ARTIFICIAL INTELLIGENCE
THE BEGINNING OF THE END FOR TELECOM FRAUD?

Unfortunately, fraud is a fact of life in telecoms, and a growing problem when it comes to international voice services which generally enjoy higher termination rates. Of course, the frequent and routine transfers of significant sums of money between operators is another key reason and the pressure on margins throughout the industry has persuaded less ethical providers to look at fraud as a way of boosting their returns.

However, the increasing complexity of call routing and rating to serve the needs of operators offering premium rated services, has opened the floodgates. As a result, retail service providers, who are often left holding the losses generated by fraud, take this very seriously and expect their international providers, at the center of the network, to take a similar proactive line.

Telecom fraud almost always requires two things. The first is the ability to originate calls into the network without paying for them, and the second is a way to extract cash from the system to make the fraud effective.

For example, calls can be generated from hacked PBXs, or from a trick to make end users call an expensive number without realizing they are doing so.

But the key lesson here is that a good fraud - in the sense that it can continue running without detection - should mirror, as closely as possible, normal traffic patterns. This will increase the chance that any simple fraud detection system will probably miss the change.

WHAT IS THE BIG DEAL?

This is where Artificial Intelligence is starting to make a major impact on the way fraud can be detected and stopped. Up to now, fraud prevention systems have always required the knowledge of industry experts to:

- Think through how the fraud could work
- Determine what the likely calling pattern behind that fraud would be
- Finally come up with approaches and measurements to detect that pattern

To give an example, with premium rate calling to Latvia, say. Traffic from a retail service provider to Latvia would follow a certain pattern with peak traffic perhaps occurring in the evening. Traffic levels would likely be relatively similar from day to day.

Measuring this average traffic and producing a report that highlighted an upward percentage change from that average could indicate that a fraud was underway.

But what should that percentage change be? That is where the industry expert comes in to understand normal variability and set the threshold above which it could be considered out of the normal range. With the report, an engineer could look at the detail call records and work out the source of the fraud, but this often occurs after several days' delay all while the fraud was continuing its damage.

However, international wholesalers have a more complex issue to tackle - their traffic volumes change depending on what their carrier customers send to them and so simple changes in volume could come from routing choices in the upstream call path.

False alerts of fraud could then come much more frequently to the point where an alert is often ignored. It is often said that a fraud system with regular false alerts is worse than no system at all, because the engineering teams basically ignore what it tells them!

To counter this, operators need a system that not only captures the fraudulent events, but it does it with minimal false positive alerts. This is where artificial intelligence can really come to the fore.

As Luis Benavente, the CTO of BTS, recently shared with me, he doesn't believe there is a foolproof solution to eliminate fraud completely. However, he is confident that the introduction of these new artificial intelligence technologies and applications, together with sound processes, will firmly bring fraud under control and reduced to levels that make it unattractive for fraudsters.

He explained that telecom operators increasingly want to identify, control and mitigate the sources of potential revenue losses and that BTS' Anti-Fraud approach is a cutting edge and reliable solution for that.

THE BEGINNING OF THE END FOR FRAUD?

Artificial Intelligence, or AI, has a number of flavors and is continually developing in effectiveness. AI systems are often tracking through four phases of development:

1. Descriptive Analytics - what happened?
2. Diagnostic Analytics - why did it happen?
3. Predictive Analytics - what is likely to happen?
4. Prescriptive Analytics - how can I make it happen (or avoid it)

Early fraud systems were clearly only descriptive. Reports were provided that showed traffic levels, changes in call duration and so on. Experts were employed to determine what was really happening and to find the root cause.

As Big Data techniques and statistical analysis developed, fraud systems evolved further up the chain into diagnostic and predictive analytics.

Let's take the example of our earlier discussed premium rate fraud and dig further into the likely causes. We know that hacked PBXs are likely sources of the traffic to the premium number range, so we can postulate that the calls will originate from a very small number range (the PBX) and then be routed to a small range of destination numbers - the premium numbers assigned to the fraudulent company. Unfortunately, we don't know what (or where) either of those number ranges are going to be.

History might give us a clue on the destination range, but even there, new number ranges are released or reassigned frequently. We also know that a fraud often has two stages - a test phase to make sure that everything is working and the calls are being routed to the appropriate numbers, and then an active phase, often over the weekend when staffing levels in operations centers reduce.

So here AI can be used to achieve the following tasks that humans could never achieve to stop the fraud almost in real time:

1. Monitor all call records from all originations
2. Look for a pattern of calls from a range of telephone numbers to another range of telephone numbers
3. Confirm that this is not a normal pattern for that pair of numbers
4. If this is found, raise an alert.

Just stating that task highlights the enormity of the problem and why human intelligence could never tackle the problem in this way. The volume of call attempts is in the millions each hour and the number of potential pairs of telephone numbers is immense.

Of course, you could do this with some massive offline database search, but we want to do this in real-time to stop the fraud before it develops. Offline database approaches rely on the gathering of all the call records and then an analysis of all the possible number combinations with the output being a report of those that match our criteria. But we want to find the frauds in real-time, and AI gives us the statistical tools to create that real-time analysis.

The statistics involved to continually assess each incoming batch of call records, derive statistical models that describe that traffic and then update that model as new records arrive are at the leading edge of research, but vendors and operators are up for this challenge!

Frauds can result in hundreds of thousands of dollars of losses and so the development of systems that are accurate enough to identify the "testing phase" of our fraud is the objective and we are well on the way to that goal.

THE END OF THE BEGINNING

The early deployments of AI in fraud systems are generally at the Diagnostic/Predictive Stage - the system is flagging up that a fraud is underway.

However, the true goal is to continue the development of the algorithms and self-learning attributes of AI systems to allow them to identify the early test phase of a potential fraud, predict what is then likely to happen, and interact with the network elements and control systems to stop the fraud from occurring in the first place.

As BTS have found in practice, beyond the ongoing development of the algorithms, collaboration between the telecom operators is needed so that a practical due diligence assessment among those operators can be undertaken when irrational market pricing is detected.

As we have seen, from the technological and application perspective, there are several indicators that reveal irregularities such as traffic patterns, specific CDR and signaling analysis, as well as tracking rates associated with destinations and comparing with other operators in the market also lead to marked improvements in detection.

As the systems gain increasing confidence that a fraud is developing, additional call and signaling records can be analyzed to confirm this and be stored to provide later evidence in the event of a dispute.

Going back to our original example one final time, this detailed analysis could result in an immediate block of call routing to the destination numbers, followed by automated alerts to the PBX owner identifying exactly how the origination of the fraudulent calling is occurring.

If the operator also manages that PBX on behalf of the customer (perhaps as a cloud based solution), then the security weakness can be immediately resolved in real time.

The end result - the systems are now working at a level that was simply unattainable with older solutions and stopping frauds before they even have a chance to get underway and learning how to prevent the security breach in the first place.

A true 360° solution to the problem!

ABOUT THE AUTHOR

Steve Heap
CTO
HOT TELECOM

Steve has a lifetime of experience in designing, engineering and operating networks, both domestic and international. With leadership experience in small technology start-ups through to global service providers, he has deep experience in a wide range of products, technologies and geographies. He has the rare skill of being able to explain complex technical issues in easily understood concepts and uses that extensively in his consulting work with HOT TELECOM.

ABOUT BTS

BTS is a technology solutions provider and one of the top worldwide wholesale and retail telecom carriers operating with cutting edge technology. Through its innovative IPX Enhanced Network, it is in a position to provide high quality managed termination globally, with unique strengths in the Latin American & African regions.

Founded over 25 years ago in Miami - USA, it handled over 8 billion minutes globally in the last 12 months and ranked in the top 15 wholesalers. It has more than 150 direct links in 85 countries as part of its over 400 interconnections worldwide. It has over 150 employees located in offices in Miami, Madrid, Zaragoza, Rome, Warsaw, Singapore, Buenos Aires, Bahrain and Dubai.

BTS recently announced a Joint Venture Agreement with SoftBank Corp., which will bring a diversified portfolio of hubbing, cloud and managed services as a key player in the global market place.

To learn more, please visit www.bts.io

BTS' wholesale portfolio of services

- The portfolio of services that BTS offers its customers includes:
- Origination and Termination of Global Voice Traffic.
- Design and Deployment of International Gateways.
- Gateway Exchange Services – Outsourcing (Partial or Full)
- IPX – HD Voice & Virtual Pop Services
- Traffic Reporting Tools and Software Applications
- Fraud & FAS Detection Services & SIM Blockage
- Benchmarking Analysis
- Prepaid Platform Services & Mobile Top Up
- International traffic management for emerging telecommunications markets
- RCS Hosted Services
- RCS Hubbing Services
- Optimization of costs through traffic exchange agreements. SLAs.
- Call Center Services – Customized for Customer Requirements