Tim Philipp Schäfers / Rico Walde

WLAN Hacking

Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen

- WLAN-Grundlagen und Verschlüsselungsmethoden erklärt
- Der Umgang mit den beliebtesten Angriffsprogrammen
- Gegenmaßnahmen in Heim- und Firmennetzwerken implementieren

1.2.7 IEEE 802.11ac

Willkommen in der Gegenwart. Der im Dezember 2013 veröffentlichte AC-Standard stellt den momentanen Stand der Technik dar. Im Endzustand könnten bis zu 6,9 GByte/s erreicht werden. Da der neue Standard aber im Vergleich zum Vorgänger viele komplexe Verbesserungen und Veränderungen enthält, hat sich die IEEE entschieden, den Standard in verschiedenen Wellen (meist Wave genannt) auszurollen. So haben Hardwarehersteller eine Chance, zeitnah entsprechende Hardware zu entwickeln. Der Standard arbeitet nur noch im 5-GHz-Bereich – wie früher einmal 802.11a. Der 2,4-GHz-Bereich ist wegen der geringen Breite des verfügbaren Spektrums und der physikalisch bedingten geringeren Übertragungsrate im Very-High-Throughput-Bereich weniger relevant geworden.

Um genügend Reichweite zu generieren, kombinieren WLAN-Router und Endgeräte die ac- und n-Standards. Auch die Kanalbreite ist weiter gestiegen. Während in der ersten Wave (Wave 1) noch 80 MHz Standard waren (maximale Datenrate 1,3 GBit/s), gibt es ab Wave 2 die Möglichkeit, 160 MHz breite Kanäle zu erstellen. Hier wären dann selbst im 5-GHz-Spektrum (in Europa) nur noch zwei nicht überlappende Channels möglich. Auch wird MIMO jetzt mit bis zu 8x8 mit acht Spatial Streams unterstützt. Sogar **MU-MIMO** (*Multi User MIMO*) ist jetzt möglich, das bei verschiedenen Clients gleichzeitiges MIMO, also eine Übertragung mehrerer Spatial Streams, ermöglicht.

Eine weitere Neuerung ist das **Beamforming**. Auch wenn es erstmals im n-Standard spezifiziert wurde, fand es bei ac-WLAN das erste Mal auch in der Praxis Anwendung. Hierbei wird das Signal wie bei einer Richtantenne so verändert, dass es in eine Richtung (vorzugsweise Richtung Client) stärker strahlt. Noch ist die Auswahl Beamforming-fähiger Endgeräte aber überschaubar. Als letzte nennenswerte Neuerung wurde ein verbessertes Modulationsverfahren eingeführt. Genau genommen wurden mehrere Modulationsverfahren eingeführt, wobei abhängig von der Übertragungsqualität, also von Abstand und Störquellen, das am besten geeignete Verfahren angewandt wird. Wenn die Übertragungsqualität sehr gut ist, wird ein Verfahren gewählt, bei dem besonders viele Bits pro Übertragungsschritt, viele Nutzdaten und kaum Sicherungsdaten übertragen werden. In der höchstmöglichen Stufe (MCS 9) wird mit QAM256 8bit/Übertragungsschritt mit einer Coderate (Nutzdaten/Gesamtdaten) von 5/6 angewandt.

Einige Hersteller fangen mittlerweile sogar an, QAM1024 in ihre Router zu implementieren (10 Bit proSchritt). Dies entspricht nicht mehr dem Standard, sondern ist ein Vorstoß von Broadcom, genannt NitroQAM. Dafür werden noch höhere Datenraten möglich. Da aber bereits für QAM256 die Verbindungsqualität nahezu perfekt sein muss, ist es unrealistisch, dass QAM1024 in der Praxis Anwendung finden wird. Um auf die anfangs genannte maximale Datenrate von 6,9 GBit/s zu kommen, muss 8x8 MIMO mit 160-MHz-Kanälen und 256QAM verwendet werden. Auch wenn in naher Zukunft entsprechende Hardware erhältlich ist, wird man in der Praxis nie solche Werte erreichen. Zurzeit mangelt es sogar noch an guten Wave-2-WLAN-Adaptern.

Während es schon genügend Wave-2-WLAN-Router gibt, ist momentan (Stand April

2017) der ASUS PCE-AC88 der einzige Dual-Band-Wireless-AC-Adapter, der 4x4 MU-MIMO ermöglicht. Er benötigt jedoch einen PCIe-Steckplatz. In Laptops sind in der Regel nur 2x2-Adapter eingebaut, auch in Smartphones ist meistens kein MIMO möglich. Lediglich die neueren Qualcomm-Chips unterstützen 2x2 MIMO. Da der Standard schon seit einigen Jahren veröffentlicht ist, sind jetzt die Hersteller dran, auch entsprechende Clienthardware zu liefern. Vor allem durch das enorme Platzproblem eines 4x4-Antennendesigns bei Smartphones dürfte dies aber noch einige Zeit dauern.

1.2.8 IEEE 802.11ad

Der ad-Standard, auch als *Wireless Gigabit* (WiGig) bezeichnet, ist der erste WLAN-Standard, der im 60-GHz-Bereich arbeitet. Der am 28.12.2012 veröffentlichte Standard zeugt nicht nur davon, dass die VHT Group offensichtlich keine Weihnachtsferien kennt[9], sondern er ist damit auch chronologisch eigentlich vor dem ac-Standard anzusiedeln. Da die Verbreitung und Entwicklung von entsprechenden Geräten aber deutlich nach der von ac-Geräten stattfand, wird er hier auch nach dem ac-Standard gelistet. Besonders ist, dass er im Bereich von 57 bis 66 GHz mit einer Kanalbreite von 2,16 GHz arbeitet, sodass vier Kanäle zur Verfügung stehen.

Durch unterschiedliche Regulatorien in verschiedenen Ländern differiert die tatsächlich zur Verfügung stehende Frequenzbreite stark. So ist in Australien z. B. nur ein einziger Kanal nutzbar (erlaubte Frequenzen 59,4 bis 62,9 GHz), während in der EU und in Japan alle Kanäle zur Verfügung stehen. Trotz eines Maximums von vier Kanälen dürfte das Problem des »überfüllten Luftraums« des 2,4-GHz-Spektrums hier so gut wie vernachlässigbar sein. Bedingt durch die hohe Frequenz von 60 GHz, findet durch die Luftabsorption und die Freiraumdämpfung eine so starke Signaldämpfung statt, dass selbst unter optimalen Bedingungen und bei Sichtkontakt maximal 20 m Reichweite realisiert werden können.

Innerhalb von Gebäuden beschränkt sich eine ad-Funkzelle auf einen Raum, da Türen und Wände so gut wie gar nicht durchdrungen werden. Hieran sieht man, dass die Grenzen zwischen WLAN und WPAN (*Wireless Personal Area Network*) schwimmend sind. Dafür sind aber auch Datenraten von bis zu 6,757 GHz möglich. Der Standard ermöglicht wie schon ac WLAN-Beamforming, unterstützt jedoch kein MIMO. Des Weiteren wurde ein Power-Management zum Energiesparen implementiert. Aufgrund der hohen Datenrate und der geringen Reichweite eignet sich dieser Standard eher für die Drahtlosanbindung von Computerperipherie statt als Ersatz der alten Standards. So könnte man sogar drahtlose 4k-HDR-Videoübertragung mit 60 fps ermöglichen.

Noch verlockender ist die Ablösung des bisherigen Kabelgewirrs an Maus, Tastatur, Drucker und Boxen. Auch drahtlose USB-3.0-Hubs könnten so realisiert werden. Obwohl der Standard schon einige Jahre verabschiedet ist, gibt es bisher so gut wie keine entsprechende Hardware. 2016 kamen mit dem TP-Link Talon AD7200 und dem Netgear Nighthawk X10 erstmals zwei ad-fähige WLAN-Router auf den Markt. Auf Clientseite unterstützt der Qualcomm Snapdragon 835 erstmals ad-WLAN, sodass man in nächster

Zeit wohl Smartphones mit Tri-Band-WLAN (2,4 + 5 + 60 GHz) erwarten kann.

1.2.9 IEEE 802.11ax

Dieser Standard befindet sich in Entwicklung und soll später einmal eine Verbesserung des 2,4-GHz- und des 5-GHz-Bands ermöglichen. Er wird damit die Nachfolge von n/ ac-WLAN antreten. Der Standard strebt folgende drei Ziele an: verbesserter Datendurchsatz, bessere Reichweite und neue Stromsparfeatures. Es sind Datenraten von 10 GByte/s geplant. Dies soll durch die Unterstützung von QAM1024, einem neuen Modulationsverfahren OFDMA (*Orthogonal Frequency Division Multiple Access*), einem bidirektionalen MU-MIMO sowie weitere Verbesserungen erreicht werden.

Der Standard soll auch mit kleinen Embedded Devices oder IoT-Devices, die nur 20-MHz-Channels unterstützen, kompatibel bleiben. Der seit Mai 2013 entwickelte Standard befindet sich momentan noch im Entwurfsstadium. Planmäßig sollte im Mai 2017 Entwurf 2.0 veröffentlicht werden. Wegen der hohen Anzahl von Kommentaren am Entwurf 1.0 könnte sich das noch etwas verzögern.

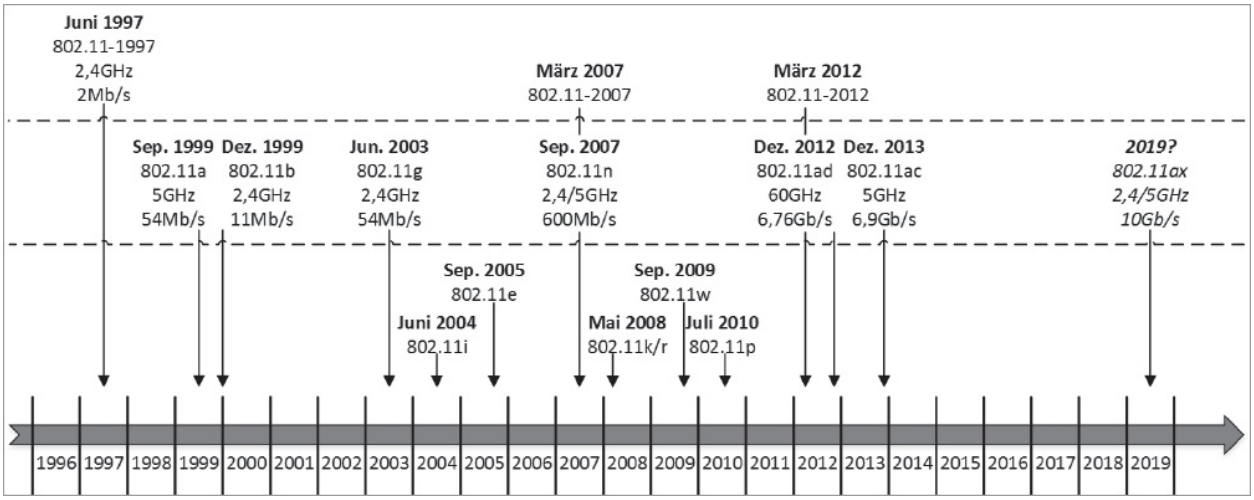

Bild 1.1: Zeitstrahl zu Spezifikationen der WLAN-Technologie.

1.3 WLAN ist nicht nur IEEE 802.11

Dies ist ein Überblick über WLAN-Technologien, die parallel zu Wi-Fi existieren. In diesem Buch werden wir uns jedoch auf Wi-Fi fokussieren. Da der Übergang zwischen WPAN, WLAN und WMAN fließend ist, werden hier auch Technologien gelistet, die man neben WLAN den beiden anderen Netzwerken zuordnen könnte.

1.3.1 Bluetooth

Meistens als WPAN (*Wireless Personal Area Network*), manchmal als WLAN bezeichnet,

ist Bluetooth der einzige Standard, der neben Wi-Fi eine größere Bedeutung hat. Er wurde in den 1990ern von der Bluetooth Special Interest Group entwickelt und unter dem IEEE-Standard 802.15.1 veröffentlicht. Möglich sind verbindungslose sowie verbindungsbehaftete Übertragungen von Punkt zu Punkt und Ad-hoc- oder Piconetze. Bluetooth wird bei drahtlosen Mäusen und Tastaturen eingesetzt. Hier bietet sich verglichen mit herkömmlichen Funkmäusen der Vorteil, dass sich (bei eingebautem Bluetooth-Empfänger) ein USB-Port für den Empfänger sparen lässt.

Auch lassen sich über Bluetooth Daten zwischen Smartphones übertragen. Seltener implementieren Spiele-Apps einen Mehrspielermodus über Bluetooth. Auch gibt es Bluetooth-Chatprogramme. Obwohl der aktuelle Bluetooth-Standard 5 bis zu 20 m (100 mW) weit sendet und seine Reichweite damit deutlich über ad-WLAN liegt, wird es meist als WPAN bezeichnet – daher wird in diesem Buch nicht näher darauf eingegangen. Dies liegt unter anderem daran, dass Bluetooth viel im Low-Energy-Bereich eingesetzt wird, um kleinere Devices miteinander zu verbinden. Da maximal 2 MBit/s an Datenrate verfügbar sind, ergibt sich ein etwas anderes Anwendungsgebiet als beim herkömmlichen WLAN bzw. Wi-Fi.

Bluetooth benutzt wie WLAN das zulassungsfreie 2,4-GHz-Spektrum, genau genommen liegt es zwischen 2,402 und 2,480 GHz. Das hat zur Folge, dass Bluetooth-Geräte in unmittelbarer Nähe zu WLAN-Sendern/-Empfängern die Empfangsqualität beeinflussen können.

1.3.2 ZigBee

ZigBee ist ein drahtloses Netzwerk, das vor allem in der Hausautomation eingesetzt wird. Es unterstützt nur geringe Datenraten und hat erst durch das Aufkommen von Smart Homes an Bedeutung gewonnen. Seitdem erscheinen regelmäßig neue ZigBeekompatible Geräte (z. B. smarte Thermostate, fernsteuerbare Steckdosen und Sensoren). Es hat eine ähnliche Reichweite wie Wi-Fi (10 bis 100 m) und funkt im 2,4-GHz- (weltweit), 868-MHz- (Europa) und 915-MHz-Bereich (USA). Dabei bietet es eine maximale Datenrate von 250 KByte/s. Es ist unter der Norm IEEE 802.15.4 spezifiziert, die trotz der Reichweite als WPAN gilt.

1.3.3 Z-Wave

Z-Wave ist ein Standard der Firma Sigma Designs und der Z-Wave Alliance, der für Heimautomation entwickelt wurde. Damit ist er ein direkter Konkurrent von ZigBee. Er funkt im 800-MHz-Spektrum und erreicht geringe Datenraten von 100 KByte/s. Trotz der niedrigen Frequenz hat Z-Wave nur eine Reichweite von maximal 150 m, da es eine geringe Sendeleistung von 25 mW spezifiziert. Das hat den Vorteil, dass das Signal zwar Türen und Wände durchdringt, jedoch kaum über die eigene Wohnung hinausreicht. Da bei Heimautomation bisher nur wenige Daten erforderlich sind, stört die kleine Datenrate

nicht. Z-Wave ist ein aktiver Standard, zu dem regelmäßig neue Geräte erscheinen.

1.3.4 HiperLAN

HiperLAN wurde ab 1991 als Wi-Fi-Alternative entwickelt und ist damit ausnahmsweise mal eindeutig ein WLAN. Die erste Version erschien 1996. Es wurden drei weitere Versionen entwickelt, die allerdings alle gleichermaßen keine Verbreitung fanden. Jedoch wurde der Physical Layer von HiperLAN/2 (Februar 2000) größtenteils in IEEE 802.11a übernommen, sodass ein Teil dieser Technologie weiterlebt. Beide Technologien basieren auf 5-GHz-EM-Wellen mit maximal 54 MByte/s Übertragungsrate, wodurch sich die Ähnlichkeit erklärt.

1.3.5 HomeRF

Eine weitere tote Technologie ist HomeRF, die eine Kreuzung von DECT und Wi-Fi darstellt. Sie wurde zwischen 1998 und 2003 entwickelt und war auf Privathaushalte zugeschnitten. HomeRF verwendet das 2,4-GHz-Spektrum, und es wurden Geräte mit bis zu 10 MBit/s Datenrate entwickelt.

1.3.6 WiMAX

WiMAX ist im IEEE-802.16-Standard spezifiziert und wurde bzw. wird vom WiMAX-Forum entwickelt. Es funkt im Frequenzbereich zwischen 2 und 66 GHz und bietet im aktuellen 802.16m-Standard bis zu 1 GByte/s Datenrate. Es operiert wie WLAN auf dem PHY- und dem MAC-Layer, eine WiMAX-Basisstation darf aber mit bis zu 30 Watt senden. So ist eine Reichweite von bis zu 50 km möglich wird. WiMAX lässt sich also auch als *Wireless Metropolitan Area Network* (WMAN) bezeichnen.

Es stellt also eher eine Alternative zu 3G/4G als zu Wi-Fi dar. Möchte man eine Datenrate von mindestens 10 MByte/s bereitstellen, sind maximal zehn Kilometer Reichweite drin. Hohe Datenraten sind erst bei einer Entfernung von unter einem Kilometer möglich. Es wird vor allem für die Datenübertragung in Städten zwischen entfernten Gebäuden über Dachantennen verwendet. Darüber hinaus gibt es auch WiMAX-USB-Adapter, die aber mit entsprechend geringerer Sendeleistung funken. Obwohl WiMAX eine eher unwesentliche Verbreitung hat und schon oftmals für tot erklärt wurde, wird es von der 802.16 Group immer noch weiterentwickelt.

1.3.7 Li-Fi

Neben der Datenübertragung im Mikrowellenbereich gibt es auch Ansätze, Daten im Spektralbereich des sichtbaren Lichts zu übertragen. Bereits 1955 kam die erste Fernbedienung für Fernseher auf den Markt, die Zenith Flash-Matic, die über Lichtblitze