Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db399

Title	**MF Blue-Box and the Toll Network**
Date	1972-00-00
Author(s)	Forsberg, Charles P.
Abstract	Technical overview of a multifrequency (MF) toll fraud detector.
Keywords	MF; multifrequency toll fraud detector; Northeast Electronics Corp.; blue box; toll fraud detector
Notes	Google books search 6/2009 suggests this was published in 1972 in the University of Kentucky Office of Engineering Services bulletin: http://books.google.com/books?id=gmzVAAAAMAAJ&dq=charles+forsberg+blue+box
Source	Alan Rubinstein

MF BLUE-BOX AND THE TOLL NETWORK

Charles P. Forsberg
Northeast Electronics Corporation
Concord, New Hampshire 03301

Summary. The toll network is surprisingly easy to defeat on billing but those guilty are not immune to being caught.

Introduction

The use of multifrequency (MF) tones in the telephone toll network allows a call to be completed quickly through any type of carrier system. It was essential to the development of the dial-anywhere system we know today. In effect though there seems to be a flaw since anyone who can generate these same MF tones from his telephone location may easily escape the billing system and call direct to many distant points. Gathering evidence to discourage and prosecute those who would defraud the telephone companies borders on wire-tapping and can be troublesome all around. However, if sufficient dialing information could be recorded directly as a printed record, then listening or taping of conversation need not be required. This approach has been approved by many courts without prior approval. The thinking here seems to be that the operating telephone companies should not be ham strung in legitimate means of obtaining evidence against those persons or organizations who would defraud them.

Interoffice Toll Signaling

Multifrequency Signaling

The majority of interoffice toll signaling is accomplished with a sequence of paired tones, eac pair representing a digit of the called number. It is the same tones one often hears in the backgrou before return supervision is heard on a toll call. These MF tones consist of six frequencies in the range 700 to 1700 Hz, which when taken 2 at a time provide 15 possible combinations of which 1 are required for interoffice calls. An MF call group might be KP 603 224 7466 ST. The KP pul is used to signal the far end to prepare to receiv digits, while the ST pulse signals the end of digit pulsing. An area code may or may not be requir but the KP and ST pulses must be used. Table I lists the tones used per each digit.

Toll Trunks

All subscriber circuits end up in a central

office be it large (10,000 lines) or very small. If one subscriber wishes to call another and both are connected to separate central offices then the connection is made over an intertoll trunk. The connection may be either a short haul or a long haul depending on the distance and circuits involved. Many central offices will have direct trunks to tandem offices which are capable of automatic routing options to complete every forward call regardless of where destined. But not every toll call will go through a tandem office since the short haul may be a direct interoffice trunk and MF may not be used to complete the call.

Single Frequency Required

A 2600 Hz single frequency (SF) tone is put on a tandem trunk to signal the tandem office that the particular trunk is idle and available to take a call. Removing the SF tone makes the trunk busy. This frequency is universal and at least a short burst is required before each new call.

Operator Codes

Every outward long distance operator has at her side a book of 3-digit codes which allow her flexibility in placing a call. Her MF keyset will put her right into a tandem office and she can reach any distant point directly. If the overseas "operator" codes are available to her she may place calls by satellite or cable and terminate call to any office or subscriber available. These "operator" codes are not given to anyone except operators and telephone maintenance people.

Blue Boxes and Phone Phreaks

Obtaining the Blue-Box

The MF blue-box* can be a simple device that will operate the toll switching networks to send the caller all around the world anonymously and without a billing record. Such a device will generate the 12 paired tones according to TableI and would preferably have a keypad that would produce the two tones per digit by a simple keystroke. One additional key is necessary for the 2600 Hz SF. Actually getting a ready made blue-box may not be too difficult but the cost is apt to be high.

Who's a Phreak!

The MFing problem appears under both the criminal and amateur headings. Whereas the criminal has a means to avoid detection and payment of tolls the amateur pursues the practice as a hobby much like a "wireless ham". The threat to the long lines network from the amateur may be the excessive use of capacity which might delay or cause a poor routing of a legitimate call. Quite a few of the amateur phone phreaks are blind and they will stay up all night to do their calling. The motivation of a free call is not as exciting as playing with the switching network for these types. The criminal problem could be a call of very long duration or a large number of short calls. Either way the attempt is to avoid payment of tolls and/or escape detection. Tapping someone elses line is not uncommon. Regardless of what they're called, phone phreaks and others who MF are doing fraud and it may be expensive fraud.

*The origin of the euphemistic term blue-box may be because the first one captured or built was painted blue, but other toll defeating boxes of a different color are also known. They usually work from the called-party to suppress return answer supervision to the originating end.

Capturing the Phreaks

The SF Trap

A prior knowledge of anyone generating SF and MF signals from a subscriber location will be hard to come by. Almost always someone has to become suspicious, an operator, a switchman, a tattletale, etc., and this will lead to further investigation of a suspect line. A simple inexpensive means of monitoring a suspect line can be the use of an "SF trap". This device will detect the presence of a long burst of 2600 Hz and trip a counter, a light circuit or perhaps switch to an intercept. The invasion of privacy is only to the extent that the presence of an illigitimate tone is occurring intentionally or otherwise. On some special trunk groupings (e.g., CAMA) it may be possible to efficiently use a scanning device to detect SF on a call. This fact might be entered on the accounting tape. When such a tone has occurred repeatedly then more elaborate (and expensive) equipment can be put to good use.

SF and MF as a Permanent Record

This special equipment could consist of the blocks shown in Figure 1. The signal processing in a simplified fashion would consist of a supervisory circuit to detect the off and on-hook conditions and stamp a date and time entry on a paper strip. The first number grouping after the off-hook time entry will be a legitimate toll free number - often an 800 number - dialed in the normal fashion with rotary of Touch Tone® dial. When the call is completed and ringing is heard a short bleep of SF is given to idle the trunk momentarily. In Figure 1 the dialing receive circuits are disconnected and the MF receiver switched in. A notation on tape is made to this effect. The party to be called will then be MF'd starting with a KP and ending with an ST burst. At the conclusion of the call rather than hang up the caller may apply another short burst of ST followed by a new MF sequence. This process can be repeated several times on one toll free number. Only a certain number of tandems can be stacked since the quality of transmission will deteriorate to preclude further MFing. But every call sequence will be recorded on tape in Figure 1. When the caller eventually hangs up then the strip printer will enter the termination time and the dialing circuits are made ready for a new call. The MF and Touch

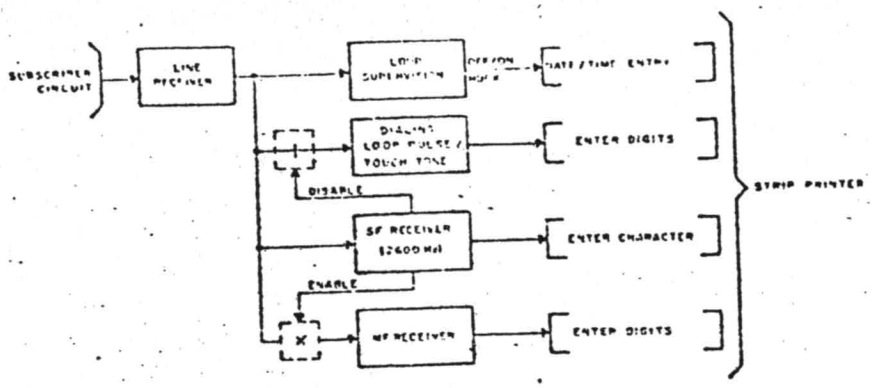

Figure 1. OVERALL SIGNAL PROCESSING

Tone circuits can not both be active at the same time since one can confuse the other on certain tone combinations.

Billing Analysis

All the previous activity does not completely escape the toll billing machines. What circumstance would anyone have to call an inward toll free number and talk for hours. The 800 numbers are almost exclusively reserved for reservation systems and information needs. For those operating companies who can do billing analysis a call of this type could stand out like a missing thumb, especially for phone phreaks careless enough to use an information operator. One should keep in mind that all toll billing information is put on punched or magnetic tape regardless of whether the call is ever completed or not. It comes to light that the extra clever phone phreaks will be a step ahead if they will willingly pay a small toll fee to a legitimate number and then SF-MF to a more distant place in the world. However, all this activity captured on a strip of paper can be presented as documented evidence of fraud.

The Blue Box Problem

Poor Phreaks and Poor Boxes

Many phone-phreaks do not have the money or skill to acquire a good blue box. But they can buy a simple cassette tape recorder and transcribe the basic required tones from a friend or an electronic organ. Any desired MF call sequence can then be made up on a second recorder. Usually the phone-phreaks only call each other so that these tones on tape will work, not efficiently but sufficiently. To get these tones on the network the choice is to acoustically couple the tones through the mouthpiece, or to use a transformer or capacitors to couple direct to the loop pair. The end result is a poor set of tones to switch the toll network and yet the phreaks often get through.

Technical Difficulties

With a poor blue-box and poor coupling the resultant MF tones may well have a third tone distortion, non-constant amplitude, shifting frequency, and have excessive twist in tone pairs. Very often the phreaks will use a high enough amplitude so that they are still able to complete most of their calls. Telephone security agents could generally care less why but would rather have the means to decode even the attempted calls. Ever bit of information may lead to new blue-boxers to be put out of action.

A New MF Detector

First Considerations

1. A valid MF burst must contain two major signal components of the six possible.

2. Each of these signal components must lie between two filter bandwidth limits that may be effectively widened when necessary.

3. That the two major signal components per pulse must not exceed a certain difference in level.

4. Where third MF tone distortion is present it may or may not invalidate the MF pulse.

5. A minimum dual tone signal duration is required for validity.

6. That producing a reliable working circuit for the above under $10 is impossible.

The Detection Circuit

The fundamental operation of the MF detection scheme (Figure 2) is the majority decision choosing the greatest and next greatest of six possible tone channels. The begining of each burst is detected by the tone switch which senses a minimum peak signal crossing and feeds the resulting train of pulses to the interval timer - a retrigger monostable circuit. Any interruption of the interval timer invalidates the tone burst. This would hopefully be the case for voice and noise interference.

Where a signal burst is valid a delay of 20 milliseconds occurs before the two greatest signa

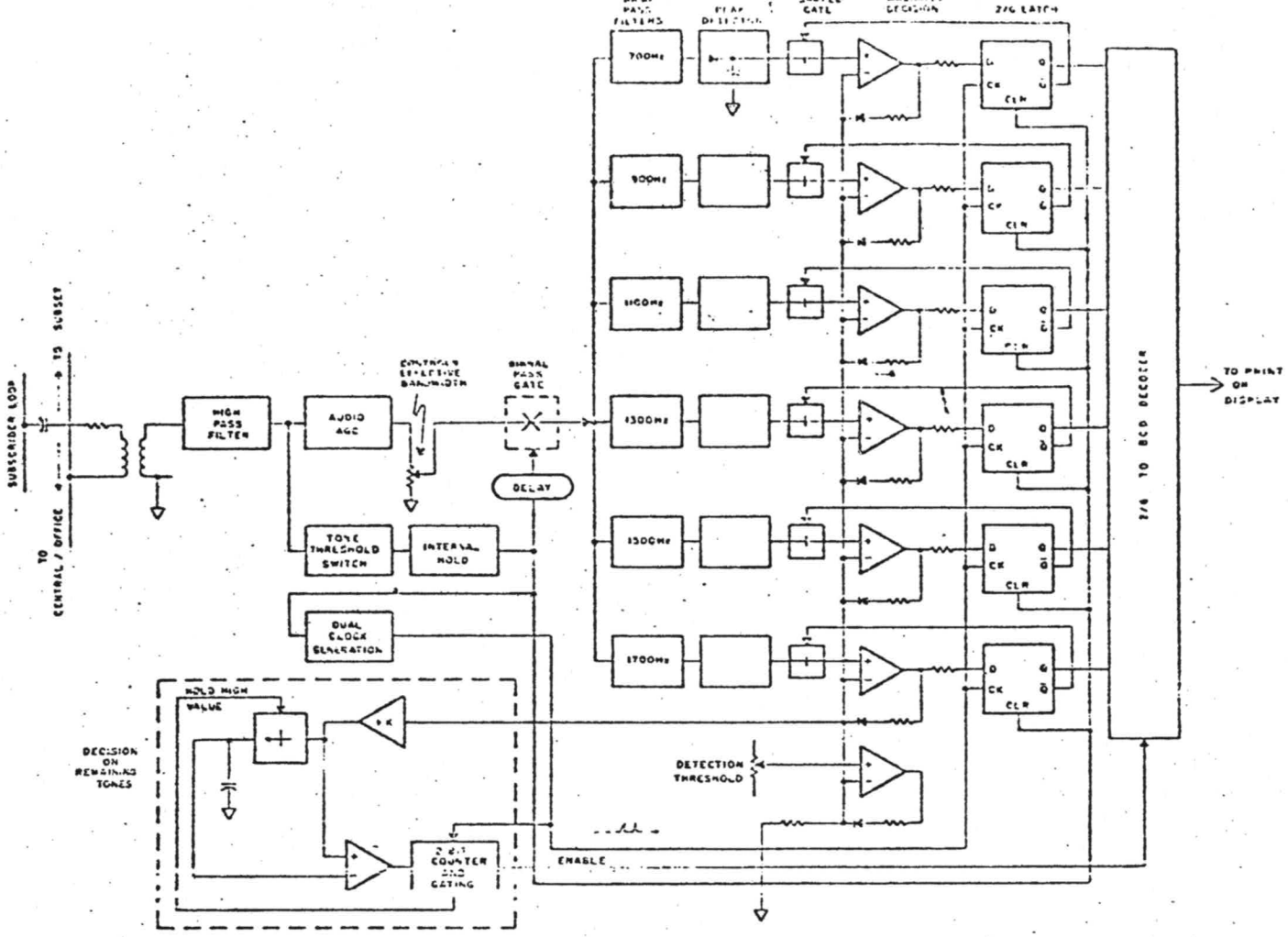

Figure 2. FOLLOW-HOLD MF DETECTOR

components are captured. The capture is required to prevent two signals close together in amplitude from toggling on the majority decision. The output of the peak detector is not DC only. Capture is accomplished by generating two clock pulses to the D-Flip Flops (D-FF). Once two of the D-FF's are latched-up, and this will not be the case if both tones do not exceed the detection threshold, one last check is made to determine validity of the MF tone burst.

The first clock pulse stores the highest signal level on a capacitor to which after the second clock pulse has passed is then compared against the remaining four band pass filter outputs. This comparison continues for a period of 5 to 20 milliseconds before the MF tones captured are considered valid. Where the comparison is too close together and requires an invalid decision, the output decoder is never enabled and nothing is printed.

Magnetic Tape Recordings

This follow-hold approach is especially useful where decoding from magnetic tape is required. In combination with a high AGC output level to give an effectively wide bandwidth on all the band pass filters the translating of tones from tape is made very easy.

Other Boxes

Although this paper has been specifically concerned with blue-boxes there are in fact other means to defeat toll billing. This author has also heard of brown-boxes, yellow boxes and black-boxes. These devices in effect defeat toll billing from the called party end by suppressing answer supervision. An example of such is where the calling party equipment will hold the line open to the called party who after tripping the ringing generator with a short duration of loop current can then capacitively couple to the loop circuit. The loop current does not flow long enough to return answer supervision to the calling party. In the end, the proper recording equipment connected to the calling party line will produce complete dialing information to contradict the toll billing computer output.

Bilbiography

1. Secrets of the Little Blue Box, Ron Rosenbaum, Esquire magazine, Oct. 71.

2. Basic Telephone Switching Systems, David Talley, Hayden Book Company, N.Y.