Funknetze sicher planen

Ganzheitliche Abdeckung und Zugriffssicherheit als Herausforderung

Kai-Oliver Detken

Die Hauptanforderungen bei der Nutzung von Wireless LANs (WLAN) betreffen die ganzheitliche Abdeckung sowie die Zugriffssicherheit. Der Aufbau von WLANs wird normalerweise im Infrastrukturmodus vorgenommen. Dieser ähnelt von der Topologie her dem Aufbau von Mobilfunknetzen. Die Basisstationen, sog. Access Points (AP), werden in dem gewünschten Bereich verteilt und sind für die Anbindung der mobilen Endgeräte zuständig. Die Basisstation sendet in einstellbaren Intervallen Datenpakete, sog. Beacons, an alle Stationen im Empfangsbereich. Diese enthalten als Informationen den Netznamen (Service Set Identifier – SSID), die möglichen Übertragungsraten sowie die Verschlüsselungsart.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Indem eine WLAN-Basisstation kontinuierlich kleine Datenpakete versendet, kann sie jederzeit die Übertragungsqualität in Richtung des Endgerätes kontrollieren. Auch kann ein Verbindungsaufbau zügiger erfolgen, da beide Knotenpunkte (Endgerät und AP) permanent bereits Daten austauschen, obwohl noch keine Nutzdaten vorhanden sind. Durch den Aufbau von vielen Basisstationen soll dann eine komplette Netzabdeckung innerhalb eines Unternehmens erfolgen. Dies impliziert eigentlich auch eine unterbrechungsfreie Anbindung mobiler Endgeräte bei einem Wechsel der Basisstation. Allerdings kommt es hier in der Praxis öfters zu Störungen. So sind die Basisstationen nicht immer weit genug voneinander entfernt, oder die Frequenzbereiche der APs stören sich gegenseitig. Hinzu kommt, dass es bei Basisstationen keine üblichen Handover-Mechanismen gibt, die ein Weiterreichen der Endgeräte an die nächste Station vor einem Verbindungsabbruch unterstützen. So reißt in den meisten Fällen die Verbindung zum AP kurz ab, bevor eine neue Verbindung aufgebaut werden kann. Dies kann aber bereits negative Folgen für eine Anwendung bedeuten – bei Echtzeitdiensten wie Voice over IP (VoIP) etwa einen Gesprächsabbruch.

Ad-hoc-Netze

Alternativ können WLANs im Ad-hoc-Modus umgesetzt werden. Hierbei sind alle Stationen gleichwertig und versuchen, sich gegenseitig zu vernetzen. Auch hier ist eine Netzkennung auf Basis der SSID erforderlich. Die Koordination wird aber von jedem Endgerät separat ausgeführt, was zwar eine höhere Flexibilität verspricht, gleichzeitig aber auch die Komplexität erhöht. Eine Weiterleitung von Datenpaketen zwischen den Endgeräten ist nicht vorgesehen, um keinen Netzüberblick weitergeben zu können. Um auch größere Ad-hoc-Netze zu ermöglichen, sind die teilnehmenden Stationen mit Routing-Fähigkeiten auszustatten. Dafür müssen Daten gesammelt, ausgetauscht und weitergeleitet sowie Routing-Entscheidungen getroffen werden.
Schließlich muss jedes Endgerät für das Routing weitergeben, welche anderen Endgeräte es sieht und wie die Verbindungsqualität ist. Durch die sich dauernd ergebenden Änderungen sind sehr oft Routing-Informationen zu verschicken, was zu einer schlechten Skalierbarkeit führt. Verschiedene Forschungsprojekte haben sich daher des Themas angenommen, das aber noch nicht zufriedenstellend gelöst ist. Routing-Beispiele sind Ad-hoc On-demand Distance Vector (AODV) oder Optimized Link State Routing (OLSR). Als Standardisierungsvorschläge wurden das Hybrid Wireless Mesh Protocol und IEEE 802.11s eingebracht.

Beispiellösungen

Als Beispiel für ein Projekt sei HiMoNN (Highly Mobile Network Node) genannt, das von der IABG mbH umgesetzt wurde. Sie bietet eine Kommunikationslösung für Einsatzorte ohne feste Infrastruktur an. Dabei ist das System mobil im Fahrzeug, stationär oder als tragbare Kommunikationslösung einsetzbar. Es werden Datenübertragungsraten von bis zu 6,5 Mbit/s bei mobiler und bis zu 16 Mbit/s bei stationärer Anwendung ermöglicht, bei Reichweiten bis zu 2 km zwischen zwei Stationen. Dadurch reicht die Bandbreite für Anwendungen wie Audio-, Video- und Datenübertragung aus. Einsatzbeispiele gibt es in diversen Katastrophenfällen, weshalb das Produkt heute von Feuerwehr, Polizei und in der Verteidigung bereits eingesetzt wird. Der Kern des

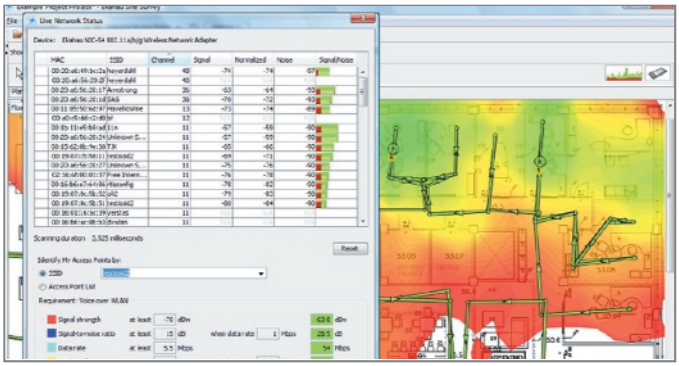
Systems besteht aus einer Anzahl mobiler Kommunikationsknoten, die sich nach der Inbetriebnahme automatisch untereinander vernetzen. Hierbei werden die Kommunikationsrouten automatisch so eingestellt, dass eine bestmögliche Verbindung aller Knoten untereinander möglich ist. Bei beweglichen Kommunikationsknoten werden die Verbindungen untereinander permanent optimiert und somit den neuen Umgebungsbedingungen dynamisch angepasst.

Als weitere Alternative kann die WLAN-Technik auch im Wireless-Bridging-Modus (nach IEEE 802.11c) verwendet werden, um beispielsweise zwei Unternehmensgebäude miteinander zu vernetzen. Im Bridging-Modus besteht zwischen zwei APs eine dedizierte Funkverbindung. Die Identifikation der Gegenstelle erfolgt über die MAC-Adresse. Aus Sicherheitsgründen werden Anmeldeversuche von drahtlosen Endgeräten verweigert. So können ohne bauliche Maßnahmen kostengünstig Gebäudeverbindungen realisiert werden.

Unternehmenseinsatz

Für Unternehmensnetze kommen solche Ad-hoc-Netze nicht in Betracht. Hier wird auf stationäre APs Wert gelegt, um Ausleuchtung und Sicherheitsbestimmungen des Unternehmens zu genügen. Anfangs wurden sehr viele APs nach dem IEEE-Standard 802.11b mit einer Bruttodatenrate von 11 Mbit/s verbaut. Man gelangte allerdings bei einer Nettoübertragungsrate von maximal 4 Mbit/s schnell an die Leistungsgrenze.

Auch war die Einrichtung sehr mühselig, da jeder AP einzeln konfiguriert und verwaltet werden musste. Da sich die Entwicklung weiterer WLAN-Techniken aber in den letzten Jahren regelrecht überschlagen hat, kann man heute bereits proprietäre Lösungen mit 100 bis 120 Mbit/s Nettodatenrate nutzen, die allerdings noch nicht 802.11n-kompatibel sind. Dieser Standard wurde erst in diesem Jahr endgültig verabschiedet, so dass standardkonforme Systeme erst demnächst zu erwarten sind. Hinzu kommen Möglichkeiten wie die Nutzung zentraler Wireless-Controller, die neben der Verteilung zentraler Sicherheitseinstellungen auch ein Firmware-Upgrade zentral steuern können. Durch den Einsatz von Power over Ethernet (PoE) müssen heutige APs auch nicht mehr zweifach (Netz- und Stromdose) angeschlossen werden, sondern können ausschließlich den Ethernet-Anschluss nutzen. Dies lässt sich heute so konfigurieren, dass bei Anschluss des APs automatisch die aktuelle Firmware geladen und Sicherheitseinstellungen umgesetzt werden. Um APs gleichmäßig ausrollen zu können, sollte man sich die Örtlichkeiten genau vergegenwärtigen. Auch die verwendete WLAN-Technik spielt eine entscheidende Rolle. So besitzen die WLAN-Standards unterschiedliche Reichweiten und Empfindlichkeiten, die von der spezifizierten max. Sendeleistung abhängen. Während IEEE 802.11b und 802.11g ca. 30 bis 50 m bei einer Sendeleistung von 100 mW schaffen, kann man bei 802.11a größere Entfernungen annehmen, da hier die Sendeleistung auf 200 bis 1.000 mW heraufgesetzt wurde.



Das Tool Ekahau Site Survey (ESS) dient zum Überprüfen der WLAN-Ausleuchtung

Einschränkende Faktoren

Die Reichweite von WLANs hängt aber von weiteren Faktoren ab – ganz wichtig sind die Räumlichkeiten und die direkte Umgebung, z.B. der Einsatz in einer Lagerhalle mit oder ohne Metall-Hochregalen. Auch die Wandbeschaffenheit ist für die Ausbreitung der Funkwellen relevant. Holzwände lassen WLAN-Verbindungen eher zu als dies bei Betonwänden der Fall ist. Hinzu kommen Herstellerunterschiede, obgleich dieselben Standards verwendet werden.

Die Sendeleistung lässt sich bei den professionellen APs regulieren, was bereits Abhilfe bei der Ausleuchtung schaffen kann. Dabei kommt auch den verwendeten Antennen eine erhöhte Bedeutung zu. Normale Antennen erreichen im Freien ca. 300 m. Innerhalb von Gebäuden sinkt die Reichweite bereits bei dünnen Wänden auf etwa 40 m ab. Starke Betonwände können sogar eine komplette Abschattung bewirken. Eine Antennenverbesserung kann hier auch im Freien Reichweiten von bis zu 20 km ermöglichen (z.B. bei Wireless Bridging), wobei in Deutschland eine Sendeleistung von 100 mW EIRP im 2,4-GHz-Bereich nicht überschritten werden darf. Antennen bringen sowohl einen Sende- als auch einen Empfangsgewinn (dBi), indem sie elektromagnetische Wellen bündeln. Daher muss statt der Sendeleistung die sog. Effektive Isotrope Strahlungsleistung (EIRP) zur Beschränkung herangezogen werden.

Bei der Umsetzung wird heute meistens auf IEEE 802.11g in Verbindung mit 802.11b für ältere Endgeräte gesetzt. Beide Standards sind zueinander kompatibel, so dass man sie gemeinsam nutzen kann. Allerdings erkauft man sich diese Flexibilität mit einer geringeren Nettoübertragungsrate. Der Standard IEEE 802.11a hat sich aufgrund seines 5-GHz-Bandes in Europa nicht durchgesetzt, da anfangs andere Sendeeinrichtungen wie militärische Radarsysteme dadurch gestört werden konnten. Inzwischen hat man dies zwar durch die Integration eines dynamischen Frequenzwahlverfahrens und Übertragungssendeleistungssteuerung kompensieren können. Dies hemmte aber die Marktver-

breitung erheblich. Der Standard IEEE 802.11n ist noch zu neu, um sich bereits etabliert zu haben. Allerdings sind bereits einige Geräte auf dem Markt, die auf der Vorabversion des Standards basieren.

Bei der Planung von 802.11b/g-Netzen sollte die Überlappung von gleichen Kanälen vermieden werden. Der Kanalabstand beträgt 5 MHz, während eine Funkverbindung eine Bandbreite von 22 MHz beansprucht. Zwischen zwei benutzten Kanälen müssen daher mindestens vier Kanäle ungenutzt bleiben, um keine Störungen zu bekommen. Daher lassen sich bei 13 Kanälen in Europa maximal drei Kanäle überlappungsfrei nutzen. Wenn sich dies nicht vermeiden lässt, sollte auf weniger ungenutzte Kanäle gewechselt werden. Bei 802.11a-Netzen lassen sich hingegen alle verfügbaren 19 Kanäle überlappungsfrei einsetzen. Dies wird durch das verwendete Frequenzwahlverfahren Dynamic Frequency Selection (DFS) ermöglicht. Mit DFS kann eine Basisstation automatische Kanalwechsel initiieren, falls auf dem verwendeten Kanal ein anderes Gerät erkannt wurde. Die Kanalauswahl erfolgt dabei zufällig. Der AP teilt anschließend den anderen Teilnehmern den neuen Kanal mit.

Neben der Vorplanung kann auch im Nachhinein der Aufbau bzw. die Ausleuchtung überprüft werden. Ein Beispiel dafür kommt von der Avanis GmbH, die mit ihrer Software Ekahau Site Survey (ESS) die Planung unterstützt, indem das Netz vor der Umsetzung visualisiert werden kann. Nach dem WLAN-Aufbau können alle Basisstationen automatisch erfasst und analysiert werden (*Bild*). Dabei werden u.a. die Signalstärke, die Datenrate, die Interferenzen und die Signalüberlappung erfasst. Dadurch kann nach dem Aufbau objektiv überprüft werden, ob alle Anforderungen an das WLAN erfüllt werden konnten. Ein ausführlicher Netzbericht dokumentiert die Umsetzung. Durch das Erfassen und Visualisieren des WLANs können Fehler im Betrieb erkannt und dokumentiert werden. Auch fehlerhaft konfigurierte APs lassen sich so auffinden.

Eine Netzanalyse kann auch mit der Open-Source-Software Wireshark erfolgen (**www.wireshark.org**). Das Programm stellt nach der Aufzeichnung des Datenverkehrs einer LAN-Verbindung die Daten in Form einzelner Pakete dar. Sie werden dabei übersichtlich und für den Anwender nachvollziehbar analysiert. Das Analysetool lässt sich durch weitere Plug-ins wie AirPcap WLAN-fähig machen. Dabei werden alle 802.11-Daten-/Management- und Control-Frames erfasst und zur weiteren Analyse an Wireshark übermittelt. Unterstützt werden 802.11a/b/g/n-Netze. Als zusätzliche Hardware ist nur ein USB-Adapter mit interner Antenne und MC-Anschluss für externe Antenne notwendig. Zusätzlich kann auch WLAN-Verkehr zur Überprüfung der WLAN-Security simuliert werden.

Absicherung

Die Absicherung der WLANs nimmt immer noch einen wichtigen Stellenwert ein. Dabei sind folgende Mechanismen von Bedeutung:

- Service Set Identity (SSID): Der Standard bietet die Möglichkeit, einen Netznamen (SSID) zu vergeben. Es wird der eingetragene Name überprüft, und nur Teilnehmer mit der gleichen SSID können am Netz teilnehmen. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie allerdings mit einfachen Mitteln in Erfahrung bringen. Etwas Abhilfe schafft die Unterdrückung des automatischen Broadcast-Mechanismus.
- MAC-Adresse: Jede Netzkarte verfügt über eine eindeutige MAC-Hardwareadresse. Prinzipiell ist es möglich, in einem WLAN MAC-Adressen zu definieren, denen es erlaubt ist, mit einem AP zu kommunizieren. Allerdings gibt es die Möglichkeit, MAC-Adressen vorzutäuschen (MAC-Spoofing).
- WEP: Vertraulichkeit, Integrität und Authentizität im Funk-LAN sollen durch das Protokoll Wired Equivalent Privacy gesichert werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder optional 104 bit und muss den am WLAN beteiligten Clients sowie dem AP vorab zur Verfügung gestellt werden. Dabei wird für das gesamte Funk-LAN ein gemeinsamer Schlüssel verwendet. Alle WEP-Implementierungen haben jedoch den Nachteil, dass sie auf dem RC4-Algorithmus aufbauen, der inzwischen als unsicher eingestuft wird. Der Schlüssel ist zudem durch geeignete Angriffstools in kürzester Zeit kompromittierbar.
- WPA2: Der WEP-/WPA-Nachfolger ist der Sicherheitsstandard WPA2 (nach IEEE 802.11i). Er bietet eine absolute Sicherheit durch die Verwendung von Advanced Encryption Standard (AES), solange keine trivialen Passwörter verwendet werden, die über eine Wörterbuch-Attacke geknackt werden könnten. WPA ist aufgrund seiner WEP-Basis nicht mehr als sicher einzustufen.
- Virtual Private Network (VPN): Über ein Overlay VPN kann auch ein WLAN komplett abgesichert werden. Die Sicherheitslösung hat zum Ziel, nur berechtigte Clients und APs miteinander kommunizieren zu lassen und diese Kommunikation vertraulich und integritätsgeschützt zu halten. Hierzu wird hinter dem AP ein VPN-Gateway installiert. Beim Verbindungsaufbau wird ein kryptographischer Tunnel (z.B. basierend auf dem Standard IPsec) zwischen dem Client und dem VPN-Gateway aufgebaut.

Leider lässt sich nicht immer die sicherste Methode einsetzen, da zum Beispiel im Lagerumfeld Handscanner nicht für VPN- oder WPA2-Kommunikation ausgelegt sind. Somit ist in der Praxis oftmals keine oder eine unzureichende Verschlüsselung anzutreffen. Sofern die Endgeräte dies unterstützen, können sichere WLANs heute aber auf jeden Fall durch Nutzung des integralen Standards WPA2 aufgebaut werden. Dabei sollte man auf zentrale Verwaltungsserver (Wireless Controller) zurückgreifen, die große Mengen von APs managen können. So ist z.B. der Wireless Controller C5110 von Enterasys Networks in der Lage, 1.050 Basisstationen zu unterstützen und gleichzeitig bis zu 8.192 Teilnehmer. (*we*)