Hauptseminar
Sicherheit in mobilen Netzen

Betreuer:
Frank Kargl und Stefan Schlott

Sommersemester 2002
Abteilung Medieninformatik
Universität Ulm

Inhaltsverzeichnis

Kapitel 1

Bluetooth Security

Karim Andreas Siebenrok
karim.siebenrok@informatik.uni-ulm.de

Abstract: Der Bluetooth-Standard ist relativ neu und enthält eine ganze Reihe von Sicherheitsmechanismen, aber wie jede neue Technologie haben auch diese ihre Schwachstellen. Nur die Kenntnis über die Funktionsweise und Angriffspunkte dieser Mechanismen, hilft dem Anwender die Technologie sicher einsetzen zu können. Bluetooth hat drei große Sicherheitsmerkmale definiert, das Key Management, die Verschlüsselung und die Authentisierung. Als Schwachstellen sind die „Location Attack" und die Berechnung der Schlüssel zu nennen.
Abschließend lässt sich feststellen, dass für Anwendungen, die ein besonderes Maß an Sicherheit verlangen, noch Bedarf an Nachbesserung besteht. Schließlich handelt es sich in den meisten Fällen um sehr persönliche oder geheime Daten, die über ein solches Netzwerk übertragen werden sollen.

1.1 Einführung

Bluetooth geht auf die Entwicklung bei der Firma Ericsson zurück. Anfang 1998 wurde die Bluetooth Special Interest Group von Ericsson, IBM, Intel, Nokia und Toshiba gegründet. Heute hat die Organisation über 1300 Mitglieder. Im Juli 1999 wurde die Spezifikation 1.0 vorgestellt. Mittlerweile liegt diese in der Version 1.1 vor.
Bluetooth ist ein neuer Kurzstrecken-Funkstandard, der eine mobile, vernetzte Welt ohne Kabelgewirr ermöglichen soll. Das Funkmodul lässt sich sowohl in diverse mobile Endgeräte, wie Notebooks, Handys, PDAs, als auch in Drucker oder Digitalkameras einbauen. Auch eine Anbindung an bestehende Netzwerke, wie LAN, GSM oder das Festnetz ist über einen Access Point möglich.
Eine kabellose Verbindung zweier Endgeräte ist nichts neues, das ist schon von anderen Wireless-Lösungen, wie zum Beispiel IrDA, bekannt. Neu ist, dass meh-

rere Geräte, bis zu einer Distanz von zehn Metern, ohne Sichtkontakt, miteinander verbunden werden können. Bluetooth wird sich eher in kleinen persönlichen Netzwerken durchsetzen, da seine Datendurchsatzrate von 1 MBit/s keine Konkurrenz für drahtlose LAN-Lösungen darstellt. Die derzeit verfügbaren Wireless LANs können bis zu 11 MBit/s übertragen und es sind bereits Netze standardisiert, die künftig eine Bandbreite von bis zu 54 MBit/s zur Verfügung stellen werden.
Diese Ausarbeitung, die im Rahmen des Hauptseminars: „Sicherheit in mobilen Netzen" an der Universität Ulm entstanden ist, soll zunächst die Funktionsweise von Bluetooth generell aufzeigen. Und später die Sicherheitsmechanismen und einige Schwachstellen der sogenannten Bluetooth Security näher beleuchten.

1.2 Bluetooth Technologie

1.2.1 Technische Spezifikationen

Zunächst wenden wir uns den technischen Spezifikationen der Bluetooth Systeme zu. Bluetooth arbeitet als kabelloses Netzwerk auf dem Frequenzbereich um 2,45 GHz. Dies ist das globale Industrial-, Scientific und Medical-Band, das nicht lizensiert werden muss, und so einer schnellen Markteinführung entgegenkommt. Um Interferenzen, mit zum Beispiel Mikrowellen oder Wireless LANs, die im gleichen Bereich arbeiten, zu vermeiden, wurde das sog. Frequency Hopping eingeführt. Dieses beruht darauf, dass die Funkmodule immer, nachdem sie ein Datenpaket verschickt oder erhalten haben zu einer neuen Frequenz springen. Dazu wurde der Bereich von 2,402 bis 2,480 GHz in 79 Kanäle, im Abstand von 1 MHz, unterteilt. Damit lässt sich eine maximale Frequenzänderungsrate von 1600 Hopps/s erreichen.

Derzeit werden hauptsächlich Interferenzen mit anderen WLAN-Lösungen nicht ausgeschlossen. Es fehlen allerdings noch die praktischen Erfahrungen, da Bluetooth noch zu wenig verbreitet ist. Es wird aber davon ausgegangen, dass ein WLAN Bluetooth wenig beeinflusst, da bei Bluetooth durch den ständigen Frequenzwechsel nur kurzzeitig Störungen auftreten. Es überschneiden sich nur wenige der 79 Bluetooth-Kanäle mit den Kanälen des Funk-LANs. Allerdings soll die Bandbreite eines Wireless LANs in direkter Umgebung eines Bluetooth Netzes um bis zu 22 Prozent verringert werden, da diese für die Fehlerkorrektur werden muss. Obwohl in der Praxis noch wenig Probleme aufgetreten sind, ist auch schon eine Lösung in Sicht. Mit den IEE802.11a und Hiperlan/2 Standards soll es künftig 54 MBit/s-WLAN-Systeme geben, die nicht mehr im kritischen Bereich von 2,45-GHz arbeiten werden. Diese werden das Frequenzband um 5 GHz nutzen. [Sch01]

Die Bluetoothverbindung hat, auch ohne Sichtkontakt, eine omnidirektionale Reichweite von zehn Zentimetern bis zu zehn Metern. Die Bluetooth Special Interest Group plant allerdings schon eine Leistungsklasse, mit der sich, durch eine Erhöhung der Sendeleistung auf 100mV, Distanzen von bis zu 100m überbrücken lassen sollen. Hier wird der Einfluss von Störsignalen durch die implementierte

„Forward Error Correction“ begrenzt.

Zur Übertragung gibt es zwei Grundtypen von Verbindungsarten:
Die erste ist die **„Synchronous Connection Oriented“(SCO)**, die in erster Linie für den Voice-Verkehr eingesetzt wird. Diese benutzt reservierte Zeitschlitze und eine reservierte Kanalbandbreite. Der Master kann gleichzeitig bis zu 3 SCO Verbindungen zu einem oder mehreren Slaves unterstützen. Jedes Paket wir nur einmal übertragen [Po01]. Es stehen maximal 3 Kanäle pro Piconet zur Verfügung, die jeweils eine Datenübertragung von 64 Kbit/s erreichen können und somit in der Bandbreite einer ISDN Verbindung entsprechen [Gm02].

Die asynchrone Verbindungsart, ist die: **„Asynchronous Connectionless“ (ACL)**, die sowohl asymmetrischen, als auch symmetrischen Verkehr unterstützt. Die Übertragung ist paketorientiert und zeitschlitzunabhängig. Der Master unterhält mehrere Verbindungen zu verschiedenen Slaves zur gleichen Zeit. Die Pakete werden wiederholt übertragen. Dabei stehen maximal 7 Kanäle pro Piconet zur Verfügung. Bei der asymmetrischen Verbindung sind Übertragungsraten von maximal 721 KBit/s in die eine Richtung und 57,6 KBit/s in die Gegenrichtung möglich. Bei einer symmetrische Verbindung werden Daten mit je 432,6 KBit/s pro Richtung transportiert [ARS00].

1.2.2 Funktionsweise

Im Bluetooth-System sind sowohl Point-to-Point als auch Point-to-Multipoint Verbindungen möglich. Das sogenannte Piconet besteht aus einer Ansammlung von zwei bis acht Geräten, die alle mit der gleichen Hopping-Sequenz synchronisiert werden. Ein Gerät fungiert im Netz als Master, der die anderen Geräte im gleichen Piconet synchronisiert. Durch ein Zeitmultiplexverfahren können Bluetooth-Geräte mehreren Piconets angehören, dies wird dann Scatternet genannt. Darin identifiziert sich jedes Piconet durch eine eigene Frequency-Hopping-Folge. (Siehe Abbildung 1.1)

Bevor eine Verbindung aufgebaut wird, stehen alle eingeschalteten Geräte im Standby-Modus. Sie lauschen in periodischen Abständen von 1,28 Sekunden nach Nachrichten und kontrollieren 32 Hop-Frequenzen [Gm02]. Ein beliebiges Gerät initiiert die erste Verbindung und macht sich dadurch zum Master. Ist die MAC Adresse der anderen Geräte bekannt wird die Verbindung durch eine sogenannte Page-Message hergestellt, falls nicht, wird davor eine Inquiry-Nachricht geschickt. Näher erläutert wird der Verbindungsaufbau im Punkt Key Management. Danach befindet sich die Station im State Verbunden. Nach Empfang der Nachricht wird Detach gesendet und der Empfänger geht wieder in den Standby Mode (Siehe Abbildung 1.2). Um Strom zu sparen, können Stationen, die nicht senden oder empfangen, in verschiedene Zustände wechseln. Diese Zustände sind in der Reihenfolge ihres Energieverbrauchs aufgelistet:

- SNIFF-Modus: Hierbei wird in einstellbaren periodischen Abständen die Schnittstelle auf Übertragungen überprüft.
- HOLD-Modus: Slaves können in diesen Zustand - vom Master oder sich selbst initiiert - wechseln. Die MAC Adresse bleibt erhalten.

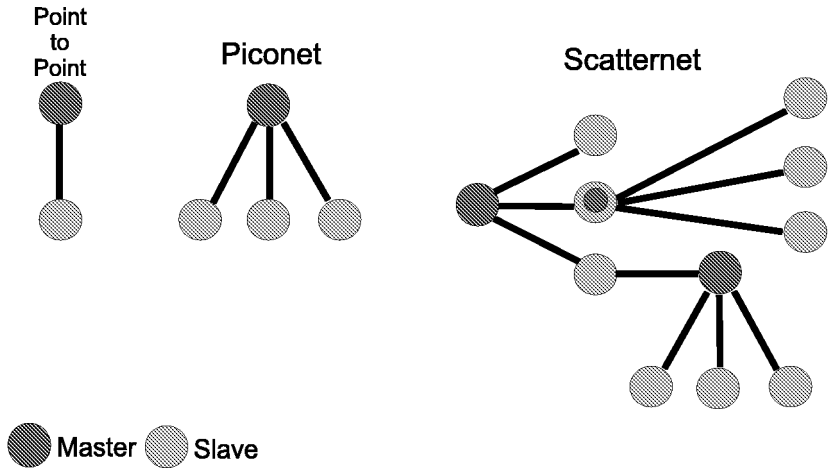

Abbildung 1.1: Aufbau der unterschiedlichen Topologien von Bluetooth-Netzen [WR02]

- PARK-Modus: Die Stationen nehmen nicht an der Kommunikation teil. Die MAC Adresse wird zurückgegeben.

Der Verkehr des Master wird aber für Synchronisationszwecke aufgenommen. Broadcast Nachrichten werden erkannt und verarbeitet. [ARS00]

Die Master-Einheit kontrolliert die Bandbreiten und teilt sie nach Bedarf den entsprechenden Slaves zu. Außerdem kontrolliert sie die Verbindungsarten der Master-Slave-Paare, die innerhalb eines Piconets verschieden sein können und im laufenden Betrieb beliebig geändert werden können.
Nachdem wir nun die Spezifikation und Funktionsweise etwas näher betrachtet haben wenden wir uns im nächsten Abschnitt der Bluetooth Security zu.

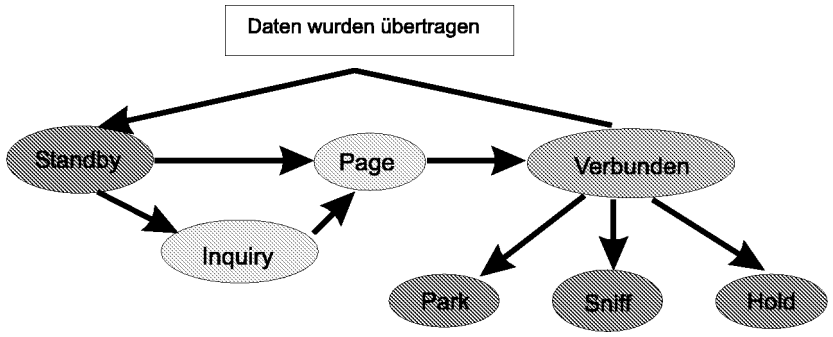

Abbildung 1.2: Übergänge zwischen den einzelnen States [ARS00]

1.3 Bluetooth Security

In diesem Teil beschäftigen wir uns mit denen im Standard definierten Sicherheitsmerkmalen von Bluetooth. Im Gegensatz zu anderen Geräten werden bei Bluetooth, wie auch bei WLAN 802.11, die Sicherheitsfeatures nicht über die Software gesteuert, sondern wurden gleich in die Firmware implementiert. Im allgemeinen Bluetooth Access Profil werden drei verschiedene Sicherheitsbetriebsarten unterschieden:

- Mode 1: Das ist der unsicherste Zustand, indem ein Bluetooth Gerät keinerlei Sicherheitsprozeduren einleitet. In diesem Zustand erlaubt es anderen Geräten mit Ihm eine Verbindung aufzunehmen.
- Mode 2: auf dem Servicelevel erzwungene Sicherheit
- Mode 3: auf dem Verbindungslevel erzwungene Sicherheit

Der Unterschied zwischen Mode zwei und drei ist, dass beim Mode 3 die Sicherheitsprozedur bereits initialisiert wird, bevor der Kanal aufgebaut wird. Die drei Bluetooth Sicherheitsmechanismen sind das Key Management, die Verschlüsselung und die Authentisierung.

1.3.1 Key Management

Im Bluetooth System gibt es verschiedene Arten von Schlüsseln, die eine sichere Übertragung gewährleisten sollen. Der wichtigste Schlüssel ist der „link key". Dieser dient sowohl als Grundlage zur Verschlüsselung, als auch zur späteren Authentisierung zwischen zwei Geräten. Alle vier verschiedene Arten des „link keys" sind 128 Bit Zufallszahlen. Diese werden entweder temporär nur für eine Sitzung oder semi-permanent gespeichert, zweiteres heißt, sie werden nach Beendigung der Sitzung zur gegenseitigen Authentisierung benutzt. Die Arten des „link keys" heißen:

- „Initialization key"
- „Unit key"
- „Combination key"
- „Master Key": Wird generiert, wenn der Master zu mehreren Geräten gleichzeitig Informationen senden möchte. Er überschreibt die aktuellen „link keys" für eine Sitzung.

Der **„initialisation key"** wird während der Initialisierung genutzt, um die Initialisierungsparameter, während der Übertragung, zu schützen. Wenn sich zwei Geräte das erste mal begegnen und eine verschlüsselte Übertragung erwüscht ist, müssen sie zunächst einen gemeinsamen Schlüssel vereinbaren. Dazu wird der init key mittels einer Funktion (E22) aus einer geheimen PIN, der Device Adresse des Geräts und einer Zufallszahl generiert. Die PIN ist eine Zahl, die in

beiden Geräten eingegeben werden muss und zwischen 8 und 128 Bits lang ist. Wird keine PIN gewählt, wird standardmäßig 0 verwendet. Die Zufallszahl wird unverschlüsselt übertragen. Die Device Adresse ist durch die vorherige unverschlüsselte Kommunikation bekannt [Ke01]. Mittels einer Hash-Funktion wird dafür gesorgt, dass das Ergebnis wieder eine Länge von 128 Bit aufweist

$$E22\,(Zufallszahl; PIN; ADDR) \longrightarrow initkey\,[128 - bit]$$

Der **„unit key"** wird von einem Bluetooth Gerät generiert, wenn es das erste mal benutzt wird. Er setzt sich aus einer 128-bit Zufallszahl und der 128-bit Geräte Adresse zusammen. Nachdem er erstellt wurde, wird dieser 128-bit Schlüssel im Speicher des Gerätes hinterlegt und eigentlich nicht mehr geändert.

Der **„combination key"** wird während des Initialisierungs-Prozesses für jedes Paar von Geräten neu generiert, wenn eine höhere Sicherheitsstufe gewünscht wird. Zunächst erzeugen beide Geräte eine Zufallszahl. Danach wird mit dem gleichen Algorithmus (E21), der auch den unit key erstellt, ein Schlüssel erzeugt. Nachdem die Zufallszahlen geheim ausgetauscht wurden, erzeugen beide Geräte den „combination key", der zwischen ihnen benutzt wird.

$$E21\,(Zufallszahl; ADDR) \longrightarrow unit/combinationkey\,[128 - bit]$$

Der **„ encryption key"** wird dann erzeugt, wenn der Link Manager die Verschlüsselung aktiviert. Er wird bei jeder neuen Verschlüsselungsanforderung neu berechnet. Der Schlüssel wird aus dem aktuellen „link key", einer 96-bit „Chiphering Offset Number" (COF) und einer 128-bit Zufallszahl durch einen weiteren Algorithmus (E3) generiert. Die COF basiert auf dem „Authenticated Ciphering Offset", der während der Authentisierung erstellt wird.

$$E3\,(Zufallszahl; COF; Linkkey) \longrightarrow encryptionkey\,[128 - bit]$$

Wie man leicht ersehen kann, sind sämtliche Schlüssel von der Erzeugung einer Zufallszahl abhängig. Innerhalb von Bluetooth ist allerdings kein Mechanismus zum Generieren einer guten, für kryptpgraphische Verfahren geeignete Zufallszahl beschrieben. Hier ist der Endkunde völlig auf die Sorgfalt des Geräteherstellers angewiesen.

1.3.2 Verschlüsselung

Das Bluetooth Verschlüsselungssystem kodiert die Nutzdaten der Pakete. Dies wird durch eine Flusscodierung (E0) realisiert, die bei jedem neuen Transfer wieder synchronisiert wird. Die Flusscodierung besteht aus einem Nutzdaten Schlüsselgenerator, einem Schlüssel Flussgenerator und dem Ver-/Entschlüsselungs Teil. Damit die Nachricht nicht unbemerkt modifiziert werden kann, wird eine Checksumme angehängt, die mit verschlüsselt wird (Siehe Abbildung 1.3). Je nachdem ob ein semi-permanenter oder ein master key verwendet wird, sind verschiedene Verschlüsselungsmethoden möglich, bei denen der Broadcastverkehr entweder verschlüsselt wird oder eben nicht.

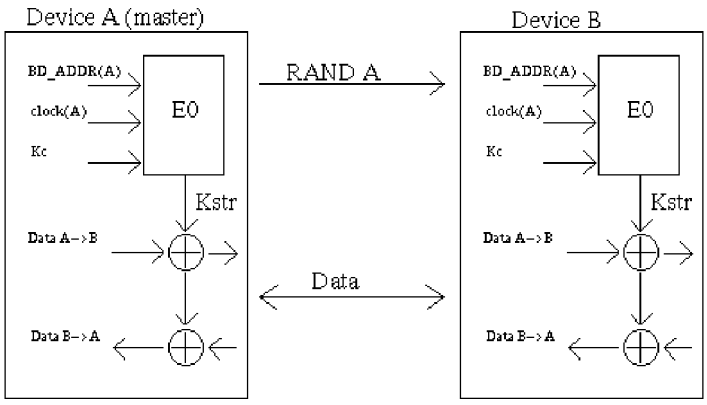

Abbildung 1.3: Beschreibung des Verschlüsselungs Prozesses [Va00]

Da der Schlüssel zwischen 8 und 128 Bit variieren kann, muss die Größe zunächst zwischen den zwei Geräten ausgehandelt werden. Jedes Gerät hat einen Parameter, der die maximal erlaubte Schlüssellänge enthält. Der Master schlägt eine Länge vor, die dann vom Slave angenommen oder abgelehnt wird, bis sich die Geräte einig sind oder die Verbindung abgebrochen wird. Dieser im Gerät vordefinierte Parameter für die Schlüssellänge lässt sich im nachhinein nicht mehr ändern oder umgehen.

1.3.3 Authentisierung

Zwei Geräte die eine Kommunikation wieder aufnehmen wollen, müssen sich zunächst authentisieren, falls die entsprechende Option gewählt wurde. Dabei wird geprüft, ob beide Geräte den gleichen link key verwenden, der bei der ersten Kommunikation generiert wurde. Die Überprüfung erfolgt analog zur Überprüfung des init keys. Das Bluetooth Authentisierungs Schema benutzt eine Challenge-Response Strategie, die durch ein Protokoll prüft, ob die andere Partei den geheimen Schlüssel kennt. Da das Protokoll symmetrische Schlüssel benutzt, beruht eine erfolgreiche Authentisierung darauf, dass beide Geräte sich denselben Schlüssel teilen.
Zunächst sendet der „Prüfer“ eine Zufallszahl, um diese zu authentisieren. Danach benutzen beide Parteien die Authentisierungsfunktion E1 mit dieser Zufallszahl, der Geräteadresse und dem aktuellen link key. Jetzt sendet der Prüfling die Antwort an den Prüfer, der die Antwort verifiziert. (Siehe Abbildung 1.4)

Die benutze Anwendung gibt vor, welche Geräte überprüft werden sollen, so muss nicht zwangsläufig der Master der „Prüfer“ sein. Manche Anwendungen benötigen nur eine Einweg-Authentisierung, wobei nur ein Teilnehmer überprüft wird. Wenn die Authentisierung fehlschlägt, muss eine gewisse Zeit vergehen,

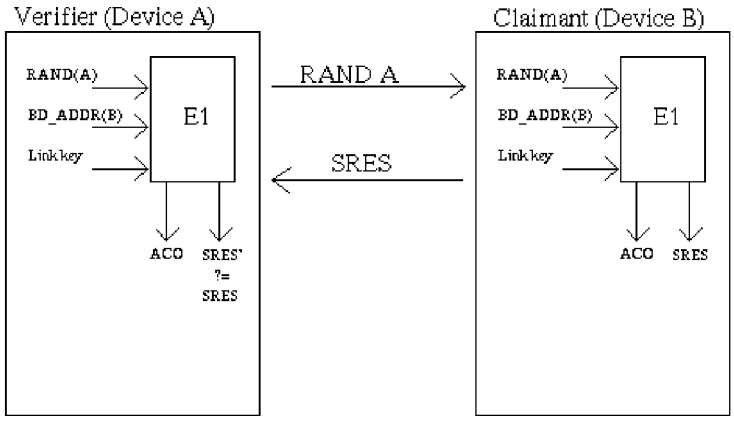

Abbildung 1.4: Beschreibung des Authentisierungs Prozesses [Va00]

bis ein weiterer Versuch gestartet werden kann. [Va00]

1.4 Schwachstellen und Attacken bei Bluetooth

1.4.1 Frequenzhopping

Manche Hersteller verkaufen die pseudozufällige Hopping-Sequenz (siehe technische Spezifikationen) als zusätzliches Sicherheitsfeature, da ein Angreifer nicht voraussagen kann, nach welchem Muster gesendet wird. Allerdings ist es heutzutage technisch überhaupt kein Problem die 79 Kanäle parallel zu überwachen und daraus die richtige Reihenfolge abzuleiten. Außerdem ist die Sequenz leicht in Erfahrung zu bringen, da die Eingabe des Zufallsgenerators sich aus der Geräteadresse und der clock des Masters zusammensetzt. Beide Informationen werden während der Initialisierung unverschlüsselt übertragen.

1.4.2 Brechen des geheimen Schlüssels

Sollte die PIN zu kurz oder schwach sein, kann der link key durch eine brute force-Attacke herausgefunden werden. Dazu belauscht der Angreifer die Initialisierungsphase und bekommt so die verwendete Zufallszahl und die Daten, die zur Verifizierung des init keys übertragen werden. Nun wählt man einen Wert für die PIN und führt die Schritte zur Initialisierung und Verifizierung offline selbst aus und vergleicht den berechneten Funktionswert mit den belauschten Daten. Stimmen diese überein ist er mit höchster Wahrscheinlichkeit im Besitz der richtigen PIN und kann die weitere Kommunikation entschlüsseln oder selbst Nachrichten einspeisen.
Noch leichter ist es bei einfachen Bluetooth-Geräten, die nicht über die Einga-

be einer PIN verfügen. Dies wären zum Beispiel Headsets oder Mikrofone, bei denen der Standard die PIN „0000“ vorsieht. Hier wird es einem Angreifer noch einfacher gemacht sich in das Netz einzuloggen, da er die PIN nicht berechnen muss. Da es Bluetooth Geräten möglich ist, in mehreren Piconetzen gleichzeitig aktiv zu sein, können so Gespräche nicht nur belauscht sondern auch weitergeleitet werden.
In einer anderen Variante dieser Attacke initiiert der Angreifer selbst die Kommunikation. Sobald das Opfer auf die Challenge geantwortet hat, kann der Angreifer wie oben beschrieben vorgehen. [Ke01]

1.4.3 Location Attack

Bluetooth Geräte können in zwei Modi betrieben werden:

- „Detectable Modus“
- „Non-Detectable Modus“

Im „Detectable Modus“ antwortet ein Bluetooth Gerät auf jede Anfrage, eines anderen Gerätes, mit seiner eindeutigen Device Adresse. Dieser Modus wurde eingeführt, um eine leichte Integration in bestehende Netze zu realisieren. Allerdings sind dadurch auch dem Missbrauch Tür und Tor geöffnet. Ein Angreifer kann so sehr einfach den Standort eines Gerätes und damit der Person bestimmen. Man kann sich vorstellen, dass dadurch zum Beispiel in einem Supermarkt Bewegungsprofile der Kunden erstellt werden können. Dazu genügt es, wenn man, im zu überwachenden Bereich, Bluetoothsender und -empfänger installiert und die erkannten Geräte einfach mitprotokolliert.
Im Standard wurde aber auch der „Non-Detectable Modus“ vorgesehen, bei dem das Gerät nicht auf Anfragen antwortet. Nun liegt es in der Hand der Hersteller dem Nutzer diese Option, leicht zugänglich, zur Verfügung zu stellen.

1.5 Zusammenfassung

Das Konsortium der führenden Hersteller hat sich bei der Schaffung des Bluetooth-Standards sehr viele Gedanken über die Sicherheit des neuen Netzes gemacht. Allerdings wurden noch nicht alle Details bis ins letzte durchdacht. So ist zum Beispiel der für sämtliche Schlüssel entscheidende Zufallszahlengenerator völlig undefiniert. Da Bluetooth noch nicht sehr verbreitet ist, fehlen natürlich noch die praktischen Erfahrungen außerhalb der Laborumgebung. In letzter Zeit ist es sehr ruhig um Bluetooth geworden, was eventuell daran liegen kann, dass die Sicherheitsmechanismen die Hauptzielgruppe, die Geschäftskunden, noch nicht zufrieden stellen. Der Einsatz außerhalb des privaten Bereichs erfordert natürlich ein besonderes Maß an Sicherheit, schließlich werden über Bluetooth-Verbindungen hochsensible Daten wie Telefongespräche oder geschäftliche Informationen übertragen.

Man darf aber auch nicht vergessen, dass Bluetooth im Vergleich zu Drahtverbindungen schon jetzt ein größeres Maß an Sicherheit zur Verfügung stellt,

da die Kabel wie Antennen wirken und der Datenverkehr in diesen ungesichert stattfindet. Zum Aufbau von großen Netzwerken oder zur Übertragung von sensiblen Daten, wie Zahlungsverkehr etc., ist Bluetooth derzeit noch nicht geeignet, da die Sicherheitmechanismen sich erst praktisch beweisen müssen. Ich denke in den nächsten Jahren wird sich Bluetooth als alternative zu IrDA- oder kurzen Kabelverbindungen vor allem im mobilen Bereich, wie bei Handys oder PDAs durchsetzen und nicht mehr wegzudenken sein.

Literaturverzeichnis

[ARS00] ARS Software GmbH: Bluetooth - ein Standard für die drahtlose Kommunikation im Nahbereich, März 2000, http://www.ars2000.com/pdf/Bluetooth-WhitePaper.PDF, Stand 05.06.2002.

[Da01] McDaid, Cathal: Cathal's Corner, Bluetooth Security - Part 1, Februar 2001, http://www.palowireless.com/bluearticles/cc1_security1.asp, Stand 12.05.2002.

[Gm02] Gmür, Chrigi: Bluetooth, http://www.e-online.de/public/chrigi/bluetooth.htm, Stand 08.05.2002.

[JW01] Jakobsson, Markus; Wetzel, Susanne: Security Weaknesses in Bluetooth, Lucent Technologies - Bell Labs, http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/-bluetooth.pdf, Stand 08.05.2002.

[Ke01] Keuser, Sabine: Sicherheit in mobiler Kommunikation, http://www.inf.ethz.ch/vs/edu/SS2001/MC/beitraege/08-security-rep.pdf, Stand 08.05.2002.

[Po01] Pohl, Winfried: Drahtlose Kommunikation im Unternehmen, 14.12.2001, http://www.competence-site.de/telekommunikation.nsf/729D9EE77572F702C1256B5F00628D05/File/bluetooth.pdf, Stand 05.06.2002.

[Sch01] Schoblick, Robert: Interferenzen auf dem 2,45 GHz-Band, funkschau 17/2001, S. 68-70.

[Va00] Vainio, Juha T.: Bluetooth Security, Department of Computer Science and Engineering, Helsinki University of Technology, 25.05.2000, http://www.niksula.cs.hut.fi/ jiitv/bluesec.html, Stand 08.05.2002.

[WR02] Weissmann, Oliver; Ruland, Christoph: Sicherheit bei Bluetooth, funkschau 10/2001, S. 43-45.