Responses and reviews for TheWebConf submission “Take a chance: Managing the Exploitation-Exploration Dilemma in Customs Fraud Detection:

Our responses

(Submitted, 973 words! Let’s keep our finger crossed.)

======

We are very grateful to reviewers for their attentive reading and constructive comments. Please find our responses:

Revenue (R2):
Securing tax revenue was the most important screening factor for developing countries that we interacted with since their fiscal income is highly dependent on the customs service. This will not be true for affluent countries, where inspection may focus on other objectives such as detecting hazardous goods or protecting intellectual property rights. The below reference illustrates the share of tax revenue secured through the customs office by country. (Example: 4.4% in Australia, 61% in Cambodia)

WCO annual report (pp.46-91): **https://tinyurl.com/y4957n9v**

Research Background (R2):
Given that customs require human-in-the-loop inspections, not all imports can be inspected. The model parameters need to be updated and prepared for the next round of inspections. This makes active learning suitable. Unlike conventional active learning methods, however, static held-out tests cannot be used. Our experimental setting is wild that new trades came in continuously and the trade patterns changed over time.

The exploration-exploitation dilemma arises in long-term efficacy. Inspecting high-risk items will benefit short-term performance but may not help to refine model parameters. This finding led us to design a hybrid approach: The exploration strategy gATE is built upon the following thoughts: First, we used a gradient embedding of the exploitation model, where its magnitude reflects the model’s uncertainty. Second, we scale the model by using additional measures of sample uncertainty and predicted revenue. To diversify our selection, we selected items if the distance between them is the largest in the embedding space. Finally, we added randomness to evade adversarial attacks from fraudsters.

Heuristic approaches are widely adopted in real-world problems since finding exact solutions is intractable, and the system prefers fast approximate solutions. Here are three heuristic methods in active learning: BADGE[ICLR'20], BatchBALD[NeurIPS'2019], CoreSet[ICLR'18].

Reinforcement Learning (R2):
Thank you for your suggestions on the relevant studies, including multi-armed-bandit (MAB). We agree that some parts of our method can be expressed by the bandit theory. For example, the term exploration-exploitation dilemma is widely used in MAB. The baseline hybrid setting with 10% random exploration corresponds to 0.1-greedy. The hybrid setting utilizing active exploration corresponds to 0.1-greedy with smart exploration.

Despite this, it is non-trivial to apply MAB to solve our problem due to continual data changes. A new set of arms is introduced at every timestamp with different underlying revenue distribution from MAB's viewpoint. Reducing estimated reward uncertainties by sequentially pulling the same arm is not possible in our setting (e.g., new importer names appear every week). Noting these differences, we would be happy to discuss the MAB approach in depth. Thank you so much for this suggestion.

Performance Interpretation (R1):
The proposed models (bATE or gATE) outperformed active learning strategies with large margins, as illustrated in Figure 6 (3-7pp improvement over BADGE). However, for a customs screening system, the performance should be measured when it is hybridized with exploitation. Random worked well in hybrid, and our model's overall performance increased by a small margin (Reported in Figure 7). Hence, we took caution in reporting the performance.

Reproducibility(R1):
Due to the NDA contract, we cannot release the real customs data. However, we will link to the project where other researchers can apply to join collaboration with the World Customs Organization to gain access to real logs and contribute their research for developing countries. We also find that a small set of synthetic customs datasets have been shared [17], and our code is compatible to them. In general, import declaration formats are similar to customs, so our methods will be handy and easily reproducible in customs.

Potential impact (All reviewers):
Thank you for this suggestion. Our work contributes to the use of active learning in customs administration and has demonstrated this idea with data collected from multiple countries. Customs data is complex and challenging to handle because of their size and continual changes (i.e., concept shift). We have shown how to adaptively determine and solve the

exploitation-exploration dilemmas and apply a semi-supervised approach for uninspected imports.

Customs offices we interact with do not incorporate any sophisticated strategies and have used random exploration methods. Therefore, introducing active learning methods has been received as a novel advancement. Another contribution is the light and efficient computation; The running time of the hybrid strategy takes a maximum of 15 minutes to handle weekly country-level data, which is practical. We tested the algorithm over data collected from multiple countries for robustness. Finally, our framework can also be applied to e-commerce recommendations where user behaviors change over time.

Other comments (All reviewers):
The major difference between our work and [16, 21] is the existence of “concept drift”. More precisely, [16] focused on data skewness and showed that including simple exploration helps margin sampling, whereas [21] combined distance-based metric for exploration and k-NN classification for exploitation. We will clarify these differences.

Active customs selection aims to achieve high performance in the long run (i,e., higher moving averaged performance). Since we simulated our model with a finite dataset, we use a notation ‘T’ to denote the total number of weeks in simulation (T is a constant), and it is not used in the optimization process.

Future studies can extend the hybrid model to determine the exploitation-exploration ratio adaptively. The amount of training data used and recent domain shift can be used then. Possible candidate algorithms are RP1 [ICML’20] or the sliding-window UCB model.

Regarding the baseline approach for the exploitation strategy, it is called DATE_CLS in the original paper. As R3 suggested, \hat{y}_cls*\hat{y}_rev can be another variant to select frauds. Although we used \hat{y}_cls, the training process minimizes dual-task objective functions, consisting of the cross-entropy loss (for illicit classification) and the mean-squared-error loss (for revenue prediction). So, we can regard \hat{y}_cls implicitly considers predicted revenue \hat{y}_rev. The weight between losses is controlled depending on target customs’ objectives.

Review texts

Dear Sundong Kim,

Thank you for your submission to the Web Conference 2021 entitled Take a Chance: Managing the Exploitation-Exploration Dilemma in Customs Fraud Detection via Online Active Learning. Below are the preliminary reviews for your paper. You have the opportunity to submit a rebuttal to the criticisms raised by the reviewers. Rebuttals are due at 23:59:59 Anywhere-on-Earth on December 2. Given the compressed reviewing schedule, we unfortunately will not be able to accept late rebuttals -- no exceptions!

To submit your rebuttal, please log into Easychair's instance for TheWebConf 2021, navigate to your submission, write your response to the reviewers, and click on Send Response.

Here are some guidelines regarding the rebuttal phase; please read them carefully:

[1] Rebuttals are optional -- you do not need to submit one.

[2] Rebuttals are limited to 1000 words.

[3] There are two purposes to the rebuttal process: to clarify misconceptions by the reviewer, and to get early feedback on your submission. As a result, if you choose to submit a rebuttal you must focus on any factual errors in the reviews and any questions posed by the reviewers to you.

[4] Naturally you may want to incorporate feedback into an updated version of the paper. However, the Web Conference does not have a shepherding process or the notion of a "conditional accept", so our accept/reject decisions will not be influenced by any promises to remedy issues identified by the reviewers.

[5] These are not the final versions of the reviews. The reviews can later be updated to take into account the discussions at the program committee meeting, and we may find it necessary to
solicit other outside reviews after the rebuttal period.

[6] The program committee will read your responses carefully and take this information into account during the discussions. On the other hand, the program committee will not directly respond to your responses, either before the program committee meeting or in the final versions of the reviews.

[7] Note that all PC members who have reviewed your paper will see your rebuttal responses. Please keep your responses civil and polite.

Again, rebuttals are due on December 2 at 23:59:59 Anywhere-on-Earth. We are planning to communicate final decisions by January 15.

Best regards,

Leila Zia, Jie Tang, Marc Najork
The Web Conference 2021 program co-chairs

REVIEW 1

SUBMISSION: 58
TITLE: Take a Chance: Managing the Exploitation-Exploration Dilemma in Customs Fraud Detection via Online Active Learning
AUTHORS: Sundong Kim, Tung-Duong Mai, Thi Nguyen D.K, Sungwon Han, Sungwon Park, Jaechan So, Karandeep Singh and Meeyoung Cha

----------- Relevance to the Web Conference -----------
SCORE: 1 (Relevant)
----------- Overall evaluation -----------
SCORE: 1 (Weak accept)
----------- Summary -----------
This paper studies the problem of custom fraud detection. In the custom fraud detection problem, the goal is to find the set of imports to be inspected in order to maximize the revenue obtained from the collected duties of the inspected imports. This problem exhibits an exploitation-exploration tradeoff since the imports to be inspected should both bring revenue but also be informative to train a better model in the future. Standard approaches to custom fraud detection consider an offline setting and train some classifier for fraud detection. However, due to the do domain shifts, the performance of these approaches potentially degrade over time. Active learning approaches are relevant to find the most informative samples. This paper proposes a novel hybrid method which blends exploitation algorithms from custom fraud detection together with active learning. The exploitation component is a previous method called DATE. The exploration component is called gATE builds upon an ac!
 tive learning approach called BADGE in multiple aspects.

The authors evaluate their approach on datasets of import declarations from three countries. They first show that for one of the three countries, the performance of the full exploitation algorithm degrades over time. For the two other countries, it performs similarly, but slightly worse, than a hybrid approach. The performance of different exploration strategies is then analyzed. It is shown that the previous active learning

method BADGE and the proposed exploration methods bATE and gATE outperforms a naive random exploration strategies when the algorithm is full exploration. For a hybrid algorithm that combines exploitation together with different exploration strategies, the different exploration strategies perform similarly.
----------- Originality -----------
SCORE: 3 (Creative: Only a few people in our community would have put these ideas together)
----- TEXT:
The idea of incorporating active learning for customs fraud detection is significant
----------- Potential impact -----------
SCORE: 3 (Broad: Could help ongoing research in a broader research community)
----------- Reproducibility -----------
SCORE: 2 (Some but not all code, data or the details of the experimental setup are made available)
----------- Quality of execution -----------
SCORE: 2 (Poor: Potentially reasonable approach, but certain core claims lack justification)
----- TEXT:
the experimental results do not demonstrate that the proposed exploration strategy improves on previous active learning methods
----------- Quality of presentation -----------
SCORE: 3 (Reasonable: Understandable to a large extent, but parts of the paper need more work)
----------- Adequacy of citations -----------
SCORE: 3 (Comprehensive: Can't think of any important paper that is missed)
----------- Ethics -----------
SCORE: 1 (No)
----- TEXT:
None
----------- Strengths -----------
This paper studies an important problem of customs fraud detection. They provide a strong motivation for their approach by arguing that previous methods only consider a static setting and that the performance of these previous approaches might degrade over time due to domain shifts (as shown in experiments).

The experimental section compares and analyze different approaches thoroughly and clearly. These experimental evaluations could be useful for customs fraud detection in practice.

The related work clearly discusses and compares the proposed approach to previous approaches in customs fraud detection and active learning

----------- Weaknesses -----------

The authors propose a novel exploration strategy that builds upon a previous existing exploration strategy called BADGE but the experimental results do not demonstrate that the proposed exploration strategy improves on the previous method.

The related work mentions "Recent studies have come up with interpolating exploration and exploitation strategy in the context of active learning, as pure exploration or exploitation is not applicable to test datasets that are prone to domain shifts [16, 21]." The authors should elaborate on this previous work and how it differs from their approach.

----------- Reasons to accept -----------

Overall, the authors show that a hybrid strategy which combines exploration techniques from active learning and exploitation techniques from customs fraud detection improves upon existing methods for custom fraud detection which either only do exploitation or do exploration via random sampling. I think the idea of incorporating active learning for customs fraud detection is significant enough for weak acceptance.

----------- Reasons to reject -----------

A main issue is that the proposed method for exploration does not seem to improve over existing active learning methods. Simply combining existing exploitation and exploration techniques seem to perform well.

----------- Rebuttal -----------

A main issue is that the proposed method for exploration does not seem to improve over existing active learning methods. Simply combining existing exploitation and exploration techniques seem to perform well.

REVIEW 2

SUBMISSION: 58

TITLE: Take a Chance: Managing the Exploitation-Exploration Dilemma in Customs Fraud Detection via Online Active Learning

AUTHORS: Sundong Kim, Tung-Duong Mai, Thi Nguyen D.K, Sungwon Han, Sungwon Park, Jaechan So, Karandeep Singh and Meeyoung Cha

----------- Relevance to the Web Conference -----------

SCORE: 1 (Relevant)

----- TEXT:

The submission is not directly relevant to the state of the *Web*. However, its topic falls in the general area of topics that authors and attendees of The Web Conference typically care about, and as such, I still consider it relevant.
----------- Overall evaluation -----------
SCORE: -2 (Reject)
----------- Summary -----------
The authors consider the following setting. A customs agency is facing a sequence of arriving produces, and must decide which of them to inspect further. When an item is inspected, it is revealed whether it is a fraud or not, and in the former case, the agency also obtains monetary reward in the form of a fine levied against the fraudulent product. To guide the decisions, the agency has access to some basic features about the items. The goal of the agency is to maximize the total fines collected over time.
A straightforward approach would be to try and learn a classifier to best predict which types of items are frauds. However, the authors observe that this can change over time, and therefore, algorithms need to keep exploring, sometimes even when items are unlikely to be frauds based on the current classifier. This leads to a classical exploration/exploitation dilemma.
The authors propose various heuristics that are combined to lead to a decision making procedure that randomly (but not uniformly) samples items to explore with a certain probability, and otherwise to exploit.
The submission also reports on experiments that are run on real data collected from three countries in Africa. The experiments reveal that such drift of fraud classifiers appears to happen, and that the proposed algorithm is able to obtain larger benefit in the long run.
----------- Originality -----------
SCORE: 2 (Conventional: Rather straightforward, a number of people could have come up with this)
----- TEXT:
I do not see any particularly interesting insight in the submission. It does combine a number of different heuristics, each of which is plausible. But there does not seem to be a clear underlying thread of ideas that guides the approach, or a novel insight that had eluded earlier work.
----------- Potential impact -----------
SCORE: 1 (Low: Will likely have no impact)
----- TEXT:
The proposed solution may well have practical impact if being deployed by customs agencies. But I do not see as much impact on future research - the authors define a possibly interesting application of explore-exploit paradigms, but do not clarify what aspect of the application makes it different from traditional setups with drifting truth, or

contribute novel ideas. As a result, it's not clear to me that this work will inspire a lot of follow-up work.
----------- Reproducibility -----------
SCORE: 3 (All code, data, and the details of the experimental setup are made available)
----- TEXT:
The authors have included a link to an archive that supposedly contains relevant code and data. I did not check it myself, but trust the authors on this.
----------- Quality of execution -----------
SCORE: 3 (Reasonable: Generally solid work, but certain claims could be justified better)
----- TEXT:
I feel this question does not fit the paper all that well. The authors clearly are aiming for combining various heuristics to build a solution that works in practice. It seems that they did this well, so in this sense, the idea is well executed.
However, as a reader/reviewer, I would have liked to see more principled insights into the domain specifics, or a more unified approach, rather than a collection of different heuristics.
----------- Quality of presentation -----------
SCORE: 3 (Reasonable: Understandable to a large extent, but parts of the paper need more work)
----------- Adequacy of citations -----------
SCORE: 1 (Inadequate: Literature review misses many important past papers)
----- TEXT:
The citations for the areas the authors *do* cite are adequate. However, exploration-exploitation is a very very widely studied area, and the literature on expert learning and multi-armed bandits is vast, including a lot of work on drifting truth. I am myself not a major expert, so I am not claiming that any of this work is directly relevant or solving the problem, but the submission focuses on a lot of work that is not directly relevant (in particular in the citation of ski rental problems, which have no relationship to this work at all), which should instead be spent on the much more relevant literature. In particular, it should be explained why this past work is not directly applicable.
Another perhaps more directly applicable line of work is the recent work on security games, in particular in relationship to protecting National Parks from poachers. There, one faces the same problem that to learn the distribution of where poachers go, one has to invest effort, and the behavior of poachers changes over time. It may be worth checking that literature.
Finally, I recommend that the authors check out the work on Gaussian Process Bandits and Bandits in Metric Spaces, e.g., the work of Srinivas/Krause/Kakade/Seeger and Kleinberg/Slivkins/Upfal, and the significant follow-up work. These works (and the

related works) provide a fundamental way to draw inferences about one type of product from a "similar" type of product.
----------- Ethics -----------
SCORE: 1 (No)
----- TEXT:
.
----------- Strengths -----------
1. The paper defines a problem that might serve as an interesting application of the exploration-exploitation paradigm. It is possible that this application has particular features that would lead to interesting questions.
2. The authors show a dedication to deploying their solution and working with real data.
----------- Weaknesses -----------
1. The submission is prefaced on the assumption that the agency's goal is to maximize revenue. Is this in fact true? Wouldn't the primary goal be to prevent fraud, and fines are intended as a deterrent, rather than revenue?

2. The submission aims to work in the exploitation/exploration paradigm, but fails to explain why it eschews standard MAB and similar approaches to the domain as well as past work on MAB with drift.

3. The collection of heuristics that are combined appear to lead to decent performance in practice. However, it is not clear that so many heuristics are needed. There is no underlying train of thought that really explains how the heuristics work together - it appears as though the performance of any of the approaches that "should" have been good enough was not, so more heuristics were piled on top.

REVIEW 3

SUBMISSION: 58
TITLE: Take a Chance: Managing the Exploitation-Exploration Dilemma in Customs Fraud Detection via Online Active Learning
AUTHORS: Sundong Kim, Tung-Duong Mai, Thi Nguyen D.K, Sungwon Han, Sungwon Park, Jaechan So, Karandeep Singh and Meeyoung Cha

----------- Relevance to the Web Conference -----------
SCORE: 1 (Relevant)
----------- Overall evaluation -----------
SCORE: 1 (Weak accept)
----------- Summary -----------

Summary

The paper studies a fraud detection problem, where an algorithm predicts a set of suspicious items to be inspected. Out of these inspected items, those that are truly fraudulent generate revenue. The authors focus on the online aspect of the problem where batches of items arrive online. For each batch of items, the algorithm has a fixed budget for inspection, and can rely on previously inspected items as training data in making predictions for the current batch. The goal is to maximize the total revenue in the presence of "domain shifts", i.e., the distribution of items and their labels keep changing over time.

The main challenge the paper aims to tackle is the "exploitation vs exploration" tradeoff: ideally the algorithm should focus on inspecting items that are most likely fraudulent, but as domain shifts happen, without taking into consideration new training data, the algorithm may gradually become less accurate; on the other hand, if the algorithm focuses solely on exploration, i.e., inspecting uncertain items to keep future predictions accurate, it may incur a loss in terms of revenue collected. To this end, the authors propose using a hybrid strategy, where in each batch, a large fraction of the budget is used for exploiting the most suspicious items to generate revenue, while a relatively small fraction of the budget is spent exploring uncertain items to generate new training data and update the algorithm itself.

For exploitation, the authors propose inspecting the most suspicious items as predicted by the state-of-the-art DATE algorithm. For exploration, they propose a method (with two major variants, bATE and gATE), which works roughly by considering the gradient induced by each item (which corresponds to the "change" the item would induce on the DATE algorithm), clustering these gradients, and sampling items according to how far a cluster is to other clusters in order to maximize diversity. The sampling procedure also takes into consideration the magnitude of the gradient and the potential revenue of the item. In each batch, both the exploitation algorithm and the exploration algorithm make a certain fraction of all predictions according to some predetermined ratio.

The authors then conduct experiments on 3 real-world customs datasets from 3 different African countries. They first try to verify the (non)existence of domain shifts in these datasets, and the findings are that domain shifts do exist in 1 of the 3 datasets, while in the other 2 there are no significant domain shifts. They then examine the performance of the exploration algorithms alone without any exploitation. They test 4 algorithms: random selection, BADGE (the state-of-the-art exploration algorithm), bATE, and gATE, and the conclusion is that all 3 advanced methods (1) significantly outperform random selection, (2) are quite close to each other in terms of the total

revenue, and (3) are not quite close to pure exploitation on datasets without significant domain shifts, so exploitation is still needed. Finally, they examine hybrid algorithms by combining each of the exploration methods with exploitation. Their findings suggest that the hybrid algorithms (1) significa!
ntly outperform pure exploitation in the presence of domain shifts, (2) are no worse (and sometimes slightly better) than pure exploitation without significant domain shifts, and (3) are quite close to each other, in terms of the revenue.

Strengths

The paper is overall well written. The problem studied is of practical importance. The methods proposed make sense (I'm not sure how novel the ideas are, but they also appear quite elegant). The experiments on real-world datasets confirm the existence of domain shifts in customs operations, and suggest that the hybrid algorithms developed in the paper do work much better than pure exploitation methods. The authors also provide code for the experiments, which could be useful for future research and/or practical use.

Weaknesses

I'd expect more discussion on related work -- exploration vs exploitation is generally not a new topic, and I guess there are existing methods that can (at least in principle) be applied to this setting. Of course those methods may not suit the setting as well as those proposed in this paper, but I'm still curious how they perform and/or why they (are likely to) fail.

Some choices in the design of the algorithms appear a bit arbitrary to me (also see detailed comments). Of course the paper is more empirically focused, so probably the performance of the algorithms is self-explanatory, and these choices are indeed data-driven -- which brings up my next concern.

The authors show their algorithms work well on customs data, but it's not immediately clear to me the algorithms can work well on other tasks of a different nature. The results would appear more exciting with experiments conducted also on, for example, data from online marketplaces.

Overall evaluation

weak accept with low confidence

Detailed comments

While the customs operations example makes sense, in practice government agencies often care about something different than just the total revenue. I understand the authors did their experiments on customs data, but also wonder if there's a better example for how their results can be applied.

Line 230: what's an HS code? (I did google that and find the meaning, but it would probably be better to briefly explain in the paper.)

Line 277: what if we don't know T (in reality items don't stop to arrive after a certain date)? Do the proposed algorithms still work (with minor modifications)? I think they do but I'd appreciate it if the authors could confirm.

Algorithm 2: the exploitation algorithm makes decisions only based on fraud scores. Is it possible to do better by taking predicted revenue into consideration? It seems like Pr[item is fraudulent] * (predicted revenue) makes more sense?

Line 560: "the these countries"

Line 657: "performance of drops"
----------- Originality -----------
SCORE: 2 (Conventional: Rather straightforward, a number of people could have come up with this)
----- TEXT:
Somewhere between 2 and 3 seems appropriate here
----------- Potential impact -----------
SCORE: 2 (Limited: Impact limited to improving the state-of-the-art for the problem being tackled)
----------- Reproducibility -----------
SCORE: 3 (All code, data, and the details of the experimental setup are made available)
----------- Quality of execution -----------
SCORE: 3 (Reasonable: Generally solid work, but certain claims could be justified better)
----------- Quality of presentation -----------

SCORE: 3 (Reasonable: Understandable to a large extent, but parts of the paper need more work)

----------- Adequacy of citations -----------

SCORE: 2 (Reasonable: Coverage of past work is acceptable, but a few papers are missing)

----- TEXT:

This is more like 1.5.

----------- Ethics -----------

SCORE: 1 (No)

----- TEXT:

The paper presents no ethical concerns

----------- Strengths -----------

Please see summary

----------- Weaknesses -----------

Please see summary

----------- Reasons to accept -----------

Practically important problem, studied and executed well. Could be of reasonable practical use.
