Secure Data Broadcasting

The present invention relates to a method and apparatus for including data within a digital television signal while providing protection against analysis of the destination of the data to the intended recipients.

A digital video broadcast (DVB) channel may be used to transmit datagrams to individual receivers, groups of receivers (multicast) or all receivers (broadcast) which have access to the broadcast channel within a DVB/MPEG-2 Transport Stream. Datagrams are prefixed with a header that contains a protocol-independent destination address within the data broadcasting network and a protocol identifier. If the destination addresses are clear (i.e. not encrypted) it is possible for the traffic of data being transmitted to receivers accessing the channel to be monitored and commercial information relating to this traffic may consequently be exposed.

The present invention is concerned with a method and apparatus for protecting the destination addresses of data being transmitted over a digital video broadcasting channel.

According to one aspect of the invention, there is provided a method of receiving data addressed to one or more receivers each having an individual identifier wherein the data is included in a digital signal comprising destination addresses successively encrypted from a sequence of control words, and control messages containing the control words in encrypted form, address flags and control flags, the method comprising:

processing the control messages to construct receiver addresses from the control words and the receiver identifier;

directing the receiver addresses to update a receiver address register selected by the associated control flag in response to the transmitted control flags;

directing each destination address to be compared with the receiver address to one of the address registers selected by the associated address flag in response to the address flags and;

This Sheet Has Been Replaced



accepting each packet of data having a destination address matching the receiver address to which it was compared.

According to a second aspect of the present invention, there is provided apparatus for receiving data addressed to one or more receivers each having an individual identifier wherein the data is included in a digital signal comprising destination addresses successively encrypted from a sequence of control words, and control messages containing the control words in encrypted form, address flags and control flags, the method comprising:

processing means for processing the control messages to construct receiver addresses from the control words and the receiver identifier;

a first directing means for directing the receiver addresses to update a receiver address register selected by the associated control flag in response to the transmitted control flags;

a second directing means for directing each destination address to be compared with the receiver address to one of the address registers selected by the associated address flag in response to the address flags and;

accepting means for accepting each packet of data having a destination address matching the receiver address to which it was compared.

According to a third aspect of the invention, there is provided a method of creating a secure data-stream containing one or more data packets to be transmitted to one or more receivers each having an individual identifier, the method comprising the steps of;

allocating control messages comprising control flags and control words in encrypted form and multiplexing these with the data-stream;

encrypting the destination address in the header of the or each data packet using the receiver identifier and the control word as inputs;

allocating an address flag for inclusion within the or each data packet for use by a receiver.

This Sheet Has Been Replaced

The invention will now be described, by way of example with reference to the accompanying drawings in which:

Figure 1 shows an overview of the architecture of a system according to the invention,

Figure 2 shows a transmission system included in the architecture of Figure 1,

Figure 3 shows a reception system included in the architecture of Figure 1,

Figure 4 shows the sequence of generating receiver addresses and comparing the generated receiver addresses with incoming destination addresses in the system of Figure 3 and,

Figure 5 is a timing diagram of elements in a digital broadcast signal used in the system of the preceding Figures.

Referring to Figure 1, there is shown a system architecture for a system including a network generally designated 10 connected to a server/gateway 11 which supplies digital video broadcast signals to a multiplexer 12. The signals are broadcast via a satellite link 13 to a number of subscribing receivers of which one is shown at 14. The receiver has an individual identifier distinguishing the receiver. The system may be used to address transmissions to individual receivers, to groups of receivers (multicast) or to all receivers (broadcast). The receiver 14 is shown connected in a Local Area Network (LAN) 15. A return path from the receiver 14 to the network 10 is shown at 16.

Turning now to Figure 2, there is shown the transmission system included in the architecture of Figure 1. A data transmission system 17 receives datagrams from a protocol stack for transmission. The datagrams consist of packets of data prefixed with a header containing a protocol independent destination address and a protocol

identifier. The datagrams are inserted into a DVB/MPEG-2 data-stream as shown at 18 for supply to the multiplexer 12.

A conditional access system 19 supplies control words to the data transmission system and the actual destination address in the header of each datagram is generated using a cryptographic function with the receiver identifier and a control word as inputs. The control word supplied by the conditional access system 19 is changed frequently so that a sequence of control words arrive at the data transmission system 17. As a result, many different destination addresses are used to identify an individual receiver, and many different receivers potentially use the same destination address at different times. The cryptographic function is chosen such that the control word cannot be used to convert a destination address back into a receiver identifier. It thus becomes very difficult to perform any kind of traffic analysis on the transport stream transmitted by the system.

Data packets to be broadcast to all receivers are handled by allocating a non specific receiver identifier such as OxFFFFFFFF. The same cryptographic function is applied to this identifier, using the current control word and yielding the destination address for broadcast packets. Multicasts may be handled by allocating a further range of identifiers, such as OxFFOOOOOO to OxFFFFFFFE. To secure the contents of a datagram, it may be encrypted using another cryptographic function based on the receiver identifier, or a unique key associated with the receiver or a further control word.

The conditional access system 19 also supplies entitlement control messages including the control words in encrypted form to the multiplexer 12 to be multiplexed with the data-stream 18. As will be explained later, each datagram includes an address flag which is used in the receiver to control the processing operations of the receiver. Additionally each entitlement control message includes a control flag to control the processing operations of the receiver.

In Figure 3, the digital video broadcast signal is received at a demultiplexer 20 where the entitlement control messages containing the encrypted control words are directed to a conditional access system 21. In the conditional access system 21 the entitlement control messages are processed to construct receiver addresses by calculation from the control words with the receiver identifier which is individual to the receiver.

As shown in Figure 4, each incoming entitlement control message has a structure to include a control flag 22 and the encrypted control word 23 constituting the payload of the message. The control flag may be either an odd or an even control flag and the conditional access control system 21 will direct the receiver addresses that are constructed into either one of two paths according to the significance of the control flag. The control words and the receiver addresses are passed to the data reception system 24 where the receiver addresses are used to update an odd address register if the associated control flag was odd and an even address register if the associated control flag is even.

The data reception system 24 receives the datagrams in the data-stream from the demultiplexer 20 including the address flag associated with each datagram. As shown in Figure 4, each incoming datagram has an address flag, the encrypted destination address and the payload of data 27. The address flag represents either an odd or an even datagram destination address which determines how the destination address is processed. After decryption using the control words supplied by the conditional access system 21, the datagrams are passed for comparison with either the dynamic receiver address in the odd address register or the dynamic address registered in the even register. The choice of comparison depends on whether the address flag for the datagram being processed is odd or even.

If a match is found between the destination address for a datagram and the receiver address with which it is compared, the datagram is accepted by the data reception system. There is a delay in the operation of the conditional access system in processing each entitlement control message and the resulting provision

of a receiver address to the appropriate odd or even register. For this reason, the timing of the control flags 22 has to be advanced relative to the timing of the address flags 25 as shown in Figure 5. In Figure 5, the odd control flags 22 and the odd address flags 25 are labelled O and the corresponding even flags are labelled E.

It will be apparent that the method and system described herein provides for a plurality of dynamic addresses for each receiver. In the specific example described, each receiver has two dynamic addresses of which one is in use at any one time while the other is being updated by way of the conditional access system.

CLAIMS

1. A method of receiving data addressed to one or more receivers each having an individual identifier wherein the data is included in a digital signal comprising destination addresses successively encrypted from a sequence of control words, and control messages containing the control words in encrypted form, address flags and control flags, the method comprising:

processing the control messages to construct receiver addresses from the control words and the receiver identifier;

directing the receiver addresses to update a receiver address register selected by the associated control flag in response to the transmitted control flags;

directing each destination address to be compared with the receiver address to one of the address registers selected by the associated address flag in response to the address flags and;

accepting each packet of data having a destination address matching the receiver address to which it was compared.

2. The method of claim 1, further comprising directing the receiver addresses, in response to the control flags, alternately to two receiver address registers.

3. The method of claims 1 or 2, further comprising directing each destination address, in response to the address flags, to be compared alternately with the receiver addresses in the two address registers.

4. The method of claims 1, 2 or 3, further comprising advancing the timing of the control flags relative to the timing of the address flags.

5. The method of claims 1, 2, 3 or 4, wherein the method of encryption employed uses calculation.

6. The method of any of claims 1 to 4, further comprising using two address flags, one odd and one even, to divert data to either an odd or even destination address.

7. Apparatus for receiving data addressed to one or more receivers each having an individual identifier wherein the data is included in a digital signal comprising destination addresses successively encrypted from a sequence of control words, and control messages containing the control words in encrypted form, address flags and control flags, the method comprising:

processing means for processing the control messages to construct receiver addresses from the control words and the receiver identifier;

a first directing means for directing the receiver addresses to update a receiver address register selected by the associated control flag in response to the transmitted control flags;

a second directing means for directing each destination address to be compared with the receiver address to one of the address registers selected by the associated address flag in response to the address flags and;

accepting means for accepting each packet of data having a destination address matching the receiver address to which it was compared.

8. The apparatus of claim 7, wherein the first directing means directs the receiver addresses alternately to two receiver address registers.

9. The apparatus of claims 7 or 8, wherein the second directing means directs each destination address to be compared alternately with the receiver addresses in the two address registers.

10. The apparatus of claims 7, 8 or 9, further comprising advancing means to advance the timing of the control flags relative to the timing of the address flags.

11. The apparatus of claims 7, 8, 9 or 10, further comprising encryption means encrypting by calculation.

12. A method of creating a secure data-stream containing datagrams to be transmitted to one or more receivers each having an individual identifier, the method comprising the steps of;

allocating control messages comprising control flags and control words in encrypted form and multiplexing these with the data-stream;

encrypting the destination address in the header of the or each data packet using the receiver identifier and the control word as inputs;

allocating an address flag for inclusion within the or each data packet for use by a receiver.

13. The method of claim 12, further comprising changing the control word frequently.

14. The method of claims 12 or 13, wherein the cryptography function employed is such that the control word cannot be used to convert a destination address back into a receiver identifier.

15. The method of claims 12, 13 or 14, further comprising encrypting the contents of the or each data packet using a separate cryptographic function.

16. The method of claim 12, further comprising transmitting the data within a DVB/MPEG-2 Transport Stream.

This Sheet Has Been Replaced