SENSORSTREAM

INVENTOR:

JASON W. RUPE

Description

A proximity streaming telemetry protocol that utilizes existing network solutions but relies on proximity and security for sharing of data, to facilitate troubleshooting and setup. Scan QR or initiate a default local exchange of other means such as by wireless radio, get keys to find (method, frequency, etc.) and read (protocol details, decryption keys, etc.) a signal, download apps and tools from internet automatically, and subscribe to the stream of telemetry.

Consider the scenario of a network device sharing telemetry and a reading device that needs instructions before it can communicate with the network device.

In one version the default could be a bootstrap from either a wireless RF signal or scan of the physical item, either of which assures proximity and can be controlled by the device owner. Any simple RF emission including Bluetooth, could be used as the delivery mechanism. The protocol would set up the bootstrap exchange to allow a reading device to scan for "pilot" signals which contain basic information for identifying how to obtain the telemetry from the device, including any data stream formats, where to obtain YANG Models, or other form of instructions for decoding the telemetry, including frequency bands to tune to for reading the data streams. The information encoded could be as simple as a MAC address or serial number which the reading device then can look up in a database to learn the protocol to follow (like getting a printer driver), or the pilot signal can contain the full instructions if monitored long enough, or it can be a simple redirect to a broader spectrum or data rate to enable more efficient instructions to be shared. Once the instructions are shared and interpreted by the reading device, the reading device can test and confirm interpretation of the data by a reference that is calibrated, and then the full data stream can be read and used for multiple purposes including network management, fault monitoring and management, troubleshooting, monitoring, installation assistance, and more.

For example, this method can be used to allow a user or technician to install a new network device like a cable modem, obtaining real time telemetry of the initialization process, and allowing an application on a cell phone, computer, or other device to interpret the signals for the user or technician.

This same approach can be used to form ad-hoc mesh networks over any wired or wireless network, for network management, monitoring, or even sensor network sharing.

The telemetry can be a stream of telemetry across one carrier, multiple carriers, based on existing telemetry models or protocols, or more. The idea here is to create the hardware and software and protocol to allow the bootstrapping of existing protocols in a one way or two way fashion so that greater automation of fault management, installation support, and other use cases are supported.

Security is enabled by the proximity need if using visual information or a local wireless or wired technology to interface. Otherwise, encryption, local storage, etc. would be added to allow only readers that are authenticated to be able to read the telemetry. Also, once networked, a device can have this turned off if desired, or the signal can be manually initiated with a button or proximity method such as a "turn on" signal from a reading device or plug in with a cable or other means.

Method flow 1:

0) sensorstream is turned on for a network or telemetry device, and a reading devices is started or is running.

1) A network or telemetry device encountered and either a physical designator (MAC address, QR code, etc.) or an RF signal (Bluetooth, Wi-Fi, IR, single carrier beacon, etc.) are detected by a reading device.

If physical:

2) The reading device reads the physical designator, looks up the information in a database to find instructions (perhaps utilizing a local data base or a network to reach a remote database).

3) The instructions indicate the physical connection technology, how to read the signal, and any protocol needed to turn the signal into information to use for the next step. The reading device implements the needed change in software to use its hardware to collect the information. If the information in this step is complete and the result is a telemetry feed (stream, packets, etc.) then the use case for needing the information begins. If not, repeat this step with the new information to the next connection step.

If an RF signal:

2) the RF pilot signal sends a repeated set of data according to a default, simple protocol of a start sequence, data, and end sequence, so that a reading device can bootstrap monitoring from this point. Note that pilot signals can be broadcast in multiple physical ways (even as packets if needed, analogous to the RF described here), and on multiple technologies including bluetooth, LoRa, Wi-Fi, even over Coax, twisted pair, Ethernet, optical, etc. The reading device reads the information, and puts tougher the complete set of data based on identifying the start and end sequences, plus the full data set. Based on the default protocol interprets the data set as instructions.

3) If instructions say to look up a code in a database for more information, the reading device uses its own information or a network to access information to look up and find the next instructions, indicating how to connect to the telemetry or next level of communication reading. The reading device implements the needed change in software to use its hardware to collect the information. If the information in this step is complete and the result is a telemetry feed (stream, packets, etc.) then the use case for needing the information begins. If not, repeat this step with the new information to the next connection step.

If a wired signal (including the intended network connection or an extra one such as a serial cable, USB, etc.), the behavior is the same as the RF signal if the wired signal is RF. Likewise, if optical, then replace RF with optical (light), and other technologies if analog. If a digital technology, meaning the physical connection is established and the method is applied on a network at higher level protocols, then there are network monitoring solutions today which do something like this, but using MIB databases. But this idea can extend that to create the one protocol to allow these monitoring solutions to bootstrap.

This idea as described thus far is a one way communication. However, a two way solution is possible as well, to allow local control in a limited way. The bootstrap process can complete in the reverse direction, or the instructions provided can also reveal role-based capabilities for recofiguration or control of the network device by the reading device, if authentication is added, and the reading device is reconfigured and has proper permissions to allow.

Background

Network devices require networks to even share telemetry about state, condition, faults, etc. This Catch 22 requires a solution for cases where installation and maintenance are needed but connectivity are not yet established. While we often rely on a person to set up the equipment, they may not be able to do so properly or fully due to complex equipment or service. We often hope that a basic connection can be established and then remote access can complete the installation properly, or some automated follow up. But that only works in ideal conditions.

Also, network monitoring solutions may not always be able to identify network devices fully to know what telemetry they can provide. This limits the ability to do fault management without more manual work and set up of systems, which becomes resource intense with questionable utility by those who need to do the work, so often set up is not complete.

A customer who is installing equipment in their home will often (more often than not) struggle and may fail at properly installing a device on their home network, or even an appliance that is not network connected, or troubleshooting said device if malfunctioning. A default telemetry protocol would allow a cell phone or other computing device to interface directly with the home device (networked or not) to allow interpretation of the telemetry to inform the customer of action to take, or even to share the information back to a manufacturer or maintenance company to identify and address the faults indicated through the telemetry.

Abstract

Create a simple protocol to allow bootstrapping of telemetry in support of installation and troubleshooting of network devices, or devices that are not normally networked, or sensors, either as a one to one (network or telemetry device to reader) or as part of an ad-hoc sensor network, etc.