

# Der Verlust der informationellen Selbstbestimmung ? Anonymitätsaspekte bei Bluetooth und WLAN

*M. Handy, M. Haase, D. Timmermann  
Institut für Angewandte Mikroelektronik und Datentechnik  
Universität Rostock, Richard-Wagner-Str. 31, 18119 Rostock  
{matthias.handy, marc.haase, dirk.timmermann}@technik.uni-rostock.de*

## 1 Einleitung

Das Recht auf informationelle Selbstbestimmung setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Bei der Einführung drahtloser Kommunikationstechnologien in Bereiche des täglichen Lebens findet der Sicherheitsaspekt oft nur in der Ausprägung einer abhörsicheren Kommunikation zwischen mobilen Geräten Beachtung. Dagegen gewinnt jedoch der Schutz der Anonymität der Benutzer mobiler Geräte immer stärker an Bedeutung. Um diesen zu gewährleisten, ist es notwendig zu verhindern, dass das Kommunikationsgerät des Nutzers Informationen übermittelt, die eine Verkettung verschiedener Aktionen ermöglicht, die mit diesem Gerät durchgeführt wurden. Das bedeutet, dass sobald mit dem Gerät eine den Benutzer identifizierende Transaktion durchgeführt wird, können sowohl bereits früher durchgeführte als auch zukünftig durchzuführende Aktionen des Geräts auf diese Identität zurückgeführt werden.

Zum Schutz des Rechts auf informationelle Selbstbestimmung bei der Nutzung von mobilen Geräten mit drahtlosen Kommunikationsschnittstellen verfolgen wir folgende Ansätze:

Bei Diensten, die auf virtuellen Verbindungen aufbauen, werden oft die Adressen der darunter liegenden Schicht zur Zuordnung von Paketen zu Verbindungen benötigt. Daher muss diese Adresse für die Dauer einer Verbindung konstant bleiben. Um aber zu verhindern, dass parallele Verbindungen über die Adresse als von dem gleichen Gerät herrührend erkannt werden, sollte ein mobiles Gerät für verschiedene Verbindungen unter unterschiedlichen Adressen auftreten.

Eine weitere Möglichkeit ein Gerät wieder zu erkennen, ist das Verfolgen der Spur seiner Funkaktivität unabhängig von der Dienstenutzung. Deswegen sollte die Kommunikationsschnittstelle nicht kontinuierlich aktiv sein, und die Dichte von potentiell kommunizierenden Geräten hoch genug sein.

In diesem Artikel wird untersucht, inwieweit die Kurzstreckenfunktechnologien Bluetooth und IEEE 802.11 {a|b} (WLAN) die Anonymität ihrer Nutzer unterstützen bzw. schädigen. Folgende Kriterien werden von uns dabei genauer betrachtet:

**Änderbarkeit identifizierender Gerätemerkmale.** Damit die Verkettung von Funkaktivitäten über identifizierende Gerätemerkmale wie statische MAC-Adressen ausgeschlossen werden kann, muss die Technologie die Möglichkeit bieten, derartige Merkmale zu ändern.

**Schweigsamkeit.** Damit ein mobiles Endgerät nicht aufgrund von protokollbedingten Funkaktivitäten von anderen Netzwerkteilnehmern bemerkt werden kann, soll die Funktechnik nur aktiv sein, wenn der Nutzer es verlangt.

**Broadcastfähigkeit.** Die dritte Anforderung, die an eine geeignete Funktechnik gestellt wird ist die Broadcastfähigkeit, die es Benutzern von mobilen Endgeräten ermöglicht, Dienstbeschreibungen von angebotenen Dienst Anbietern passiv zu empfangen.

## 2 Bluetooth

### 2.1 Bluetooth und Adressänderung

Jedes Bluetooth-Gerät besitzt eine eindeutigen 48-bit Adresse (BD\_ADDR). Abbildung 1 zeigt den Aufbau der Adresse, bestehend aus einem 24-bit Lower Address Part (LAP), einem 8-bit Upper Address Part (UAP) und einem 16-bit Non-significant Address Part (NAP). Der LAP wird von dem BT-Gerätehersteller vergeben. UAP und NAP bilden die Hersteller-Identifikation, die von der IEEE vergeben wird.

Die BT-Geräteadresse kann vom Nutzer nicht geändert werden. Eine Maskierung der Adresse für ein anonymes Inquiry oder Paging ist folglich nicht möglich. Lediglich bei einigen Entwicklermodulen ist es möglich, mit Hilfe eines speziellen Kommandos, die Geräteadresse zu ändern. Auf höherer Ebene des BT-Protokollstacks besteht zusätzlich die Möglichkeit, BT-Geräteadressen durch Alias-Adressen zu ersetzen. Damit ließe sich die Geräteadresse eines Kommunikationspartners zumindest auf höheren Protokollschichten verbergen. Eine derartige Protokollimplementierung müsste jedoch „tamper-proof“ sein, um eine Aufdeckung der Geräteadressen zu verhindern.

company assigned						company id					
LAP						UAP		NAP			
0000	0001	0000	0000	0000	0000	0001	0010	0111	1011	0011	0101

Abbildung 1. Format der BT Geräteadresse

## 2.2 Bluetooth und Schweigsamkeit

Die Forderung nach Schweigsamkeit verlangt, dass eine Funktechnologie ihre Kommunikations-Aktivitäten auf die wirklich notwendigen Phasen beschränken soll. Bluetooth erfüllt diese Forderung, da bei Bluetooth die Sichtbarkeit und Kontaktierbarkeit gegenüber externen Geräten steuerbar ist. Dies wird durch zwei Scan-Modi erreicht. Der Inquiry-Scan-Modus steuert die Sichtbarkeit eines BT-Gerätes nach außen und der Page-Scan-Modus die Kontaktierbarkeit. Sind beide Modi deaktiviert, ist ein Bluetooth-Gerät vollkommen unsichtbar und kann nicht kontaktiert werden.

Zusätzlich dazu unterstützt Bluetooth drei Power-Safe-Modi (Sniff, Park und Hold), die die Kommunikation zwischen Bluetooth-Geräten reduzieren. Dies geschieht primär, um Energie zu sparen, lässt sich jedoch ebenso nutzen, um die „Gesprächigkeit“ von Bluetooth-Geräten einzuschränken.

**Sniff Mode.** Beim Sniff-Mode kann der Master eine Übertragung zu einem Slave nur zu bestimmten Zeitpunkten starten. Das Intervall zwischen zwei dieser Zeitpunkte wird als Sniff-Intervall  $T_{\text{Sniff}}$  bezeichnet. Ein Slave hört demnach nicht kontinuierlich auf dem Kanal mit und reduziert damit seinen Energieverbrauch. Der Sniff-Modus reduziert jedoch nicht die Sendeaktivität des Slave. Bedingung für den Eintritt in den Sniff Mode ist das Bestehen einer ACL-Verbindung zwischen zwei Bluetooth-Geräten.

**Hold Mode.** Befindet sich ein Slave eines Piconetzes im Hold-Modus, unterstützt dieser keine ACL-Pakete mehr, bis ein Zeitpunkt *HoldTo* erreicht ist, den Master und Slave vorher vereinbart haben. SCO-Verbindungen können während der Hold Phase aufrecht erhalten werden.

**Park Mode.** Der Park Mode wird in der Regel dazu benutzt, mehr als sieben Slaves an einem Piconetz teilhaben zu lassen. Slaves, die zwischenzeitlich nicht an der Übertragung teilnehmen, können in den Parkzustand versetzt werden und verlieren damit ihre Active-Member-Adresse (AM\_ADDR), die sie in einem Piconetz identifiziert. Ein geparkter Slave erhält stattdessen eine PM\_ADDR (Parked Member Address) sowie eine AR\_ADDR (Access Request Address). Die PM\_ADDR wird vom Master genutzt, um einen geparkten Slave wieder aufzuwecken. Die AR\_ADDR wird vom geparkten Slave genutzt, um selbst ein „Entparken“ beim Master zu verlangen.

Power-Safe-Modi sind geeignet, die Kommunikation zwischen Bluetooth-Geräten zu reduzieren, wenn diese bereits Mitglied in einem Piconetz sind. Ebenso wichtig ist die Minimierung des Kommunikationsaufkommens vor der Bildung eines Piconetzes, d.h. bei Inquiry- und Paging-Prozessen. Beim Inquiry beschränkt sich die Kommunikation, wie bereits erwähnt, auf den Austausch von ID- bzw. FHS-Paketen. Zusätzlich kann ein Nutzer festlegen, wann und wie lange sein Bluetooth-Gerät von anderen Geräten gefunden werden kann (Inquiry Scan Substate). Auch der Page Scan Substate, bei dem ein Bluetooth-Gerät auf Verbindungsanfragen von anderen Geräten wartet, lässt sich zeitlich beschränken, so dass der Nutzer bzw. eine Applikation die Gesprächigkeit eines Bluetooth-Gerätes, das nicht Mitglied in einem Piconetz ist, gut überwachen kann.

## 2.3 Bluetooth und Broadcast

Das *Bluetooth Profiles Book* [1] definiert ein Service Discovery Protocol (SDP), mit Hilfe dessen Bluetooth-Geräte angebotene Dienste von Geräten in Reichweite entdecken können. Dabei wird vorausgesetzt, dass Geräte vor der Dienstonutzung entdeckt und kontaktiert wurden. Ein Service-Discovery-Vorgang bei Bluetooth lässt sich demnach nicht ohne ein vorangegangenes Verbinden der Geräte durchführen. Bei der Herstellung einer Verbindung zwischen zwei Bluetooth-Geräten werden jedoch immer die BT-Geräteadressen ausgetauscht [2]. Eine Anonymisierung dieses Vorgangs ist ohne Maskierung oder Blendung dieser eindeutigen Geräteadresse nicht möglich.

Da keine Nutzdaten ohne vorherigen Verbindungsaufbau und Adresstausch übertragen werden können, besitzt die Bluetooth-Technologie per Definition keine Broadcast-Funktionalität. Die Bluetooth-Spezifikation erwähnt zwar ein so genanntes Broadcast-Schema. Dieses bezieht sich jedoch nur auf die Kommunikation innerhalb eines Piconetzes, nämlich dann, wenn der Master eines Piconetzes an alle Slaves gleichzeitig senden will. Dabei werden die Bits der AM\_ADDR (Active Member Address), die einen Teilnehmer des Piconetzes identifizieren, im Header der Master-to-Slave Nachricht auf Null gesetzt. Slaves quittieren den Empfang einer derartig präparierten Nachricht nicht. Bei dieser Form des Broadcast handelt es sich aber nicht um die oben definierte, da ein Slave immer eine Verbindung zu einem Master aufbauen und damit seine BT-Geräteadresse preisgeben muss, bevor er einem Piconetz beitreten kann.

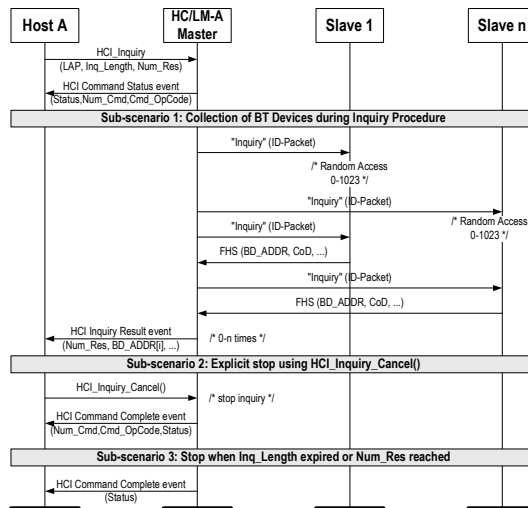


Abbildung 2. Sequenz Diagramm des Bluetooth Inquiry

Der einzige Vorgang bei Bluetooth, der Broadcast-ähnliche Eigenschaften besitzt, ist die Inquiry-Prozedur – das Suchen nach Geräten in der Umgebung (Abbildung 2). Ein Bluetooth-Gerät sendet dabei in regelmäßigen Abständen ID-Pakete aus. ID-Pakete enthalten einen so genannten Inquiry Access Code (IAC), der Bluetooth-Geräten in der Umgebung signalisiert, dass jemand versucht sie zu finden. Der IAC ist zwar von dem Lower Address Part (LAP), den 24 niederwertigen Bits einer BT-Geräteadresse, abgeleitet, es lässt sich daraus jedoch nicht die Bluetooth-Adresse rekonstruieren [2]. Das ID-Paket eines Bluetooth-Gerätes enthält demnach keine verwertbaren Informationen über seine Quelle. Eine Bluetooth-Inquiry-Prozedur ist demnach für den Initiator anonym.

Gefundene Geräte antworten auf ein Inquiry mit einem FHS-Paket (FHS=Frequency Hopping Synchronisation). Ein FHS-Paket enthält unter anderem die BT-Geräteadresse und den aktuellen Wert der Systemuhr des Absenders. Das Eintreffen eines FHS-Paketes wird vom Empfänger nicht quittiert. Abbildung 3 zeigt den Aufbau des FHS-Paketes.

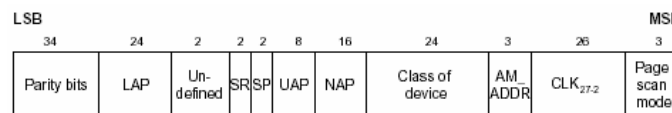


Abbildung 3: Payload Format des FHS-Paketes

Der Payload eines FHS-Paketes bietet die Möglichkeit, den Inquiry-Vorgang als Service-Discovery-Prozedur zu nutzen. Das darin enthaltene 24-bit-breite Feld *Class of Device* kann Informationen über die angebotenen Dienste eines BT-Gerätes enthalten. In [3] wird das Feld *Class of Device* (CoD) für den ersten Format-Typ (Feld *Format type* = 00) wie folgt definiert (Abbildung 4):

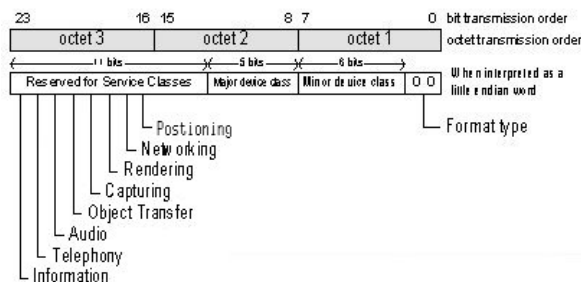


Abbildung 4. Format des CoD Feldes im FHS-Paket

Bit no	Major Service Class
13	Limited Discoverable Mode [Ref #1]
14	(reserved)
15	(reserved)
16	Positioning (Location identification)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speaker, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, ...)
23	Information (WEB-server, WAP-server, ...)

Tabelle 1. Bluetooth Service Klassen

Ein Nutzer erhält demnach als Antwort auf ein anonymes Inquiry nicht nur Geräteadressen sondern zusätzlich codierte Informationen über Service-Klassen sowie Geräteklassen der möglichen Kommunikationspartner. Tabelle 1 zeigt mögliche Serviceklassen (*Major Service Class*). Die Felder *Major device class* und *Minor device class* in Abbildung 4 enthalten Informationen über Geräteklassen (PDA, Laptop, VCR ...).

Der Inquiry-Broadcast hat jedoch einen Nachteil. Die beim Inquiry versendeten ID-Pakete des suchenden Bluetooth-Gerätes enthalten den LAP der BT-Geräteadresse. Wie bereits erwähnt, lässt sich daraus die gesamte Geräteadresse nicht ableiten, es wäre jedoch eine Art von Tracking möglich, indem alle Orte registriert werden, an denen ein BT-Gerät mit einem bestimmten LAP ein Inquiry durchgeführt hat.

Insgesamt besitzt Bluetooth nur bedingt Broadcast-Qualitäten. Bei der Inquiry-Prozedur kann ein Nutzer anonym nach Geräten und Serviceklassen in der näheren Umgebung suchen. Der Informationsgehalt ist jedoch durch die Größe des *CoD*-Feldes im FHS-Paket begrenzt, womit nur eine sehr grobe Dienstbeschreibung möglich ist. Beim Inquiry-Broadcast ist außerdem die Gefahr eines Tracking-Angriffes gegeben. Jegliche andersgerichtete Kommunikation ist nur nach vorangegangenem Austausch der Geräteadressen möglich.

### 3 IEEE 802.11{a|b} (WLAN)

IEEE 802.11{a|b} ist ein drahtloser LAN Funknetz Standard, der von der IEEE entwickelt und 1997 verabschiedet wurde [4]. Die Funkübertragung findet im lizenzfreien 2,4 GHz ISM Frequenzband statt. Im ISO OSI Schichtenmodell spezifiziert 802.11 die physikalische Schicht und die MAC Schicht. Der Standard unterstützt sowohl den Aufbau eines aus mehreren Funkzellen bestehenden drahtlosen Netzwerkes (Infrastruktur-Modus), als auch den Aufbau eines auf eine Funkzelle reduzierten Ad-Hoc Netzwerkes (*Ad-Hoc Mode*).

Im *Infrastructure Mode* ist ein 802.11 LAN in einzelne Funkzellen aufgeteilt. Jede Zelle, auch Basic Service Set (BSS) genannt, wird von einem Access Point (AP) gesteuert. Die APs einer jeden Zelle sind über einen Backbone, auch Distribution System (DS) genannt, miteinander verbunden. Alle Zellen bilden für die höheren Schichten des ISO OSI Modells ein zusammenhängendes 802.11 Netzwerk, das als Extended Service Set (ESS) bezeichnet wird. Im *Ad-Hoc Modus* besteht das drahtlose Netzwerk nur aus einer Funkzelle, ohne einen AP, die durch mindestens zwei Stationen gebildet wird.

Im Folgenden wird untersucht, ob die in der Einleitung genannten Kriterien von diesem Standard erfüllt werden.

#### 3.1 IEEE 802.11{a|b} und Adressänderung

Jede Station in einem IEEE 802.11{a|b} Netzwerk besitzt eine eindeutige und nicht änderbare EAI-48 MAC Adresse. Diese ist Voraussetzung für das Paket Handling in der MAC Schicht. Bei der Produktion von 802.11 kompatiblen Netzwerkkadaptern wird diese Adresse vom Hersteller vergeben. In Abhängigkeit von der konkreten Implementierung der Netzwerkkadappter ist jedoch eine nachträgliche Änderung dieser Adresse per Software möglich. Dieses ist jedoch nur dann sinnvoll, wenn die Station keine aktive Bindung zu einer Zelle besitzt. Pakete die nach einer Änderung der MAC Adresse an die alte Adresse gesendet werden, können nicht mehr empfangen werden.

Beim Wechsel der MAC Adresse muss jedoch berücksichtigt werden, dass zwei oder mehrere mobile Geräte die gleiche MAC Adresse besitzen können und es zu Kollisionen kommen kann. Jedoch unter der Voraussetzung, dass die Kommunikationsbeziehung nur kurzzeitig besteht und die Geräte im Ad-Hoc Modus miteinander kommunizieren, ist das Auftreten dieses Falles eher unwahrscheinlich.

#### 3.2 IEEE 802.11{a|b} und Schweigsamkeit

IEEE 802.11{a|b} bietet ähnlich wie Bluetooth die Möglichkeit, den Netzwerkkadappter in einen stromsparenden Betriebszustand zu versetzen. Der Netzwerkkadappter wechselt dabei vom Active Mode (AM) in den Power Save Mode (PSM). Im PS Mode wird der Adapter nur zum Empfang von Zeit-Synchronisationspaketen (TIM) aktiviert. Zusätzlich zu dem PS Mode lässt sich der Netzwerkkadappter über das Betriebssystem vollständig deaktivieren. Der Wechsel zwischen den Stromspar-Modi erfüllt jedoch die Forderung nach Schweigsamkeit nur zu einem Teil.

Bevor ein IEEE 802.11{a|b} Netzwerkkadappter im Infrastruktur oder Ad-Hoc Modus kommunizieren kann, muss dieser sich in dem drahtlosen Netzwerk anmelden. Dieser Prozess erscheint im ersten Moment nicht ohne aktive Kommunikation abzulaufen. Eine genaue Analyse dieses Prozesses zeigt jedoch, dass eine aktive Kommunikation nicht unbedingt erforderlich ist, um zumindest Broadcast Pakete empfangen zu können.

Ausgangspunkt für die Analyse ist eine Zelle mit einem AP. Der AP bestimmt die gemeinsame Zeitbasis der Zelle. Für die Synchronisierung von neu hinzukommenden Stationen sendet dieser in regelmäßigen Abständen Beacons mit Zeitinformationen (TIM).

Eine Station, die Broadcast Pakete empfangen möchte, muss zuerst diese Zelle lokalisieren und sich auf deren Zeitbasis synchronisieren. Hierfür bietet der IEEE 802.11{a|b} Standard die Möglichkeit einer aktiven oder passiven Suche. Bei der aktiven Suche sendet die Station „Probe Requests“ nacheinander auf allen Kanälen im ISM Band und wartet auf ein „Probe Response“ eines AP. Diese Methode erfüllt jedoch nicht die von uns ge-

stellte Anforderung an Schweigsamkeit. Diese wird jedoch durch die passive Suche nach AP Zeitinformationen erfüllt. Die Station sucht dabei nacheinander auf allen Kanälen nach Beacon Paketen des AP. Wenn die Station ein solches Paket empfangen hat synchronisiert sie sich mittels der gelieferten Zeitinformationen mit den AP der Zelle. Die passive Suche eignet sich ebenfalls für den Ad-Hoc Modus.

Die im Schritt 2 der Anmeldeprozedur durchzuführende gegenseitige Authentifizierung lässt sich überspringen, wenn man davon ausgeht, dass die per Broadcast verbreiteten Informationen für jedermann zugänglich sein sollen und eine Authentifizierung hier nicht sinnvoll ist.

Der Aufbau einer Bindung der Station zur Zelle im Schritt 3 lässt sich ebenfalls überspringen, wenn man sich die Funktionalität des „Promiscuous Mode“, den viele 802.11 Netzwerkadapter unterstützen, zu Nutze macht. Dieser Ermöglicht das Empfangen von Datenpaketen ohne eine vorausgegangene Bindung zum AP.

Zusammenfassend lässt sich sagen, dass für den Empfang von Informationen die per Broadcast zur Verfügung gestellt werden, die beschriebene Methode, die nur auf passivem Empfang von Zeitinformation des AP und der Nutzung des „Promiscuous Mode“ beruht, vollkommen ausreichend ist. Wenn jedoch Daten von der Station zum AP übermittelt werden sollen, ist mindestens Schritt 3 auszuführen, der jedoch die MAC Adresse der Station dem AP mitteilt.

### 3.3 IEEE 802.11{a|b} und Broadcast

Die Broadcast Funktionalität ist fester Bestandteil der Asynchronen Daten Dienste von IEEE 802.11{a|b}, die von der MAC Schicht zur Verfügung gestellt werden. Jede Station ist in der Lage Broadcast-Pakete zu empfangen oder selbst zu senden. Für den Empfang von Broadcast-Paketen empfiehlt sich die im vorherigen Abschnitt beschriebene passive Empfangsmethode. Zum Senden von Broadcast-Paketen ist diese ungeeignet. Bevor eine Station Broadcast-Pakete senden kann, muss diese einer Funkzelle beitreten. Dieser Prozess erfolgt in den bereits genannten drei Schritten. Im Schritt 1 lokalisiert die Station eine Zelle und synchronisiert sich auf die gemeinsame Zeitbasis der Zelle (Synchronization Step). Im Schritt 2 erfolgt in Abhängigkeit von der Konfiguration der Zelle eine gegenseitige Authentifizierung zwischen AP und Station (Authentication Step). Zum Schluss erfolgt im Schritt 3 der eigentliche Beitritt der Station zur Zelle über die Verbindungsprozedur (Association Step). Jetzt ist die Station in der Lage Broadcast Pakete zu senden. Im Ad-Hoc Modus gestaltet sich der Beitritt ähnlich. Die Funktionalität des AP wird von den am Ad-Hoc Netzwerk beteiligten Stationen übernommen. In beiden Fällen wird beim Senden von Broadcast-Paketen die MAC-Adresse des Netzwerkadapters an die Kommunikationspartner weitergegeben.

## 4 Zusammenfassung

Nach den in der Einleitung definierten Kriterien bietet IEEE 802.11 {a|b} einen größeren Schutz der Anonymität, da dieser Standard im Gegensatz zu Bluetooth den passiven Empfang von Daten ermöglicht. Des Weiteren ist bei IEEE 802.11 die Funkschnittstelle nur während der Nutzdatenübertragung aktiv. Bluetooth schneidet bei dieser Untersuchung schlechter ab, da die MAC-Adresse bei kommerziellen Bluetooth-Geräten nicht änderbar ist und außerdem ein Piconetz-überschreitender Broadcast nicht möglich ist. In Tabelle 2 sind die Ergebnisse der Untersuchung nochmals zusammengefasst.

	<b>Identifizierende Geräte-merkmale</b>	<b>Schweigsamkeit</b>	<b>Broadcast</b>
<b>Bluetooth</b>	vorhanden und fest	wird unterstützt	nicht möglich über Piconetzgrenzen hinaus
<b>IEEE 802.11{a b}</b>	vorhanden, aber Änderung möglich	möglich durch Ausnutzung des Promiscuous Mode	wird unterstützt

**Tabelle 2** Gewährleistung der Anonymitätsaspekte bei Bluetooth und IEEE 802.11 {a|b}

## Referenzen

- [1] Specification of the Bluetooth System (Profiles), Version 1.1, Februar 2001.
- [2] Specification of the Bluetooth System (Specification), Version 1.1, Februar 2001.
- [3] Assigned Numbers – BT Baseband, <http://www.bluetooth.org/assigned-numbers/baseband.htm>
- [4] IEEE 802.11 Wireless Local Area Networks, <http://grouper.ieee.org/groups/802/11/>

Diese Arbeit wurde unterstützt von der Gottlieb Daimler- und Karl Benz-Stiftung, Ladenburg und der Deutschen Forschungsgemeinschaft (DFG).