Pairing for Distributed Camera Architecture in Telepresence

In a typical network each node has a unique IP address. We need to know the IP address of the device to communicate with. This prompts us to discover the interested devices before communication could begin. These devices have to be paired in order to establish secure communication.

In our current Telepresence products, cameras are connected to codecs directly using interfaces like HDMI, DVI, etc. With the concept of IP enabled Telepresence cameras would be connected to the network along with the codec in the meeting room. To establish the communication between the cameras and the codec we need a discovery and pairing mechanism.

The objective is to provide a seamless connectivity solution as an out of the box experience for the distributed camera architecture in Telepresence. Inspired by the immersive experience of Telepresence, we intend to incorporate the context of mobile devices as well as wireless technology like Bluetooth to provide an intuitive discovery, pairing and configuration solution. This mechanism takes into consideration that cameras do not have a display to provide identification information nor does it have any input devices.

Proposed Solution

Bluetooth and Wi-Fi-enabled devices are increasingly common nowadays especially in mobile devices. Simple Pairing enables two devices to communicate with one another over wireless technologies like Bluetooth/ultrasound/WI-FI etc. Pairing and configuring the Codecs and cameras using smartphone will enable ease of Use of Video Telepresence systems. Wireless technologies are useful when two or more devices are in proximity and require only modest bandwidth.

In such scenario we solve the problem using Proximity detection. We use a smartphone Proximity Application to configure our camera and codecs. Existing Wireless Medium between Camera/codec/Smartphone/BYOD devices is used as a communication channel to pair and configure.

Wireless communication is inherently vulnerable to security; we cannot rely on the wireless channel alone for establishing credentials. Thus, we rely on an additional security exchange over the primary IP channel.

These are the channels.

* Primary Channel [IP network based]

This is for secure media transfer and functions only after secure key exchanges like CA certificate, public/private keys.

* Secondary Channel.[Wireless channel]

This acts as a control medium responsible for configuration and Pairing. This channel exists between smartphone with the proximity application, codecs and cameras in the meetings rooms

First we establish a secondary channel over wireless medium between Smartphone/Codecs and Cameras. Cameras are paired with the Codec and configured with either Static IP or SSID/Wireless channel etc. incase of Wi-Fi Cameras. Once secondary channel is established Primary channel is established between the Cameras and the Codec and Video streaming can be initiated after authentication.

Some use case scenarios:

1. When Codec goes down/ New codec comes up

* When the codec goes down its safe to unpair the cameras with the codec and move the Camera to Configuration mode.
* This will be discovered based on periodic health pings between camera/codec
* Codec will have persistent memory that caches the pairing information.

1. When the Encoding camera goes down (Reboots)

* When an Encoding camera reboots, there is already an established communication channel established between Codec/camera.
* The codec can reinitiate the connection.
* If connection doesn’t happen in a given interval of time, we can move the camera to Configuration stage again)
* Reset button can be used to unpair the camera

Features:

* Maintains a consistent user experience across devices.
* Preserves simplicity to reduce vulnerabilities.
* This fits to seamlessly work with future distributed architecture products
* Our video Telepresence products as well have either USB support [to plug in wireless dongle] and also our pipelined products have inbuilt wireless chip support.