Truly Uninterrupted Train-to-Ground Communications with Sub-50 ms Turbo Roaming

Scott Suen
Manager/Software Engineering
Moxa Inc.
A CBTC must be protected by a robust security system, and still maintain continuous communications in an environment where roaming occurs at very high speeds.

A data communication system (DCS) for railway applications provides both ground-based and onboard applications with a solution for exchanging information where and when it’s needed, irrespective of the position of the train. The usual DCS architecture for railway applications is an integrated Ethernet-IP network that includes a wired backbone network, wireless wayside network, and onboard network, with the onboard network handling communications between all communication-based train controller (CBTC) sub-systems. A CBTC must be protected by a robust security system, and requires continuous communication in circumstances where roaming is an unavoidable reality and occurs at very high speeds. For this reason, fast secure roaming and complete redundancy for a DCS are fundamental requirements for achieving smooth CBTC operation.

Major Challenges in Achieving Train-to-Ground Communications

A moving train is only connected to any one wayside AP for a few seconds, and handover times that exceed 100 ms could create significant data loss.

Perhaps the most crucial aspect of onboard vehicle stations is that they cannot lose any data during handover. For train-to-ground communication links that do not use an improved 802.11 roaming mechanism, the handover time may take up to several seconds. This is not acceptable, particularly since a moving train is only connected to a particular wayside AP for a few seconds, and handover times that exceed 100 ms could result in significant data loss. Reducing this roaming “break time” to a negligible level is a challenge faced by the rail industry.

Train passengers now expect data connection services with the same level of quality that they experience at home or in the workplace, and sensitive data must be reliably authenticated to ensure that the communications network is protected from outside attacks and internal threats. An important question then is this: How can we create a secure high-speed communications link between train and ground to ensure seamless data services for all passengers, keeping in mind that the networking devices will be affected by many tough operating environments?

Key Drawbacks of Currently Available Roaming Solutions

Client-based roaming takes up to 350 ms, because the clients must authenticate, re-associate, and exchange security keys. Complex controller-based roaming passes all the data through the controller, and handoff times are greater than 100 ms.

Until recently, only two general types of roaming solutions have been available on the market. The first approach is client-based roaming. In this case, each handoff must perform authentication, re-association, and security key exchange processes, which consumes a lot of time and can result in roaming times ranging from a few hundred milliseconds up to several seconds. Roaming times of even 1 second are intolerable for railway environments since the vehicle stations are highly mobile and need to frequently switch from one AP to another. The second approach involves using expensive complex controllers. In this case, all of the data must be transmitted through the controllers when a vehicle station...
needs to roam to a new AP and corresponding thin APs with only routing capability consume a huge amount of bandwidth. The undesirable outcome is that the costly heavy duty controllers result in handoff times greater than 100 ms.

Secure Sub-50 ms Turbo Roaming

For some time now, railway operators have been on the lookout for products that guarantee near-zero handoff latency between train and ground. Keeping the roaming “break-time” under 50 ms at high speeds ensures uninterrupted connections for transmitting critical data, such as real-time voice and video streams. The CBTC is performed by the non-vital Automatic Train Operation (ATO) components under the supervision of the vital Automatic Train Protection (ATP) components. Therefore, security is very critical for DCS to authenticate all communication between subsystems.

<table>
<thead>
<tr>
<th>Roaming Decision</th>
<th>Client-based</th>
<th>Complex Controller-based</th>
<th>Moxa Controller-based</th>
</tr>
</thead>
</table>
| Functionality    | • Only one channel in secure mode  
• Increases handoff delay due to authentication and re-association process | • All traffic must pass through a complex controller  
• Large bandwidth and slow traffic  
• Manages fewer APs with longer roaming delay  
• Costly, heavy-duty controller | • Central security key exchange only  
• No data pass-through  
• Three channels in WPA2 mode  
• Smooth traffic  
• Cost-effective alternative to “thin AP and complex controller” solution |
| Performance      | Handoff > 350 ms | Handoff > 100 ms | Handoff < 50 ms |

Comparison of different Roaming methods

Enable Pre-authentication Using a Wireless Controller

Moxa’s rail-specific Turbo Roaming is enabled by WAC wireless access controllers that provide centralized security management, and reduce the handoff time to 50 ms.

To overcome slow handoffs on high speed railways, Moxa’s rail-specific Turbo Roaming technology uses WAC wireless access controllers that provide centralized security management. When roaming to the next available AP, the client can be pre-authenticated by the WAC, which eliminates the need for authentication, and reduces the handoff time to 50 ms. Train speeds of 120 km/hr and more are supported to guarantee stable roaming handover for light rail and metro vehicles. With a proactive encryption and authentication mechanism, sub-50ms Turbo Roaming supports a high level of security features, including WPA, WPA2, and 802.11i, which ensure secure end-to-end communications.
A Small-scale WLAN only needs one controller

Deploying Small-scale WLANS: In a small-scale LAN, only a single WAC controller is needed, at the operations control center (OCC). This WAC is associated with several APs. In fact, a single WAC-1001 can manage up to 200 APs to deploy small-scale of WLANs on the same LAN.

Inter-controller Roaming enables larger WLANs with more APs and more controllers

Deploying Large-scale WLANs with Inter-Controller Roaming: To accommodate a larger scale WLAN, inter-controller roaming can be used to support hundreds of APs and multiple WACs. When the client hands over to a new AP associated with a different controller, the new WAC exchanges the authentication key with the original controller, and the new controller copies the security key to the new AP. In this way, the client spends less than 50 ms roaming, and does not compromise security.

Three-channel Roaming: On a WLAN, adjacent access points...
should work over different channels to avoid channel interference. In general, only a small number of non-overlapping channels are available for APs. In addition, other interference sources that can affect the operation of APs on a WLAN include radars and microwave ovens. To get around these problems, Moxa develops a roaming mechanism with three non-overlapping channels to minimize adjacent channels and co-channel interference.

**Excelling in Many Wayside Antenna Scenarios**

To ensure effective handoff for both vital and non-vital applications, Moxa offers a universal roaming method suitable for a variety of wayside antenna scenarios. Roaming is governed by the following 3-step logic:

1. Threshold 1: When AP1 is below this threshold, and
2. Threshold 2: when AP2 is above this threshold, and
3. Roaming offset: when AP2’s signal is stronger than AP1 with at least this RSSI offset, roaming is triggered.

By tweaking the various parameters, network operators can configure a roaming logic that works for their particular antennas and AP layout. For example, consider the 5 different wireless coverage scenarios below:
Scenario 2

Roam from AP1 to AP2, if
- AP1 below threshold1 (-55 dBm)
- AP2 above threshold2 (-45 dBm), and,
- AP2 is better than AP1 with at least offset value (5 dB)

Scenario 3

Roam from AP1 to AP2, if
- AP1 below threshold1 (-55 dBm)
- AP2 above threshold2 (-45 dBm), and,
- AP2 is better than AP1 with at least offset value (5 dB)
Links with Complete Redundancy

Multi-redundancy guarantees that the DCS system can provide uninterrupted, robust, and seamless mobility and continuous train-to-ground communications. A communication-based train controller (CBTC) is a train automatic control system based on a DCS architecture. Because of recent advances in wireless transmissions, CBTCs now rely heavily on WLANs to ensure constant train-to-ground data connections. The best way to avoid a link failure on a WLAN is through redundancy, which ensures that clients remain “always on” and allows critical network links to continue to transmit data. Moxa’s dual-RF products can be configured to operate as either redundant APs or redundant clients, with Turbo Roaming added to enable redundant roaming. APs and clients are then able to communicate with each other as long as at least one of the two links remains connected. WLAN products support Ethernet redundancy using RSTP and power redundancy using dual DC inputs and PoE. These multi-redundant features guarantee that the DCS system can provide uninterrupted robust seamless mobility, and ensure that safe and secure communication will always be available to meet the demands of video, voice, and other bandwidth-demanding
applications, such as maintenance tasks and passenger information systems.

**Sample Application Scenario**

Seamless roaming handover with a complete redundant DCS architecture provides reliable and sustained communication for smooth CBTC operations. Train-to-ground links are based on a radio frequency communication network that provides a connection between each client on the vehicle and an access point linked to the wayside network.

The DCS consists of both wired and wireless network systems:

**Redundant Wired Backbone Network:** The wired components of the DCS include the combination of Ethernet switches and fiber-optic cabling. The Ethernet switches can aggregate the interconnection of many APs and wayside control units, and are interconnected using single mode fiber optic cabling to establish a high-speed Ethernet backbone. Dual Ethernet switches are installed to form a redundant wired network.

**Redundant Wireless Wayside Network:** APs are placed at fixed locations along the track and perform as the interface between the wired network and wireless coverage area. Each access point is connected to an Ethernet switch with overlapping pattern, and uses fiber optic cabling to form ground radio connectivity. Dual APs are installed in the cabinet to provide the wireless wayside networks with redundancy.

**Redundant Onboard Vehicle Network:** Clients act as the mobile component of the train’s CBTC subsystems, and each train unit can be connected to the wayside network through the active client. It is crucial that clients on the moving trains do not lose any data during handover. The diagram shows two clients, with one at each end of the train, simultaneously connected to access points; however, only one client is actively transmitting data. The back-up client will be enabled if the active client experiences a loss in transmission while roaming from one access point to another. Installing a redundant client ensures that the network connection always performs as strictly expected.
Building More Successful Train DCS Systems

Three major factors contribute to the success of DCS deployments:
• Seamless high-speed roaming
• Universal roaming for different antenna scenarios
• Complete redundant links

Many successful train-to-ground projects have been completed using railway-specific sub-50ms Turbo Roaming and multiple redundant technologies to ensure reliable DCS connectivity. Get started on building a more secure and fast train-to-ground connection network now by visiting www.moxa.com.