Revenue Assurance: Managing Cable Fraud across Video and HSD

SCTE CABLE-TEC EXPO® – June, 2008

Dan Rice, Marcel Schemmann, Mike Gordish, Bob Cruickshank

ARRIS Incorporated
1825 NW 167th Place
Beaverton, Oregon 97006-4828
USA

Contents

Introduction

Revenue Assurance (RA) is a topic of growing interest among service providers in the current economic and regulatory climate. As consumers are continually evaluating the necessity of advanced services, it is more essential than ever that service providers deliver quality services while managing capital and operational expenses as reliably and efficiently as possible. The increasingly competitive environment, a result of the convergence of voice, video, data and mobility architectures, is enabling telephone, cable, satellite and wireless providers to compete head to head. This technical convergence is also complicating the value chain as "over-the-top" content and advertising delivered over the Internet is creating many more third-party entities that are involved in the delivery of content and services. This competition in turn creates pricing pressure on service providers. Many service providers are under pressure from investors to continually increase the number of Revenue Generating Units (RGUs), Average Revenue Per User (ARPU) and profit margins, while efficiently spending capital -- especially during periods of generally lower economic growth. One way service providers can increase the number of RGUs, ARPU, and profit margins is to focus on Revenue Assurance, which allows them to optimally monetize their business and service delivery platforms and process while simplifying complex technology.

While many have considered RA a hidden and uncontrolled cost of doing business, some analysts and industry consortiums such as the TeleManagement Forum (TMF) predict that the exposure of revenue leakage, cost leakage and fraud is between 3% to 15% of total revenue for Communication Service Providers (CSP), depending on factors such as networks and services type, geography, carrier type, and Revenue Assurance maturity level.[i]

Cable fraud has been a challenge for the industry since its early days. At the time, fraud took the form of an ambitious neighbor installing free services, or upon moving when a subscriber's services were left on for the next residents. Today, the problem brings more complexity, both from the perspective of traditional cable as well as the potential of revenue loss from new data services. With the authors' estimates pegging fraudulent CPE activity for one of the use cases examined in this paper at nearly two percent for video services, it is important that operators find methods to assure revenue and manage cable service fraud. This paper will investigate options that MSOs can implement today to help identify, prevent and "recover the leakage" from fraud across voice, video and HSD services.

Definitions

Several definitions for Revenue Assurance terms have been developed generally by the TMF Revenue Assurance - Business Solutions team. This paper defines these terms consistent with the TMF with some clarifications to provide context in this paper. This paper, in particular, focuses on some of the Fraud, Cost Leakage, and Revenue Leakage use cases for Cable MSOs.

- Revenue Assurance – Data quality and process improvement methods that improve profits, revenues and cash flows without influencing demand. Includes components of Process, People, and Technology and may be implemented with different levels of maturity in a business
- Revenue Leakage - Revenue not received due to missed opportunity, failure to bill for the services provided or failure to collect the payment
- Cost Leakage - Overpayment of costs for chargeable services to third parties or inefficiencies in operations and asset management
- Fraud - Intentional and deliberate illegal use of the MSO's services, network or intellectual property. Fraud can be committed internally or externally

Revenue and Cost Leakage can take a variety of forms that involve or can be managed by the service provider's Operational Support Systems (OSS)

- Failed synchronization of billing and service provisioning and authorization systems
- Loss or inefficient management of asset inventory or critical data
- Inefficiency in operations process and network operation
- Un-informed violation of service contract
- Fraudulent access to network or premium services

Revenue Assurance in the New Service Lifecycle

Revenue Assurance should be considered throughout the life cycle of creating, delivering and supporting new services, as shown in Figure 1. Planning and engineering of the services should evaluate revenue risks as a standard part of any product definition. As the product is developed and tested, these RA cases need to be validated and then audited as part of ongoing operational workflow. These stages repeat themselves when a current service is enhanced or extended to provide more functionality or performance, hence the term "lifecycle," and each stage has specific network and resource management needs as outlined below:

Network Analysis and Service Planning - During this phase, MSOs must evaluate the current status of their networks, including quantifying network resources in great detail and estimating the capacity, transaction reliability, potential data quality issues and security features necessary and available as part of the delivery platform for the new service. The impact of marketing on the customer from a new revenue, churn, retention and acquisition perspective is also important.

Deployment and Integration - Once the service delivery has been architected and the first integration and deployment has begun, it is essential to closely monitor the solution and provide negative and positive testing of RA use cases identified in the planning stage. First, the MSO must verify that services are functioning as promised, with the expected performance and reliability. Second, the MSO must test possible fraud and security holes to ensure proactive fraud prevention. Initial trial deployments are used to adjust and validate the assumptions made in planning prior to network-wide deployment. Accurately anticipating the service success, and all possible transaction failure scenarios or security issues, is difficult with new, complex services. Having fast access to usage trends and service integrity can play a major role in avoiding RA issues and ensuring a positive customer experience. Deploying Network Management Systems (NMS) capable of auditing RA issues is a significant, often, and unfortunately, deferred until later, element of this stage in the lifecycle.

Manage and Support - Once the service offering starts to reach critical mass, small outages or impairments have a large impact on day-to-day operations as many customers can be affected. The customer experience metrics and assumptions used for analysis and planning should also be used for ongoing service management to ensure the revenue goals are being met. It is critical to prevent quality, security, and fraud issues by performing proactive RA analysis, network maintenance and optimizing network capacity to manage operational costs. Doing so can decrease cost leakage quantified by the number and length of trouble calls and non-revenue generating truck rolls, as well as improve capital efficiency by allowing the MSO to delay infrastructure upgrades and mange CPE inventory. Fewer network outages through proactive problem resolution and reduced Mean Time to Repair (MTTR) result in better availability reducing customer churn. Discovery of security holes that can be plugged before they can be widely exploited saves operational expense and revenue leakage.

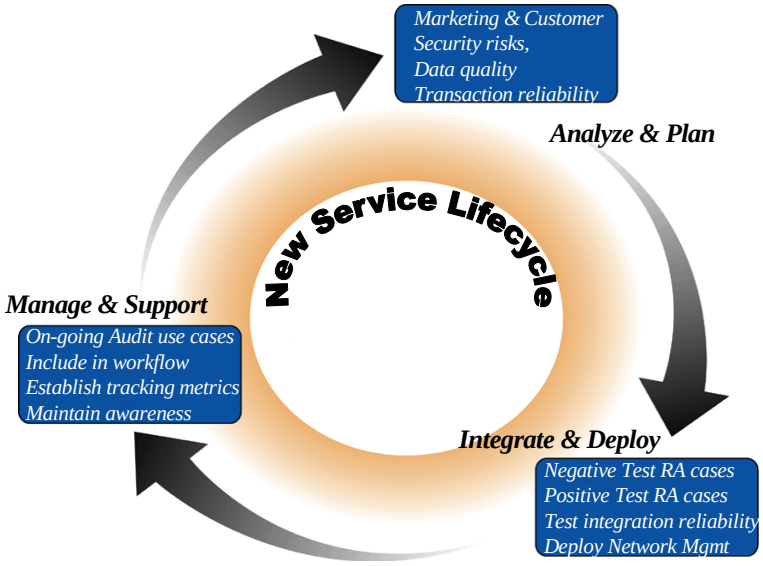


Figure 1: Revenue Assurance in the New Service Life Cycle

Revenue Assurance is no longer the sole responsibility of the finance and auditing departments with compliance and risk management; MSOs need to manage costs and productivity with an eye towards their impact on the top and bottom line. For example, consider the following roles and how they can contribute to more mature RA process.

Product management and marketing - Consider security and revenue risks as part of product definition. Monitor impact and how RA policy affects customer retention, churn and acquisition.

Engineering, QA and IT - Consider security, transactional reliability, and data quality in the design, test, and systems integration.

Network operations - Leverage security features in deployment and proactively monitor, audit and prevent fraud and customer dissatisfaction use cases. Design ongoing workflow process to eliminate gaps and resolve discrepancies in data integrity.

Customer care – Alert Billing, OSS/BSS synchronization issues, special package and discount elements.

The role of OSS in Revenue Assurance

Operational Support Systems (OSS) are central to the success of most advanced services deployed by MSOs today. The OSS provides the infrastructure to activate, authorize, and install new services by translating billing system events into network provisioning, configuration and workforce activities. The role of OSS in RA was described by Martin Creaner, TM Forum President & CTO as following:

"Revenue Assurance spans across OSS and BSS because it requires a holistic view of the operator's environment to encompass both OSS systems such as network management and BSS systems such as the billing and CRM systems …"[iii]

OSS solutions provide ongoing Service Assurance through measurement of service quality and customer experience, fault management, resource utilization, data synchronization, and security issues. Effective OSS systems can simplify increasingly complex systems, enabling clear and compelling services. Technology, process, people, and third-party relationships can all be

managed through these systems, which is especially important as more third parties are involved in the end-to-end service delivery.

Several use cases highlight the role that OSS can play in RA. The following list includes just a few of the many use cases related to this topic. Several of these will be explored with more detail in this paper.

- Devices provisioned on network not in billing system
- Billing system updates not propagated to network
- CPE with service levels greater than the currently subscribed package
- Cable drop connections and traps for non-video customers
- Management of inventory by warehouse and workforce
- CPE devices belonging to the same account, but located in different physical locations
- CPE devices that have moved physical locations
- Which modems are cloned to enable fraud?
- DOCSIS device, network, and bandwidth consumption monitoring
- Locking down the CPE provisioning process

Network not Synchronized with Billing Use Case

As described above, one common reason for revenue leakage is lack of synchronization between the billing system and the network. OSS provides the infrastructure to activate, authorize, and install new services by translating billing system events into network provisioning, configuration and workforce activities. Service providers should ensure that any customer account transactions flow through or are updated to the billing system to avoid having revenue collection being out of synch with the service provided by network elements. Occasionally, for a variety of reasons, transactions and services are manually created outside of the flow through the billing system. This can occur through un-reliable transactions and protocols, which can be problematic with older billing system technology, or integrations that do not leverage the latest APIs. Lack of synchronization can also occur, often due to bypassing the correct process which eventually results in revenue leakage.

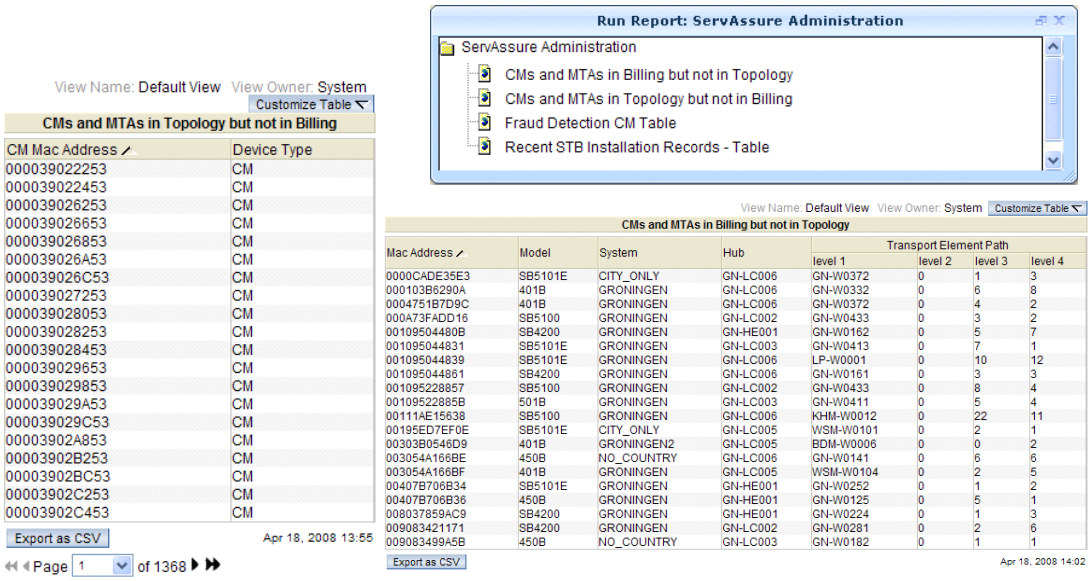


Figure 2: Network not synchronized with Billing use case examples

To audit and avoid these types of issues, scheduled reporting should be setup to identify devices that exist on the network but not known to the billing system as shown in Figure 2. By periodically exporting account information and correlating with device information which is auto-discovered from the network, both devices that are going un-billed or being paid for that may not be on the network can be prevented. Payment for services not actually delivered due to network issues will result in customer dissatisfaction. The first case should be considered as an opportunity to begin collecting for services delivered increasing the number of RGUs. The second case should be considered as an opportunity to proactively resolve a service issue, increasing customer satisfaction and reducing churn. The second case may also represent an up-sell opportunity for devices in accounts not subscribed to services, and the device is capable of such, as is a MTA without voice service.

Provisioned Services not Synchronized with Billing Use Case

As previously described, lack of synchronization between the billing system and the service delivery platform may result in revenue leakage. It becomes more complicated than the simple synchronization of devices on the network and in the billing system with different tiers of service or different elements of service to which a customer may subscribe. For example, most MSOs today offer several tiers of data service differentiated by the maximum data rates or data consumption. Advance video services such as Video on Demand (VoD) have complex entitlement product offerings with elements such as fee subscription VoD when subscribing to the premium channel broadcast television service. OSS can be used to compare the service level or entitlements provisioned to the service delivery platform and the billing system as shown in Figure 3. The OSS and back office should provide the data as shown in these examples to update and remediate these issues through APIs and GUIs.

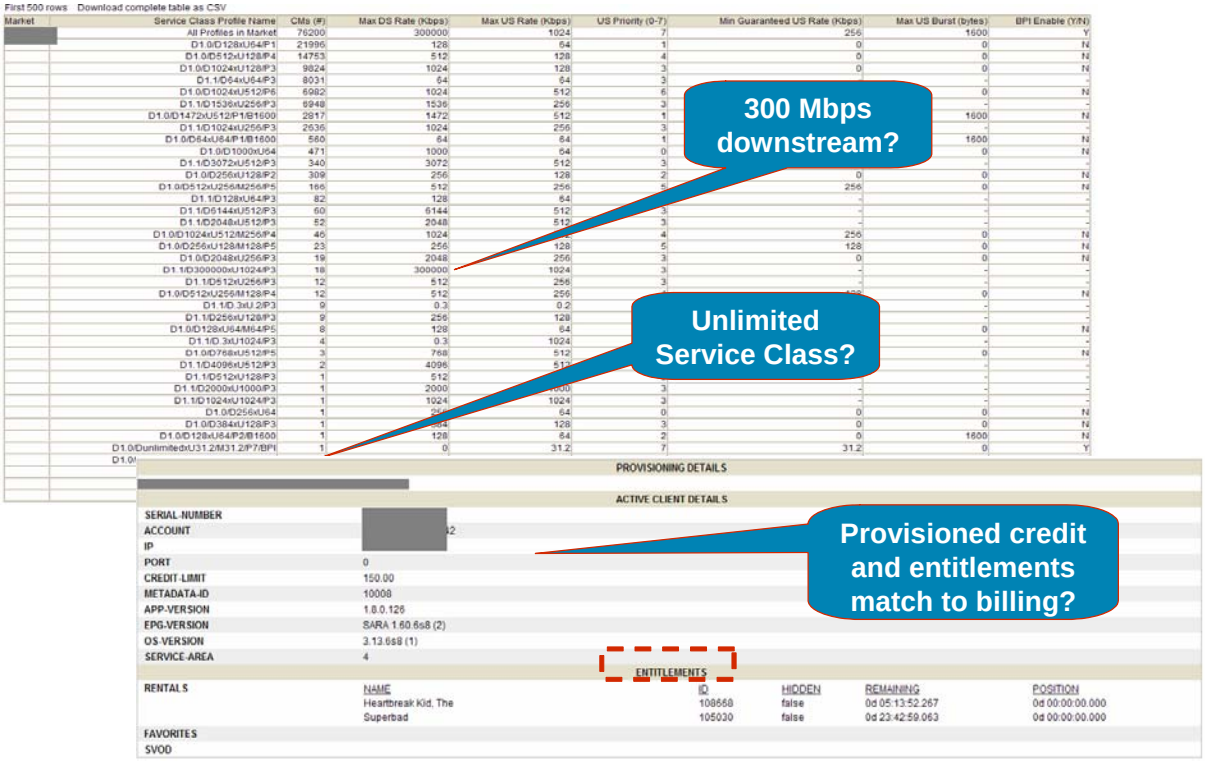


Figure 3: Provisioned Service Not Synchronized with Billing Use Case

This recently obtained report from a production cable system shows that a set of DOCSIS 1.0 modems has been provisioned with 300 Mbps downstream maximum rate limits which is an order of magnitude greater than what is technically possible. Is this a configuration error or an attempt at fraud as described in the section *Cable Modem Theft of Service Use Case*? Is the customer with unlimited download speed on an official service package? This type of reporting is essential to identify the exceptions and ensure their validity.

Some billing systems or versions of billing systems may not have a real-time authorization API or ability to fully synchronize with external OSS systems. Other billing systems may occasionally drop connections and become unavailable. Based on policy or necessity, many MSOs may, for example, choose to enable a VoD entitlement cache so that a VoD request is not denied if the connection to the billing system is down, assuming it can be accounted for later. If billing transactions are lost due to lack of connection with no synchronization, the possibility of revenue leakage exists resulting in one of the following results among others.

- Denial access to certain programs: based on entitlements the customer should have creating customer dissatisfaction and missing a revenue opportunity to increase ARPU
- The wrong account gets billed for a service based on a STB which has been moved to a new account, but the transactions to keep this in synch were not reliable or synchronized

Tap Audit Automation Use Case

One of the oldest forms of cable fraud or revenue leakage is due to the lack of security around old fashioned analog television (TV). When analog TV broadcast is turned off in the US on February 17, 2009, and in a similar time frame in other countries around the world, delivery of analog TV by MSOs may be considered an even more valuable service feature. Physical access to the network by the millions of existing analog TVs provides the end user access to the analog tier. Many MSOs have even blocked access using a filter known as a trap to block the analog TV for customers who sign up for high-speed data service, but not video service. When a customer discontinues subscription to any services, their physical connection to the tap or at the home is disconnected so that they are no longer able to receive analog TV or any other services. This can be a problem in Multiple Dwelling Units (MDU) where there is frequent turnover and the work order to disconnect the cable may not happen in a timely manner or may be reconnected un-intentionally. Tap Audit Automation is a methodology that can be used to determine illegal connections to the network and use them as up-sell opportunities or as opportunities to stop fraud or revenue leakage.

The value of implementing a solution to the RA use case is fairly straight forward to estimate. How many un-authorized connections exist? How many of the un-authorized accounts will subscribe or upgrade their service? Plug in your own numbers to estimate the financial impact.

- 1 Million HHP
- 10% HHP with un-authorized analog tap connections
- Assume 25% of unauthorized customers will convert to paying customers
- Customers that convert upgrade ARPU by $15
    - Ex: Basic analog tier
- 25% of these take a second service
- Second service upgrade ARPU by $50 more
    - Ex: Basic digital with 1 box and a remote
- **Revenue leakage recovered = $8.3M annually!**

Tap Audit Automation requires the following elements to effectively optimize this process and the related workforce.

- Real-time interface to billing system through workforce OSS
    - Creation and scheduling of audit work orders
    - Instantaneous distribution of audit work orders
    - Automatic updates when customer accounts change
- Tracking of field sales representatives\auditors with GPS/GIS
    - Mapping solution tracks auditor location
    - Track progress over several days to evaluate effectiveness and productivity
- Auditors need real-time access to customer information
- Automating creation of evidence for fraudulent connections
    - Take pictures immediately tied to the account and stored in the database for recall

There are two key roles within the process of tap audit automation: the audit supervisor and the auditor / direct sales representative. The former can be an individual with the skills to audit, direct sell, and install new services or the functions could be split. To improve the efficiency of this role, the vision is that a single field technician could perform all three functions and all technicians have access to the capability. The auditor could identify a disconnected or un-authorized connection, then up-sell the customer to a new service package and do an instant installation. The tools and capabilities supplied to the auditor through a mobile handheld device across a wireless or wired network include:

- View customer Information from the billing system on the handheld device
- Update status of the account's tap connection by the auditor with several states
    - Confirmed – Drop is still disconnected, or trap in place as required per billing system
    - Illegal – Connected to network or no trap and not authorized per billing system
    - No Access – Technician did not have access to tap or home to make a determination
- Sell new services to accounts with un-authorized connections
    - Update customer Information which is sent to billing system
    - Add campaigns/services/packages/CPE
        - Schedule installation
            - Instant installation by real time creation of an installation work order and completion of the installation while onsite; or
            - Creation of a referral work order which is routed to a technician with the skill set and CPE equipment to complete the installation
    - Capture Pictures
        - Evidence of un-authorized or fraudulent connections are obtained by digital cameras, now common on mobile devices, which can be associated with work order and customer account and stored in the workforce OSS.

The Audit Supervisor can organize and track the auditor performance to analyze the productivity and success of the auditing and direct sales activities resulting in increased revenue and decrease leakage. The accounts to be audited can be selected by criteria such as accounts which have recently disconnected or were non-pays over a recent time frame within a certain network segment. Another possible set of accounts can be obtained from other Revenue Assurance applications such as the CPE device location example in the section titled, *CPE Device Location Use Case*. Graphical- and map-based visualization of previous audit activity can be valuable to direct current efforts. For example, if up-sell service was declined

three months ago, another direct sales engagement may be an option. The tools supplied to the audit supervisor who manages, tracks and schedules the work of the auditor include:

- Track daily activity in real time
  - GPS/GIS-based maps
  - Gantt view of field sales representative\auditor status and work completed
- Account Organization
  - Updating selection criteria such as
    - Non-pays and recent disconnects in Fiber Node X
    - CPE Device Location Fraud use case
  - Updating routing configurations
- Auditor performance tracking
  - Reporting per field technician and over time
  - # of audits, # of up-sells, # of disconnects utilized to derive RA metrics
  - View trends toward fewer fraudulent accounts and new RGUs
  - Visualization of status and past activity for audits

Tap Audit Automation Workflow

An effective way to visualize the audit history to inform and direct future work may be a graphical mapping solution as shown in Figure 4**Error! Reference source not found.**. The audit supervisor can review real time and historical activity to understand what the conversion rate and sales efficiency is for the team or individual auditor. One set of workflow processes that can be used for this use case as described above is shown with details in Figure 5.

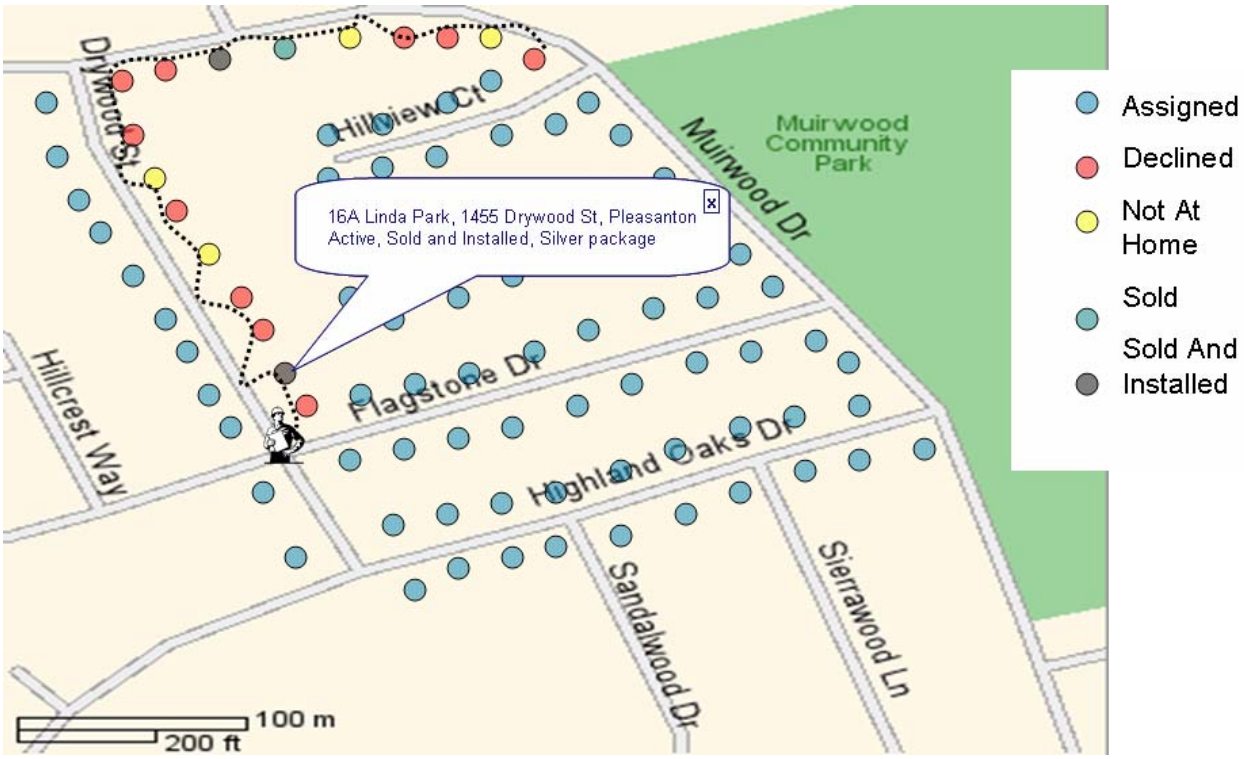


Figure 4: Mapping visualization of auditing activities

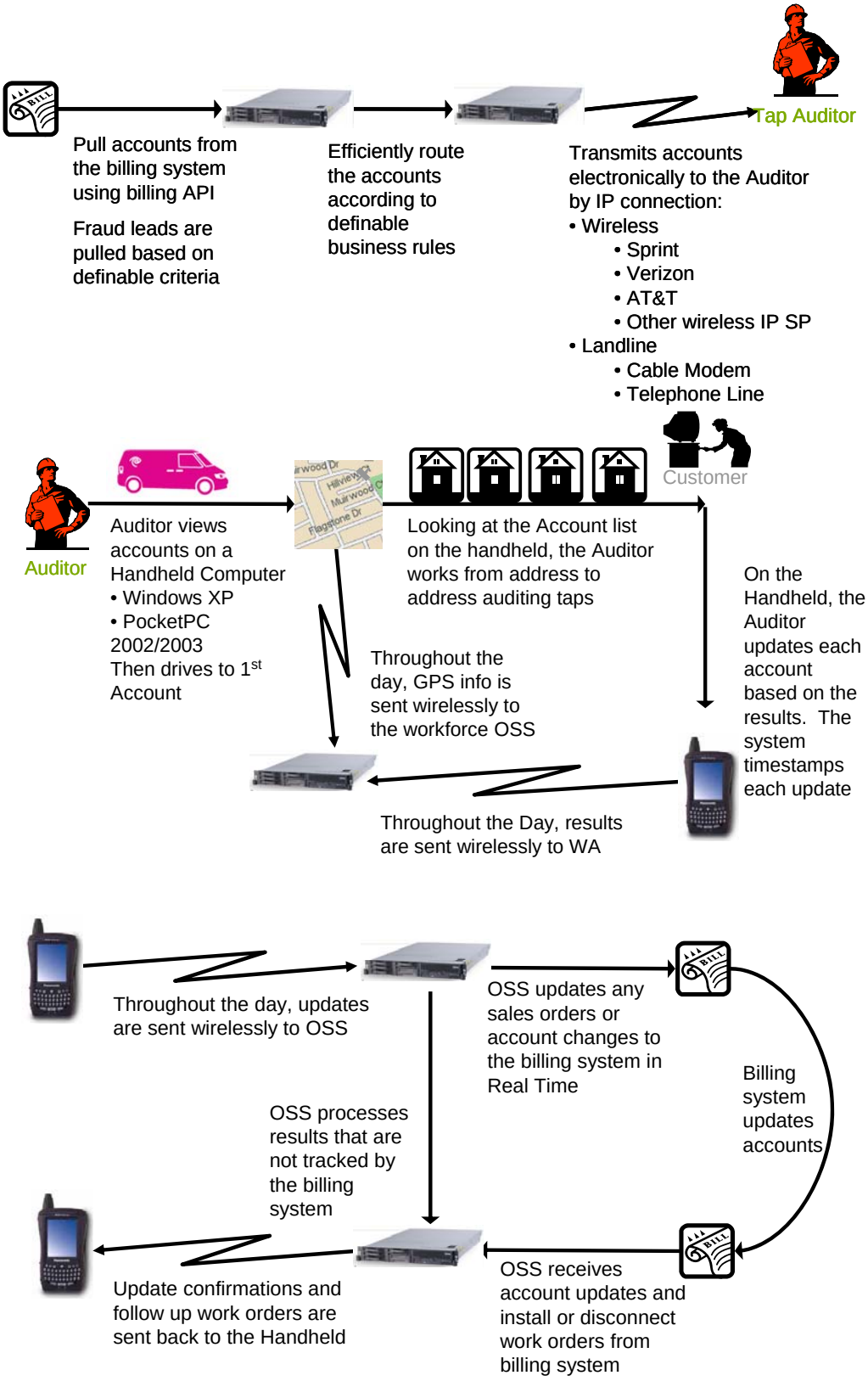


Figure 5: Tap Audit Automation workflow process diagrams

CPE Device Location Use Case

There are a variety of operational and RA use cases related to knowing the location of a CPE device on the network. The author's have participated with MSOs in several investigations on techniques that could be used to accomplish this. These cases include, among others:

- Stolen modems able to access network due to provisioning issues
- MTAs that are not in the location associated with emergency services database
- STB in violation of digital video service contract

This section focuses specifically on the STB in violation of digital video service contract use case including lab and field data from testing and conclusions on the feasibility of this technique. The STB fraud use case is generally described by the following type of events and rationalization, which breaches many MSOs digital video service contracts as shown in Figure 6 and described below.

- Joe Subscribes to the Platinum STB Package with unlimited subscription premium channels and VoD for $150 / month and adds 4 "additional outlet" STBs for $6.95 / month each
- Joe decides its less expensive to use one of his home STBs at his office in his busy waiting room rather than pay the $200 / month for his business video
- Joe invites his friends over to watch a PPV event and brags about his great VoD Service with unlimited selection
- Joe's friend complains that he doesn't want to pay for the $150 package, but thinks the service is really great
- Joe offers to set his friend up – Joe's friend pays Joe $50 / month for lending him the STB from the guest room which isn't really used that often
- MSO Revenue Loss ~ $350 / month

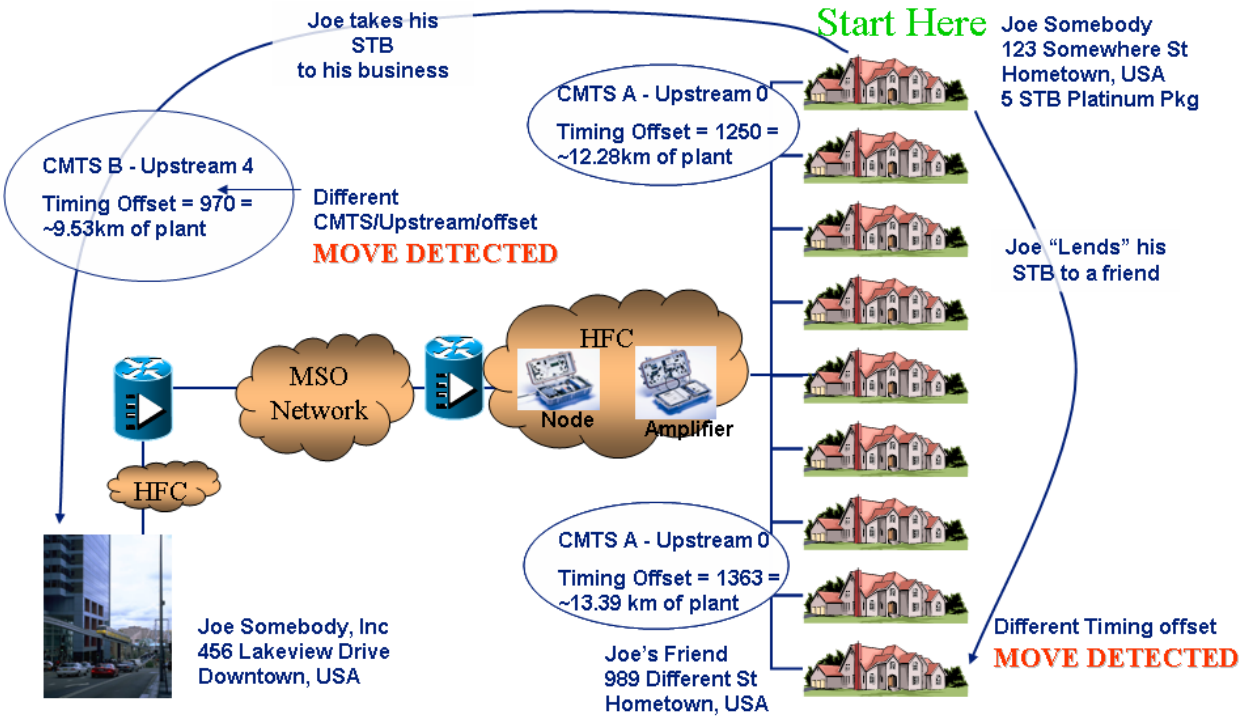


Figure 6: Digital Video STB fraud use case

The value of implementing a solution to the RA use case is fairly straight forward to estimate. How many Joe's are out there? How many of Joe's friends will subscribe or upgrade their service? Data obtained from the field estimates as high as 2% in some areas. Plug in your own numbers to estimate the financial impact.

- 1M video customers
- 2% of boxes fraudulent
- Assume 25% of fraud STBs will convert to paying customers
- Customers that convert upgrade ARPU by $50
    - Ex: Basic digital with 1 box and a remote
- 10% of these take a second service
- Second service upgrade ARPU to $75
    - Ex: Basic Digital with HD and premium channel
- **Revenue leakage recovered = $3.5M annually!**

CPE Device Location Workflow

One set of workflow processes that can be used for this use case, as described above, includes the following steps. Validation can be achieved after checking whether a phone call or VoD session is in progress using the same OSS architecture. Validation is especially important for the timing offset / distance case because statistics are used to determine the probability of the STB not being in the account premises as shown in the data presented in this paper.

1) Correlate billing account and network auto-discovered CPE data with NMS
2) Periodic device discovery, measurement of timing offset and network connectivity with NMS
    a) Establish home distance from headend and home network connectivity leveraging CMTS and CPE information
3) Periodically schedule report identifying possible fraud candidates based on fraud algorithm
4) Work order generated to validate potential fraud case
5) Field audit team validates connectivity to box as drop is temporarily disconnected
    a) Could be performed along with Tap Audit Automation
6) If CPE remains on line – Referral work order delivered to security team for fraud remediation

An example of the Fraud report is shown in Figure 7. Account and subscriber data in this example were generated for test purposes only, not from any production cable system. Report data can be exported through API for integration with Workforce Management OSS in a similar workflow as described in the section titled, *Tap Audit Automation Use Case*.

Both STBs in account 131 should be located at the same physical street address and are attached to the same CMTS upstream interface. Per fraud timing offset, algorithm they are determined not to be in the same physical location because of the distance apart they are on the network.

Both STBs in account 140 should be located at the same physical street address and are connected to the completely different CMTSs. With this auto-discovered connectivity, it is impossible for them to be in the same physical location

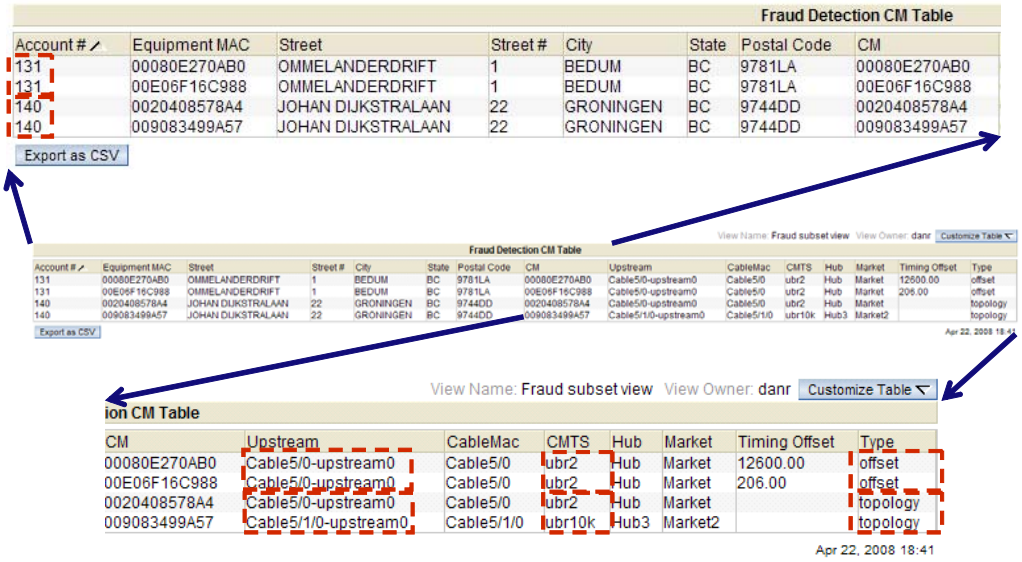
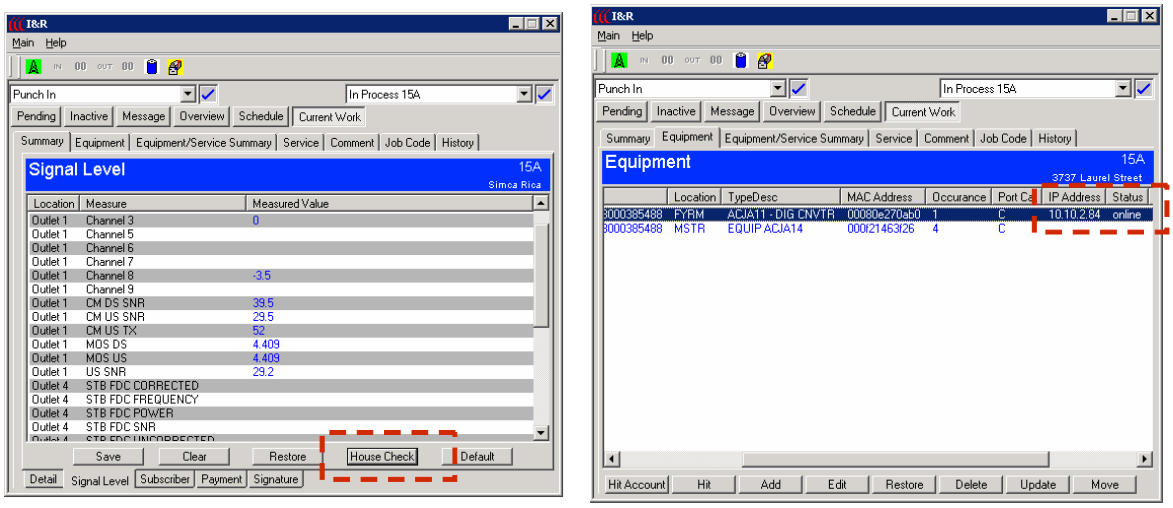


Figure 7: Example Fraud report with both topology and timing offset / distance fraud cases

Figure 8 shows a couple examples of tools that could be used by the auditors or the audit supervisor to validate that the STB is not located in the premises associated with the account. As previously described, the online status for all of the STBs in the account are evaluated while the drop is temporarily disconnected.

The first scenario in Figure 8 shows how a handheld device connected to the workforce OSS can perform a house check to evaluate the status of all devices in the home and even collect performance data. The house check is performed by communicating over a wired or wireless network with a service assurance OSS which can check device status and health on-demand. The second scenario in this figure shows how an audit supervisor or dispatcher working in the office while communicating with the auditor can track the STB status in high resolution while the drop is temporarily disconnected using the service assurance OSS.



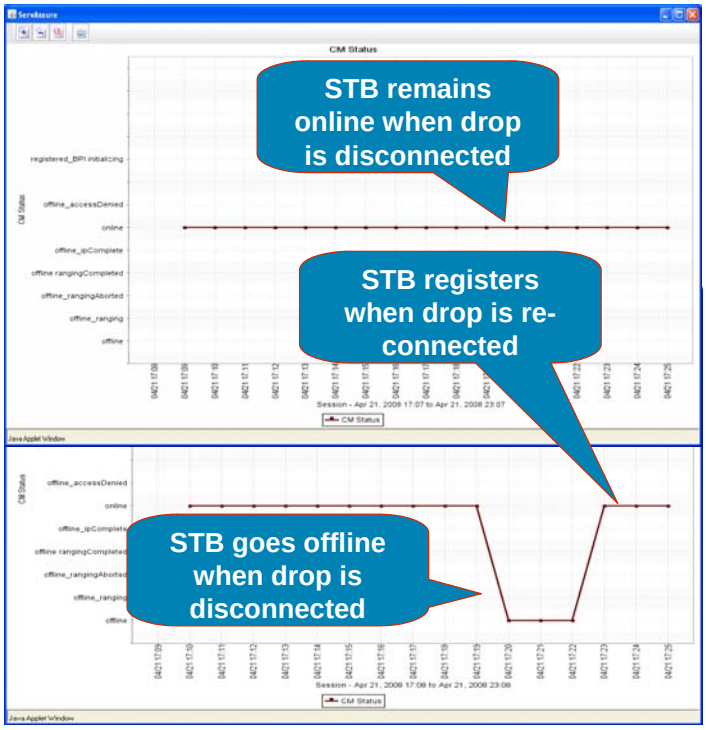


Figure 8: Validation of STB fraud by disconnecting account owner drop to determine if STB is on premises

CPE Device Location Test Results

Both laboratory and field data collection have been done to examine the feasibility of detecting device location based on topology auto-discovery and through the use of timing information to determine the distance from the headend. All of the video and data platforms deployed by MSOs today use ranging techniques to adjust power levels and synchronize the timing differences caused by the propagation of signals through the HFC network.

The data presented next and these experiments were performed on STBs using a DOCSIS out-of-band control channel and the conclusions are based on the DOCSIS platform. Other non-standard video delivery systems were also evaluated and have similar characteristics and appear to support this type of technique although with a lower resolution. The field data is based on evaluation across a variety of market areas with large numbers of STBs. The fraud RA use case candidates were identified and validated by field auditors. Both topology fraud on different CMTSs and interfaces as well as timing offset / distance fraud on the same CMTS interface were discovered. A successful algorithm was developed yielding **100% validated accuracy at >300 feet** device movement within the HFC network while residing on the same CMTS interface.

The results of lab testing are shown in Figure 9. During these tests the fiber distance in the HFC network was incremented in steps of 5 km by connecting different spools of fiber between headend optics and fiber node, while measuring and monitoring the DOCSIS timing offset for a variety of CM, MTA, and STB devices. The following conclusions were obtained.

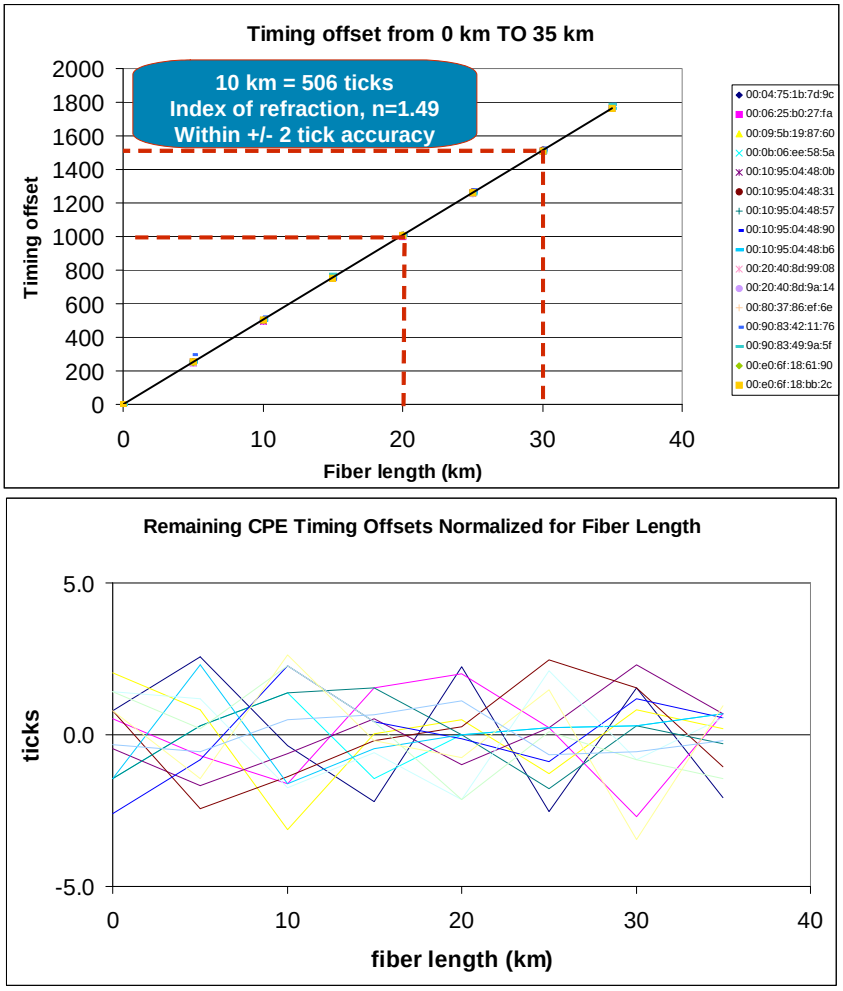


Figure 9: Lab testing results for timing offset / distance accuracy

The increase in the length of fiber resulted in a linear increase in timing offset with a slope consistent with the expected speed of light in fiber as determined by the following calculations and within the error of the fiber spools and coaxial network actual length.

- Phase velocity for light in free space, c = $3x10^8$ m/sec
- Index of Refraction for HFC fiber and coaxial cable
  - Fiber, n = 1.49
  - Teflon(PTFE), n = 1.45
- Phase velocity for light in Fiber = c/n = $2.0x10^8$ m/sec, which is about 67% of c

The resolution of the timing adjust parameter per DOCSIS spec for TDMA is 1 tick = ($1/10.24x10^6$) = 97.6 nsec[iii]. DOCSIS prescribes accuracy at the CMTS to within ±½ of a symbol for the TDMA symbol rate used for testing which is equal to 2 ticks. A different accuracy is required for the CM than CMTS. Based on these specifications, the following calculations can be made:

- Distance per timing offset unit = $2.0x10^8$ m/sec * $97.6x10^{-9}$ sec = 19.7 meter / tick
- Ticks per 10 km of fiber = $10x10^3$ m / 19.7 meter / tick = 508.9 ticks

The measured ticks per 10 km of fiber were 506 ticks, which is within the accuracy of the fiber and DOCSIS bounds. Deviation accuracy bounds were measured at ±2 ticks as expected per

specification and evolve for DOCSIS 2.0 modems to higher resolution and accuracy for SCDMA. It was necessary to measure both CM and CMTS timing offset to predict fraud with 99.9%+ confidence. Lab data confirms accuracy and need for device type normalization.

The example shown in Figure 10 identifies an STB from an active production subscriber account with four STBs identified as a fraud candidate based on the timing offset / distance algorithm. The y-axis represents the timing offset value for each of the CPE over several days sampled once per hour. Note, that the timing offset is fairly stable with a few periodic ranging updates. During the analysis and algorithm development it was shown that periodic ranging updates can be beneficial to the accuracy of the fraud algorithm. The blue STB is seen at about 16 ticks or 516 feet different than the others in the same account. This case was validated as an actual case of the STB not being located on the premises by field auditor using the method similar to that described above.

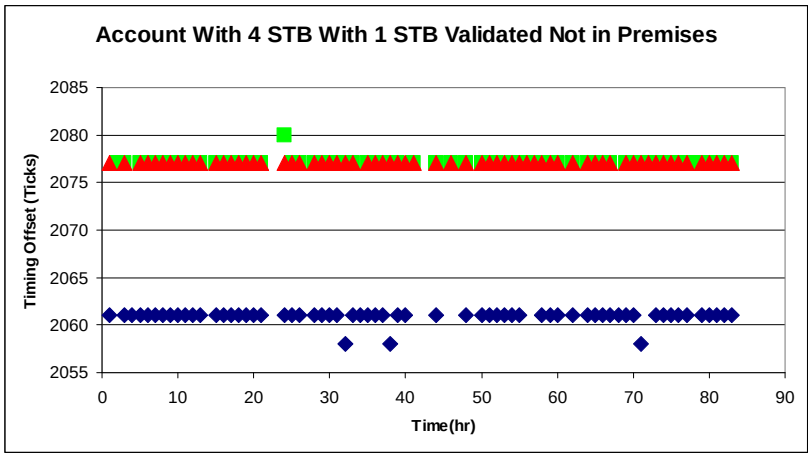


Figure 10: Example of validated STB fraud

The field data shown in Figure 11 reveals that a small percentage of units have unstable timing data in the CMTS. This is not system drift due to temperature or network changes, but a CMTS reporting issue. It was found during the trial and further field testing that the CPE provides highly reliable timing offset data. The data shows that at 3 ticks offset from the home average < 0.3 % error probability exists. Based on this, the authors believes that fraud can be reliably predicted in > 5 tick range. This setting can be configured in the algorithm to increase or decrease the probability of actual fraud cases being detected with high confidence based on the network characteristics such as premises and network size. Detection in < 3 tick range may require resolution enhancement such as DOCSIS 2.0 SCDMA resolution or a method leveraging long-term averaging and forced periodic ranging. It's clear that the more accurate the data reported and more samples evaluated by the algorithm, increase the confidence. Both CPE and CMTS data can be leveraged to increase confidence.

In the lower graph in Figure 11, the total population percent fraud is only considering timing offset. The confidence estimate does not include topology Fraud. If the total cases of Fraud due to timing offset are low, than the confidence of identifying a fraud case accurately will be reduced. For example:

- There is a 99.99% confidence level of finding a non-fraud STB within 5.3 ticks from the home average
- There is a 90% confidence level of finding a STB fraud case outside 5.3 ticks from the home average if the total population fraud percentage is 0.1%

- There is a 99% confidence level of finding STB fraud outside 5.3 ticks from home average if the total population fraud percentage is 1.0%

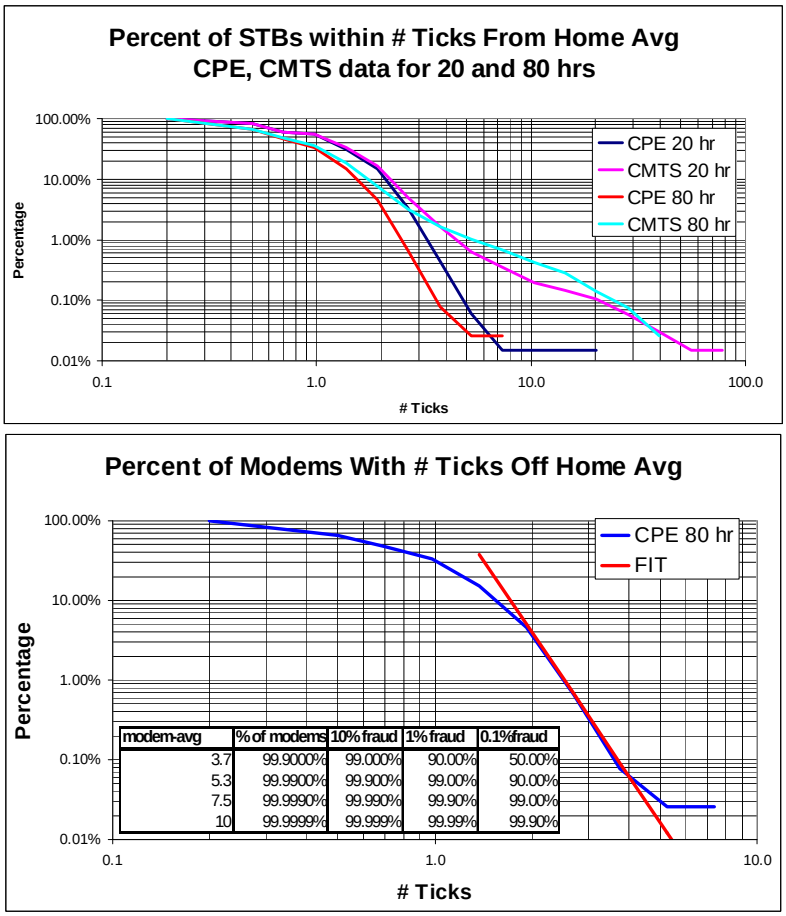


Figure 11: Field Data distribution used to evaluate data and confidence in fraud estimation algorithm

In summary, the following conclusions were obtained from these test efforts.

- For 10 tick offset (300 feet, or ±5 ticks), 99.99% confidence level is possible
  - Better resolution is possible with long term averaging to target MDUs
- CPE timing information is an order of magnitude more reliable than CMTS data for timing offset for the CMTS vendor used by the MSO for the trial
  - Needed in parallel with CMTS data to analyze unstable results
  - Field data reveals that a small percentage of units have unstable timing data in the CMTS. This is not system drift, but a CMTS reporting issue
  - Both CMTS and CPE data points can be used to improve estimation
- Time Averaging and Re-ranging of CPE enhances precision, reduction in distribution widths
- Timing offset data represents round trip propagation time

Cable Modem Theft of Service Use Case

Over time, cable MSOs have had a relatively good track record of preventing theft of service for advanced services. In many cases, when security breaches have occurred, the holes have been plugged by implementing OSS solutions that identify the issue and then by leveraging some of the features in DOCSIS that had not been configured previously. Even today, some of the security mechanisms have not been widely used such as the PacketCable Key Distribution Center server for secure provisioning. Often it seems that a breach has to occur before some of the latent

security features are leveraged. The key to the cable industry success has been the security infrastructure built around DOCSIS with an open review process resulting in the most robust technology as opposed to what some refer to as "security through obscurity."

Over the history of cable modem technology, several "theft of service" or "theft of quality of service" methods have widely seen the light of day. Pre-DOCSIS modems from LanCity at one point were "un-capped" to raise the MSO configured limits or tiers. In the 2000/2001 time frame another method surfaced on the Internet for accomplishing the same for DOCSIS modems. While this hole has largely been closed, there is still evidence of it in production networks for older modems as shown above in Figure 3. This method could have had a smaller impact through the use of DOCSIS features such as Shared Secret MD5 CMTS MIC and time of day checking. Another alternative would be the use of service class names to build an abstraction. Updates to a particular modem model which allows loading a configuration file from the Ethernet port helped prevent the simple method of "uncapping".

In recent years, the ability to change the firmware in some modems has been published for sale on the Internet and included in a book sold on amazon.com. The goal of this method is to change the MAC address stored in the Flash memory to match or "clone" a MAC address from a legitimate modem. With a legitimate MAC address the modem can obtain service from the provisioning system since that is the key used to authenticate the modem; thus, obtaining service without paying for it. In addition, this particular method also attempts to obtain higher quality of service. A recently discovered example of this is shown in Figure 12.

Legitimate Cable Modem	
sysDescr.0	Modem <<HW_REV: 02; VENDOR: Arris Interactive, L.L.C.; BOOTR: 5.01; SW_REV: 4.5.52T; MODEL: TM502G>>
ifPhysAddress.1	0:15:96:40:7d:5f
ifPhysAddress.2	0:15:96:40:7d:60
ifPhysAddress.5	0:0:ca:0:0:3
ifPhysAddress.16	0:15:96:40:7d:61

Cloned Cable Modem	
sysDescr.0	<<HW_REV: 7; VENDOR: Motorola Corporation; BOOTR: 2142; SW_REV: SB5100-2.3.1.6-SCM01-FATSH; MODEL: SB5100>>
ifPhysAddress.1	0:15:96:40:7d:60
ifPhysAddress.2	0:15:96:40:7d:60
ifPhysAddress.5	0:15:96:40:7d:60
docsDevSwCurrentVers.0	SB5100-2.3.1.6-SCM01-FATSH

Figure 12: Cable Theft of Service Use Case, example from production network

MAC address ranges are handed out by the IEEE, where the first 3 bytes, known as the IEEE OUI, identify the vendor of the device. The modem in the first table is a legitimate ARRIS DOCSIS 1.1 modem with MTA. In this case, the MAC address, **00:15:96**:40:7d:60, indicates it is indeed an ARRIS modem. The modem in the second table is another vendor's modem that has been compromised using the "cloning" method. This case is easily detected because of the following:

- Two identical MAC addresses were online at the same time on different CMTSs and logged in the Assurance OSS
- Labeled Motorola Modem Software and System Description with ARRIS IEEE OUI!
    - Software is known version described in a book on "hacking the cable modem"
- Same MAC Address for all interfaces!
- 0.2% clone cable modem candidates in this cable system

The assurance OSS has discovered manufacturing errors in the past where the same MAC address was mistakenly input to more than one modem. This is clearly not a manufacturing error.

While this paper is not intended to be a full discussion of DOCSIS security facilities, a variety of DOCSIS techniques listed below can be used to prevent these fraudulent activities. The cloning of the cable modem becomes particularly difficult when the MSO configures BPI+ where the cable modem is authenticated by an x.509 digital certificate, assuming the certificate cannot be cloned. Provisioning modifications could be developed to reject the cloned MAC address. DOCSIS 3.0 adds a variety of new features to strengthen and extend encryption and provide additional checks and verification to prevent fraud.

- Pre-DOCSIS 3.0
    - Message Integrity Checks (MIC), Time of Day, BPI+, Digital Certificates, Secure Software Download, DOCSIS 1.1 minimum, SNMP community strings, keep firmware up to date
- DOCSIS 3.0 security features to prevent theft of service and protect privacy
    - Encrypted multicast and 128-bit encryption
    - Early authentication and encryption with certificate revocation - no access to unencrypted IP address and configuration file
    - Source Address Verification and ARP limits – prevent CPE IP spoofing
    - Configuration file - name authorization, stronger MIC Hash, and content validation

Conclusions

Revenue Assurance is an important area of focus for service providers that will improve both financial and operational metrics. Some analysts estimate that the exposure of revenue leakage, cost leakage and fraud is between 3% and 15% of total revenue for Communication Service Providers (CSP), depending on factors such as networks and services type, geography, carrier type, and Revenue Assurance maturity level.[i] Consideration of the RA implications throughout the lifecycle of a new service including the technology, process, and people will be one of the keys to success for MSOs. Proactively managing both revenue generating and cost reduction activities is important for RA to have a positive impact on the business.

Operational Support Systems (OSS) are central to the success of most advanced services deployed by MSOs today. Several use cases, described in this paper, highlight the role that OSS can play in RA to identify issues and resolve them along with leveraging the security features of DOCSIS.

Abbreviations and Acronyms

API	Application Programming Interface
ARP	Address Resolution Protocol
ARPU	Average Revenue per User
BPI	Baseline Privacy Interface
BSS	Business Support System
CM	Cable Modem
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CRM	Customer Relationship Management
CSP	Communication Service Provider
DOCSIS	Data over Cable Service Interface Specification
GIS	Geographic Information System
GPS	Global Positioning System
GUI	Graphical User Interface
HSD	High-Speed Data
IT	Information Technology
MDU	Multiple Dwelling Unit
MIC	Message Integrity Check
MSO	Multiple System Operator
MTA	Multimedia Terminal Adapter
MTTR	Mean Time to Repair
NMS	Network Management System
OSS	Operational Support System
QA	Quality Assurance
RA	Revenue Assurance
RGU	Revenue Generating Unit
SCDMA	Synchronous Code Division Multiple Access
SNMP	Simple Network Management Protocol
STB	Set-Top Box
TDMA	Time Division Multiple Access
TMF	TeleManagement Forum
VoD	Video on Demand

[i] UK research firm Analysys, Telemanagement Forum Revenue Assurance Overview and Revenue Assurance Guidebook, http://www.tmforum.org

[ii] http://tmforum.org/RevenueAssurance/2140/home.html

[iii] DOCSIS_1.1_RF_Interface_Specification(SP-RFIv1.1-I10-030730).pdf, http://www.cablelabs.com