CSMAC Enforcement Subcommittee
Findings and Recommendations
November 17, 2017

Contents

Subcommittee Members

Members included Mary Brown, Mark Crosby, Dale Hatfield, Paul Kolodsky, Mark McHenry, Janice Obuchowski, Rick Reaser, Dennis Roberson, Andrew Roy, Mariam Sorond, Bryan Tramont, Jennifer Warren and Bob Weller. NTIA advisors were Bruce Jacobs, David Reed, and Yang Weng.

Questions from NTIA

1. What options do you see for making enforcement more robust, including by increasing automation to prevent interference, and to identify and respond to interference when it does occur in the near or longer term?

2. What are the principal technical and operational options for enabling automated enforcement, at both the network and device levels, and how would you address cybersecurity and privacy requirements? Please consider, among others, options related to: station IDs; data cloud/fog architectures; and crowd-sourcing.

3. What options for automated enforcement are unique to the development and deployment of 5G technologies/applications?

4. What steps do you recommend the Federal Government, specifically NTIA, take to implement automated enforcement processes? What steps will the private sector need to take? Please consider steps relating to technical, process and policy issues, including potential operator-to-operator coordination approaches.

Introduction

The subcommittee did not have sufficient time to address every question in its entirety. We did not address the aspects of automated enforcement addressing cybersecurity requirements, steps that the private sector can take, or operator-to-operator coordination approaches. We believe that there is a possibility to address those questions in future CSMAC groups. In response to the above questions, the Enforcement Subcommittee has identified five (5) findings and is proposing five (5) recommendations as NTIA action items.

Findings

1. Most companies hire consultants to locate and identify interference, though some larger companies (*e.g.*, wireless carriers) have internal teams. Current framework limits

the ability of consultants to precisely locate and identify sources due to privacy and access issues.

2. Sources of interference with regard to developing automated enforcement broadly divide into three types (see also Addendum I):

   a. Intra-system (self-interference). Interference due to mechanisms entirely within the control of the system operator. This interference is often due to poor system implementation practices, errors in equipment configuration, and less-commonly, malfunctioning equipment.

   b. Proximate (nearby) interference.[1] Interference affecting just one site or user. This interference is often the most challenging to resolve, as it may not be observable using external equipment and there are often multiple sources. For example, the exquisite sensitivity of tower-top antennas with low-noise amplifiers often means that the interference is not "visible" to external observers and so location of the source becomes difficult. Proximate interference also includes cases where an equipment issue may impact multiple sites or users, but the interference is localized to individual sites.

   c. Widespread interference. Interference affecting multiple sites or users. This interference is generally easy to identify because it is usually strong, but there may be challenges in identifying the precise source(s) due to access or privacy issues, for example.

3. "Automated" systems are relatively primitive or limited to specific standards-compliant systems (*e.g.*, cellular PCIs, WiFi SSID/MAC addresses, Structured packet Detection, Preamble Detection, IEEE 802.11y identifier including a geo tag, etc.). There are significant challenges that these systems must overcome. (See FCC TAC statement of work for next generation enforcement architecture.[2]) Currently, there are basically four categories of automated systems that are used for transmitter identification and specifically interference identification, and one system that is presently under development:

   a. The first is the class of sophisticated systems that have been developed to assist wireless carriers in identifying transmissions in the various cellular bands. These

[1] Proximate interference also includes cases where an equipment issue may impact multiple sites or users, but the interference is highly localized to individual sites.

[2] https://transition.fcc.gov/oet/tac/tacdocs/reports/2016/A-Study-to-Develop-a-Next-Generation-System-Architecture-V1.0.pdf

systems have dominantly supported cellular coverage studies, but have also been used to identify the sources of interference in specific cellular bands and geographies. Examples of such equipment is the Rohde and Schwarz TSMA Autonomous Mobile Network Scanner[3] and Keysight Channel Scanner[4].

b. The second class is perhaps best represented by the professional "Interference Hunters" who have developed sophisticated interference detection systems often composed of very expensive customized configurations of spectrum analyzers, unique antennas systems, and data capture and analysis software systems. These systems usually can be configured for a variety of spectral bands to address a broad set of communications, radar, and navigation systems.

c. The third class is composed of applications running on tablets and smart phones that have been developed to support transmitter identification and monitoring, usually in specific bands and for specific applications (*e.g.*, Wi-Fi "sniffers" in the 2.4 and 5 GHz unlicensed bands), which can discover signal strength, SSIDs and MAC addresses. These applications can be useful in interference identification, especially if they are connected through a crowd sourcing arrangement.

d. The fourth class is also exemplified by Wi-Fi networks, where access points can operate not just as simple routers, but can natively or via a cloud architecture, transmit unique identifiers, including geographical tagging information. This capability (802.11y) was originally developed for use in the television band to help address issues of unlicensed-to-broadcast reception interference. In addition, standards exist that allow unauthenticated queries to an access point (802.11u) that would, if implemented to do so, permit a "who are you" query from an 802.11 client device. Unfortunately, these latter two examples aren't appropriate for providing broad spectral coverage or coverage of widely varying transmission types (*e.g.*, radars and satellites).

e. Spectrum Access System (SAS) entities may play a significant role in the future in facilitating automated interference mitigation and enforcement activities. However, automated enforcement activities conducted by SASs must be precisely defined including, among other issues, what specifically is necessary to enforce in what bands and where geographically, along with concurrent rights, responsibilities, reporting requirements, and enforcement limitations. A preliminary set of questions regarding the potential to use the resources of SASs were distributed to the SAS

[3] https://www.rohde-schwarz.com/us/product/tsma-productstartpage_63493-103042.html
[4] http://www.keysight.com/en/pd-2664704-pn-N9951A/channel-scanner?cc=US&lc=eng and http://literature.cdn.keysight.com/litweb/pdf/5992-2056EN.pdf?id=2825675

community by the Sub-committee, and are attached to this document in Addendum II for NTIA's information and consideration.

4. Next generation wireless systems (*e.g.*, 5G) are providing additional challenges for automated systems. We are amid a veritable revolution in the physical layer of wireless systems. This revolution is in the process of completely disrupting the capabilities of the established spectrum sensing order.

    a. One notable, but not exclusive, source of disruption is the movement toward active antenna systems with multiple-antenna arrays. Multi-array systems use active antennas to achieve transmission gain, or reception gain, in a given spectral region, in order to enable much higher data rate transmissions. The resulting type of signal can be significantly more complex to detect, understand and analyze because it relies on the specific propagation path between the transmitter and receiver. For example, the signal can be spatially focused (beam forming) on the User Equipment (UE). This feature can make detecting a transmission source (here in particular an interference source) very difficult.

    b. Also, the move to the so-called millimeter wave (mmW) spectral region (*i.e.*, usually taken to mean spectrum at or above 24 GHz) can complicate interference detection and location. mmW systems use very wide spectral transmission bandwidths to enable very high data rates. Unfortunately, mmW signals also have very poor propagation characteristics relative to sub-6 GHz spectrum. This makes it more difficult to monitor the interference except at the victim receiver site. If the interference is intermittent, detecting its source can be very difficult indeed. Taken together, mmW Multi-Input/Multi-Output (MIMO) systems imply the ability to have very large numbers of antennas in a very small space.

5. Modern spectrum usage trends are such that many services utilize a number of separate bands and channels to provide the service. This is especially true for the next generation of cellular and other data services (*e.g.*, 5G). Therefore, automated enforcement systems (for bands that are being shared with those services) may be able to use more commercially novel interference management mechanisms.

Recommendations

1. NTIA should recognize that automation with regard to enforcement is not a panacea. Manual investigations will continue to be needed for the foreseeable future. However, NTIA should continue to establish and encourage capabilities and processes in order to someday enable more fully automated systems.

a. NTIA plans should include the investigation of better ground-up designs for the identification of problems (see database recommendation); and/or regulatory changes to address privacy concerns as well as to facilitate easier identification of interference and interferors.

b. NTIA should study the bounds of impact based on intermittent interference to ascertain levels that effect the performance of victim receivers. This will require establishing better definitions of interference. The output of this study will assist in the determination of the responsiveness and sensitivity needed for an automated system.

c. NTIA should analyze the different enforcement process 'stages' to determine the automation approaches and the costs/benefits of automation at each stage. Subsequently, NTIA should develop an automated enforcement architecture for shared spectral bands (an example is shown in Figure 1).[5]

2. NTIA should develop a standard for interference detection, classification, logging, and report generation software capabilities that could be mandated, when practical, for insertion into radios that share spectrum with federal systems. This should include the development of a machine-readable report standard for interference detection results (*e.g.*, time, location), classification results (bandwidth, cyclo-stationarity characteristics), and logging.

3. NTIA should investigate the establishment of an information sharing program/database of experiences of discovering and identifying interference. This would help enable automated identification of interference sources. NTIA should investigate who would pay for and who would operate the 5G enforcement activity. A few examples of such mechanisms are provided below[6] and a possible implementation for NTIA.[7]

---

[5] This includes the characteristics for enforcement software that goes on end-user devices (*e.g.*, 5G), and it includes the enforcement software that fuses the end user device enforcement reports together to localize and identify the interference sources. This includes software to control/remediate ("kill switch"). The architecture should consider privacy issues and security issues.

[6] The FCC's Technological Advisory Committee found that more extensive and detailed exchanges of information on interference incidents and complaints would be invaluable to industry researchers and systems designers, incumbent providers and new entrants in the wireless space, academic and government researchers and to advisory groups like the TAC and CSMAC. In addition, more widespread availability of technical data about documented interference cases would be extremely helpful to manufacturers, especially where an equipment design issue led to the interference problem.

a. Some information on interference complaints and investigations is being collected today on both an informal and formal basis. In the informal category, the Wireless Internet Service Providers Association (WISPA) maintains several mailing lists where information on interference problems and incidents are regularly shared among participants. In the formal category, the USCG Navigation Center operates an interference reporting system that shares information on GNSS/GPS interference detection and mitigation (IDM) with similar systems in other countries or regions.[8]

b. The FCC operates a system for handling public safety and other interference complaints. Some of the interference complaints come through the Enforcement Bureau's Cellular Telephone Interference Complaint webpage).[9] While basic information on the complaint and its disposition are collected and published online, the system does not encompass technical and operational details (including root causes) nor does it include information on those incidents that are voluntarily resolved without any formal involvement by the FCC.

4. NTIA should analyze the different enforcement process 'stages' to determine the automation approaches and the costs/benefits of automation at each stage. Subsequently, NTIA should develop an automated enforcement architecture for shared spectral bands.

5. NTIA may wish to further study some fundamental questions that would need to be addressed if automated enforcement were to be broadly deployed.

   a. How is interference defined and, related, how is "interference" distinguished from "harmful interference?"

---

[7] This would include voluntary, regularly scheduled (*e.g.*, quarterly) on-line meetings among professional interference hunters using virtual meeting tools such as WebEx. The Interference Hunter Information Exchange (IHIE) mission would be "to facilitate the exchange of information among interference hunters on radio interference incidents, trends, and resolution and mitigation techniques for the purpose of protecting users of the increasingly valuable and congested radio spectrum environment against harmful interference of all types – incidental, unintentional, and both malicious and non-malicious intentional interference." See Dale N. Hatfield, "Proposal for an Interference Hunter Information Exchange," March 2017. The IHIE would be a purely private, voluntary, multi-stakeholder organization, that status would not preclude government employees with interest in or knowledge and experience in interference hunting from those participating entities.

[8] See https://www.gps.gov/multimedia/presentations/2017/02/COPUOS/hamilton.pdf

[9] http://transition.fcc.gov/eb/ctix

b. How are externally-generated intentional/malicious forms of interference, such as jamming and spoofing, detected and handled?

c. How does the handling of externally-generated intentional/malicious interference differ from that associated with unintentional interference?

d. How are externally-generated unintentional forms of interference (*e.g.*, harmonics from other transmitters) detected and handled?

e. For interference incidents that may lead to formal enforcement actions, what evidence should be collected and how are "chain of custody" issues associated with that evidence maintained?

Addendum I – Status of Enforcement Operations, Current Policy Framework, and Previous Work in Automated Enforcement

Limitations

1. Legacy laws, rules and policies are not amenable to automated enforcement. While interference within an operator's system can generally be dealt with, localization and identification of sources outside an operator's system can be challenging. Market-based licensing practices often mean that there is no database of specific transmitter locations and frequencies that can help facilitate automated enforcement. Ultimately, resolution becomes the responsibility of the FCC.

2. Lack of information sharing. Interference often originates from common sources and has technical characteristics that might be cataloged and shared to speed and automate enforcement. There is no such public database and the agency with the broadest experience (FCC) has been unwilling to share case information even with the identity of the offending organization redacted.

3. Existing automated systems are limited to particular waveforms, frequency bands, and/or technologies. Most companies hire consultants to locate and identify interference, although some larger companies have internal teams. Manual enforcement will continue to be vital for the foreseeable future.

Examples

1. Determining the general location of the interference source is usually much easier than determining the precise source. For example, interference to a UHF LTE system was rapidly located to a major-chain hotel building. The source was one malfunctioning telephone handset located in a particular room. Identifying the precise source required walking down various hotel hallways and finding areas outside one or two rooms where the interfering signal was strongest. While the hotel was agreeable to allow access to its property, the rooms could not be accessed while occupied by guests, and the specific telephone could not be identified until the hotel guests in those rooms had checked out.

2. Aggregation of individual sources can challenge identification and resolution. For example, interference to a distributed antenna system (DAS) in a large venue could not be localized by isolating branches of the system, and was "harmful" only when the entire DAS system was enabled. The source turned out to be individual lighting system components that were distributed throughout the building. Replacement of thousands

of individual lighting fixtures was required. It would be helpful to get details on actual interference events, including cause, impact, difficulties in identifying the source, etc.

Taxonomy

Various taxonomies of interference have been proposed including those that differentiate between receiver and transmitter issues.[10] At some level, we simply admit that interference exists and turn-away from things like receiver standards, guard bands, and emission masks. Such things are important, of course, in minimizing interference *ex ante*, but for purposes of determining the extent to which enforcement can be automated the subcommittee found that the level of effort required to track down and remediate the interference depends chiefly on whether the interference is internal to the affected system, and whether the interference is localized or widespread. Based on our discussions, we divide interference broadly into three types:

1. Intra-system (self-interference). Interference due to mechanisms entirely within the control of the system operator. This interference is often due to poor system implementation practices, errors in equipment configuration, and less-commonly, malfunctioning equipment.

2. Proximate (nearby) interference. Interference affecting just one site or user. This interference is often the most challenging to resolve, as it may not be observable using external equipment and there are often multiple sources. For example, the exquisite sensitivity of tower-top antennas with low-noise amplifiers often means that the interference is not "visible" to external observers and so location of the source becomes difficult. Proximate interference also includes cases where an equipment issue may impact multiple sites or users, but the interference is localized to individual sites.

3. Widespread interference. Interference affecting multiple sites or users. This interference is generally easy to identify because it is usually strong, but there may be challenges in identifying the precise source(s) due to access or privacy issues, for example.

[10] One example of an alternative categorization of interference can be found in a NOAA report entitled "GPS Dependencies in the Transportation Sector", Report Number DOT-VNTSC-NOAA-16-01, released August 2016.

Addendum II – Questions for SAS Entities Regarding Automated Enforcement

1. How should enforcement of spectrum "rights" entitled to Citizen's Broadband Radio Service (CBRS) users and Incumbent Access users factor into the Spectrum Access System (SAS) construct?

2. With respect to enforcement, what should the roles be of:

    a. Spectrum Access System (SAS) Administrators
    b. Citizen's Broadband Radio Service (CBRS) users
    c. Incumbent Access users
    d. Federal Communications Commission (FCC)
    e. National Telecommunications and Information Administration (NTIA) be in the enforcement process?

3. What methods might a SAS Administrator use to receive reports of interference and requests for additional protection from Incumbent Access users? (47 CFR 96.53 (o))?

4. How should SAS Administrators define interference?

5. How should SAS Administrators distinguish interference from "harmful interference?"

6. What actions should a SAS Administrator take when interference is reported by CBRS users?

7. What actions should a SAS Administrator take when interference is reported by an Incumbent Access user?

8. Should SAS Administrators detect and handle externally generated unintentional forms of interference such as harmonics from other transmitters?

9. If necessary, what methods might a SAS Administrators use to detect and handle externally generated unintentional forms of interference such as harmonics from other transmitters?

10. How should SAS Administrators detect and handle externally generated intentional and/or malicious forms of interference such as jamming and spoofing?

11. Should SAS Administrators be able to identify “rogue” users?

12. If necessary, what methods might a SAS Administrators use to identify “rogue” users?

13. What data should SAS Administrators collect to support enforcement actions?

14. How should SAS Administrators collect, protect, and manage data to support enforcement actions?

15. Should SAS Administrators handle externally generated intentional and/or malicious interference differently from unintentional interference?

16. For interference incidents that may lead to formal enforcement actions, what evidence should a SAS Administrator collect?

17. How should a SAS Administrator address “chain of custody” issues associated with that evidence?

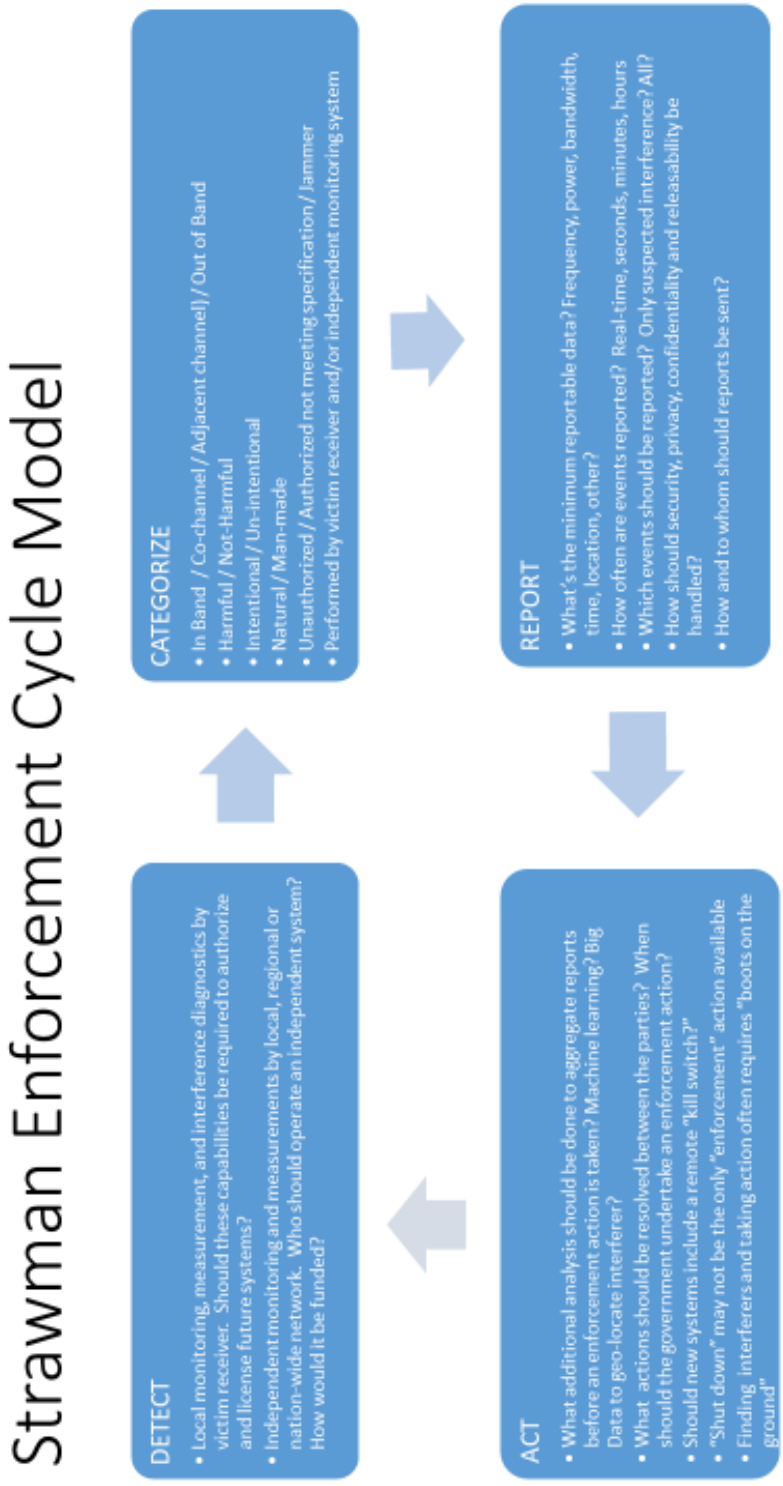

Figure 1. Straw Man Enforcement Cycle Model