

1

CONTROL WORD AND ASSOCIATED ENTITLEMENT CONTROL MESSAGE CACHING AND REUSE

BACKGROUND

The number of channels and/or services offered or available is increasing from hundreds to tens of thousands. Providers are increasingly attempting to consolidate the number of network elements needed to provide services. As a result, fewer devices may support a far greater number of services. In providing such services, encryption and decryption techniques may be implemented to prevent unauthorized access to the services.

The Digital Video Broadcasting (DVB) standard, ETSI TS 103 197 v1.5.1 (2008-10) offers a technique for producing and consuming a control word and associated entitlement control message (ECM) for one cryptographic period (also referred to herein as a crypto period) at a time. A control word may be a secret key that may be used to scramble a clear media stream at an encryption device such as, for example, an Encryptor, an Edge Quadrature Amplitude Modulation modulator (EQAM) with an embedded encryptor, a Converged Cable Access Platform (CCAP) device with an embedded encryptor, computer, and/or other computing device, and to descramble a scrambled media stream (e.g., a channel) at a receiver device such as, for example, a set-top box, computer, tablet, and/or other computing device.

As a result, once a network element (e.g., a scrambler) inserts an ECM for one cryptographic period into a media stream, the network element may communicate with generator of the control words and the generator of the ECMs to obtain the next control word and ECM for the next cryptographic period. As a result of retrieving control words and associated ECMs on a per cryptographic period basis and because a cryptographic period typically may be a few seconds in length, the network elements may frequently communicate with the generators resulting in inefficient bandwidth usage across the network. Additionally, the cryptographic period may be set to a longer timeframe than is desired to account for latency in retrieval of the next control word and associated ECM from the generators. For example, the latency time may include the time taken to send a request for the next control word and associated ECM from the scrambler to the generators, the time the generators take to create the next control word and associated ECM, and the time taken for the scrambler to receive the next control word and associated ECM. Furthermore, the frequent retrieval of the control words and associated ECMs impedes scaling consolidated systems to support thousands of services. These and other shortcomings are addressed by the disclosure.

SUMMARY

Some aspects of the disclosure relate to computer hardware and software. In particular, one or more aspects of the disclosure generally relate to computer hardware and software for providing control word and associated entitlement control message (ECM) management functionalities.

Various aspects of the disclosure provide more efficient, effective, functional, and convenient ways of controlling creation, retrieval and distribution of control words and associated ECMs in an increasingly consolidated cable and internet service architecture. In one or more embodiments discussed in greater detail below, control word and associ-

2

ated ECM management functionalities are deployed, implemented, and/or used in a number of different ways to provide one or more of these and/or other advantages.

In some embodiments, a computing device may cache concurrently a first set of control words and a first set of entitlement control messages (ECMs) associated with the first set of control words. The computing device may encrypt a transport stream with a particular control word of the first set of control words. The computing device may insert into the transport stream a particular ECM, of the first set of ECMs, corresponding to the particular control word sent to a device downstream from the computing device.

In some embodiments, a computing device may encrypt a transport stream using a first control word during a first cryptographic period and may encrypt the transport stream using a second control word during a second cryptographic period after the first cryptographic period. The computing device may encrypt the transport stream using a first copy of the first control word during a particular cryptographic period after the second cryptographic period.

In some embodiments, a computing device may schedule a first control word and an associated first ECM for use during a first cryptographic period and a second control word and an associated second ECM for use during a second cryptographic period. The first cryptographic period may be different from the second cryptographic period. The computing device may schedule based on information received from an entitlement control data device and indicates a use order associated with the first control word and the second control word.

These features, along with many others, are discussed in greater detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is illustrated by way of example and not limited in the accompanying figures in which like reference numerals indicate similar elements and in which:

FIG. 1 illustrates an example communication network on which various features described herein may be used.

FIG. 2 illustrates an example computing device that can be used to implement any of the methods, servers, entities, and computing devices described herein.

FIG. 3 illustrates an example of another system block diagram that can be used to implement any of the various features described herein.

FIG. 4 illustrates a message flow diagram in accordance with one or more illustrative aspects described herein.

FIG. 5 illustrates a flowchart of an exemplary method of retrieving and using a batch of control words and associated ECMs in accordance with one or more illustrative aspects discussed herein.

FIG. 6 illustrates a flowchart of an exemplary method of maintaining a threshold number of control words and associated ECMs in accordance with one or more illustrative aspects discussed herein.

FIG. 7 illustrates a flowchart of an exemplary method of retrieving and using multiple batches of control words and associated ECMs for use with multiple services in accordance with one or more illustrative aspects discussed herein.

FIG. 8 illustrates a flowchart of an exemplary method of reusing control words and associated ECMs via a round-robin approach in accordance with one or more illustrative aspects discussed herein.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying draw-