Datenübertragung über Funk

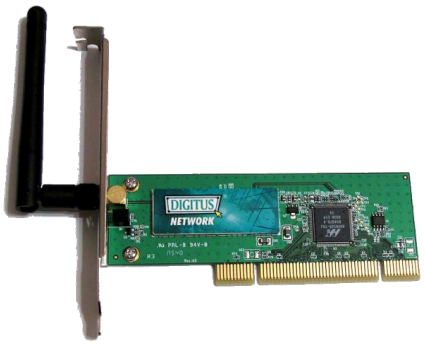
Wenn man Computer in einem Netzwerk mit Kabeln verbindet, hat das einige Nachteile:
Die Verlegung von Kabeln ist aufwendig und kostet in großen Gebäuden viel Geld. Außerdem kann man die mit Kabeln angeschlossenen Computer nicht bewegen. Für PCs ist das kein Problem, die stehen ja auf einem Schreibtisch. Aber Laptops und Smartphones wurden dazu erfunden, sich mit ihnen zu bewegen. Es wäre lästig, sie immer mit einem Kabel verbinden zu müssen.

Daher hat man die Verbindung von Computern über Funk entwickelt: ein WLAN ist ein „wireless local area network“, also ein „drahtloses“ Netzwerk, das eben ohne Kabel funktioniert.

Für eine Datenübertragung per Funk braucht man zwei Antennen, die beide jeweils Funksignale senden und empfangen können. Das heißt, die Antennen können Radiowellen aussenden und gleichzeitig auch Radiowellen einer anderen Antenne aufnehmen. Radiowellen sind elektromagnetische Schwingungen. Diese entstehen, wenn in einer Drahtspule innerhalb einer Antenne rhythmisch Strom fließt – also der Strom schnell zwischen „an“ und „aus“ hin und herschaltet. In einem modernen WLAN können Daten bis ca. 1 Gigabit pro Sekunde übertragen werden. Das entspricht einer Datenmenge von ca. 100 MB pro Sekunde. Um diese Geschwindigkeit zu erreichen, müssen die Antennen Radiowellen mit einer Frequenz von ca. 5 GHz erzeugen – also 5 Milliarden mal pro Sekunde zwischen „an“ und „aus“ hin und herschwingen.

WLAN-Adapter und Access Point

Für PCs ist ein WLAN-Adapter eine Steckkarte, die in einen PCI-Slot auf das Mainboard gesteckt wird. An dieser Steckkarte ist außerhalb des Gehäuses eine Antenne befestigt, mit der der Adapter Radiowellen senden und empfangen kann. Auf die Steckkarte sind elektrische Bauteile und Mikrochips gelötet, die für die Erzeugung der Radiowellen und für das Umwandeln der Funksignale in Daten zuständig sind. Für Laptops und Handys sind diese WLAN-Adapter wesentlich kleiner, funktionieren aber auf die gleiche Art. Je nachdem, wie schnell die Übertragungsgeschwindigkeit sein soll, gibt es einfache oder schnelle und teure WLAN-Adapter.



Zwei Computer, die jeweils einen WLAN-Adapter eingebaut haben, können prinzipiell schon miteinander Daten austauschen. Meist werden in Gebäuden aber sogenannte Access Points installiert. Ein Access Point hat die gleiche Rolle wie ein Switch in einem kabelgebundenen Netzwerk: er funktioniert als Verteiler zwischen mehreren Computern, Laptops, Handys usw. Ein Access Point hat eine oder mehrere Antennen zum Senden und Empfangen. Jedes Gerät verbindet sich über Funk mit dem Access Point und kann dann Daten mit den anderen Geräten austauschen. Der Access Point wird außerdem mit einen Router verbunden, der mit dem Internet verbunden ist.

WLAN in großen Gebäuden

Die Antennen von WLAN-Adaptern und Access Points haben nur eine geringe Reichweite. Die Funksignale können gut durch Luft übertragen werden, aber Wände (insbesondere Betonwände) schwächen die Signale ab. In einer kleinen Wohnung genügt ein einziger Access Point, aber in größeren Häusern braucht es mehrere Access Points, damit man überall „WLAN hat“. In einem Gebäude wie unserer Schule können 50, 100 oder mehr Access Points nötig sein. Es müssen ja auch hunderte von Geräten wie Handys, Laptops und iPads mit dem WLAN verbunden werden. Moderne Access Points haben dazu viele Antennen und intelligente Steuerungseinheiten, so dass sie sich selbstständig untereinander koordinieren können. So können sie z.B. aushandeln, welcher Access Point welches Gerät übernimmt.

Verschlüsselung

Funk gehört zu den Übertragungswegen, die sich am leichtesten abhören lassen. Um Funkverkehr zu „belauschen“, muss man nur eine Antenne im Bereich des Access Points aufstellen – für ein WLAN genügt es also, wenn man mit einen Handy oder einem Laptop in der Nähe des Access Points herumläuft. Jemand mit kriminellen Absichten könnte so zum Beispiel Passwörter anderer Menschen abhören und diese dann zu Betrugszwecken einsetzen. Um das zu verhindern, muss Datenübertragung über Funk verschlüsselt werden.

Mit der Zeit haben sich immer bessere Verschlüsselungstechniken für WLANs entwickelt. Der aktuelle Standard nennt sich „WiFi protected access“ (WPA), wobei die erste Version schon nicht mehr sicher ist, und auch bei der zweiten Version, WPA2, schon Zweifel bestehen. Die nächste Version WPA3 ist momentan in der Entwicklung. Mit WPA lässt sich die Datenübertragung verschlüsseln. Außerdem kann man einstellen, dass nur bestimmte Geräte, oder bestimmte Personen Zugang zum WLAN erhalten. In einem einfachen WLAN wird ein Passwort verwendet, das für alle Benutzer gleich ist. Für WLANs mit vielen Benutzern ist das jedoch zu unsicher. In größeren WLANs kann man daher auch einstellen, dass jeder Benutzer sein eigenes Passwort benutzen muss. Dann kann man nämlich zurückverfolgen, welche Person im WLAN zu welcher Zeit online war, und ob diese Person in dieser Zeit z.B. eine Straftat begangen hat.

Tipps für die Recherche

Recherchiere zu den aktuellen WiFi-Standards, z.B. WiFi 5 und WiFi 6.
Wie kann ein Access Point mit mehreren Geräten gleichzeitig kommunizieren, und wie kann er die Funksignale dieser Geräte unterscheiden? (siehe „Funkkanal“)
Was ist ein Repeater?
Welche Möglichkeiten wenden Hacker an, um WLAN-Verschlüsselung zu knacken?