Automatischer Netzwerkaufbau bei Zugwagenkopplung

Robuste WLAN-Access-Points mit intelligentem Verbindungsprotokoll

Detlev Schaadt, Produkt-Manager ELTEC Elektronik AG, Mainz

Viele Bahnbetreiber rüsten aktuell Ihre Züge mit WLAN-Lösungen aus, insbesondere um Passagieren Zugang zum Internet zu ermöglichen. Neben Access-Points, die den Netzwerkzugang erlauben, werden die Geräte mittlerweile auch dafür eingesetzt, ein Netzwerk (Ethernet-Backbone) über alle Zugteile hinweg automatisch aufzubauen oder die Verbindung nach außen zu gewährleisten. Per automatischer und eindeutiger WLAN-Netzwerk-Kopplung lassen sich die Netzwerke verschiedener Zugteile automatisch zusammenschalten, etwa beim Ankoppeln von Waggons oder Zusammenkoppeln zweier Züge. Moderne, robuste Access-Points mit ausgefeilten Protokoll- und Sicherheits-Algorithmen sorgen dafür, dass sich ausschließlich die richtigen Geräte verbinden und ein sicherer Datenverkehr gewährleistet ist.

WLAN Access-Points („Hot Spots") sind in Verbindung mit ihren Antennen im Allgemeinen so ausgelegt, dass Anwender (Clients), die sich in ihrem Funkfeld befinden, sich mit mehreren Geräten (gleichzeitig) verbinden können. Bei der geforderten eindeutigen Wagenkopplung für den Netzwerkaufbau ist die Zielsetzung jedoch anders. Sowohl in ICEs und anderen Fernzügen als auch im Nahverkehr mit S- und U-Bahnen werden einzelne Wagen und Lokomotiven oder auch zunächst autarke Züge zu einem einzigen Zug gekoppelt bzw. später wieder getrennt, wobei es keine Vorzugsrichtung gibt. Im fertig gekoppelten Zug soll ein durchgehendes Datennetz zur Verfügung stehen, das unabhängig von anderen Datenverbindungen automatisch bei der Zusammenführung der Wagen aufgebaut wird. Es ist nur eine einzige Verbindung von einem Zugwagen zum nächsten gekoppelten Zugwagen zulässig (Bild 1).

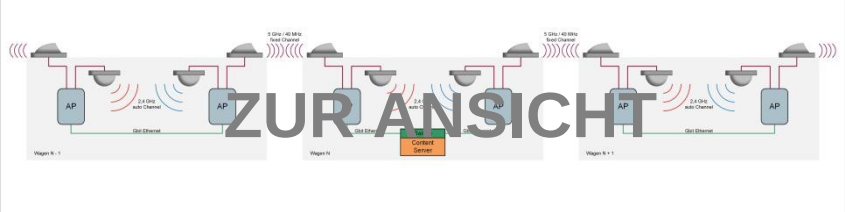

Bild 1: Prinzipieller Aufbau eines Ethernet-Backbone mit Waggon-Kopplung mittels WLAN Access-Points

Dies wird bei der drahtgebundenen Zugwagenkopplung dadurch erreicht, dass der eine Zugwagen eben nur mit dem ihm zugekoppelten Zugwagen über eine Verbindungsleitung und deren Steckverbindung elektrisch verbunden ist. In bestehenden Zügen ist jedoch meist kein Platz mehr für eine nachträglich zu installierende Ethernet-Verbindung vorhanden.

Bei der drahtlosen Zug-Netzwerk-Kopplung geht es also um die Aufgabe, automatisch eine eindeutige paarweise Verbindung zwischen gegenüberstehenden Wagenenden verschiedener Zugwagen aufzubauen. Insbesondere muss verhindert werden, dass baugleiche und gleich konfigurierte Access-Points in der näheren Umgebung, wie zum Beispiel Zugwagen auf dem Nachbargleis, fälschlicherweise verbunden werden.

Eindeutige und automatische Verbindung

Die drahtlose Datenübertragung zwischen zwei gekoppelten Zugwagen erfolgt beim Senden ausgerichtet. Dabei muss die Strahlrichtung (Antennenkeule) räumlich so gewählt werden, dass die Verbindung nur in einer bestimmten räumlichen Position der paarweise zu koppelnden Zugwagen und deren Einrichtungen zum Senden und Empfangen von Daten besteht. Die eindeutige Verbindung zwischen zwei zu koppelnden Zugwagen zu erreichen stellt eine Herausforderung dar, da bei Hochfrequenzverbindungen immer mit Reflexionen der übertragenen elektromagnetischen Wellen zu rechnen ist.

Um wirklich den nächstliegenden Access-Point anzusprechen, ist die Einstellung der Sendeleistung und/oder dir Empfängerempfindlichkeit essenziell. Üblicherweise strahlen die Sender möglichst stark und die Empfänger sind möglichst empfindlich. In der beschriebenen Situation wird das Risiko einer Fehlkopplung zum Nachbargleis aber geringer, wenn die WLAN-Komponenten eine definierte eingeschränkte Reichweite haben. Das wird durch gezielte Senkung der Sendeleistung und Empfängerempfindlichkeit erreicht.

Eine Herausforderung stellt hierbei die Kurvenfahrt der Züge dar. Um die Aufrechterhaltung der Verbindung zu sichern, können die Antennen je nach Applikation entsprechend konfiguriert werden. Reißt die Verbindung dann doch einmal ab, versucht der Access-Point innerhalb einer definierten Zeit diese wieder aufzubauen. Überschreitet die Ausfallzeit den definierten und vorher konfigurierten Schwellenwert, nimmt der Access-Point an, dass der Waggon abgekoppelt wurde. Komplette Ausfallsicherheit kann durch eine Ring-Architektur mit Redundanz erreicht werden.

Intelligentes Protokoll für die automatische, sichere Kopplung

Um die beschriebene Aufgabenstellung zu bewältigen, müssen die Access-Points über eine gewisse „Intelligenz“ verfügen. Sie benötigen einen Algorithmus für das automatische und fehlerfreie Finden des Partners (Master und Client) und für die verschiedenen Betriebsfälle. Außerdem muss die Verbindung verschlüsselt werden.

Das von ELTEC entwickelt ICCP (Inter Carriage Connection Protocol) ist ein Bridging-Algorithmus für die automatische Etablierung eines WLAN-Backbones in Zügen. Der Algorithmus ist in der Firmware des WLAN Access-Points (CyBox AP) abgelegt. Die drahtlosen Backbones können in bestehenden Applikationen eingesetzt werden, wo es nicht oder nur erschwert möglich ist, Ethernet-Kabel für die Wagen-Kopplung einzufügen. Die Haupt-Charakteristika des ICCP-Algorithmus sind:

- Nutzung des RSSI (Received Signal Strength Indicator) für die Auswahl des Kopplungspartners im Reichweitenbereich. Der RSSI stellt einen Indikator für die Empfangsfeldstärke kabelloser Kommunikationsanwendungen dar.
- Master-Client-Verbindung über den WDS (Wireless Distribution System)-Modus
- Unterstützung für alle gängigen Verschlüsselungen (WPA2-PSK, etc.)
- One-Time-Konfiguration
- Automatisierter Kopplungs-/Entkopplungs-Prozess, Abspeicherung von bestehender Verbindung nach Verlust der Spannungsversorgung
- Freie Kanalwahl mit 2,4 oder 5 GHz mit allen HT-Modes (20/40+/40-)

Das Kopplungsverfahren basiert darauf, dass SSIDs (Service Set Identifier) alphanumerische Bezeichnungen nutzen, die übertragen werden können. Mittels SSID ist der Access-Point eindeutig ansprechbar. So kann der SSID dafür genutzt werden, Informationen zu übertragen und zu einem bestimmten Zeitpunkt auch in einem Dialog-Modus Informationen auszutauschen. Grundsätzlich nutzen die Access-Points ihre achtstellige Seriennummer für die eindeutige Identifizierung. Darüber hinaus können SSIDs auch noch Statusinformationen für das Monitoring der Verbindung beinhalten. Bei der CyBox AP/ICCP-Lösung beginnen die SSIDs immer mit einer definierten Buchstaben-Sequenz („CYAP“), um die Funkaktivitäten gegenüber anderen Access-Points, die nicht zum Intertrain-Netzwerk gehören zu filtern.

Die Kopplung mittels ICCP erfolgt nach folgendem Schema: Der aktivierte Access-Point (anfänglich sind alle Master) sendet seine SSID mit seiner Seriennummer. Dabei sucht er nach dem geeignetsten Partner mit der besten Signalstärke. Dieser Vorgang wird mehrmals wiederholt, um eine stabile Verbindung sicher zu stellen. Nach erfolgreicher Suche bilden die Partner ihre IDs gegenseitig ab und codieren diese in ihre eigene ID. Damit wird eine einzigartige SSID erstellt, die nur für diese Verbindung gültig ist. Das Gerät mit der höheren Seriennummer wird nun zum Master, das andere zum Client. Die SSID ist nun verborgen und geschützt.

Geht die Verbindung verloren (Funkstörung, Zug-Neukonfiguration, etc.), versucht der Access-Point die letzte Verbindung innerhalb einer vorkonfigurierten Zeit (siehe Bild 2) wieder herzustellen. Gelingt dies nicht, geht das Gerät in den „Idle“-Status und wartet auf einen neue Peer-Verbindung.

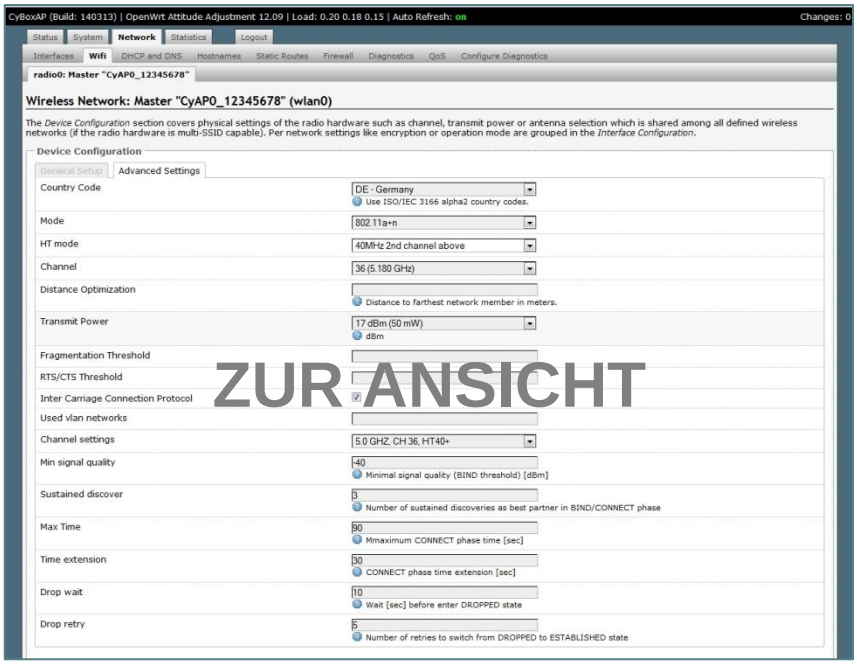

Bild 2: Das ICCP (Inter Carriage Connection Protocol) ist ein Bridging-Algorithmus für die automatische Etablierung eines WLAN-Backbones in Zügen. Mittels ICCP können die Access-Points entsprechend konfiguriert (z.B. die Sendeleistung, Zeit für den Verbindungsaufbau, etc.) werden.

Sichere Anwendung dank Client Isolation und VLAN

Ein weiteres Feature der CyBox AP und ihrer Firmware ist die Client Isolation über den gesamten Backbone hinweg. Die Client Isolation stellt sicher, dass WLAN-Clients nur den Content-Server erreichen können, nicht jedoch andere Clients. Im Funkbereich eines einzelnen Access Points wird dies bei entsprechender Konfiguration bereits im Radio-Modul erledigt. Allerdings leitet der Access Point alle Datenpakete, die er von WLAN-Clients bekommt, an den Backbone weiter (Ethernet-WLAN Bridge). Diese Pakete erreichen neben dem Content-Server auch alle anderen Access Points des Backbone-Netzes. Gemäß ihrer Bridge-Funktion würden diese Pakete so von allen anderen Access Points abgestrahlt und wären für alle Clients sichtbar. Die CyBox AP besitzt auf Layer-2 wirksame Filter, die verhindern, dass Pakete, die nicht vom Content-Server kommen, angenommen und auf das eigene WLAN gebrückt werden. So ist die Privatsphäre aller WLAN-Clients über den gesamten Backbone sichergestellt.

Der Backbone muss, neben den Nutzkanälen für die Internet-Nutzer, auch Verwaltungs- und Abrechnungsinformationen zwischen Content-Server und Access Points austauschen. Der Backbone und seine Verwaltungskanäle müssen als geschlossenes und gesichertes Netz, aber die Content-

Bereitstellung als offener Teil betrieben werden. Die sichere Trennung von Content und Verwaltungsinformation ist also zu gewährleisten, um eine Angreifbarkeit dieser gesicherten Kanäle zu verhindern. Hierfür unterstützt der Access Point - auch bei Nutzung des ICCP – die Verwendung von Virtual Local Area Networks (VLANs).

Ein Wireless Access Point kann mehrere SSID zugleich tragen. Solche multiplen SSID ermöglichen es, mehrere VLANs anzubieten. Ein VLAN ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks. Es trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches die Frames (Datenpakete) eines VLANs nicht in ein anderes VLAN weiterleiten, und das obwohl die Teilnetze an gemeinsame Switches angeschlossen sein können. VLANs können Netze gegen das Ausspionieren und Abhören sichern. Sie sind robuster als „geswitchte Netze“, denn zur Verbindung der VLANs kommen Router zum Einsatz, die gegen Layer-2-Attacken systembedingt unempfindlich sind.

Von ELTEC ist eine Demo-Implementierung erhältlich, die VLANs für die ICCP-Kommunikation nutzt (Bild 3).

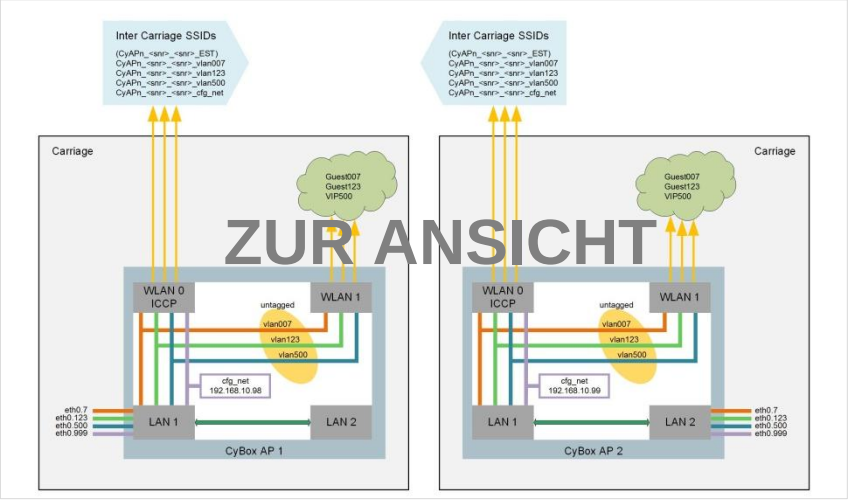

Bild 3: Eine Beispiel-Konfiguration, die VLANs für die ICCP-Kommunikation nutzt

WLAN Access-Point CyBox AP

Die CyBox AP (Bild 4) ist ein Wireless Access Point, der speziell für die rauen Umgebungsbedingungen in Schienenfahrzeugen, aber auch Automotive- und Industrie-Applikationen entwickelt wurde. Mit der CyBox AP können mehrere mobile WLAN-fähige Geräte in einem Personenzug, Bus oder der U-Bahn mit dem Internet kommunizieren oder auf lokale Daten wie Fahrplaninformationen,

Videos etc. zugreifen. Außerdem kann die CyBox AP für die dargestellte automatische Zugkopplung und den Aufbau eines durchgängigen Zug-Netzwerkes genutzt werden.

Bild 4: CyBox AP ist ein Wireless Access Point, der speziell für die rauen Umgebungsbedingungen in Schienenfahrzeugen, aber auch Industrie- und Automotive-Applikationen entwickelt wurde.

Die Spannungsversorgung für die CyBox AP ist sehr flexibel ausgelegt: Sie kann über eine lokale 24-110-V-Gleichspannung versorgt werden. Als weitere Möglichkeit zur Spannungsversorgung bietet die CyBox AP einen PoE-Eingang (gemäß IEEE802.3af) für eine Class 3-Versorgung.

Die nur etwa 1 kg schwere CyBox AP hat kompakte Einbaumaße (105 mm x 54,12mm x 194mm) und eine Leistungsaufnahme von maximal 12 W. Die maximal 6 Antennen werden über SMA-Steckverbinder angeschlossen. Das robuste Aluminiumgehäuse gemäß IP30 erlaubt einen lüfterlosen Betrieb bei -40°C bis +70°C (EN 50155, Class TX) und hohe Schock- und Vibrations-Belastungen gemäß den gängigen DIN-, EN- und IEC-Industriestandards.

Hart im Nehmen

Industrial Ethernet hat sich als Backbone für alle bandbreitenintensiven Applikationen innerhalb von Bussen und Bahnen etabliert. Die Anforderungen für die in diesen rauen Umgebungen eingesetzten Komponenten sind beispielsweise in Standards dokumentiert wie e-Mark für den Straßenverkehr,

EN50155 für Schienenfahrzeuge oder EN50121 für Signal- und Telekommunikationseinrichtungen neben der Schiene.

Die CyBox AP verfügt über die Zulassung gemäß der Bahn-Norm EN 50155. Nach EN 50155 entwickelte Produkte sind ausgelegt für erhöhte Vibrations- und Schockfestigkeit, verbesserte EMV sowie erweiterte Sicherheit in Bezug auf Entflammbarkeit und Entwicklung von Rauch und giftigen Gasen. Die CyBox AP erfüllt die Temperaturklasse TX, d.h. das Gerät kann dauerhaft in Umgebungstemperaturen von -40 °C bis +70 °C betrieben werden und toleriert eine Übertemperatur bis +85 °C für 10 Minuten. Die EN 50155 schreibt weiterhin Schock- und Vibrationstests vor, deren Grenzwerte und Durchführung in der EN 61373 näher erläutert sind. Die geprüften Grenzwerte entsprechen der Kategorie 1, Klasse B.

Die CyBox AP erfüllt auch alle relevanten EMV-Vorgaben und übertrifft die in der EN 50155 vorgeschriebenen Anforderungen hinsichtlich der Toleranz gegenüber Schwankungen der Versorgungsspannung. Selbst kurzzeitige Unterbrechungen der Versorgungsspannung bis zu 10 ms werden bei vollem WLAN-Betrieb überbrückt, so dass das Gerät konform zu EN 50155, Klasse S2 ist.

Fazit und Ausblick

Die CyBox AP ist ideal für den automatischen Aufbau von Netzwerk-Backbones in Zügen, S- und U-Bahnen. In Kombination mit dem Bridging-Algorithmus ICCP in der Firmware der CyBox AP wird die automatische und zuverlässige Einrichtung und Aufrechterhaltung des Netzwerkes unter allen Betriebsbedingungen gewährleistet. Darüber hinaus gibt es Zugapplikationen, die eine Landverbindung mit dem Backoffice erfordern, wie z.B. für Verbindungsinformationen, Sitzplatzreservierungen oder Signal- und Betriebsinformationen. Derzeit wird dies (d.h. der Zugfunk) über GSM-R (Railway) mit eingeschränkter Bandbreite erledigt. Zukünftig bietet sich für die schnelle und breitbandige Zug-Land-Verbindung der LTE-Standard an. Auch dafür steht mit der CyBox LTE eine Lösung bereit.

Weitere Informationen erhalten Sie unter www.eltec.de.

ELTEC Elektronik AG

Die ELTEC Elektronik AG mit Firmensitz in Mainz bietet zielgerichtete, anwendungsorientierte Systemlösungen auf Basis leistungsfähiger Hardware- und Software-Produkte für ein breites Spektrum von Industrie-Applikationen. Der Fokus liegt dabei auf der Automatisierungs-, Steuerungs- und Prozesstechnik. Das umfangreiche Produktportfolio umfasst CPU/SoC-Boards, Framegrabber, I/O-Produkte, Imaging-Lösungen, Software sowie komplette System-Lösungen. ELTEC entwickelt und fertigt nach CE- und ISO 9000-zertifizierten Qualitätsstandards.

KONTAKT

ELTEC Elektronik AG
Daniela Höhn
Galileo-Galilei-Str. 11
55129 Mainz

Fon +49 6131 918 0
Fax +49 6131 918 195
Email dhoehn@eltec.de
www eltec.de

KONTAKT AGENTUR

MEXPERTS AG
Rolf Bach
Trimburgstraße 2
81249 München

Fon +49 89 897361 14
Fax +49 89 897361 29
Email rolf.bach@mexperts.de
www mexperts.de

Text und Bild können Sie unter www.eltec.de/über uns/news herunterladen.