Conditional Access Interoperability in Digital Broadcasting

Nerey H. Mvungi

***Abstract*—**These instructions give you guidelines for preparing papers for conferences or journals. Use this document as a template if you are using Microsoft Word. Otherwise, use this document as an instruction set. The electronic file of your paper will be formatted further at JIVE. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column. Page margins are 1,78 cm top and down; 1,65 cm left and right. Each column width is 8,89 cm and the separation between the columns is 0,51 cm.

***Keywords*—**Business model, interoperability, conditional access, digital broadcasting.

I. Introduction

DIGITAL television can be delivered to users via terrestrial transmissions, satellite transmissions, cable, or some other medium. An appropriate Set-Top-Box (STB) is required to provide interface between signals from the different

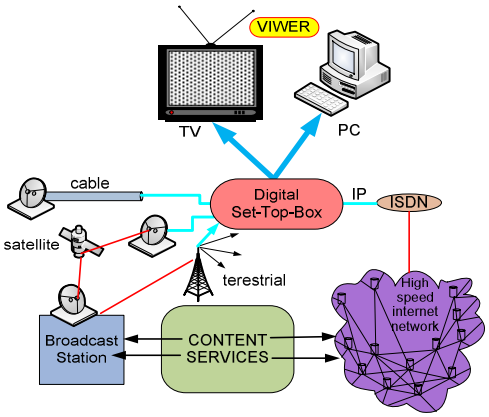

Fig. 1 Role of Set-Top-Box

transmission media and the display devices. In the digital broadcasting era the STB serves as an interface between digital broadcasting and existing analogue television sets to facilitate their use for digital broadcasting reception, see fig. 1.

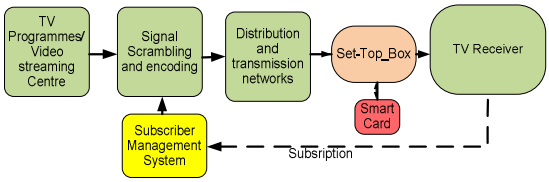

Fig. 2 Basic CA System Structure

N.H. Mvungi is with the School of Informatics of the College of Informatics and Virtual Education of the University of Dodoma, P.O.Box 490, Dodoma, Tanzania. (e-mail: nhmvungi@udom.ac.tz).

STB is an electronic box containing a collection of a number of small functional blocks or modules, with each module

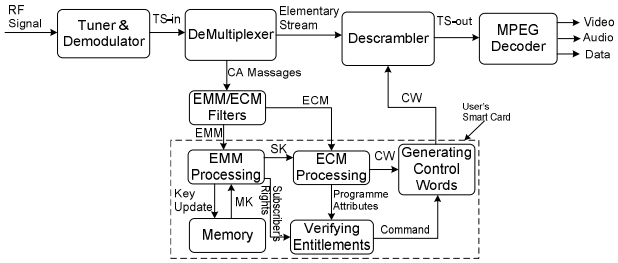

Fig. 3 CA Reciever Side

performing a well defined function. It has the necessary hardware, software, and interfaces to select, receive, unscramble and view the programmes. In digital broadcasting environment both free-to-air and pay-per-view services are realized in terrestrial broadcasting. Many services provided via digital television platforms will be encrypted in order to protect the intellectual property rights of the creators and packagers of content. Thus, conditional access systems are an important component of digital television delivery platforms

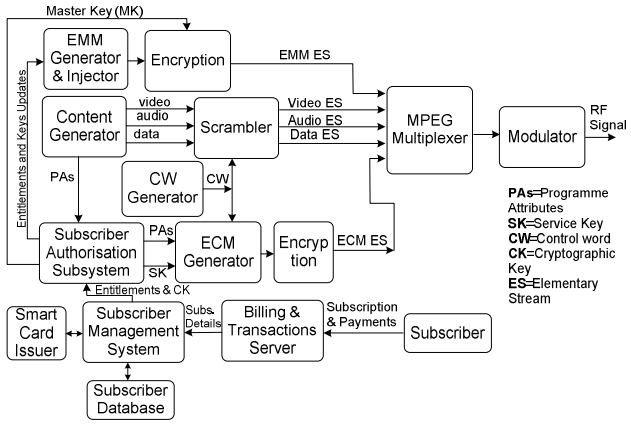

Fig. 4 CA Transmitter Side

and have an impact on actual and potential competition among platforms. A conditional access (CA) system basic structure is shown in fig. 2. Fig. 3 shows the structure of the CA system at the receiver side and Fig. 4 is for the transmitter side [13]. Broadcasters go for pairing of smart card and stb to ensure that CW is always scrambled when transmitted outside the stb or smart card (fig. 3).

Conditional access systems offer a means of ensuring that only authorized subscribers are able to view a particular package of programming. They serve as gateways for the delivery of audiovisual information. As a result, conditional

access service operators play an important gatekeeper role [1,2,11]. The CA system can be incorporated in the STBs. The challenge is interoperability between different conditional access systems and hence of STBs because of the different CA proprietary implementations. Interoperability ensures that one STB can be used by consumers to access services controlled by any CA system and/or the transmission media to the convenience of the user and the take up of digital broadcasting. A global interoperable solution is a major challenge since an end-to-end solution will involve addressing audio codec, video codecs, security, meta data, interactivity, streaming protocol and transport network.

There have been concerted efforts to standardize the CA system like those reported in DVB [3], NRSS [4] and DAVIC [5] to facilitate interoperability of CA used in STBs. There are two principle approaches that influence implementation of CA system; SimulCript and MultiCript. The SimulCrypt approach uses common ways of scrambling MPEG content and transferring CA messages to the STB via the MPEG transport stream. The MultiCrypt approach allows an STB to operate with different CA systems by using a detachable module, typically a smart card or PC card or CI module that implements a particular CA system. The interface to this module is standardized. It is significant to note that the temptation to use bundling CAS and content provision and closing the STB to other competitors business model is very high, to force premature market capture. There is also the fear of free riders by new comers.

The different solutions to make CA used in STB interoperable have limitations; for example SimulCript need service providers to share systems, which increase bandwidth usage while for MultiCrypt are inflexibility, more costly and offer limited functionality. There are options to use software download over-the-air or having common interface. It was correctly urged by Oftel of the United Kingdom that "If conditional access systems prove expensive to duplicate and if the issue of conditional access is not sufficiently addressed in the regulatory regime, it might then be possible for one company to dominated the delivery of broadband channels by satellite, and by extension by an expanded terrestrial system as well." 30 Hence, regulations shall have significant role to play here.

II. MULTICRYPT AND SIMULICRYPT

Multicrypt is a common interface approach that would allow detachable conditional security modules to be connected to the set-top box. By inserting different CI cards (usually PCMCIA cards), viewers could use the same set-top box to choose among programmes using different conditional access systems. However, a separate CI module would be necessary for each CA system used by a broadcaster/service provider. Proponents of Multicrypt argue that there should be a common interface between the consumer's basic receiver unit and the access module unit to ensure that no conditional access service operator will obtain a dominant market position. They assert that with Simulcrypt, conditional access service operators will have an incentive to close out competing programme providers by denying them access to the set-top boxes.

Simulcrypt is a method whereby scrambled signals can be sent simultaneously to receivers using different conditional access systems but the same DVB unscrambling algorithm. Broadcasters transmit to the target set-top box by sending all of the necessary messages simultaneously. Simulcrypt enables service operators to send signals comprehensible to decoders that do not all have the same conditional access system. Proponents of Simulcrypt argue that Multicrypt would make the production of set-top boxes more costly. They also assert that, without proprietary technology, companies will not take the large financial risk necessary to get decoders to consumers.

III. OPERATIONAL STATUS IN DIFFERENT COUNTRIES

The operating conditions differ in North America, Europe

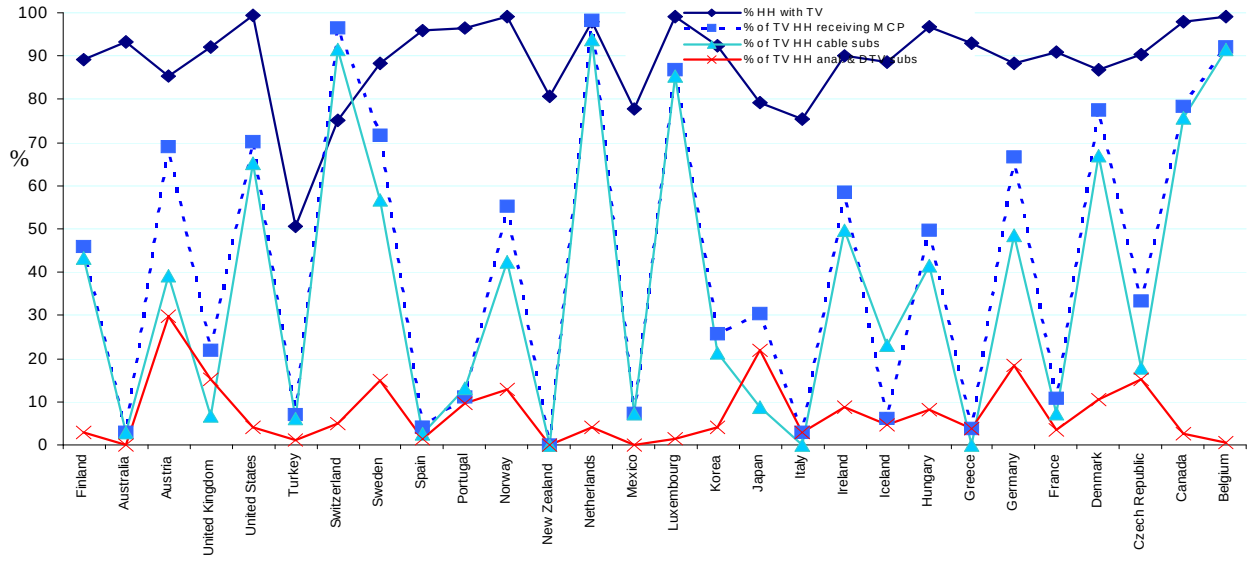

Fig. 5 TV Penetration in OECD Countries in 1996 (HH is house hold, MCP is multi-channel programmes) [11]

and Japan. The United States digital broadcasting through satellite service providers have different conditional access systems 22. However, there are companies like DirecTV and USSB that behaved like a single provider by offering complementary products. They used same CA system and shared the same receiving equipment. However, one could subscribe to both or either.

In Canada, Satellite broadcasting services were using different transmission technologies hence it was not easy for customers to switch from one service provider to another. Their conditional access system was designed for use within Canada because copyright and regulatory constraints limit the areas in which the service may legally be provided. The set-top-boxes were clearly marked and programmed for reception of Canadian broadcasts or for US signals only to ensure the network services are sold only in their respective countries [24].

France had three main satellite digital broadcasting service providers in the late nineties where two of them signed an agreement to use simulcrypt that enabled them share the same smart card. One of the companies had to pay the other access fees.

In Germany eight of broadcasting service providers formed a Multimedia Betriebsgesellschaft consortium that used SECA technology for conditional access; however another main operator used irdeto technology. However, there was agreement to offer programmes in a non-discriminatory way, hence agreed to broadcast all programmes from the different broadcasters via cable network where they could be accessed using a single stb.

Spain adopted rules from the onset to ensure compatibility of conditional access systems where all digital satellite broadcasting were received using a single set-top-box. Japan on the other hand was working in the late nineties to have universal receiver and decoder. Sweden and Norway each are using single conditional access systems in their respective countries.

Australia favoured common interface, allowing for the use of multiple conditional access systems, so as to support manufacturers' proprietary conditional access systems. It asserts that no transport service provider or operator should be allowed to present a barrier to the customer, or interpose a relationship between a customer and a service or content provider. According to the Australian regulatory change as of 1 July 1997 satellite subscription television broadcasting licences will be subject to the condition that their domestic reception equipment and subscriber management systems are accessible by other satellite broadcasting services 39.

A relevant observation was made by Oftel of the UK that when controlling conditional access technology it is essential that it is not used to distort, restrict or prevent competition in television and other content services. This can be significant when a conditional access service provider is also involved in broadcasting business while providing conditional access services to its competitors (or would-be competitors). This need be avoided wherever possible. The objective being to avoid artificial restrictions on consumers' choice of equipment, the range of services available via the equipment or the packaging of services." or interoperable across different networks using different CA systems.

IV. SOFTWARE DOWNLOAD OVER-THE-AIR (OTA)

Software downloading on the other hand is a form of MultiCrypt, and allows service providers to operate independent of each other. The method advocates that software downloading to STBs can enhance flexibility in CA-STB interoperability. When using software solution to achieve interoperability, it is essential to use widely accepted language while taking advantage of the increasing microprocessor computing power. The scheme introduces application interoperability that facilitates achieving CA-STB interoperability. A downloadable software (interoperability application) is used for communication between an STB application and the CA security module (smart card or PC card), inserted into the STB [10]. One approach to achieve interoperability between STB applications and standard security modules is by defining an API that provides low-level access to the security module. The interoperable CA sub-system (CASS) software that implements access to the security module via the API can be made downloadable and could be part of the application. A second approach uses the basic STB functions. The software that implements the CASS interoperable is made downloadable. This approach extends the idea of MultiCrypt to all CA software in the STB, making highly standardized security modules redundant. The basic STB functions needed by the CA system are made accessible to the downloaded CA software through APIs. The basic requirements for the system to operate are: The security module low-level communication with the STB be of MPEG-2 TS carrying encrypted services will carry in encrypted form the Entertainment standard type, a common scrambling algorithm be used and a few APIs need to be defined especially for this purpose. The challenge for this scheme is cooperation of STB vendors. The major problem here is being allowed or provided by proprietor of STB access to its internal parts.

V. CONDITIONAL ACCESS IN SET-TOP-BOX

In DVB, conditional access system standards are provided in specifications for Conditional Access (DVB-CA), the Common Scrambling Algorithm (DVB-CSA) and the Common Interface (DVB-CI). These standards define a method by which a digital television stream can only be accessed by those entitled having valid decryption smart cards. This is be realised by a combination of scrambling and encryption. Entitlement Management Message (EMM) containing list of pay TV services payees and duration and the Entitlement Control Message (ECM) carrying control word (CW). The CW is encrypted as ECM during transmission to receivers and the authority to decrypt the CW is provided by

EMM. The DVB scrambling algorithm has been standardized, but the algorithms used for ECM/EMM encryption are not. Hence, the different ECM/EMM encryption DVB CSA compliant algorithms for CA systems in use are closely guarded secret since security of a given CA system depends primarily on their efficiency. When the relevant decryption algorithm is embedded in the CA module of the STB it cannot be "Open Architecture" or interoperable across different networks using different CA systems.

The challenge for content service providers is to protect their paid services content from hackers. Their worries are founded since the common usage of CA in DVB has enabled tools and conditional access module emulators based on reverse engineering to circumvent encryption to exist. The different CA system vendors use long CW, a combination of software and hardware and continuously changing CW, ECM and EMM. The changing interval being different for the three and for different service providers. Television Par Satellite used monthly period for EMM that was lowered to 12 minutes after being hacked, British Sky Broadcasting used 6 weeks while digital+ used 3 days. The CW was being changed typically every 12 seconds. A large proportion of the systems currently in use for DVB encryption have been opened to full decryption at some point, however it does not imply that they are now insecure.

CW can be transmitted through different ECMs at once facilitating use of several CA systems at the same time, like CNN International that use up to 7 CA systems in parallel. Several companies provide competing CA systems; SafeAccess, VideoGuard, Irdeto Access, Nagravision, CoreTrust, Conax, Viaccess, Latens, Verimatrix, and Mediaguard (a.k.a. SECA) are among the most commonly used CA systems.

VI. DVB Common Interface

Another method to make to make a STB interoperable across different networks using different CA systems is to use of a DVB Common Interface (DVB CI) international standard. In this case the STB contains only those elements that are needed to receive "clear" broadcasts. The CA system is contained in an external module, which communicates with the STB via the common interface connector provided on the STB. Thus STB fitted with the DVB CI connector is interoperable across different networks using different CA systems. The user has to get the plug-in CA modules from different service providers.

The most important software in a STB is the operating system (OS) and the "Kernel" layer that is loaded into memory once the STB is powered up and remains there until the STB is powered down is the heart of the OS. The STB has a 'loader' to enable the TV operator to upgrade 'resident applications' or download 'OS patches' to STB and 'drivers' to control the various hardware devices. In addition the STB OS incorporate a set of Application Programme Interfaces used for high-level applications.

There is no standard STB OS. The broadcasters and consumer electronic companies promote their own in-house solutions like Power TV OS, Vx Works pSO System, Microware's DAVID OS-9, Microxoft Windows CE etc.

VII. Interoperable STB for Different Transmission Media and Compression Schemes

There are three basic transmission standards used in digital broadcasting; cable, satellite and terrestrial. A very significant feature of these standards is that they have identical source coding/compression and service multiplexing/transport based on MPEG – 2/4 standard(s). However, channel coding/modulation is optimized for the respective transmission media/standard. Thus whereas satellite and cable transmission are based on single carrier modulation schemes of QPSK and QAM, terrestrial transmission uses a multicarrier modulation scheme called Orthogonal Frequency Division Multiplexing (OFDM).Technology is available to enable interoperability among set-top boxes and to make single set-top-box compatible with prevalent digital video broadcast signals or compression-MPEG2, MPEG4, HD video, DVB-T (terrestrial), DVB-S (satellite) or DVB-C (cable). The drive for this has been subscribers desire to get more flexibility. STB is said to be interoperable if it can receive any service from any network. Another drive for interoperability from regulators' point of view is lowering the price of STBs to facilitate digital take up. The STBs should be based on an 'Open Architecture' and 'interoperable' across different networks to reduce their costs. There is no willingness to go for interoperability option as older players and early starters have invested heavily in creating the market for Direct-To-Home (DTH). It is common for DTH operators to sell their own customized STBs manufactured from third party vendors. The cost of the customized STB restricts mobility of customers from drifting to other DTH service providers. Furthermore, packages are used to lock customers to a particular service provider. In many countries, market forces have not managed to force for interoperability making regulators in many countries to intervene. It is a fact that interoperability norms will allow third party manufactures to independently sell STBs like in the case of GSM mobile phones. This in turn will invite tough competition among STB manufactures and help in lowering the cost of STBs and foster creativity in STBs.

VIII. Interoperability and Business Models

Enforcing interoperability in STBs for terrestrial digital broadcasting is expected to create new business model in the digital broadcasting market similar to what transpired in the mobile phone services. Things like video-on-demand or movie-on-demand or pay-per-view, cards on the line of calling cards where subscribers will be free to use services offered by different service providers by using just one STB. The price of STBs can only be lowered at a fast rate while improving functionalities if they are interoperable. In terrestrial digital broadcasting, there are several possible business models; the

content service provider centered, the MUXO centered, the conditional access service provider centered and the hybrid model involving both the content service provider and the multiplex operator.

A. *Content Service Provider Centered Model*

This business model shown in fig. 6 overlaps well with that used by most analogue terrestrial television broadcasters in Tanzania, hence the natural choice for them. Broadcasters are

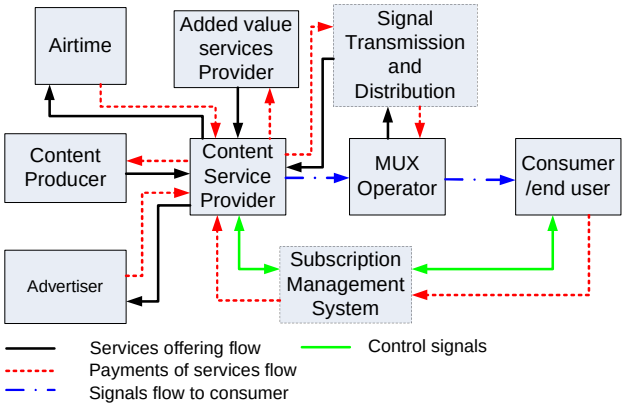

Fig. 7 Content Service provider centered model

skeptical on entrusting another entity to control collection of its revenue, which is not without basis. Many were swindled by their agents. In this model the content service provider (CSP) manages the subscription system and the data of all its customers. The CSP collects payments for providing airtime, contents, added value services and for advertisement and pays for services offered to CSP by other players in the broadcasting value chain.

Most subscription services for cable and satellite broadcasting services used this model. In satellite, the CSP rents space in the satellite, while in cable broadcasting delivery model the CSP either owns the infrastructure or rent space. Hence, the emerging conditional access broadcasting services providers are going for this model.

B. *The Multiplex Operator Centered Model*

The Multiplex Operator (MUXO) in this business model shown in fig. 7 control the subscription, the customer data base

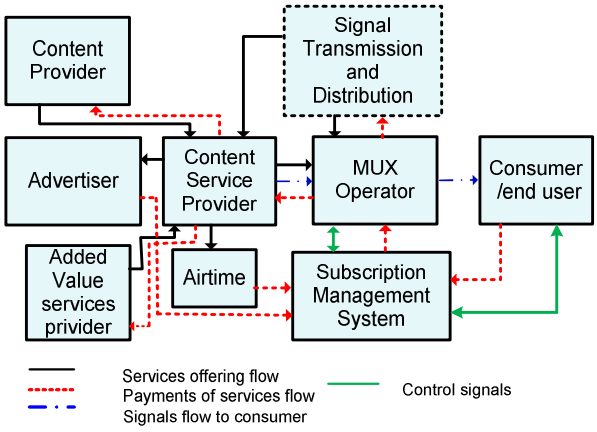

Fig. 7 Multiplex operator centered model

and collects payments for all services rendered to customers and pays the different players in the broadcasting value chain. In this model, the MUXO operates and manages the scrambling of contents from content service providers. This makes the position of MUXO very powerful in the broadcasting value chain. Although the regulations requires MUXO to provide services to CSPs in a fair and non-discriminatory manor and terms and conditions that promotes competition but in practice MUXO may choose who to carry and under which terms. The MUXO concentrates on marketability aspect of the contents. The MUXO operators in developing countries either owns a CSP or has partnership with a CSP hence tending to promote the satellite and cable broadcasting delivery model for digital terrestrial broadcasting.

C. *Hybrid CSP-MUXO Business Model*

The hybrid business model the MUXO administers subscription and customer data base. At the same time the CSP also paid for some of the services other than those involving

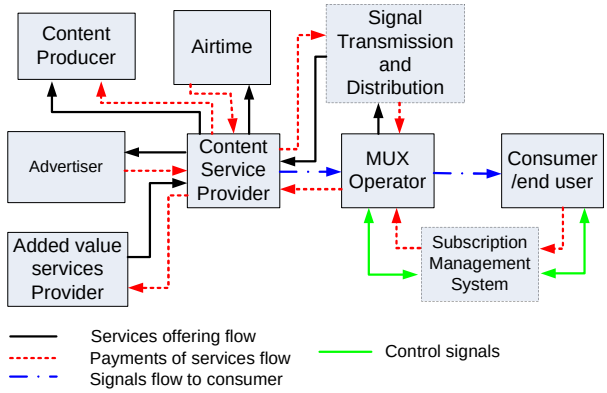

Fig. 8 Hybrid (MUX/CSP) centered model

conditional access. The services payable to CSP can be seen in fig. 8.

D. *The Conditional Access Service Provider Centered Model*

This business model introduces an additional service

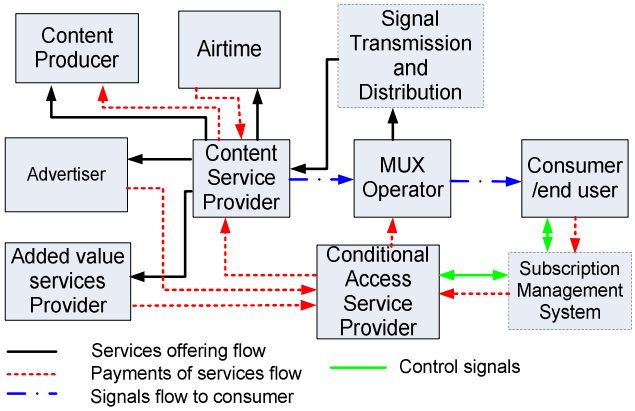

Fig. nx Conditional access provider centered model

provider in the broadcasting value chain.

XXXXdocument is a template for *Word (doc)* versions. If

you are reading a paper version of this document, so you can use it to prepare your manuscript.

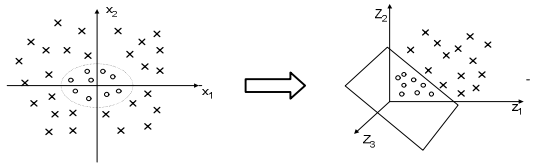

Fig. 3 Mapping nonlinear data to a higher dimensional feature space

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[3] H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[4] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[5] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

[6] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[7] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[8] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].

[9] M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

[10] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility (Periodical style)," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.

[11] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, July 1993.

[12] R. W. Lucky, "Automatic equalization for digital communication," *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.

[13] S. P. Bingulac, "On the compatibility of adaptive controllers (Published Conference Proceedings style)," in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8–16.

[14] G. R. Faulhaber, "Design of service systems with priority reservation," in *Conf. Rec. 1995 IEEE Int. Conf. Communications*, pp. 3–8.

[15] W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.

[16] G. W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IEEE Summer power Meeting, Dallas, TX, June 22–27, 1990, Paper 90 SM 690-0 PWRS.

[17] J. G. Kreifeldt, "An analysis of surface-detected EMG as an amplitude-modulated noise," presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

[18] J. Williams, "Narrow-band analyzer (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.

[19] N. Kawasaki, "Parametric study of thermal and chemical nonequilibrium nozzle flow," M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

[20] J. P. Wilkinson, "Nonlinear resonant circuit devices (Patent style)," U.S. Patent 3 624 12, July 16, 1990.

[21] *IEEE Criteria for Class IE Electric Systems* (Standards style), IEEE Standard 308, 1969.

[22] *Letter Symbols for Quantities*, ANSI Standard Y10.5-1968.

[23] R. E. Haskell and C. T. Case, "Transient signal propagation in lossless isotropic plasmas (Report style)," USAF Cambridge Res. Lab., Cambridge, MA Rep. ARCRL-66-234 (II), 1994, vol. 2.

[24] E. E. Reber, R. L. Michell, and C. J. Carter, "Oxygen absorption in the Earth's atmosphere," Aerospace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (420-46)-3, Nov. 1988.

[25] (Handbook style) *Transmission Systems for Communications*, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.

[26] *Motorola Semiconductor Data Manual*, Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.

[27] (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)

[28] J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com

[29] (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)

[30] R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3)*. pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar