

Security Extension for the SatNEx Satellite Platform

Department of Computer Sciences,
University of Salzburg



1. The SatNEx Satellite Platform

The SatNEx platform was created to facilitate easy interaction between the SatNEx partners distributed in Europe. It is hosted on the Eutelsat W3A satellite. The central up-link station, i.e. where the data is fed to the satellite, is maintained by the Fraunhofer FOKUS Institute (FhI) in Birlinghoven (near Bonn), Germany. Figure 1 shows a schematic of the SatNEx platform.

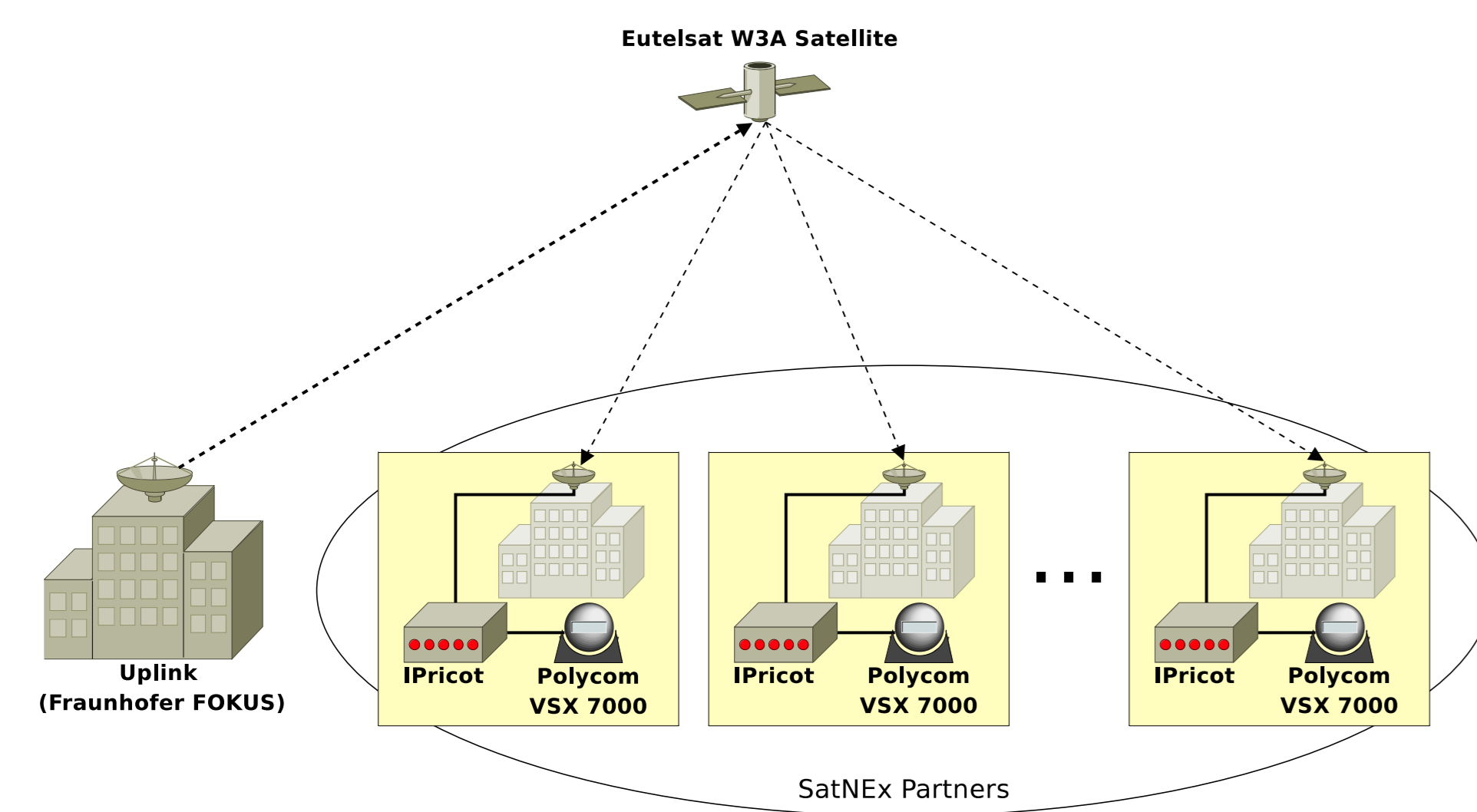


Figure 1: Overview of the SatNEx Platform.

For meetings, the Polycom VSX 7000 video conferencing system is used. The data of the platform is transported using IP multicast. The total capacity allotted to the SatNEx platform is 1 Mbit.

Every SatNEx partner receives a satellite dish along with the IPricot receiver device which is connected to the LNB of the dish. The IP data is transmitted using Multiprotocol Encapsulation (MPE). The IPricot device tunes to the transponder on Eutelsat W3A where the SatNEx platform is hosted, decodes the MPE data and outputs the extracted IP packets on the client LAN which is attached to its Ethernet port.

2. Security Extension

In the current configuration, everybody with a satellite dish in Europe and the necessary tuning information could (passively) join all meetings and view all broadcasts which take place on the SatNEx platform.

When (re-)broadcasting talks or lectures, the permissions of all lecturers have to be present. These permissions will certainly be granted more easily when there

is only a closed group of potential receivers. This can be achieved by encrypting the broadcasts.

The security extension devised for the SatNEx platform (SXPsec) and described here is a transparent solution for encrypting IP multicast using IPsec and consists of a sender and a receiver component. Figure 2 shows the software modules that comprise the sender and the receiver.

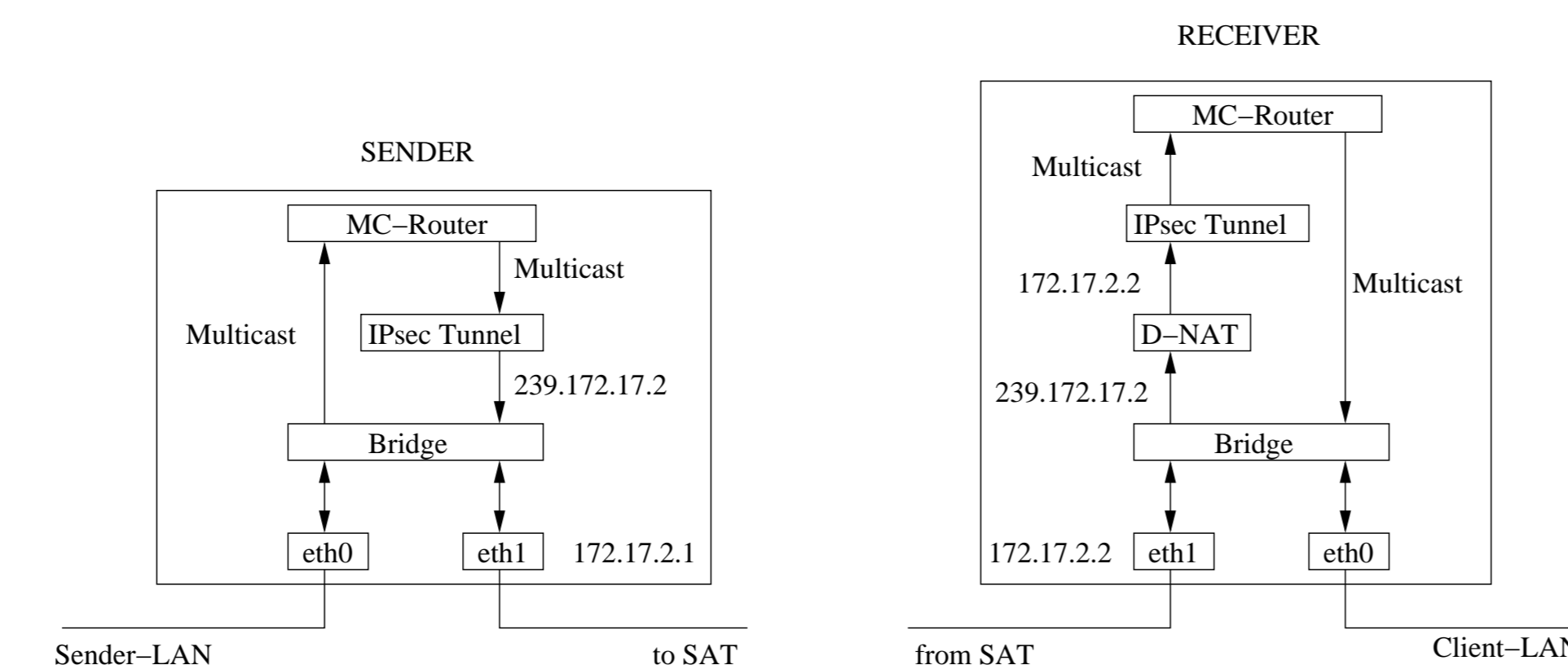


Figure 2: Software components involved in the SatNEx platform security extension.

The sender-side part of the security extension is a **Multicast Encryption Gateway (MEG)** which is placed between the multimedia conferencing bridge and the satellite up-link. Basically, the MEG acts like an Ethernet bridge, passing everything from one Ethernet interface to the other. However, multicast Ethernet frames are treated in a special way: they are passed up the network stack where the multicast IP packets are routed through an IPsec tunnel and encrypted. The resulting IP packets carrying the Encapsulated Security Payload (ESP) are sent to a special multicast address, the **Multicast Tunnel Endpoint (MTE)** address.

At the receiver, a device is placed between the IPricot and the client LAN, to which, for example, the Polycom VSX 7000 is attached. This device is called the **SXPsec client**. It behaves similar to the MEG in that it passes all non-multicast traffic that it receives from the IPricot on to the client LAN. However, IP packets destined to the MTE address are routed via the IPsec tunnel and decrypted. The clear-text IP multicast packets are then forwarded to the client LAN if at least one host reported to be a member of the corresponding multicast group, using the Internet Group Management Protocol (IGMP) Report message.

3. Demonstration Setup

The demonstration setup is intended to show two things: first, everything that is needed (such as hardware platform, software modules, etc.) is already available, and second, the performance suffices for enabling secure, high-quality multimedia transmissions.

Figure 3 shows a schematic overview of the demonstration setup. There is basically a PC acting as a **Video Sender** that transmits a stream containing video (6 Mbit/s) and audio (256 Kbit/s) via IP multicast over a transmission path to another PC that renders it, called the **Video Viewer**.

For securing the multimedia transmission, a transparent Security Extension is inserted at the network layer. It consists of the **Multicast Encryption Gateway** at the sender side (left) and the **Decryption Gateway** at the receiver side (right). They establish an Multicast IPsec Tunnel, as described in section 2, that is used for transporting IP multicast packets from the Video Sender to the Video Viewer.

Table 1 shows performance results of the SXPsec client that were obtained from a setup similar to the demonstration setup but without the DVB-T link.

Table 1: Performance of the SXPsec Client

Cipher Algorithm	Max Throughput
3des-cbc	2 Mbit
des-cbc	6,2 Mbit
blowfish-cbc	12 Mbit

The transmission path contains a wireless DVB-T link that is formed by two PCs: the **IP Encapsulation Gateway** is equipped with a PCI OFDM Modulator and acts as the sender, broadcasting an MPEG-2 Transport Stream (TS) that is created by taking all packets that it receives on its network interface and encapsulating them using Unidirectional Lightweight Encapsulation (ULE). The other PC, having a DVB-T PCI receiver card, performs as the **IP Decapsulation Gateway**. It receives the DVB-T signal carrying the ULE TS, decodes it and forwards the resulting packets to its network interface.

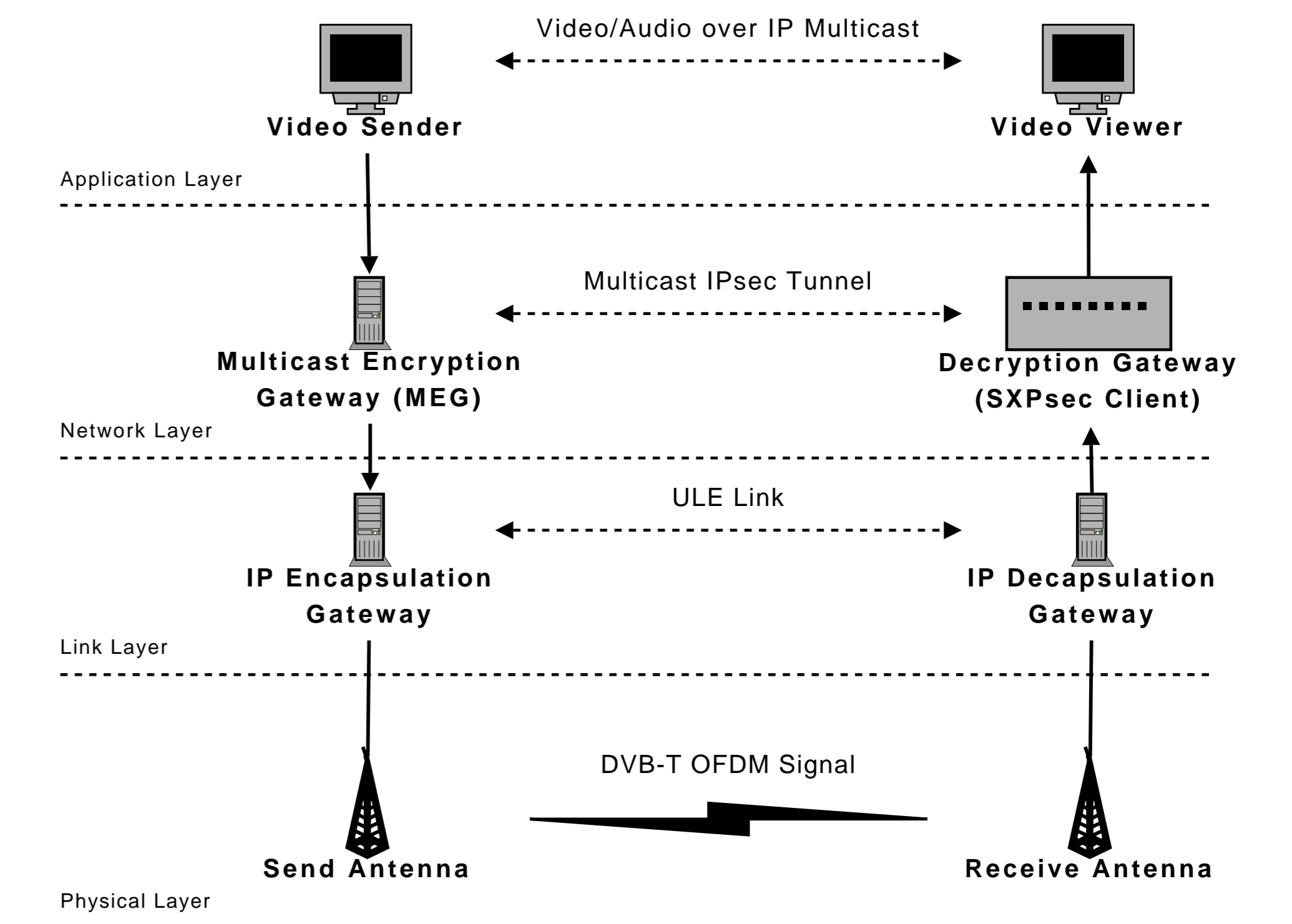


Figure 3: Overview of the demonstration setup

Here is a brief summary description of the components which comprise the setup:

Video Server The video server streams video/audio over IP multicast and is connected to the Multicast Encryption Gateway.

Multicast Encryption Gateway The Multicast Encryption Gateway uses IPsec to encrypt the multicast video/audio data. It sends the resulting IP packets which carry the encrypted video data to the IP Encapsulation Gateway.

IP Encapsulation Gateway This gateway takes all IP packets received on its input interface, encapsulates them and feeds the resulting MPEG-2 Transport Stream to the attached PCI OFDM Modulator.

IP Decapsulation Gateway The OFDM signal is received by this host and the ULE stream is decoded. The extracted IP packets are sent to the attached Decryption Gateway.

Decryption Gateway The Decryption Gateway filters all IP packets that are destined to the Multicast Tunnel Endpoint (MTE) address, decrypts the security payload and forwards the resulting IP packets (as received by the MEG) to the Video Viewer.

Video Viewer The Video Viewer receives the multicast video/audio stream from the Video Server and plays it.