalous execution traces are also detected in a long-term deployment of a socially assistive mobile robot supporting independence of elderly people living alone at home.

The main original contribution of this paper is the novel application of two theoretical tools, HMMs and Hellinger distance, to autonomous robots and LTA. Specifically, we contribute:

- A new *online* anomaly detection algorithm based on HMMs and Hellinger distance.
- A new *offline* anomaly detection algorithm based on a bounded distance between HMMs derived from the Hellinger distance. This distance abstracts the comparison between two behaviors from the level of observations to the level of learned HMMs, providing interpretability and diagnostic capabilities.
- An extensive experimental campaign on real robots involved in two applications requiring LTA.

2 RELATED WORK

Fault Detection in Autonomous Robots. FDD approaches can be divided into three categories: model-based, knowledge-based, and data-driven [22]. Model-based approaches [19] require explicit analytical models (i.e., mathematical equations or logic formulas) of robotic components and therefore need expert knowledge to be built. Knowledge-based approaches typically associate each known fault to a detection rule which is triggered when the specific behavior is observed. Data-driven approaches are instead based on (usually probabilistic) descriptions of behaviors or faults that are automatically learnt from previous observations of the system. Their advantage is that they do not need any explicit prior knowledge of the system and of the faults.

Online data-driven methods are mostly used for autonomous robots and generate probabilistic representations of system behaviors in real-time, from data streams, and use them to statistically differentiate potential faults from normal behavior. Some approaches use statisticalfi ltering such as Kalman and particlefi lters [1, 12, 36]. Other works propose supervised machine learning approaches [6] to classify data produced in real-time by a robot. The problem with supervised methods is that they need fully labelled data, which are not always available; hence, recent developments tend to focus on unsupervised and semi-supervised approaches to FDD. Unsupervised techniques do not require a labeled training set, while techniques that operate in a semi-supervised mode assume that the training data have labeled instances for only the nominal class [10]. In [23], the authors introduce an online multivariate data-driven fault detection approach which uses the Mahalanobis-distance to compare correlated streams of data with previously observed data. In [14], a self-awareness approach is proposed which builds a probabilistic model on the basis of the whole discrete event-based data interchange inside the robot. Finally, some works [21, 23] explicitly deal with contextual faults [10], namely faults that depend on the fact that observations which are legitimate under one context might not be legitimate under another. We consider a similar scenario, with the difference that our proposed approach represents different contexts as different states of an HMM, while those in the literature consider recent past observations as context.

HMM-Based Fault Detection. HMMs have been often used for anomaly detection. Most of the works in the literature train HMMs with data recorded during non-anomalous executions and use one of the following two approaches for detecting anomalies: *(i)* compute the likelihood of current observations and classify them as anomalous if the likelihood is lower than a threshold, *(ii)* compute the probability of the underlying Markov chain and compare it with afi xed threshold [15, 37, 38].

The works that most resemble ours are [30] and [32], in which HMMs are trained using multimodal sensory signals for detecting anomalies in assistive robots. At run time, the trained HMMs provide likelihood scores for data inside a window, which are compared to an adaptive detection threshold to identify putative anomalies. In this paper, we substitute the likelihood estimation with the computation of a more informative and interpretable measure, and also provide a new offline methodology for detecting long-term shifts from the nominal behavior. Another similar work, but with a different application focus, is [34], in which anomalies represent credit card frauds and are identified by directly comparing HMMsfi t at consecutive periods rather than comparing acceptance probabilities (i.e., likelihoods). Our approach is different in the fact that, instead of just comparing the emission probabilities of the states of two HMMs, we propose a single-value metric representing the overall dissimilarity between two HMMs.

Deep Learning-Based Spatio-Temporal Modeling. Recently, deep learning models have been used to re-address many spatio-temporal modeling tasks providing improvements over the state-of-the-art methods. Few works employ deep neural networks for online anomaly detection in robot systems, two recent examples are [31, 35], which employ LSTM variational autoencoders. However, these works cannot be considered as alternatives to our online method since they require datasets composed of thousands of execution traces sampled at high frequency. Moreover, the dataset employed in [35] is fully labeled (i.e., also anomalies are labeled, setting a problem different from ours), and both datasets of [31, 35] are heavily high-dimensional (e.g., [31] considers, in addition to joints' data, also video and sound recordings). In the settings we consider, there are few execution traces (for example, 11 for thefi rst experiment and 149 for the second experiment of Section 4) with low dimensionality, so we cannot perform direct comparisons with those models. For offline anomaly detection, to the best of our knowledge, no method exists in the literature for computing the distance between two trained neural networks by directly comparing their learned weights. Being model explainability and interpretability at the core of our offline method, deep learning models are not adequate, since they are hard to interpret and explain, despite some initial results toward explainable AI [11, 18].

3 THE PROPOSED METHOD

In this section, wefi rst define the problem we address, then introduce some mathematical background, andfi nally present the proposed online and offline anomaly detection methods.

3.1 Problem Definition

We represent by $\boldsymbol{O} = \{\boldsymbol{o}_1, ..., \boldsymbol{o}_n\}$ a d-dimensional time series composed of n observations, where $\boldsymbol{o_t}$ is a d-dimensional vector representing the multivariate (multi-valued) observation at time t. The nominal behavior of a robot system is then represented as $\boldsymbol{O}^N = \{\boldsymbol{o}_1^N, ..., \boldsymbol{o}_{n^N}^N\}$ and the observed behavior of the same system along some time period as $\boldsymbol{O}^O = \{\boldsymbol{o}_1^O, ..., \boldsymbol{o}_{n^O}^O\}$.

If we consider $\boldsymbol{O}^O$ as a (possibly infinite) data stream, *online anomaly detection* at time t is the task of classifying the portion of the stream included in a sliding window (up to t) as anomalous or non-anomalous wrt $\boldsymbol{O}^N$.

Given afi nite batch of observations $\boldsymbol{O}^O$, *offline anomaly detection* is the task of classifying the behavior displayed by the system in $\boldsymbol{O}^O$ as anomalous or non-anomalous wrt $\boldsymbol{O}^N$.

We assume the availability of $\boldsymbol{O}^N$ and, for this reason, our approach belongs to the semi-supervised family. This choice is motivated by the fact that, in robotics, the availability of nominal observations for repetitive tasks, which are the kind of tasks on which we focus, is quite common, since it is often plausible to make ad hoc executions in nominal conditions.

3.2 Mathematical Background

We use HMMs [33] as a probabilistic model for the system that generated a given multivariate time series $\boldsymbol{O}$. An HMM is a statistical model in which the system being modeled is assumed to be a Markov process with K hidden states. The mathematical notation $\lambda = \{\boldsymbol{\pi}, \boldsymbol{A}, \boldsymbol{B}\}$ is used to represent an HMM, where $\boldsymbol{\pi} = \{\pi_i\}_{i=1}^K$ is the set of initial state probabilities, $\boldsymbol{A} = \{a_{ij}\}_{i,j=1}^K$ is the set of state transition probabilities (i.e., a_{ij} is the probability to move from state i to state j), and $\boldsymbol{B} = \{b_i(\boldsymbol{o})\}_{i=1}^K$ is the set of the probability distributions over observations in each state (emission probabilities). In our setting, we assume a multivariate Gaussian distribution for the emission probabilities, which means that $\boldsymbol{B} = \{\mathcal{N}(\boldsymbol{\mu}_i, \Sigma_i)\}_{i=1}^K$, where $\boldsymbol{\mu}_i$ and Σ_i are the mean and the covariance matrix for state i, respectively. Theory of HMMs provides algorithms to solve three important problems:

- Compute the probability (i.e., likelihood) that an observed (sub)sequence $\boldsymbol{O}$ is represented by an HMM, e.g., using the Forward algorithm [3].
- Find the parameters of an HMM, λ, to maximize the fit (likelihood) to an observed sequence $\boldsymbol{O}$, e.g., using the Baum-Welch algorithm [4].
- Compute the optimal HMM state sequence (known as Viterbi path) that best explains a given observed (sub)sequence $\boldsymbol{O}$, e.g., using the Viterbi algorithm [13].

The optimal number of hidden states and the covariance type can be found by minimizing the Bayesian information criterion (BIC), whichfi nds the optimal trade-off between maximizing the likelihood of the training data wrt the model and minimizing the number of parameters required (i.e., the number of hidden states) [6].

The Hellinger distance [16], used in both our online and offline anomaly detection methods described below, is a $[0, 1]$-bounded metric that quantifies the similarity between two probability density functions $f(x)$ and $g(x)$. It is computed as follows:

$$H^2(f, g) = \frac{1}{2} \int \left(\sqrt{f(x)} - \sqrt{g(x)}\right)^2 dx. \tag{1}$$

For the case of two multivariate Gaussian distributions $f(x) \sim \mathcal{N}(\mu_1, \Sigma_1)$ and $g(x) \sim \mathcal{N}(\mu_2, \Sigma_2)$, the Hellinger distance can be computed in closed form as:

$$H^2(f, g) = 1 - \frac{det(\Sigma_1)^{1/4} det(\Sigma_2)^{1/4}}{det\left(\frac{\Sigma_1+\Sigma_2}{2}\right)^{1/2}} \cdot \cdot exp\left\{-\frac{1}{8}(\mu_1 + \mu_2)^T \left(\frac{\Sigma_1 + \Sigma_2}{2}\right)^{-1} (\mu_1 - \mu_2)\right\}. \tag{2}$$

3.3 Online Anomaly Detection

The nominal behavior of the robot system is modeled as an HMM λ^N that is trained from $\boldsymbol{O}^N$ using the Baum-Welch algorithm. The number of hidden states and the covariance type are selected by minimizing the BIC. Online anomaly detection at time step t is performed by means of a sliding window $\boldsymbol{W}_t = \{\boldsymbol{o}_{t-w+1}^O, ..., \boldsymbol{o}_t^O\}$ of length w which includes the last w observations. For each window $\boldsymbol{W}_t$, a score is computed and, when the score exceeds a predefined threshold τ, the behavior is considered anomalous. The score is the Hellinger distance between the estimated distribution of the observations corresponding to the state $\hat{s}_t$ occurring most frequently in the Viterbi path $S_t = \{s_{t-w+1}, ..., s_t\}$ of window $\boldsymbol{W}_t$ and the emission probability of the same state in λ^N.

The detailed procedure for online anomaly detection is in Algorithm 1. The algorithm starts byfi tting the nominal HMM λ^N with the number of hidden states suggested by the BIC score (lines 1-2). After having specified the desired window length w (line 3) and threshold τ (line 4), the algorithm waits until w observations are collected (line 5) and then starts the online procedure (lines 6-17). The online procedure computes the Viterbi path of the multivariate time series inside the window (line 8). For the state $\hat{s}_t$ occurring most frequently in the Viterbi path (line 9) a multivariate Gaussian distribution $\mathcal{N}(\boldsymbol{\mu}, \Sigma)$ isfi t through maximum likelihood with the data inside the window (lines 10-12). Then the Hellinger distance is computed (using equation (2)) between $\mathcal{N}(\boldsymbol{\mu}, \Sigma)$ and the emission probability of state $\hat{s}_t$ in λ^N (line 13). If the distance is larger than τ, then a warning is reported (line 14).

3.4 Offline Anomaly Detection

Offline anomaly detection is performed by learning two different HMMs, λ^N and λ^O, and computing the distance between them in order to discover if (and how) the behavior of a robot system has changed over time.

To this end, wefi rst need to learn λ^N and λ^O from $\boldsymbol{O}^N$ and $\boldsymbol{O}^O$, respectively, with the Baum-Welch algorithm. We constrain the two models to have the same number of hidden states (i.e., the number of states of λ^N), which is reasonable since we assume the overall behavior of the robot system we model is the same.

Algorithm 1: Online anomaly detection

$K \leftarrow$ number of hidden states
$\lambda^N \leftarrow$ Baum-Welch($\boldsymbol{O}^N$, K)
$w \leftarrow$ window size
$\tau \leftarrow$ threshold
$t \leftarrow w$
repeat
  $\boldsymbol{W}_t \leftarrow \{\boldsymbol{o}^O_{t-w+1}, \ldots, \boldsymbol{o}^O_t\}$
  $\boldsymbol{S}_t \leftarrow$ Viterbi(λ^N, $\boldsymbol{W}_t$)
  $\hat{s}_t \leftarrow$ most frequent state in $\boldsymbol{S}_t$
  $\boldsymbol{X} \leftarrow \{\boldsymbol{o}^O_j \in \boldsymbol{W}_t \ : \ s_j = \hat{s}_t\}$
  $\boldsymbol{\mu} \leftarrow E[\boldsymbol{X}]$
  $\Sigma \leftarrow E[(\boldsymbol{X} - \boldsymbol{\mu})(\boldsymbol{X} - \boldsymbol{\mu})^T]$
  if $H^2(b^N_{\hat{s}_t}, \mathcal{N}(\boldsymbol{\mu}, \Sigma)) > \tau$ **then**
    echo warning
  end
  $t = t + 1$
until *new data keep coming*;

Given the model parameters of two HMMs, defining an appropriate similarity measure between the two models is not straightforward. Most of the works in the literature employ the Kullback-Leiber (KL) divergence [25] as a distance measure between two HMMs [20]. Given two probability density functions $f(x)$ and $g(x)$, the KL divergence can be computed as:

$$D_{\mathrm{KL}}(f, g) = \int f(x) \, log \, \frac{f(x)}{g(x)} dx. \tag{3}$$

The KL divergence has a closed-form expression for many probability distributions, including Gaussians and, more generally, the exponential family. For more complex distributions, such as mixture models and HMMs, the integral involves the logarithm of sums of component densities, and no simple closed-form expression exists. As a consequence, the KL divergence between HMMs can only be approximated via Monte Carlo sampling [20] or through variational approximation [17]. In this paper we are interested in computing the Hellinger distance between HMMs instead of the KL divergence, since, as seen before, it is a bounded measure that can provide interpretability to the anomaly detection model. Furthermore, to the best of our knowledge, no work in the literature has attempted to compute the Hellinger distance between HMMs.

We start the derivation of our Hellinger-based distance between HMMs (for offline anomaly detection) observing that although no closed-form solution exists for the KL divergence between two HMMs, some upper bounds have been proposed which can be computed in closed form. One such bound is proposed by [39] for left-to-right HMMs:

$$D(\lambda^1, \lambda^2) \leq \sum_{i=1}^{K} \Bigg\{ l^1_i \Bigg[\overbrace{D_{\mathrm{KL}}\left(b^1_i, b^2_i\right)}^{\text{contribution of emission probabilities}} + \overbrace{\log\left(\frac{a^1_{ii}}{a^2_{ii}}\right)}^{\text{contribution of transition matrices}} \Bigg] + \\ + \, l^2_i \Bigg[D_{\mathrm{KL}}\left(b^2_i, b^1_i\right) + \log\left(\frac{a^2_{ii}}{a^1_{ii}}\right) \Bigg] \Bigg\}, \tag{4}$$

where $D_{KL}\left(b^1_i, b^2_i\right)$ is the KL divergence between the emission probabilities of state i in the two models and represents how the emission probabilities differ, $\log\left(a^1_{ii}/a^2_{ii}\right)$ is the log-likelihood ratio of the transition probabilities, representing how much the two transition matrices differ, and $l_i = 1/(1 - a_{ii})$ approximates the expected duration of state i. The second term of equation (4) makes the distance symmetric.

The problem with equation (4) is that all of its components are unbounded, resulting in an overall unbounded measure very difficult to interpret and threshold in practical applications. Moreover, the contribution of the emission probabilities and that of the transition matrices can grow with different orders of magnitude, making it even more difficult to intuitively interpret the overall distance.

We take inspiration from equation (4) maintaining the idea of the two contributions and propose a new bounded (with values in $[0, 1]$) approximation of the distance between two HMMs which is based on the Hellinger distance and on the long-term probabilities of a Markov chain:

$$D(\lambda^1, \lambda^2) \approx \sum_{i=1}^{K} \Bigg\{ l^1_i \frac{1}{2} \Bigg[\overbrace{H^2\left(b^1_i, b^2_i\right)}^{\text{contribution of emission probabilities}} + \\ + \underbrace{\frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{K} \left(\sqrt{a^1_{ij}} - \sqrt{a^2_{ij}}\right)^2}}_{\text{contribution of transition matrices}} \Bigg] \Bigg\}, \tag{5}$$

where $H^2\left(b^1_i, b^2_i\right)$ is the Hellinger distance between the emission probabilities of state i in the two models (i.e., the contribution to the distance of the emission probabilities for state i) and the sum under the square root is the Hellinger distance between the rows of state i in the transition matrices of the two models (i.e., the contribution to the distance of the transition matrices for state i).

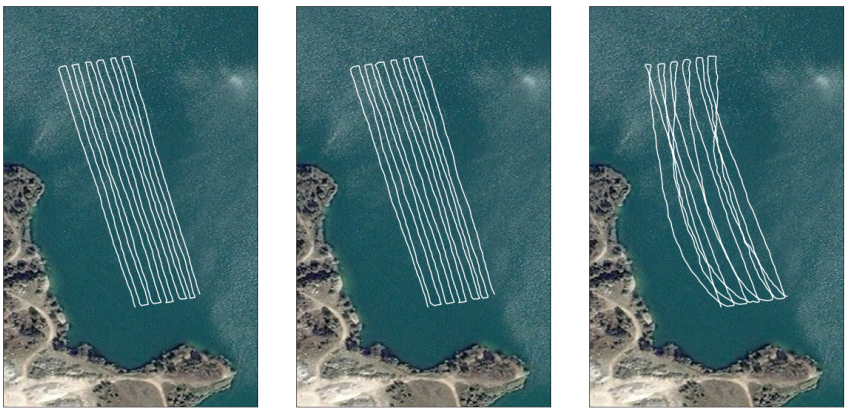
We drop the term corresponding to the second half of equation (4), which would make the distance symmetric, since we are only interested in how λ^O is dissimilar from λ^N and not vice-versa.

Computing the contribution of the transition matrices as in equation (5) instead of as in equation (4) has the advantage of taking into account the difference between the transition probabilities to all the states, while the log-likelihood ratio in equation (4) considers only the transition probabilities on the main diagonal that correspond to transitions to the same state.

In equation (5), l^1_i is computed as the long term probability of remaining in state i^1 wrt the transition matrix $\boldsymbol{A}^1$. Let $\boldsymbol{A}$ be a regular transition matrix (i.e., such that some power of $\boldsymbol{A}$ has all positive entries) with states $\{1, 2, \ldots, K\}$, long-term probabilities $\boldsymbol{l} = \{l_1, l_2, \ldots, l_K\}$ are the unique solution to:

$$\begin{cases} l_j = \sum_{k=1}^{K} l_k a_{kj}, \quad j = 1, 2, \ldots, K \\ \sum_{i=1}^{K} l_i = 1 \end{cases} \tag{6}$$

Long-term probabilities have two advantages over their approximations used in equation (4): *(i)* they are a better proxy of the time spent in each state, since they are obtained by simulating the



(a) Day 1 (b) Day 2 (c) Day 11

Figure 1: Water drone trajectories

system's behavior on the long run, and *(ii)* they sum up to 1, making equation (5) a weighted average.

To compute equation (5), we perform a bijective matching between states of λ^N and states of λ^O using the Hungarian algorithm [24] and considering the Hellinger distance between each pair of states, namely, the distance between the emission probability distributions of those states.

In practice, for diagnostic purposes, equation (5) can be unrolled and its components can be inspected separately. In particular, for each state, the two contributions can be inspected and, depending on the value of l_i^1 the impact of state i on the overall distance can be identified. This could greatly help in the diagnostic process to identify the precise reason(s) why two behaviors are dissimilar and to possibly recover to a non-anomalous behavior.

Beyond interpretability, one of the main strengths of our offline approach is that it is not negatively affected by differences in the lengths of the sequences $\boldsymbol{O}^N$ and $\boldsymbol{O}^O$ (as the standard likelihood) or by possible misalignments in such sequences, since it abstracts the comparison of behaviors to the level of learned HMMs.

The detailed procedure for offline anomaly detection is reported in Algorithm 2, which starts byfi tting the nominal HMM λ^N with the number of hidden states suggested by the BIC score (lines 1-2). Then the observed HMM λ^O is learned with the same number of hidden states as λ^N (line 3) and the detection threshold τ is selected (line 4). Long-term probabilities of the nominal model are computed with equation 6 (line 5). Then, after having matched the states in the two models with the Hungarian algorithm (line 6), the distance between λ^N and λ^O is computed with equation (5). If such distance is larger than τ, a warning is issued (lines 7-9).

The use of HMMs makes both our online and offline approaches capable of dealing with reactive and adaptive behaviors recorded in $\boldsymbol{O}^N$ and $\boldsymbol{O}^O$ (such as dynamic obstacle avoidance) as long as they do not jeopardize completely the global behavior of the robot. Relatively small deviations from the expected behavior could slightly increase the variance of the emission probability. However, if examples of perturbations of robot behavior are present in $\boldsymbol{O}^N$, they will be considered non-anomalous when they appear in $\boldsymbol{O}^O$.

Algorithm 2: Offline anomaly detection

```
1 K ← number of hidden states
2 λ^N ← Baum-Welch(O^N, K)
3 λ^O ← Baum-Welch(O^O, K)
4 τ ← threshold
5 l^N ← long-term probabilities of A^N
6 Hungarian(B^N, B^O)
7 if D(λ^N, λ^O) > τ then
8 |   echo warning
9 end
```

4 EXPERIMENTAL RESULTS

In this section we present the results obtained by applying the proposed approach to detect anomalies of two robots operating in real-world LTA scenarios.

4.1 Water Monitoring Robot

Thefi rst robot operates in the context of the INTCATCH Project[1], a H2020 EU project aiming to develop a new paradigm for water monitoring in river and lakes by harmonizing a range of innovative tools into a single efficient and user-friendly model. A dataset (see Figure 1(a)) has been gathered that contains 11 runs of a predefined path traveled by a Platypus drone (see Figure 2) in the Lake Garda (Italy). The dataset consists of 76213 observations, collected at 1Hz frequency, of the following variables concerning the robot state: heading (i.e., compass direction), speed, acceleration, power signals to the left and right propellers, latitude, and longitude. A domain expert has certified the readings of thefi rst day (see Figure 1(a)) as representing the nominal behavior and we use them to train an HMM. The BIC score suggests an optimal number of states $K = 3$ intuitively corresponding to:

- going *upward*, line segment A-B in Figure 3(a);
- going *downward*, line segment C-D in Figure 3(a);

[1] http://www.intcatch.eu
[2] http://senseplatypus.com/

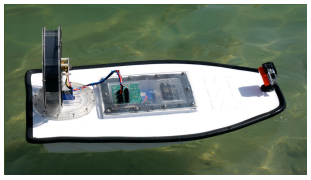


Figure 2: Platypus[2] Lutra boat usedin the context of the INTCATCH project, about 1 m long and 0.5 m wide.

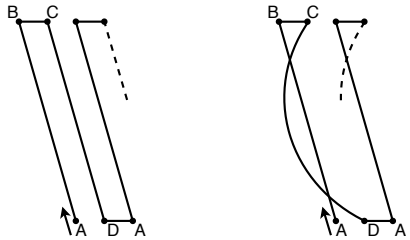


Figure 3: Nominal (a) and anomalous (b) behaviors

- going *right*, line segments B-C and D-A in Figure 3(a).

The domain expert classified the runs from day 2 to day 10 as non-anomalous (Figure 1 just reports the trajectory of day 2) and the run of day 11 as anomalous (as it can be clearly seen from the corresponding trajectory in Figure 1. Figure 3 schematically shows the difference between the regular (days 1-10) and the anomalous (day 11) behaviors.

4.1.1 Online anomaly detection. We compare our technique to two standard approaches (e.g., used in [30, 37, 38]): the negative log-likelihood with respect to the nominal HMM and the negative of the logarithm of the probability of the Viterbi path. The former one (which for brevity will be referred to as likelihood) is computed with the Forward algorithm as the negative of the logarithm of $P(\boldsymbol{W}_t|\lambda^N)$. The latter is obtained by computing the Viterbi path of $\boldsymbol{W}_t$ with the Viterbi algorithm and then by taking the negative of the logarithm of the multiplication of the transition probabilities between the states in the Viterbi path.

The window size w must be set to a value between a minimum, which allows to robustly estimate a multivariate Gaussian distribution from data inside the window, and a maximum, which depends on the dynamics of the analyzed behavior (if w is too large, anomalies relative to short behaviors could be missed). After some empirical tests, we selected a window size of 50 samples.

In Figure 4, our anomaly measure (in red) and the likelihood (in blue) for the second day are depicted. As expected, our measure maintains always a very low value while the likelihood seems to be high during the downward segments, which visually appear to be regular. As we will see, a negative log-likelihood of 1000 is not very high (when compared to the values reached in the eleventh day), anyway, being the likelihood unbounded, it would be hard to decide a priori that such a value of likelihood does not reflect an anomaly.

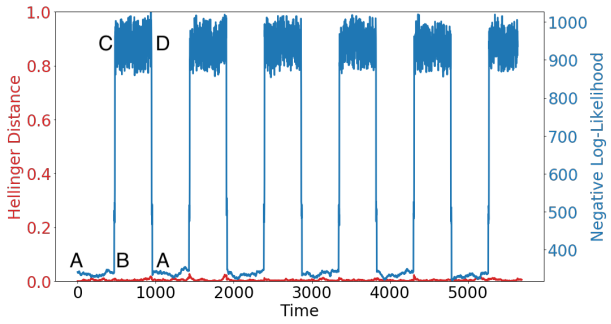


Figure 4: Online anomaly detection day 2 ($w = 50$)

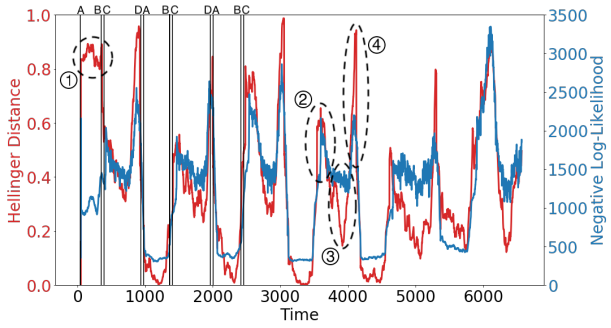


Figure 5: Online anomaly detection day 11 ($w = 50$)

Figure 5 reports the measures for the eleventh day, the anomalous one. The following remarks can be made:

- During thefi rst upward segment ① an anomaly occurs, due to the fact that the speed of the robot is much higher than that observed during the nominal upward behavior. Our technique empasizes this anomaly (which is not evident from the trajectories of Figure 1) better than the likelihood.
- Our anomaly score better reflects the anomalies present in the downward segments. Indeed, our approach correctly assigns an higher Hellinger distance to thefi rst half of the C-D segment ② (when the drone moves away from the optimal trajectory) and assigns a lower value to the second half ③ (when the drone gets back on track), while the negative log-likelihood reaches a plateau and does not decrease during the second half. In this sense, we can say that our approach is more expressive in capturing and representing anomalies.
- The second spike in the C-D segment ④ is correctly identified by both techniques and is due to an anomalous increase in the speed of the robot.

Figure 6 shows the ROC curves as τ is varied for the three methods considered. Our method outperforms the others, improving the area under the curve (AUC) of the standard approach based on the likelihood by 6%. We omit the plots of the negative logarithm of the Viterbi path in Figures 4 and 5 since it does not detect anomalies as good as the other two approaches (as evidenced also by the lower AUC in Figure 6).

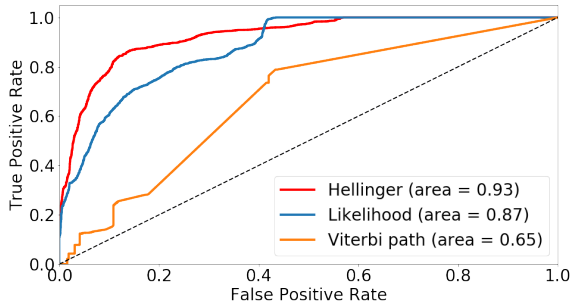


Figure 6: ROC curves day 11

Besides reflecting anomalies more expressively, another advantage of the technique we propose is the ease with which it is possible to set a threshold due to its bounded nature.

If diagonal covariance matrices for the emission probabilities are used, the computational complexity of our online algorithm is linear in the number of dimensions and in the window length, while it is quadratic in the number of hidden states (i.e., the same as the two baseline methods we consider). For each window, the anomaly score can be computed in approximately 5 ms in our case study, making our method definitely suitable for online settings.

4.1.2 Offline anomaly detection. We consider the observations of thefi rst day as representing the nominal behavior and we use them tofi t an HMM λ^1. We thenfi t ten more HMMs, one for each of the remaining days, called λ^2 to λ^{11}, respectively. We then compute the distance between each HMM and λ^1. Table 1 reports the distance between λ^1 and λ^2 (which serves as a representative for days from 2 to 10, i.e., non-anomalous days) and between λ^1 and λ^{11}. The results show a much bigger distance for the eleventh day highlighting the presence of an anomaly, mainly caused by the downward state, which contributes 87% of $D(\lambda^1, \lambda^{11})$. The contribution of the downward state can be, in turn, further decomposed by inspecting the two contributions of equation (5) separately. By looking at the contribution of the transition matrices, an higher self-transition probability suggests a lower velocity. By looking at $H^2(b^1_{\text{downward}}, b^{11}_{\text{downward}})$, the contribution of the emissions probabilities, we can notice a lower mean for the velocity, confirming that the downwards segments are traversed slower than in the nominal case, and also an higher variance for the heading, which suggests that during the downward state the water drone does not manage to maintain rectilinear motion. This is an example of how the distance can be interpreted for diagnostic purposes. Note that expecting a very high distance between λ^1 and λ^{11} (i.e., close to 1) would be incorrect, since only one of the three states corresponds to anomalous behavior. In fact, the overall coverage task can be considered as partially accomplished even in presence of anomalies.

A rule of thumb to set the detection threshold τ is to choose the value of the average distance between two nominal behaviors plus x times the standard deviation. For instance, $x = 3$ provides a good statistical confidence that the observed behavior is not nominal. In our experiments, the behavior of day 11 is considered anomalous since its distance from the nominal behavior of day 1 is significantly

Models	State	Distance	Total
$D(\lambda^1, \lambda^2)$	upward	0,0048	0.0112
	downward	0,0052	
	right	0,0012	
$D(\lambda^1, \lambda^{11})$	upward	0,0063	0.2424
	downward	0.2103	
	right	0.0258	

Table 1: Offline anomaly detection

Figure 7: Giraff-X socially assistive robot, developed for the MoveCare project [28]

far away from the distribution of distances between day 1 and days 2 to 10. The z-score of day 11 with respect to this distribution is 69.08 (i.e., much greater than the standard threshold of 3). The p-value is < 0.0001.

4.2 Socially Assistive Robot

The second set of experiments is performed on data collected during the testing phase of the MoveCare project [27], a H2020 EU project developing an innovative, multi-actor platform centered around an autonomous robot for supporting the independence of elderly people living alone at home. The socially assistive autonomous mobile robot is called Giraff-X (Figure 7) and moves in domestic environments, which represent a typical context for LTA [28]. The goal of the robot is to provide notifications to the user. For doing so, the robot searches, identifies, and approaches the elder, and interact with him/her for stimulation by suggesting activities that aim to counteract physical and cognitive decline, as well as isolation. To localize the person, the robot starts from its charging base and visits in sequence three different rooms (living room, bedroom, and bathroom) of the test house until the elder is found. When the elder is found, the robot approaches him/her following a path suitable for Human-Robot-Interaction (HRI). After the notification is provided to the user, the robot autonomously returns back to its charging base [29]. When idle, the robot stays at its charging base.

Data are collected in a 9-day experiment simulating the same number of interventions performed in a month of use of this social assistive robot, thus performing multiple interventions per day for assessing LTA [28]. The dataset contains 149 runs, each one composed of a sequence of observations collected at 1 Hz and including: heading, speed, acceleration, position wrt the x-axis, and

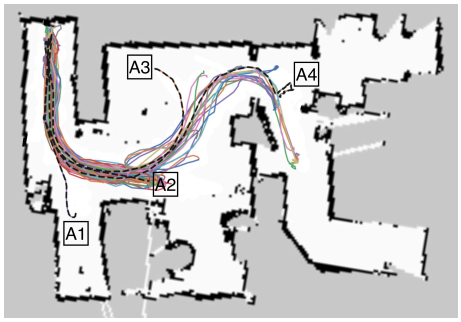


Figure 8: Runs of Giraff robot

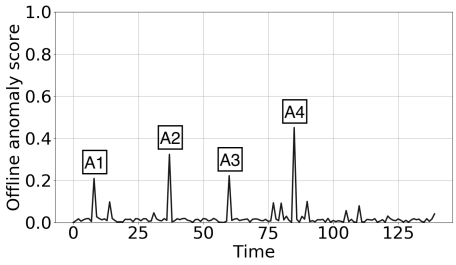


Figure 9: $D(\lambda^N, \lambda^{O_t})$ for runs of the Giraff robot

position wrt the y-axis (see Figure 8, different runs are depicted in different colors).

Out of the 149 runs, 4 are labeled as anomalous by a domain expert (denoted as A1, A2, A3, and A4 in Figure 8). Runs A1, A3, and A4 represent anomalous behaviors due to departures from the expected trajectories, while run A2 constitutes an anomaly since the robot moves at a higher speed than the nominal one. More precisely, anomalies in runs A1 and A3 are due to the fact that the robot identified the user at a different location than expected, and had to modify its path in order tofi nd a suitable location for HRI. In run A4, after performing HRI, the robot placed itself in a position too close to furniture and got stuck there.

In this dataset a run is assessed as anomalous by considering it as a whole, thus we present only results about offline anomaly detection. A ROC curve computed online, as in Section 4.1, would require knowledge of which observations are actually anomalous within an overall anomalous run. Since we have not such information, we cannot apply online anomaly detection in this case.

For each task of reaching one of the three rooms, an HMM λ^N is trained with a single run labeled as non-anomalous by the expert and considered as representing the nominal behavior. The remaining runs are tested for anomaly using our offline method. For each test run, an HMM λ^{O_t} is trained and compared with the nominal one for the task of reaching the same room. Results are shown in Figure 9. Our approach successfully identifies all four anomalies while reporting a low distance for all the other (correct) runs. Note that, although computing the negative log-likelihood of each whole run wrt its nominal HMM could result in a plot similar to that of Figure 9 (yet unbounded on the y-axis), it would not be theoretically sound since each run consists of a different number of observations and, being the likelihood sensitive to trace length, the scores obtained would not actually be comparable.

5 CONCLUSIONS

In this work we have presented two novel approaches based on HMMs and Hellinger distance for online and offline anomaly detection, and showed how they improve over traditional methods both in detection performance and in interpretability of the results.

Unlike other works in the literature, we show that even a single run is enough for learning the nominal behavior, making the semi-supervised setting effectively applicable in practical real-world scenarios. Note that, in the context of LTA, a small initial supervision effort by a domain expert may be acceptable, given that the robots will operate autonomously for a long time.

In our experiments, we show that a constant detection threshold τ is enough and that the bounded nature of our anomaly scores gives a semantic meaning to such threshold. A suitable threshold τ should be chosen depending on the specific application, for example to minimize false alarms (e.g., when human verification is very costly) or to be sure to detect all anomalies also permitting false alarms (e.g., when the robot could harm people). Although for the online approach it is easy to give a semantic interpretation to the selected threshold, for the offline approach one should choose the threshold trying to answer the question "How much am I willing to let the observed behavior be different from the nominal one and still consider it as non-anomalous?". For example, consider a case with $K = 3$ (equally important) states and two behaviors that overlap perfectly except for one state, in which they are completely different. In this case, the offline anomaly score is approximately $1/3$ and, if the application requires that an anomaly is detected when the behaviors are different in at least one state, the threshold τ should be set to a value less than $1/3$.

Future work includes employing HMMs with Gaussian Mixture emission probabilities (GM-HMM) and developing a variation of the Maximum Mean Discrepancy (MMD) in order to overcome the assumption on the same number of hidden states for the HMMs representing nominal and observed behaviors. Finally, we plan to apply the proposed approach to other autonomous robot applications involving the need of detecting anomalies in the context of LTA.

ACKNOWLEDGMENTS

DA is supported by the ABB-Politecnico di Milano Joint Research Center, which providedfi nancial support. The MoveCare project, whose data are used here, is funded by the European Union H2020 grant ICT-26-2016b– GA 732158. ML is partially supported by the MoveCare project. AC and AF contribution comes under the INTCATCH project funded by the European Union H2020 under grant agreement No 689341. This work reflects only the authors' view and the EASME is not responsible for any use that may be made of the information it contains. The research has been also partially supported by the project "Dipartimenti di Eccellenza 2018-2022", funded by the Italian Ministry of Education, University, and Research (MIUR).

REFERENCES

[1] Angelo Alessandri, Massimo Caccia, and Gianmarco Veruggio. 1999. Fault detection of actuator faults in unmanned underwater vehicles. *Control Eng Pract* 7, 3 (1999), 357–368.

[2] Brenna Argall, Sonia Chernova, Manuela Veloso, and Brett Browning. 2009. A survey of robot learning from demonstration. *Robot Auton Syst* 57, 5 (2009), 469–483.

[3] Leonard Baum and John Eagon. 1967. An inequality with applications to statistical estimation for probabilistic functions of Markov processes and to a model for ecology. *Bull Amer Math Soc* 73, 3 (1967), 360–363.

[4] Leonard Baum, Ted Petrie, George Soules, and Norman Weiss. 1970. A maximization technique occurring in the statistical analysis of probabilistic functions of Markov chains. *Ann Math Stat* 41, 1 (1970), 164–171.

[5] Aude Billard, Sylvain Calinon, Ruediger Dillmann, and Stefan Schaal. 2008. Robot programming by demonstration. *Springer Handbook of Robotics* (2008), 1371–1394.

[6] Christopher Bishop. 2006. *Pattern recognition and machine learning*. Springer.

[7] A. Castellini, G. Beltrame, M. Bicego, D. Bloisi, J. Blum, M. Denitto, and A. Farinelli. 2018. Activity Recognition for Autonomous Water Drones based on Unsupervised Learning Methods. In *Proc. 4th Italian Workshop on Artificial Intelligence and Robotics (AI*IA 2017)*.

[8] A. Castellini, M. Bicego, F. Masillo, M. Zuccotto, and A. Farinelli. 2020. Time series segmentation for state-model generation of autonomous aquatic drones: A systematic framework. *Eng Appl Artif Intel* 90 (2020), 103499.

[9] Alberto Castellini, Francesco Masillo, Manuele Bicego, Domenico Bloisi, Jason Blum, Alessandro Farinelli, and Sergio Peigner. 2019. Subspace Clustering for Situation Assessment in Aquatic Drones. In *Proc. SAC*. 930–937.

[10] Varun Chandola, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly detection: A survey. *ACM Comput Surv* 41, 3 (2009), 1–58.

[11] Xi Chen, Yan Duan, Rein Houthooft, John Schulman, Ilya Sutskever, and Pieter Abbeel. 2016. Infogan: Interpretable representation learning by information maximizing generative adversarial nets. In *Proc. NIPS*. 2172–2180.

[12] Zhuohua Duan, Zixing Cai, and Jinxia Yu. 2006. Adaptive particlefi lter for unknown fault detection of wheeled mobile robots. In *Proc. IROS*. 1312–1315.

[13] David Forney. 1973. The Viterbi algorithm. *P IEEE* 61, 3 (1973), 268–278.

[14] Raphael Golombek, Sebastian Wrede, Marc Hanheide, and Martin Heckmann. 2010. Learning a probabilistic self-awareness model for robotic systems. In *Proc. IROS*. 2745–2750.

[15] Nico Görnitz, Mikio Braun, and Marius Kloft. 2015. Hidden Markov anomaly detection. In *Proc. ICML*. 1833–1842.

[16] Ernst Hellinger. 1909. Neue begründung der theorie quadratischer formen von unendlichvielen veränderlichen. *Journal für die reine und angewandte Mathematik* 136 (1909), 210–271.

[17] John Hershey, Peder Olsen, and Steven Rennie. 2007. Variational Kullback-Leibler divergence for hidden Markov models. In *Proc. ASRU*. 323–328.

[18] Irina Higgins, Loic Matthey, Arka Pal, Christopher Burgess, Xavier Glorot, Matthew Botvinick, Shakir Mohamed, and Alexander Lerchner. 2017. beta-VAE: Learning Basic Visual Concepts with a Constrained Variational Framework. In *Proc. ICLR*. 6.

[19] Rolf Isermann. 2005. Model-based fault-detection and diagnosis – status and applications. *Annu Rev Control* 29, 1 (2005), 71–85.

[20] Biing-Hwang Juang and Lawrence Rabiner. 1985. A probabilistic distance measure for hidden Markov models. *AT&T Tech J* 64, 2 (1985), 391–408.

[21] Mateusz Kalisch. 2016. Fault detection method using context-based approach. In *Advanced and Intelligent Computations in Diagnosis and Control*, Z. Kowalczuk (Ed.). Springer, 383–395.

[22] Eliahu Khalastchi and Meir Kalech. 2018. On fault detection and diagnosis in robotic systems. *ACM Comput Surv* 51, 1 (2018), 9.

[23] Eliahu Khalastchi, Meir Kalech, Gal Kaminka, and Raz Lin. 2015. Online data-driven anomaly detection in autonomous robots. *Knowl Inf Syst* 43, 3 (2015), 657–688.

[24] Harold Kuhn. 1955. The Hungarian method for the assignment problem. *Nav Res Logist Q* 2, 1-2 (1955), 83–97.

[25] Solomon Kullback and Richard Leibler. 1951. On information and sufficiency. *Ann Math Stat* 22, 1 (1951), 79–86.

[26] Lars Kunze, Nick Hawes, Tom Duckett, Marc Hanheide, and Tomás Krajník. 2018. Artificial Intelligence for Long-Term Robot Autonomy: A Survey. *IEEE RA-L* 3, 4 (2018), 4023–4030.

[27] Francesca Lunardini, Matteo Luperto, Marta Romeo, Jennifer Renoux, Nicola Basilico, Andrej Krpič, Simona Ferrante, and N.Alberto Borghese. 2019. The MOVECARE Project: Home-based Monitoring of Frailty. In *Proc. BHI*. 1–4.

[28] M. Luperto, D. Fusi, A. Borghese, and F. Amigoni. 2019. Robot Exploration Using Knowledge of Inaccurate Floor Plans Robot Exploration Using Knowledge of Inaccurate Floor Plans. In *Proc. ECMR*. 1–7.

[29] Francisco-Angel Moreno, Javier Monroy, Jose-Raul Ruiz-Sarmiento, Cipriano Galindo, and Javier Gonzalez-Jimenez. 2020. Automatic Waypoint Generation to Improve Robot Navigation Through Narrow Spaces. *Sensors* 20, 1 (2020), 240.

[30] Daehyung Park, Zackory Erickson, Tapomayukh Bhattacharjee, and Charles Kemp. 2016. Multimodal execution monitoring for anomaly detection during robot manipulation. In *Proc. ICRA*. 407–414.

[31] Daehyung Park, Yuuna Hoshi, and Charles Kemp. 2018. A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder. *IEEE RA-L* 3 (2018), 1544–1551.

[32] Daehyung Park, Hokeun Kim, and Charles Kemp. 2019. Multimodal anomaly detection for assistive robots. *Auton Robot* 43, 3 (2019), 611–629.

[33] Lawrence Rabiner. 1989. A tutorial on hidden Markov models and selected applications in speech recognition. *P IEEE* 77, 2 (1989), 257–286.

[34] William Robinson and Andrea Aria. 2018. Sequential fraud detection for prepaid cards using hidden Markov model divergence. *Expert Syst Appl* 91 (2018), 235–251.

[35] Maximilian Sölch, Justin Bayer, Marvin Ludersdorfer, and Patrick van der Smagt. 2016. Variational inference for on-line anomaly detection in high-dimensional time series. In *Proc. ICML 2016 Anomaly Detection Workshop*.

[36] Vandi Verma, Geoff Gordon, Reid Simmons, and Sebastian Thrun. 2004. Real-time fault diagnosis [robot fault diagnosis]. *IEEE Robot Autom Mag* 11, 2 (2004), 56–66.

[37] Christina Warrender, Stephanie Forrest, and Barak Pearlmutter. 1999. Detecting intrusions using system calls: Alternative data models. In *Proc. SSP*. 133–145.

[38] Nong Ye. 2000. A Markov chain model of temporal behavior for anomaly detection. In *Proc. Workshop on Information Assurance and Security*. 171–174.

[39] Yong Zhao, Chengsuo Zhang, Frank Soong, Min Chu, and Xi Xiao. 2007. Measuring attribute dissimilarity with HMM KL-divergence for speech synthesis. In *Proc. SSW*. 206–210.