TABLE OF CONTENTS

Introduction 3

1. Can you spot when your data goes against the flow? 4
   What is an Anomaly
   Why Detecting Anomalies is important?
   How Travel Organisations can Benefit from Anomaly Detection

2. Anomaly detection: 5 Key considerations for managing your agents 7
   Ironing out Performance Wrinkles
   The Clients’ Ups and Downs

3. Anomaly detection: Fixing availability glitches before the storm 10
   Using anomaly detection techniques to get smarter at spotting inventory issues to avoid revenue leakage.

Triometric is the leader in API analytics with 20 years’ experience working with the world’s leading travel distributors and enterprises. The Trio platform captures, processes, aggregates and visualises large volumes of search and booking data in real-time and by leveraging this data our customers gain valuable insights to manage distribution, optimise inventory and maximise revenue to keep them ahead.

© 2019 Triometric. All rights reserved.
©Triometric is a registered trademark of Hypertrak Limited.
Introduction

For most online travel companies, the requirements from an anomaly detection system is to produce near real time detection at very large scale, while producing concise anomalies and being able to adapt to normal changes in data behaviour. In time series signals, an anomaly is any unexpected change in a pattern in one or more of the signals. There are obvious things that are important to measure such as transaction volume and value, number of search hits, Look-to-book ratios and conversions, and other similar metrics. People do have a notion of what “normal” is, and they understand it because, in the end, it affects revenue. By understanding “normal”, they also understand when something is “abnormal”.

Anomaly detection forms an essential component of real-time analytics, which can help B2B online travel organisations gain significant actionable insights across their distribution channels. However, detecting anomalies accurately can be difficult. As electronic distribution practices evolve, inventory situations fluctuate and buying behaviours change, the anomaly detection capabilities need to be continuously updated to detect an anomaly effectively.

This white paper explores what anomaly detection in real-time is and how it can be applied to travel distribution to make operations more efficient and alert to potential system failings or market opportunities.

Originally published as three separate but connected articles.
1. Can you spot when your data goes against the flow?

**Introduction**

Anomaly Detection can be applied to operational monitoring metrics or business metrics that support decision-making right across the travel ecosystem and beyond. We discuss here how detecting small deviations in your traffic data can make a big difference to your revenue potential.

More and more data is flowing through our systems with our ability to collect and store it attempting to keep up with the flow. But our capacity to consume all this data and mine it for critical insights is being challenged. We have our human limits and need business intelligence (BI) tools to help us see our KPIs more clearly. Today AI is being introduced to complement BI in this endeavour. The aim is to help humans concentrate on using the data rather than the tasks involved in getting it.

These limitations can result in missed opportunities to discern patterns, identify events and their causes, and take corrective actions, especially at a time when unexpected business incidents occur. Large datasets have become difficult to manage as organisations are needing to make faster decisions in real-time. Anomaly detection using AI techniques is emerging as one of the critical technologies that organisations are leveraging to overcome this challenge.

**What is an Anomaly?**

In the time and price sensitive world of selling travel products, things inevitably can change or go wrong and there is an imperative to sound the alarm and identify the fix as soon as possible. To do this, the issue needs to be identified. This is where the ability to detect data anomalies early becomes a business differentiator.
An “anomaly” is simply a deviation from what is standard, normal, or expected and Anomaly Detection is the identification of atypical patterns in large data sets. An easy to understand example is your bank identifying out-of-the-ordinary purchases as fraudulent. But in practice, anomaly detection is more complex and nuanced which can make it daunting, although critical for organisations to implement.

**Why Detecting Anomalies is important?**

For travel product suppliers (such as hotels, airlines and intermediaries) selling inventory through API connections and websites makes their business success increasingly reliant on connectivity between a myriad of electronic platforms. Every room, seat or service sold involves high volumes of search data and transactions related to bookings. So early detection of events that could cause a negative impact to this flow of transactions (i.e. conversions and sales) becomes imperative. For businesses running thousands, millions, or even billions of dollars’ worth of transactions every day, the impact of this can’t be overstated. Time is definitely money.

**How Detection Works**

Detecting changes in time series data has a wide applicability. In a complex time-series data environment (which is what most travel transactions are), the detection tool uses a mix of rule-based checks, and machine learning algorithms to determine the parameters of normal behaviour and the instances when ‘normal’ is breached. This breach of expectation is highlighted as an anomaly. The detector looks at historical data, calculates anomaly
points and presents the information visually in a separate Anomaly Detection data view. And all this, while accumulating more intelligence for the next time.

At the practical level, patterns can be identified to reflect the norms of doing business over given periods, be it daily, weekly, or monthly. Anomaly detection should then be able to absorb these patterns and uncover the unusual, rather than the norm. Since booking patterns can change with the introduction of deals, or events, or seasonal fluctuations, the detection algorithms quickly need to be able to learn the new patterns and adapt the detection profile.

Automated, real-time anomaly detection platforms can delve deep into data to pinpoint anomalies that wouldn’t be noticed by a human user monitoring datasets on a dashboard with subtle but potentially costly implications. The more traditional method of setting thresholds on KPIs to trigger alerts when the numbers go either too high or too low is proving less efficient when compared to the efficacy of machine-learning systems.

That said, anomaly detection can be difficult to get right at first and a pitfall to bear in mind is that complex data may sometimes result in false positives or negatives, i.e. an incorrect reading for what is really happening. Evaluating anomaly detection is a particularly fine balance. False negatives can be detrimental, but too many false positives can also render the system useless, or impact reputations. Real time systems don’t allow for second review of any potential anomalies so here there is a need for as much accuracy as possible in the detecting models used. Think of the example, where your bank is constantly blocking your funds due to false positives.

The solution here is to spend the time upfront on the detection engineering to make sure not too many false negatives or positives occur and to ensure learning, refinements and improvements continue, even after the model is in production.

How Travel Organisations Can Benefit from Anomaly Detection

Anomaly detection can be set for any KPI metric, and there are many business functions that stand to benefit from this innovation. Anomalies don’t always have to indicate that something is wrong. They can also be used to detect or predict slight changes in customer behaviour that could be translated into a shift in the way a product is marketed or sold. Basically insights to help businesses stay a step ahead of new trends.
Wherever critical KPIs are measured, Anomaly Detection can be used to dig deeper and see further. Some of the most valuable metrics organisations wish to monitor can also be the most variable. Application throughput, search requests and replies, response times and timeouts are all important metrics with pronounced peaks and valleys, depending on the time of day or the day of the week. Accurate detection can go a long way to successfully predicting potential failures or opportunities. Below are just three examples where Anomaly Detection could be used:

Traffic dropped or spiked: Detect unusual changes to the normal levels of traffic, which might not be steady over the year. Anomaly Detection can determine what the normal traffic pattern is and flag an anomaly when traffic deviates from that norm.

When bookings or revenue drop off: Anomaly Detection can determine the normal pattern for transactions or revenue and flag an anomaly when they drop below that norm.

Scraping attacks: In travel searches, anomalous pattern detection combined with deep traffic analysis, can help identify instances of excessive price scraping by competitors. Detecting and mitigating malicious bots that scrape pricing data and unique content could help protect travel business against pricing and content leakage.

In summary, Anomaly Detection can be applied to operational monitoring metrics or business metrics that support decision-making right across the travel ecosystem and beyond. The unifying factor is the ability to detect small changes or differences in system or data message flow that might otherwise go unnoticed. Uncovering anomalies using machine learning allows humans (or indeed other automated systems) to take action based on these deviations. Depending on the circumstance, it is this action taking that saves costs, avoids losses and/or improves revenues.
2. Anomaly detection: 5 Key considerations for managing your agents

Putting it simply, Anomaly Detection uses advanced mathematical modelling to accurately detect unexpected changes in activity over time even when the activity is quite ‘up and down’ in nature. For example we may see an hourly or daily pattern that means comparing it with a fixed value or rule would lead to a significant number of false positives.

The Anomaly Detection system effectively uses a curve fitting approach which means the detection rule can become dynamic by tracking the curve and an exception is then based on there being a significant variance at some point in time. For a fuller description of Anomaly Detection please read the first article in this series.

Anomaly Detection is an extremely powerful technique and although the range of its application is very wide the thrust of this article is around performance, quality of service and clients.

IRONING OUT THE PERFORMANCE WRINKLES

Platform Load

The overall performance of the platform is a major factor in determining the response times to individual anomaly detection - critical performance factor transactions. The challenge is that the API operator has relatively little control over how individual agents behave in terms of traffic volumes. An agent with the best of intentions can run a campaign or offer which results in a significant surge in price and availability requests which has the potential to not only impact the platform but also other agents’ service levels and overall bookings. Tracking the load in terms of overall number of searches and bookings is a basic defence against this scenario but the challenge is detecting a genuine surge which is over and above daily traffic peak or indeed fall.

Response Times

The actual response time experienced by Agents is driven by the culmination of a wide range of factors including ambient platform load, database performance, third party suppliers, and network transit times and so on. Once again there will be natural cycles in response time measurements which need to be discounted whilst any deviations are highlighted. Ideally the response times are tracked at the destination level since this allows the Anomaly Detection to be significantly more specific regarding delays with larger responses or more third parties. (Read more about response times performance)

Error Levels

Overall general error levels should be tracked using Anomaly Detection at IT, connection and XML levels and each API platform will have its specific error concerns one of the most critical is timeouts. Most agent system will set a timer when they send a request to an API, if the timer expires before they receive response they will abandon the request and just use the product offers they probably already have from competitors. This is seen as a timeout on the API, the client simply break the connection. Network based analytics tools can detected these timeouts and specifically report on them. Losing the chance to respond to that request is bad enough, but the Agent system usually track timeouts over time and if you are repeatedly too slow (for them) then they will escalate to a cut-off – stop sending search requests all together. The Agent system is necessarily being destination selective so this means that a series of slow requests for a subset of destinations can impact your overall business. (Read more about XML error monitoring)

The Clients’ Ups and Downs

The online travel business is a numbers game. Most travel distribution platforms rely on the long
Anomaly Detection

Anomaly Detection

Client Activity

Depending upon the role of the clients accessing the API e.g. OTA, it is highly likely they will be handling traveller searches from specific geography/market and as a result their traffic pattern will have a clear daily pattern with super imposed weekly pattern. This is ideal scenario for Anomaly Detection and its capabilities to detect unexpected dips or peaks in traffic and their timing.

Bookings

Bookings are obviously the end game. Drop offs in bookings are clearly a significant problem and if not preceded by a corresponding drop in searches i.e. the look-to-book ratio has changed then it may be a sign of booking error or too high a price. A casual idea that booking increases are all good news is equally misguided. Sudden increases in bookings, so a change in the book rate, might indicate an inappropriately lowly priced offer. Many travel providers have made major pricing errors e.g. misplaced decimal point only to start offering products at a dramatic loss.

Conclusion

Travel suppliers and distributors can lose a lot if they don’t find and act quickly on business problems or opportunities. Clients can be lost, new sources of revenue missed, or profit margins dented.

Many anomalies are symptomatic of problems that affect (directly or indirectly) a company’s revenue stream. The longer that issues remain unfixed, the more money is being leaked. This is just as true for striking anomalies as it is for more subtle ones. Striking anomalies may cause bigger losses in the short term, but they are also easier to spot because they tend to cause larger deviations in the key metrics being monitored. Subtle anomalies however, can go undetected for longer because they’re harder to pick out in the data. A subtle anomaly that persists for a long time can do just as much damage as a drastic, but brief one.

Success in travel hinges on making the right decisions at the right time. This is where an analytics platform with anomaly detection capabilities can help make that crucial difference. Whether helping companies to chart a course through a storm or take advantage as the tide of business shifts in their favour, quick detection and analysis can enable them to adjust course in time to generate more revenue or avoid losses.

The examples covered here are just some of the many applications of Anomaly Detection in both a technical and business context. This article is design to highlight the opportunities in a platform performance and basic client management context.

The next article in this series will look at Product Availability, Pricing and related business areas associated with Offer Management that form the next step up in deployment of automated technologies such Anomaly Detection.
3. Anomaly detection: Fixing availability glitches before the storm

Using anomaly detection techniques to get smarter at spotting inventory issues to avoid revenue leakage.

The importance of keeping an eye on your performance

“You have to be in it to win it” is a great way of characterising this challenge. If all the hard work of setting up the platform, optimising its performance, forging distribution contracts with clients is going to pay off then it’s vital to have a good supply of products and services to be able to respond with when the hard won search traffic hits the API. Triometric often refers to its 4 pillars model because it reflects the key drivers of conversion which all need to be covered – it doesn’t work if you come up short in any of areas.

The idea of Anomaly Detection is to track the normal variation and flag the unexpected events. So in the world of availability tracking, what could possibly go wrong? Whilst this article isn’t about the mechanics of tracking searches, there are two specific categories that tend to be tracked and their importance will vary depending on how the API is configured or where your organisation is in the supply chain. The first category is responding to what can be described as collective searches and the second as individual or list based product searches. In the hospitality sector, these categories would correspond to city and specific property searches. In flight, it would be route or carrier specific searches.

With individual searches, the API can respond with either an offer of a product, so zero or more rooms in the simplest case, and typically I would be interested in the percentage of responses that have and don’t have offers e.g. %Availability or %No Availability. If the booking platform is more sophisticated then I can take the Amazon shopping approach of "other
customers looked at...” and offer similar alternates when I lack availability of the requested item.

With collective searches, the API can respond with a list of offers based on the collective criteria, for example a set of hotel rooms for Paris. On some occasions, this may be “no rates available” type list which the API may flag as an error rather than send back an empty list, or it may contain a reasonable number of room offers. The question is then what constitutes reasonable and does that vary over time? For example, an API platform might normally offer 200 rooms in Paris but when this drops down to 50, this translates into a more limited choice for prospective travellers. At the same time 50 room offers might be amazing to travellers for Tierra del Fuego. It could be that a major event in Paris means many rooms are sold out so the 50 rooms offer could be viewed as reasonable given that context. Understanding what constitutes reasonable for which destinations at any given time is the challenge and solving it means that we can view drops in room counts as predictive. In these scenarios, hard and fast rules, even per destination, would likely produce a lot of false positives alerts. The alerting system needs to appreciate that there may be new even temporary levels that constitute a new normal.

All of these individual and collective searches are examples of product centric tracking. In other words Anomaly Detection being deployed to adjust to what constitutes a “normal value” and react to any changes from that normal which is established for a destination or individual property but also combined with the dates of stay.

Detecting the availability anomalies in search responses is only the start of the fix process which demands significant additional detail to diagnose the issue. I would expect to bring in supporting data that might include:

- Mapping errors where product has been wrongly listed on the API platform
- Inventory pricing buckets not yet ready for allocation
- Poor or incorrect availability allocations by channel
- Supply issue with contracted third parties
- Inventory exhausted – sold out – good news?

The second article in this series considered Anomaly Detection with regard to Client Management examples, so largely from the client behaviour and traffic viewpoint including areas such as Look-to-book, booking counts and booking rates. It equally makes a lot of sense to consider using Anomaly Detection for Availability being offered to clients too. In this case, the Anomaly Detection is used to track the %Availability levels being offered in search responses to the traffic being driven by individual clients. Tracking this will identify significant changes in availability and deliver intelligence on when clients search patterns are diverging from what you have on offer or their contractual commitment, say specific destinations. In this case the underlying causes could be due to the Client:

- Exceeding allocated availability
- Searching for products not being offered
- Has mapping data issues of their own

Depending on role in the supply chain, the remedial actions in most of the above cases revolve around simply fixing a mapping problem, talking to the client or liaising with a supplier to allocate more inventory. In short, the fixes are often very actionable, which is the key to driving a return on any investment in analytics.

As a final comment, exhausting availability isn’t necessarily good news if the underlying cause is a pricing error. Two recent examples of unwelcome anomalies are those of British Airways and Cathay Pacific, who found have both themselves selling normally expensive tickets at erroneous bargain basement prices.