MULTIPLE HOME TERMINAL UNITS: SUBSCRIBER CONVENIENCE--SECURITY RISK

James R. Cherry, Director, Product Design Engineering
Tony Chen-tung Li, Manager, Product Design Engineering

Oak Communications Inc.
16516 Via Esprillo
Rancho Bernardo, California

ABSTRACT

The need of the subscriber to simultaneously operate multiple TV sets and/or VCR's from his cable service has led to significant use of multiple home terminal units (HTU). If a subscriber pays a lower fee for a secondary HTU that is authorized to receive the same premium service as his primary unit a risk exists that the unit will be sublet to a neighbor. For addressable cable systems using out-of-band data carriers, a master/slave configuration is proposed as a solution to the problem of subletting secondary units. The master/slave consists of two HTU's: the master used with the primary set and the slave used with the secondary sets. The slave unit does not function unless its address-control channel is protected by a master HTU. Thus, if the slave unit is used in a neighbor's home without its master, the secondary, or slave, unit will not function. Both master and slave HTU's can still respond with all addressable features. The uniqueness of the scheme lies in the selective blocking, by the master unit, of deauthorize commands directed at all slave HTU's. A high level of security is maintained without the requirement for complex, handshaking duplex data communications between the two HTU's.

INTRODUCTION

The home terminal unit (HTU) converts any cable channel to a channel that can be received by the standard TV receiver or recorder (typically Channel 3 or 4) and it descrambles premium channels for which it is authorized.

If a subscriber desires to utilize a cable channel which is outside of the usable band in his TV receiver or recorder, or which is scrambled, he must do so through an HTU. For simultaneous use of multiple TV receivers or recorders to receive different cable channels, one HTU per video device must be used. Thus, we find some subscribers utilizing multiple HTU's for the convenience of operating second TV sets and VCR's.

In systems where a substantially lower fee is charged for premium services received on a subscriber's second or subsequent HTU, a significant security risk is incurred. The lower second-unit fee can be the result of franchise agreement mandate or system policy.

Assuming that additional HTU's provided to a subscriber are identical to the initial unit, then they can be used on any outlet in the system to receive the service for which they are authorized. Thus one subscriber can pay a nominal fee for a second HTU authorized to receive the same premium service as his primary unit, and sublet this unit to a neighbor, thereby circumventing the normal premium service fee.

The security risk is strongly a function of the subscriber cost differential between initial and subsequent HTU's. Also, it is a function of the social norms in the area covered by the franchise.

For addressable cable systems capable of out-of-band data transmission, a solution to the risk brought on by low-priced second sets is a system in which the HTU provided as a secondary set will only operate in the presence of a primary set...a master/slave arrangement.

THE MASTER/SLAVE SOLUTION

Three approaches to master/slave configurations will be described: 1) master-to-slave control channel, 2) separate master-to-slave control line, and 3) control channel interruption.

1. Master-to-Slave Control Channel

Figure 1 shows a functional block diagram of the master-to-slave control channel configuration. The control channel is assumed to be 10.7 MHz in this example.

Master HTU. The master HTU has been designed to retransmit the control channel back onto the input cable at 10.7 MHz. The master HTU is controlled by the standard control channel at 104.7 MHz.* The 10.7-MHz channel is interrupted whenever the master HTU receives an inhibit command from the headend via the standard control channel. The inhibit command is sent to all master HTU's in the system as a group. The duration of the 10.7-MHz channel interruption is of sufficient duration to disrupt the following message which is directed to only slave HTU's. The 10.7-MHz channel operates continuously as long as the master HTU is powered.

* 104.7 MHz is one of the FSK control data channel frequencies used in Oak systems. This data channel transmits a continuous stream of 64-bit message packets addressed to individual HTU's, or groups of HTU's.

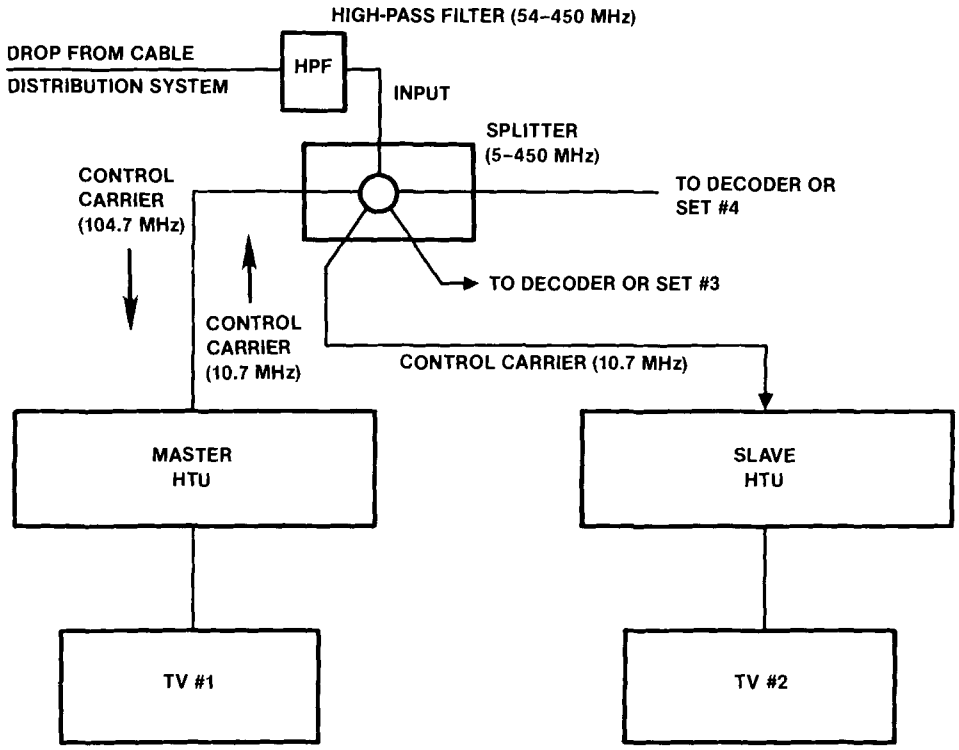

Figure 1. Master-to-Slave Control Channel

Slave HTU. The slave HTU is designed to receive the 10.7-MHz control signal retransmitted by the master HTU. The slave decoder can be addressed and controlled by the headend, provided that the control signal is received via the master HTU, which retransmits the 104.7-MHz control data at 10.7 MHz.

Periodically, deauthorize messages are sent to all slave HTU's as a group, preceded by an inhibit command sent to all master HTU's. If the slave decoder is receiving its 10.7-MHz control channel via a master HTU, then the deauthorize signal will have been inhibited and the slave will continue to function normally. If the slave is connected to the control channel by an independent converter, (i.e., without the master being present), then it becomes deauthorized following reception of the first deauthorize message.

Both slave and master HTU's are manufactured identically and shipped as master HTU's. At installation a message from the headend is sent via the standard control channel that will configure designated HTU's as slaves. Slaves thereafter respond to only 10.7-MHz control.

Splitter. The splitter is standard, except for the requirement to pass the 10.7-MHz signal. The 10.7-MHz control signal is retransmitted from the master HTU to the splitter. The 10.7-MHz signal passes through the splitter to its input port and is reflected from the high-pass filter in that line. It is then, in turn, passed to the other output ports.

High-Pass Filter. A high-pass filter is used to block the 10.7-MHz signal from entering the system by reflecting the signal back into the splitter.

2. Separate Master-to-Slave Control Line

Figure 2 shows a functional block diagram of the separate master-to-slave control line configuration. This system operates on the same inhibit/deauthorize principle described in the master-to-slave control channel configuration.

Master HTU. The master HTU has been designed to transmit a control signal to the slave HTU's that will disable the slave's control channel during a deauthorize message that follows an inhibit message. As in the master-to-slave control channel scheme, an inhibit signal is put on the control line by a master HTU whenever an inhibit command is received from the headend via the standard control channel. The inhibit command is sent to all master HTU's in the system as a group. The duration of the inhibit signal on the control line is of sufficient duration to disrupt the following message which is directed to slave HTU's. The control line inhibit function operates as long as the master HTU is powered.

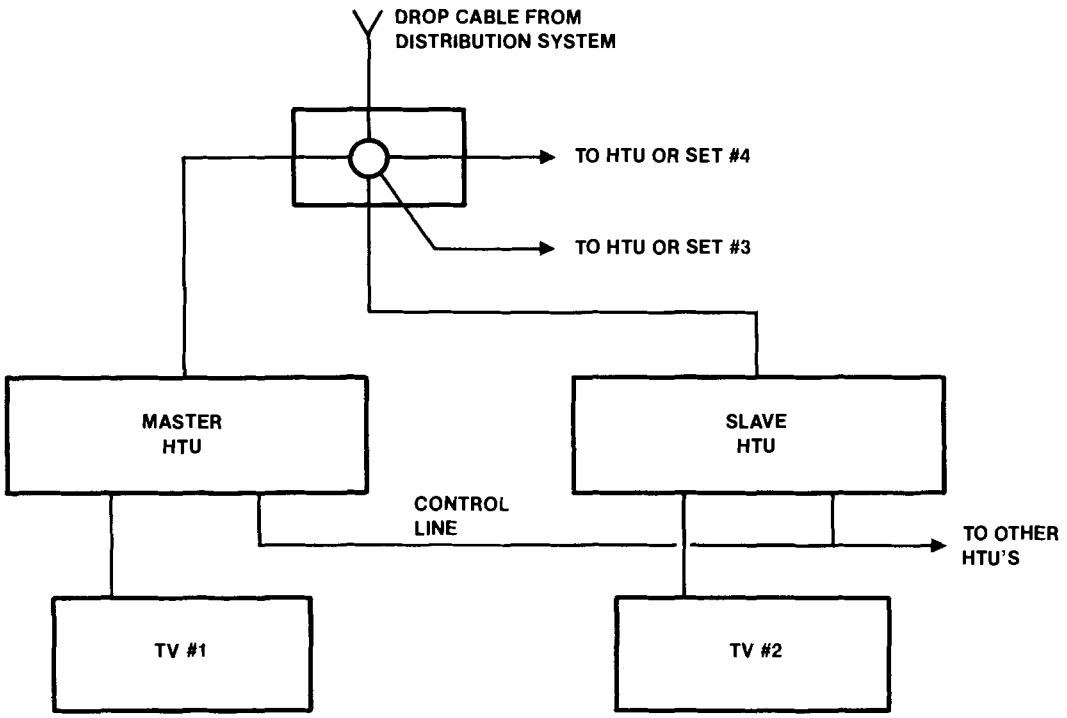

Figure 2. Separate Master-to-Slave Control Line

Slave HTU. The slave HTU is designed to respond to the control line inhibit signal. When this signal is present the standard control channel receiver is deactivated and no control messages can be received by the slave HTU.

Periodically the headend sends deauthorize messages to all slave HTU's as a group, preceded by a group inhibit command sent to all master HTU's. If the slave HTU is connected to the control line from the master HTU it will be protected from the deauthorize command and will continue to function normally. If the slave is not connected to the control line it becomes deauthorized following reception of the first deauthorize message.

Both slave and master HTU's can be manufactured the same and shipped as master units. At installation a message from the headend can be sent via the standard control channel that will configure designated HTU's as slaves.

3. Control Channel Interruption

Figure 3 shows a functional block diagram of the control channel interrupt configuration.

Master HTU. The master HTU has been designed to transmit a switching pulse on the input cable. This switching pulse is transmitted by the master HTU immediately following reception of an inhibit command from the headend via the standard control channel. The inhibit command is sent to all master

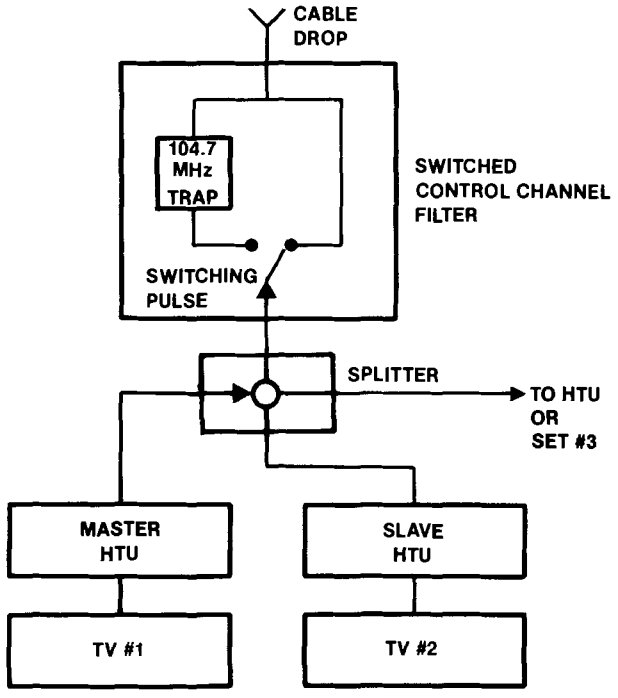

Figure 3. Control Channel Interrupt

HTU's in the system as a group. The duration of the switching pulse is sufficient to prevent the reception of the following message which is directed to all slave HTU's. The switching pulse operation is executed as long as the master HTU is powered.

Switched Control Channel Filter. The switched control channel filter is designed such that the signal from the cable drop normally passes directly through to a splitter, except when a switching pulse from a master HTU is imposed on the output port of the device, a control channel filter is switched into the line to interrupt the control channel. When the switching pulse is removed the device returns to normal operation, passing all signals on the cable. Another possible approach to designing this filter is to block all the RF signals on the cable for the entire pulse duration.

Slave HTU. In the control channel interrupt configuration, any addressable HTU that is system compatible can be used. At installation a message from the headend will be sent to the slave HTU to make it associate with the slave group. Periodically a deauthorize message is sent to all system slave HTU's as a group. If a slave is operated downstream from a master HTU-controlled switched control channel filter it will be protected from receiving the deauthorize command. If the slave HTU operates directly on the system it will deauthorize following reception of the first deauthorize message (see timing diagram in Figure 4).

MULTIPLE DWELLING APPLICATIONS

The control channel interrupt method can readily be extended to multiple dwelling situations where a large number of slave HTU's are required on the master HTU (see Figure 5). This can offer an interesting alternative to off-premises equipment in situations where unauthorized migration and use of home terminals are the principal concern.

There is no restriction to the number of slaves in one building. Each building would be treated as a separate group with its own group address. Thus, slave HTU's from one building would be useless in any other building. However, it should be pointed out that level differences in the cable spectrum between the trap on/off states of the switched control channel filter may create disturbances visible in the TV picture. Also, it does not prevent transfer of slave HTU's within the designated building.

MESSAGE SECURITY

Central to the above approaches is a technique of informing the master units of an impending slave disable command. In any system employing the described approach, the ability of a pirate to covertly mimic the master's message interruption process must be examined. The Oak approach to this danger, as well as other dangers of control channel manipulation (or tampering) is to encrypt all control channel messages using a time-varying

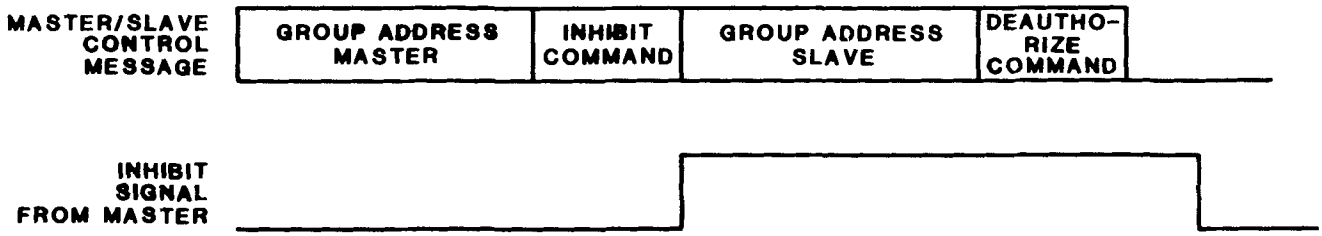

Figure 4. Timing Diagram

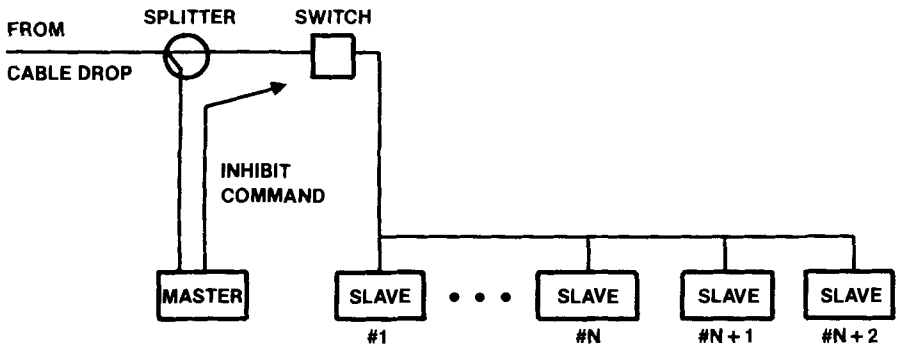

Figure 5. Extension to Multiple Dwellings

process. Thus a pirate will be unable to detect the slave disable warning message going to the master units. Patents are currently being filed for these approaches as well as the master/slave concept.

SUMMARY

The problem of secondary HTU theft for addressable cable systems is a major concern for system operators that offer lower rates for secondary HTU's. The master/slave solution will eliminate that risk.

The control channel method requires transmission of the control signal at 10.7 MHz instead of a switching DC pulse used by the other approaches. The advantages of this method are that there is no requirement for external hookups between the master and slave HTU's and that only RF signals are present on the cable.

The master HTU for the control line approach can also send a switching (DC-coupled) pulse via the RF cable instead of the external connection to each slave HTU. Several commonly used splitters tested were found to pass DC without significant degradation. During the pulse duration, a data channel message is transmitted to command the slaves to deauthorize. Thus, HTU's that are not linked to a master HTU sending such a pulse will be deauthorized for viewing. However, if the switching pulse is carried by the RF cable to each slave HTU, DC blocking devices must be used to avoid DC shorts in the cable throughout the subscriber's home. This can happen if the customer decides to hook up a VCR to the RF cable.

For both the control channel and the control line methods, the deauthorize command can be sent as frequently as desired by the system operator. While in the control channel interrupt method, the deauthorize command frequency should be limited to a minimum since the switched control channel filter may cause picture interference during switching.

For all three approaches described, the master and slave HTU's can be manufactured and shipped identically. At installation the HTU's can be reprogrammed from the central control computer to function as master or slave HTU's. The control message will utilize a time-varying encryption process to ensure maximum security. These techniques are currently under development at Oak Communications in San Diego.