RF FINGERPRINTING: AN OPERATIONALLY EFFECTIVE METHOD TO REDUCE CABLE TELEVISION SIGNAL AND EQUIPMENT THEFT

Lee Pedlow
Sony Electronics, Inc.

Abstract

Presented is a robust method to self-detect the unauthorized relocation of digital cable television appliances, especially one-way or CableCARD-based devices, as a deterrent to signal (service) and MSO-provided equipment theft. The method offered has high resolution, yet requires <u>*no*</u> *additional hardware to be added to the products in which it is implemented. Implementation of the concept uses an innovative application of resources already present in all digital cable compatible devices plus the real-time analysis of characteristic data obtained by the subscriber device through direct observation of its environment.*

A system for automated device management is also presented wherein subscribers could self-activate attached devices without need for manual intervention by the cable system operator under normal circumstances.

INTRODUCTION

Digital Cable Appliances

Digital cable television appliances are becoming mainstream devices in the modern home. These devices may be stand-alone “set top boxes” that are either leased from the cable operator or purchased by the consumer through retail channels. Alternatively, the functionality of a digital cable appliance may be integrated directly into new television receivers as part of the “plug and play” initiative for digital television, as mandated by the FCC.

As the cost of implementing digital decoding capabilities in consumer products rapidly declines and the prevalence of digital programming on cable television systems grows, the cable industry is marching toward removal of all remaining analog television services from their systems to reclaim spectrum, reduce operational costs and reduce signal theft.

In the foreseeable future cable operators will need to supply their existing customers having legacy analog televisions, VCRs, etc. large quantities of digital converters in 3to maintain continued operation of those analog devices in an all-digital network and as part of the operator’s compliance with federal regulations.

Industry estimates indicate that there may be four or more legacy analog devices attached to the cable system in a typical household in addition to existing digital cable converters for premium service access and CableCARD enabled products. Because of the sheer volume of digital converters that the cable operators will need to deploy in support of the analog devices presently in their subscribers’ homes and the fact that analog devices connected directly to the cable network do not pay for advanced services such as electronic program guides, video-on-demand or pay-per-view services, cable operators have no method to recover the huge additional capital outlay required for supplying the advanced, two-way digital cable boxes currently available.

As a result, attention is now focusing upon providing very inexpensive, one-way digital converters for this purpose, delivering current analog subscribers like-for-like digital service at a significantly lower cost to the operator than would be encountered using the presently available advanced two-way devices. The cable operators, for regulatory and other reasons, intend to provide these one-way converters at no additional cost to their subscribers and believe that the cost of providing these devices can be more than offset through the recovery of valuable cable spectrum, elimination of signal theft and reduction of operational costs such as truck rolls for service connect/disconnect.

These simple digital converters are intended only for the most basic of service tiers, ones that are presently delivered in analog form and therefore have been left unprotected against unauthorized reception, unlike the current premium services which employ modern digital encryption. A conservative estimate is that more than one third of the channels carried in modern cable systems are presently analog basic services.

A May, 2004 press release from a major cable system operator, Cox Communications, indicates that roughly 11.5 million U.S. households steal these cable services each year at an industry cost of $6.5 billion in lost revenue annually.

The transition of the basic subscription tiers from analog services to exclusively digital services having encryption applied will eliminate most of the present forms of signal theft that occur because these new digital converters will be individually addressable by the cable operator. Unlike today, merely having physical access to the cable signal either through an unauthorized connection by tampering or because there hasn't been a costly dispatch of the cable operator's field personnel to the premises to implement a disconnect will no longer suffice for basic tier customers to receive services for which the cable operator is not compensated. This also applies to new digital television receivers if the owner has not obtained a CableCARD from the cable operator and had it electronically authorized for service.

The typical conversion scenario for the all-digital transition would be for a cable operator to upgrade a headend serving a community or city to carry basic tier content in digital form in addition to the analog format presently carried. Next, all current two-way devices deployed for decoding premium digital services are provisioned with new channel maps, directing them to receive only digital forms of content, including the new digital replacements for the analog tier instead of the present mixed format. In parallel, the operator will begin distribution of the new, low-cost one-way converters to existing subscribers based upon the number of cable outlets in the home that are reported by the subscriber as connected to a legacy analog device (VCR, TV, etc.). There is no way for the cable operator to determine the analog device count in a home without either surveying the subscriber or performing a physical audit inside their premises. The operator will likely deploy these new converter devices en-masse as each node served by a cable headend is converted from mixed analog/digital format to all-digital through the removal of analog services. A network node typically serves from 500 to 2000 customers and the converters must be available to all subscribers in a targeted node prior to cutover in order to avoid service interruption

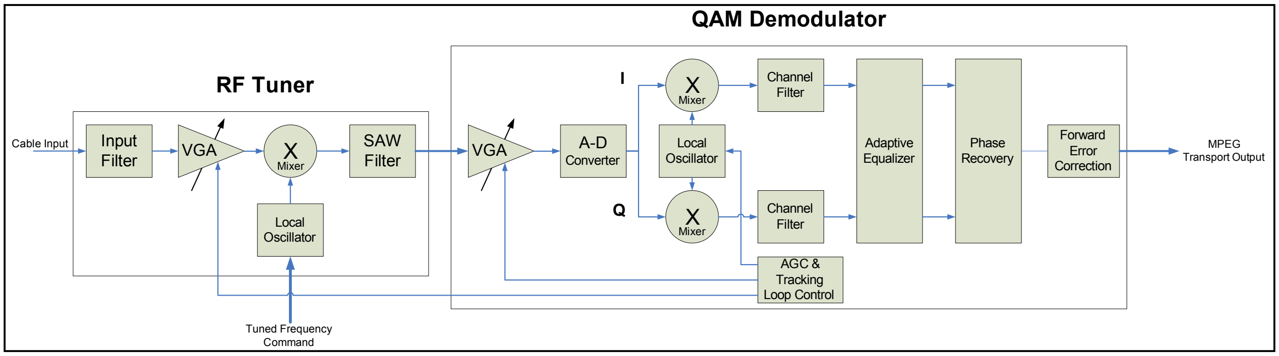

Figure 1. Generic digital cable network interface

While the introduction of all-digital services and low cost digital converters would seem to address all the issues of unauthorized viewing and signal theft, a new opportunity to deprive cable operators of fair payment for service emerges, made even more challenging because these low cost converters are likely only one-way devices,. When subscribers are contacted to determine the quantity of converters necessary for supporting the analog appliances in their home, the subscriber may intentionally "over-report" the quantity of analog appliances in the home. They can later provide the excess converters received from the cable operator to friends, family, etc. to "split the costs" of basic cable service. This is but one example of how one-way converters can be redistributed without the knowledge or consent of the cable operator in order to deny the operator of payment.

Since these new devices are issued by the operator to a valid subscriber, they remain authorized, but the cable operator is deprived of the full value of subscription revenue because the devices are present in locations other than the home of record for the authorized subscriber and the operator is therefore not compensated by the additional, unauthorized viewers.

Other one-way devices that attach to the cable network also suffer from the same vulnerability. The new CableCARD device for digital television is an example of such a device that suffers the same susceptibility to unauthorized redirection. Two-way devices, such as existing digital cable decoders for premium services, are less likely to suffer from this issue because there are means to electronically detect the location of these devices through headend interrogation and response, with the time delay to respond being measured to determine the cable distance to the device. In such an application, the response time values for two devices assigned to the same address can be compared for similarity and physical proximity inferred. While such a method provides some protection from unauthorized relocation, it will be shown later that it is an inferior method, suffering from poor resolution and other problems.

Sony's has developed technology to address the issue of detecting unauthorized relocation of one-way equipment consigned to the subscriber by the cable operator. The method in which it is accomplished uses resources already available in the appliance and adds no additional hardware cost to the product.

The Network Interface for Digital Cable

Regardless of the end use of a particular device, all appliances attached to the digital cable network share a common front-end topology. The elements that make up the network interface are available from a number of different manufacturers and may be offered in different configurations featuring flexibility, integration with other elements, support of multiple interfaces, etc. to serve as the differentiation between products.

The typical network interface is shown in Figure 1. The cable network interface consists of two major sub elements, the RF tuner and the QAM demodulator. The function of the RF tuner is to receive all signals on the digital cable system and to exclude all but one desired RF channel, containing the digital service of interest. The method used to select the desired channel is called heterodyning and this process is used to convert an entire block of incoming signals to a lower intermediate frequency (IF), with the signal of interest centered on a fixed, constant value, which is passed through a fixed, narrow filter to eliminate the unwanted carriers. The QAM demodulator processes the tuner's IF output, converting it to an error free digital stream of MPEG transport data carrying the compressed audio and video services.

Inside the RF tuner the local oscillator, controlled by the host processor, varies in frequency such that the nonlinear combination of the local oscillator signal and the incoming spectrum from the cable network inside the mixer results in the signal of interest emerging from the mixer centered at the fixed, lower intermediate frequency. The IF typically might be selected to be a value such as 44MHz. The input filter eliminates extraneous signals outside the range of valid cable audio/video services (54MHz to 863MHz) and the variable gain amplifier (VGA) is automatically adjusted so that the RF signals passing through the tuner and demodulator remain at optimum levels at all times. The final stage of the RF tuner is the surface acoustic wave (SAW) filter, which is an electromechanical device designed to only let a small band of signals centered at the IF value pass and all other RF energy to be heavily attenuated. The SAW only passes a standard 6 MHz wide channel and effectively rejects all others. The signal that emerges from the tuner is therefore only the channel carrying the service of interest and it has been downconverted to a fixed, standard (IF) frequency for processing by the QAM demodulator.

The QAM demodulator receives the incoming 6 MHz wide signal at the intermediate frequency, typically 44 MHz, and again amplifies it to a constant and optimum level through a second variable gain amplifier. The VGA is automatically adjusted by a closed control loop within the QAM demodulator. The signal is then processed by an analog to digital converter (ADC), which converts the incoming stream of time-varying voltages to a serial stream of binary bits representing the voltage levels of the signal at discrete time intervals. The ADC typically has 10 or more bits of resolution.

The digital stream is then split into two components, the in-phase component (I) and the out-of-phase component (Q). The Q term is used because the signal is in quadrature with respect to the I signal, meaning it is shifted 90° in phase. Phase separation occurs simultaneously with down conversion to a baseband signal, where the lowest frequency is 0Hz (DC) and highest frequency 6 MHz. This is in contrast to the incoming 44MHz IF signal, which has its content symmetrically centered ±3 MHz about the IF signal. The downconversion is accomplished through the use of a balanced mixer and the I-Q separation occurs because one of the two halves of the balanced mixer has a local oscillator signal output that is shifted 90° in phase relative to the signal applied to the other half of the balanced mixer. The outputs of the balanced mixer, I & Q, are then passed through identical channel filters that provide the appropriate shaping and attenuation of undesired processing artifacts occurring above the 6 MHz passband.

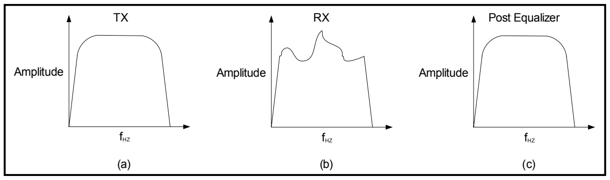

Figure 2. Digital cable channel spectrum

Next, an adaptive equalizer is applied to the outputs of the channel filters. The adaptive equalizer is an automatically self-varying digital filter network that continuously alters its filter characteristic (shape). Its purpose is to compensate automatically for echoes, reflections, dispersion, tilt, intersymbol interference and other distortions that alter the signal from its ideal, original form (Figure 2a) as it is carried by the cable operator's hybrid fiber-coax distribution network to the receiving device (Figure 2b), possibly over very long distances. By approaching the ideal of a matched filter, waveforms distorted through the communication path to the subscriber can be recovered and the data error rates for transmitted data reaching the phase recovery element (derotator) significantly reduced. This allows the system to operate successfully under non-ideal conditions, which are typical of real world applications.

The details of how the adaptive equalizer is realized differ between different QAM demodulator manufacturers. The general architecture is common between them and takes the form of a classic feed forward/feedback digital filter. A typical digital filter for such a purpose is shown in Figure 3.

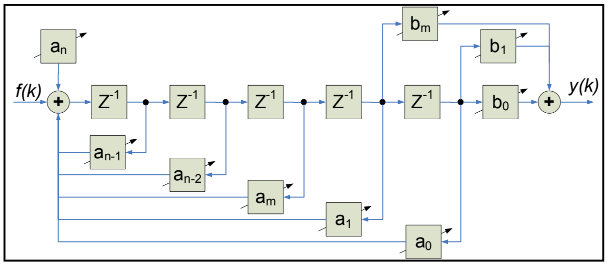

Figure 3. Adaptive equalizer

The structure of the filter is centered about a cascaded chain of delay stages (Z^{-1}), where the discrete time samples of the voltages seen at the demodulator input, converted to binary digital from by the ADC, are successively stored. The output of each delay stage tap, in addition to feeding the next cascade, may be fed back to the input or fed forward to the output. The tap feedback may be may be in conjunction with feed forward and either path may be employed exclusively on a tap-by-tap basis. Each feedback or feed forward path has associated with it an independent coefficient term. This term (a & b blocks in Figure 2) may provide amplification or attenuation of the tap output, depending upon the value of the coefficient. Because the equalizer is adaptive, the coefficients dynamically change under the control of a microprocessor or state machine. The values are varied based upon the characteristics of the equalizer output, as seen by the next processing stage, phase recovery. Typically a least mean square (LMS) algorithm is used to vary the tap values and converge upon the optimal solution. Adaptive equalizers in QAM demodulators vary in implementation between manufacturers. One design may have a total of 22 taps, where another may have a total of 40 taps – 16 feed forward and 24 feedback.

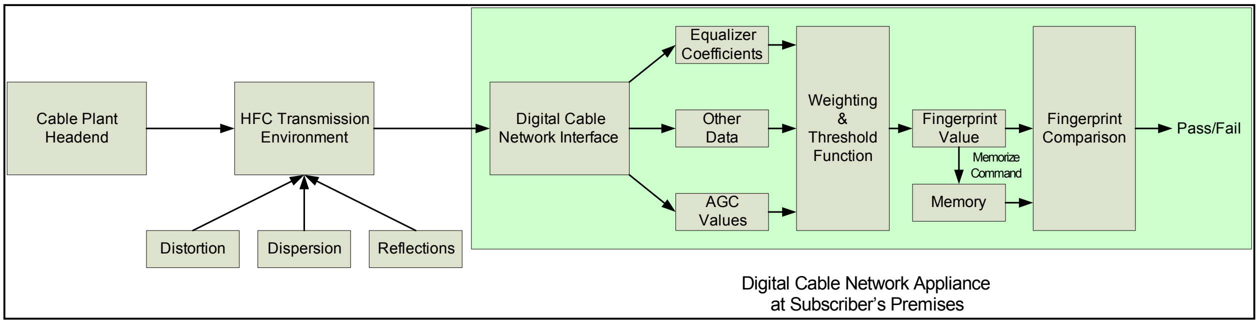

Figure 4. RF Fingerprint system

The output of the adaptive equalizer is then processed by the phase recovery block, also known as a detector or derotator. The purpose of the detector is to decode the combination of I and Q signals into a single data stream. The detector is able to expand the incoming data streams by a factor of $\log_2$(Modulation Order). This expansion is a factor of 6 for 64-QAM and 8 for 256-QAM, the two typical forms transmitted in digital cable. This expansion is the reason high transport data rates can be efficiently carried in relatively low spectrum bandwidths that appear to violate the Nyquist criterion. The coefficient values of the adaptive equalizer and the frequency setting of the QAM modulator local oscillator are both controlled by a microprocessor or state machine based upon the success of the detector to "lock" i.e. to recover valid data.

The last processing stage, the forward error corrector (FEC), applies a variety of algorithms to the raw recovered digital cable data stream to reduce the likelihood that any of the data has been corrupted in addition to formatting it appropriately for recovery of video and audio services as an MPEG transport stream. It is in this stage that de-interleaving, Viterbi (trellis) decoding, de-randomization, Reed-Solomon error correction and MPEG formatting occur. Some overhead data unique to the operation of these stages are removed from the stream so that the final MPEG transport emerging from the demodulator is identical in form, content and data rate to what the cable operator inserted into the corresponding QAM modulator at the headend for transmission.

Further processing is done to decrypt, demultiplex, decompress and convert the content to a form suitable for display on a television. These steps, while vital to the proper function of a digital cable appliance, are beyond the scope of this document.

SONY'S "RF FINGERPRINT" TECHNOLOGY

The ability to detect changes in location of a one-way digital cable receiving device is based in large part upon the adaptive equalizer. The equalizer, as indicated, acts as a matched filter to the communications channel. As a result, the values contained within the equalizer's coefficients can be mathematically manipulated to show the transfer function of the communications channel that influences signals passing through it. Stated differently, the values of the coefficients, taken as a set, represent at a specific point in time the sum total knowledge of all mismatches, reflections, phase variations, gain variations, echoes and other perturbations of the transmission media upon the transmitted signal. The fact that the QAM demodulator is able to achieve and maintain signal lock under a given environment validates that the state of the equalizer at that time is such that it accurately reflects the knowledge of the plant's effect upon the system so it can negate those effects and lock successfully. The tolerance to a suboptimal equalizer configuration is low, given the small vector error radii for either the QAM-64 or QAM-256 formats used in digital cable. The vector error radius is the composite of effects due to both amplitude and phase distortions upon a received signal.

Since the filter coefficient set is directly representative of the transmission environment, it responds dynamically to any changes in that environment. The low order feedback taps are most affected by high frequency trends, such as impedance variations at the connection or connector on the back of the appliance, reflections within the cable from the house splitter(s), etc. The middle taps are more predominantly affected by variations in the characteristics of the cabling to the tap and distribution amplifier, while the highest order taps are sensitive to channel tilt, dispersion, etc. This data, when combined with the AGC information which indicates total gain required for a constant signal level input, provides the basis for a very characteristic fingerprint of the environment where a specific cable appliance is installed.

Research by Sony indicates that the equalizer is so sensitive to such changes that one can distinguish between the short cables coming from different ports of an RF splitter to a bank of attached digital cable appliances fed by a single common source. In this case, the devices were all within one meter of each other and had identical cable lengths, yet the values observed for each device were unique and over time were relatively invariant.

If we let an equalizer coefficient be represented by a±jb, then H_1, the matrix of all equalizer coefficients representing the state of the system at one point in time, *i*, can be represented by:

$$\mathbf{H}_{1,i} = \begin{pmatrix} a_0 & b_0 \\ \vdots & \vdots \\ a_n & b_n \end{pmatrix} \qquad (1)$$

Likewise, if we let the gain value of one of the multiple nested AGC loops be represented by k, then H_2, the matrix of all AGC coefficients representing the state of the system at one point in time can be represented by:

$$\mathbf{H}_{2,i} = \begin{pmatrix} k_0 \\ \vdots \\ k_n \end{pmatrix} \qquad (2)$$

If one were to capture the equalizer tap coefficients and AGC data from a digital cable appliance, then applying an algorithm to allow the weighted summation of the coefficients a weighting function, based upon the expected statistical variance, to create a single scalar, a unary value representing the unique “fingerprint” of the environment of the device could be expressed. The threshold and weighting functions could be made unique to a particular operator and are kept secret to reduce the likelihood of tampering.

The algorithm for these operations then looks like:

$$Fingerprint_i = \Upsilon\left(\mathbf{H}_{1,i}, \mathbf{H}_{2,i}\right) \qquad (3)$$

This fingerprint value is evaluated and stored in the digital cable appliance memory upon receipt of a command message, such as an EMM, from the cable operator. The stored value should be secured through encryption and digitally signed to detect tampering.

The Fingerprint Algorithm

Most of our current research on the RF Fingerprint concept is focused upon refining the algorithm used to calculate the RF Fingerprint, specifically the coefficient values of the weighting matrix, based upon experimental observation of actual cable appliances *in-situ*. The generalized form of the algorithm to calculate the fingerprint value based upon one manufacturer's implementation of QAM demodulator is:

$$Fingerprint = \sum_{i=0}^{39}(Tap_{i,a} \bullet W_{i,a}) + \sum_{i=0}^{39}(Tap_{i,b} \bullet W_{i,b}) + SF \qquad (4)$$

Where *W* represents a value in the weighting coefficient matrix associated with a particular equalizer tap and *SF* represents the equalizer scale factor that is used to normalize all equalizer tap coefficients.

In order to determine the appropriate values for the weighting coefficients, tools were created by the team to remotely collect equalizer coefficient and other data from digital cable appliances installed throughout the Sony cable test network, an elaborate system serving the entire San Diego corporate campus closely emulating a commercial cable television network. Devices were sampled at three minute intervals and remotely tuned to services on multiple frequencies. The data gathered was subsequently compiled into a large database for further analysis.

One of the first items confirmed was the repeatability of the equalizer configuration for a given subscriber drop and cable device. Repeatability was judged based upon the measurement of the standard deviation over a four day period. Figure 6 shows the results of one such data collection experiment where two different digital cable devices were attached to the test network for a statistically meaningful period. At the end of that period the two devices exchanged locations and data collection was restarted for the same period. As can be seen in the graph, not only is the data generally quite repeatable for a given device, but the dispersion tracks the location, not the device.

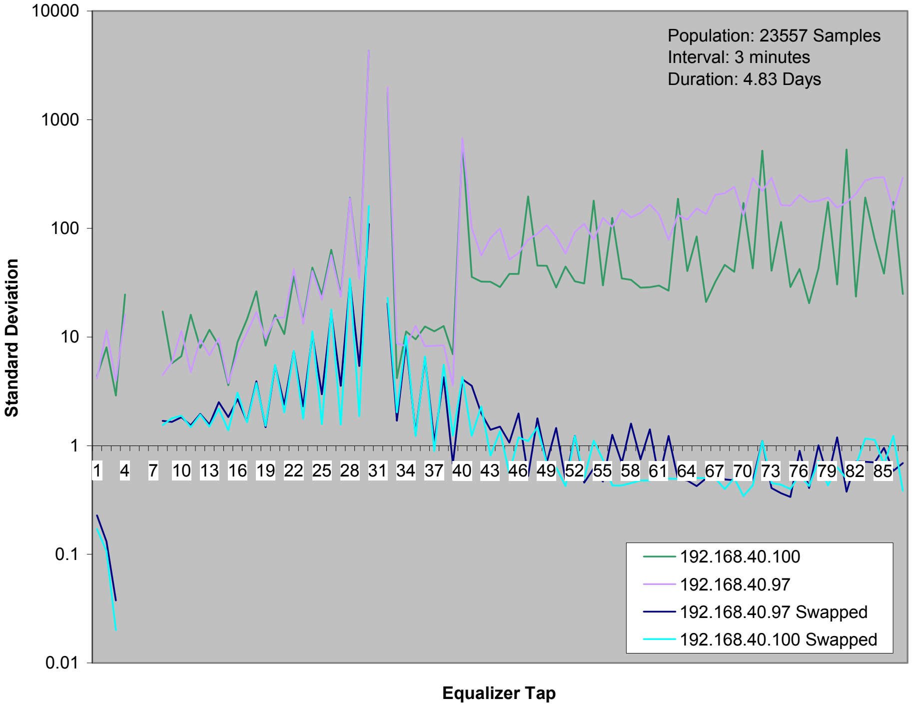

Figure 5. Positional uniqueness

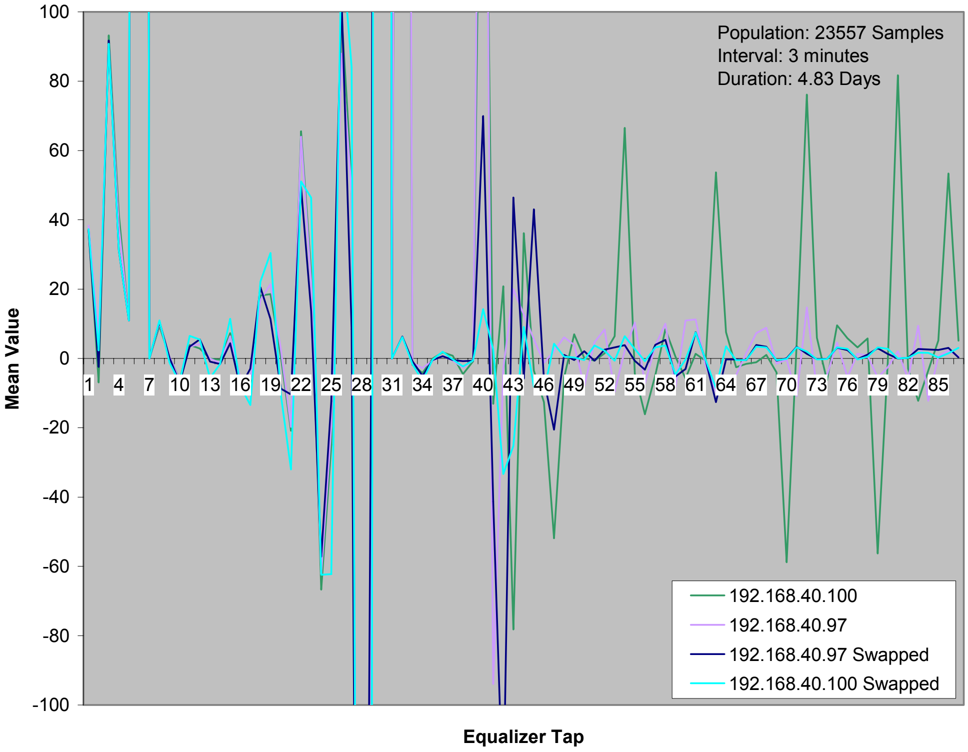

Figure 6. Equalizer coefficient repeatability

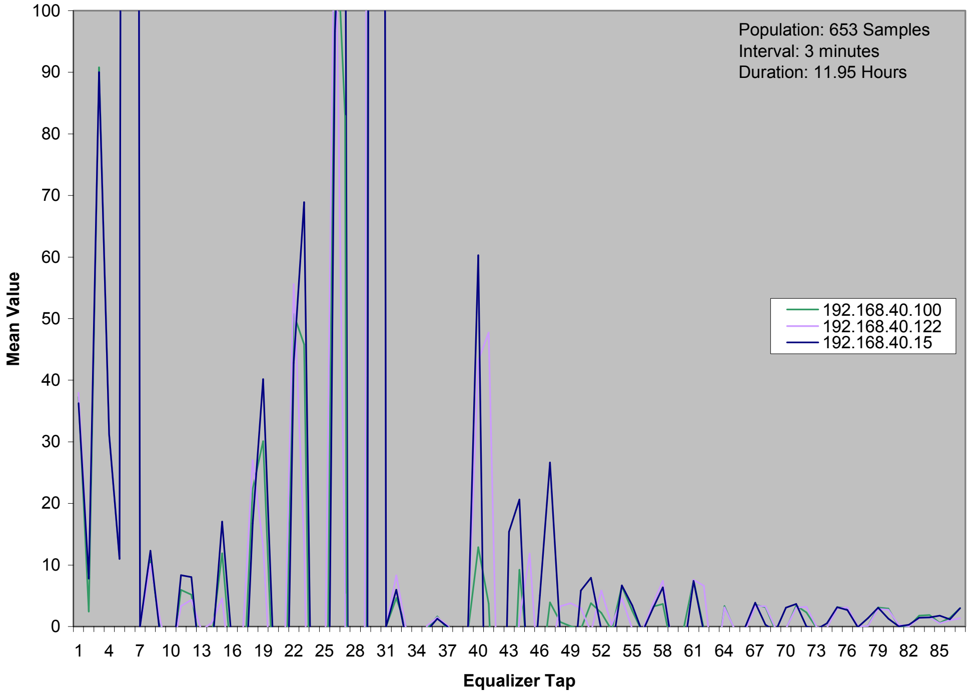

Figure 7. Uniqueness under worst case conditions

Using the data collected during the same experiment, Figure 7 shows that each of the four cases (two digital cable devices in two different locations) possesses a unique signature, allowing each to be distinguished from another device/location. The purpose of the weighting matrix is to selectively amplify those equalizer tap and AGC coefficients that express "uniqueness" terms and to attenuate those terms that contribute little in the context of distinguishing devices or tend to be unrepeatable.

In order to evaluate a worst case scenario, three cable appliances were connected through identical one meter long cables to a common splitter fed by the test network. The QAM performance of the three test units were monitored using four discrete frequencies at three minute intervals for a twelve hour period. The results of the investigation are shown in Figure 5. Confirmed was that even in an apparently identical RF environment and close physical proximity to ensure consistency of other environmental factors, the three different devices were distinguishable based solely upon equalizer and AGC coefficient values.

In practice, an installation having only one meter service drop lengths would seldom be seen and could actually be disregarded by the algorithm comparing fingerprint values to avoid false alarms due to product relocation from room to room within a home. However, it does prove that the concept is robust and applicable to high density dwellings such as apartments and dormitories where even two way methods, such as the one used in DOCSIS, fail. The DOCSIS method, for example, can only resolve location to within 63 meters, much more than the cable length differential between adjacent apartments. This is because DOCSIS and other proposed schemes use time delay measurement as the determining criteria. These other schemes also require some form of two-way communication. The RF fingerprint scheme is immune to issues plaguing methods solely related to cable length and works in a purely unidirectional environment as well as bidirectional environments.

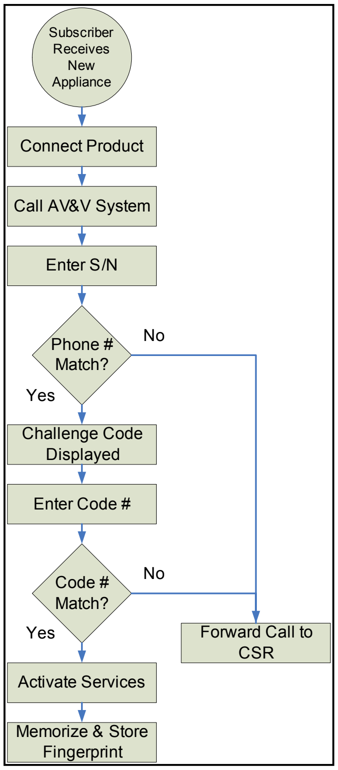

Figure 8. Digital cable appliance activation process

Operational Scenario

Regardless of the specific details associated with the implementation of the algorithm to calculate the fingerprint value, an operationally practical means of deploying a system employing RF fingerprint technology is necessary. Such a system must be automated to the greatest extent possible in order to reduce operating costs and to maximize flexibility. The practical implementation of a system employing RF fingerprinting is as follows:

1. A subscriber receives a fingerprint equipped appliance from the cable operator. The product contains labeling indicating "Call XXX-XXX-XXXX from your home phone after connecting the device to both the cable network and television for activation". This is identical in concept to the process now followed for activation of home satellite television receivers and credit or ATM cards issued through mail by the major financial institutions.

2. The subscriber follows the instructions and calls the number on the appliance label after installation, as indicated. An automated validation and activation (AV&V) system at the cable operator receives the call and prompts the subscriber to enter the serial number of the cable appliance using the keypad on the telephone and to press the "#" key upon completion.

3. Upon receiving the "#" key input, the AV&V system confirms the validity of the entered appliance serial number. The system then looks through its subscriber database and finds the record for the subscriber issued the appliance having the entered serial number. It then reads the subscriber's home phone number from the database record. Using Automated Number Identification (ANI), a non-maskable form of caller identification used for logging calls to toll-free telephone numbers (and 911 calls), the AV&V system then confirms a match between the number of record and if unsuccessful, refers the call to a customer service agent. This step validates that an authorized subscriber is attempting to activate the appliance issued to them by the cable operator.

4. If the ANI and phone number on record match, the AV&V system then sends a control message (EMM) to the appliance having the serial number the subscriber entered by phone. This EMM commands the appliance to display, on the subscriber's television screen, a challenge number sequence contained within the EMM message and generated at random by the AV&V system. The AV&V system then instructs the subscriber to enter into the telephone, the number displayed on the screen using the keypad on the telephone the and to press "#" key upon completion.

5. Upon receiving the "#" key input, the AV&V system confirms the validity of the entered challenge number and if unsuccessful, refers the call to a customer service agent. This step validates that the authorized subscriber is attempting to activate the appliance issued to them by the cable operator at the home on record.

6. If the challenge sequence is successful, the AV&V system sends another EMM to the now validated appliance, commanding it to perform two steps

A. Activate the services authorized for that subscriber

B. Calculate the RF fingerprint for the appliance at the present location and store it in persistent memory.

At periodic audit intervals, determined either by EMM or through self-initiation, which uses a timer resident in software, the appliance collects data and calculates an electronic fingerprint value, comparing it to the reference value stored in memory. If the calculated value is within predetermined

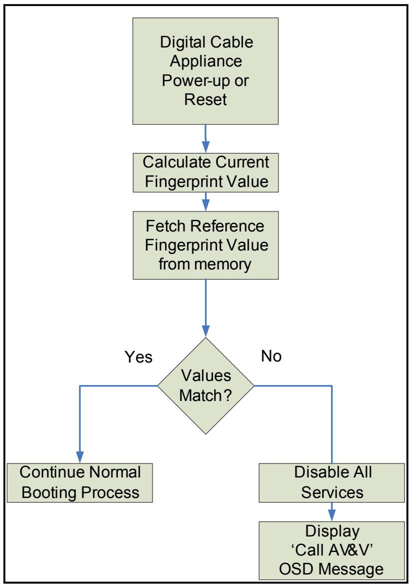

Figure 9. Digital cable appliance location audit process at reboot

limits, no further action is taken until the next audit period. If the new value for the fingerprint is sufficiently different from the stored reference value, then the reference value in memory is updated with the new reference value.

Whenever the appliance is rebooted or otherwise reset, signifying a lapse in network connectivity where the appliance may have been relocated without the authorization of the cable operator, the appliance collects data and calculates an electronic fingerprint value, comparing it to the reference value stored in memory. If the calculated value is within predetermined limits, the device continues the booting process and services are restored. If the match is unsuccessful, all television services are automatically self-deauthorized on the appliance, with an on-screen message generated and displayed on the subscriber's television screen indicating that the cable operator must be contacted at the AV&V telephone number contained within the message for appliance reactivation. This message occurs because the appliance has determined that an unauthorized relocation has possibly occurred. When the subscriber calls the displayed telephone number, the AV&V process is executed and upon validation, the location of the device is re-evaluated.

CONCLUSION

RF fingerprinting technology is one element in the toolkit available to address issues of service and equipment theft in cable television systems. Implemented in a digital decoder and coupled with simple content encryption techniques, a complete solution providing both the quality of service seen in an all-digital network as well as the system security and compensation for services delivered previously encountered only in premium digital services. All this is possible in the lowest possible cost, one-way customer premises equipment. The implementation of RF fingerprinting does not add hardware cost to the cable device and can be implemented in any digital device attached to a cable television network.

On-going development of this technology continues to focus upon optimization of weighting matrices as the technology is matured. One major U.S. cable operator has already specified the inclusion of this technology in their current system upgrades to all-digital delivery and draft specifications of the management and control aspects have been recently completed. It is quite likely that within the next 18 months, a commercial example of RF fingerprinting technology will be available and in the hands of the public.

ACKNOWLEDGMENT

The author would like to thank Eric Holcomb and Aran Sadja, both of Sony EMCSA in San Diego, for their significant contributions to the development of the RF fingerprint technology as well as the tools and systems implemented to perform automated data collection in order to validate the concept.

REFERENCES

1. ITU-T Rec. J.83:1997, *Digital multi-programme systems for television, sound and data services for cable distribution.* Geneva: International Telecommunication Union, Apr. 1997.
2. ISO/IEC 13818-1:2000, *Information Technology – Coding of moving pictures and associated audio – Part 1: Systems.* Geneva: International Organization for Standardization/International Electrotechnical Commission, Dec. 2000.
3. B. P. Lathi, *Signals, System and Controls.* New York: Harper & Row, 1974, pp. 207-214 & pp. 428-456.
4. A. Bruce Carlson, *Communication Systems*, 3rd ed. New York: Mc Graw-Hill, 1986, pp. 514-517 & pp. 550-554.
5. Edward A. Lee and David G. Messerschmitt, Digital *Communication*, 2rd ed. Boston: Kluwer Academic, 1994, pp. 442-550.
6. Richard E. Blahut, *Digital Transmission of Information.* New York: Addison-Wesley, 1990, pp. 159-170.