Anwendung von Funkvernetzungen in der Beschallungstechnik

Bachelorarbeit im Rahmen des Elektro- und Raumakustik Seminars

verfasst von

Blasius Buchegger

Stefan Könighofer

Institut für Signalverarbeitung und Sprachkommunikation der Technischen Universität Graz
Betreuer: Ao. Univ.-Prof.Dipl.-Ing. Dr.techn. Gerhard Graber

Graz, im Februar 2012

Vorwort

Wir möchten uns an dieser Stelle bei mehreren Personen für die Unterstützung bei der Entstehung dieser Arbeit bedanken.

Zuallererst möchten wir Herrn Prof. Dr. Graber für die kompetente Betreuung und Beratung danken.

Besonderer Dank gilt Herrn Christian Rosenbaum, welcher infolge seiner fachmännischen und praxisnahen Beratung sehr positiv bei der Entstehung dieser Arbeit mitgewirkt hat.

Weiters möchten wir folgenden Personen für die Bereitstellung der im Zuge der Arbeit recherchierten audio-elektronischen Systeme danken:

Herrn Diplom-Tonmeister Ulrich Gladisch

Herrn Klemens Moser

Herrn Sebastian Mandl

Herrn Florian Ainhirn

Herrn DI Franz Schober

Zusammenfassung

Fernsteuerungen bzw. Netzwerkverbindungen zwischen Rechnern und audio-elektronischen Geräten wie zum Beispiel Digitalmischpulten wecken schon seit einiger Zeit das Interesse vieler Live-Toningenieure. Eine Vielzahl von Anwendungsbeispielen, wie zum Beispiel eine kabellose Steuerung der Beschallungssituation von jedem Punkt des Raumes zeigen, dass diesem Themengebiet mit steigender Stabilität und Zuverlässigkeit von Funknetzwerken und Computerprogrammen, wie auch steigender Verbreitung von Digitalmischpulten immer mehr Bedeutung zukommt.

Aus diesen Gründen soll in der hier vorliegenden Bachelorarbeit dieses Themengebiet erörtert werden. Ziel wird es sein, zuallererst einen theoretischen Überblick über allgemeine Netzwerktechnik, den Standard für Wireless LAN und für oben genannte Zwecke verwendbare Steuerungsmedien zu ermitteln. Es werden zu den entsprechenden Verbindungsarten bzw. Programmen praxisnahe Anwendungsbeispiele vorgestellt und evaluiert. Dem Thema „Sicherheit“ wird aufgrund der Wichtigkeit dieses Aspektes ein zentrales Kapitel gewidmet. Anhand kommerziell erhältlicher Geräte werden schließlich mehrere mögliche Setups vorgestellt, welche je nach Anwendungsart ihre Stärken, aber auch Schwächen zeigen. Hierbei wurde großer Wert auf eine weitgehende Betriebssystems-Unabhängigkeit (Windows/Mac OSX) gelegt. Abschließend werden noch einige Möglichkeiten zur Erhöhung der Sicherheit und Stabilität der vorgestellten Setups erörtert.

Abstract

Remote control or network connections between computers and audio-electronic devices such as digital mixing consoles became more and more attractive for many live sound engineers. A variety of applications, e.g. the wireless control of the sound situation from every point of the room, show, that these technologies got more and more important, which is due to the increasing stability and reliability of wireless networks and computer programs, as well as the increasing use of digital mixing consoles.

For these reasons we present this topic and some typical applications. First of all, we provide an overview of the relevant theoretical background, including network technology, the standards for wireless LAN and the common protocols to control audio devices. Practical applications and setups are discussed and evaluated. Also network security and step-by-step-instructions for typical setups are part of this thesis. Finally, a few possibilities to increase the security and stability of the presented setups are discussed.

Inhaltsverzeichnis

1 Einleitung

1.1 Allgemeines

Unter dem in dieser Arbeit vorgestellten Begriff „Funksteuerung“ versteht man die Steuerung von digitalem Equipment mittels kommerziell erhältlichen, elektronischen Geräten wie z.B. Laptops oder Smartphones. Dies geschieht über ein WIFI – Netzwerk, wodurch der Benutzer völlig von einer fixen Position im Raum gelöst ist (was z.B. bei der Bedienung eines Mischpultes im Live - Betrieb der Fall wäre). Eine hohe Anzahl an Anwendungs-möglichkeiten bestätigen den Sinn und Zweck der Verwendung einer solchen Technik. Bei der Beschallung von Musikgruppen, aber auch im Studioalltag kann eine Funksteuerung eine erhebliche Arbeitserleichterung mit sich bringen. So wird es dem Techniker ermöglicht, - ohne zusätzliche Hilfe eines Kollegen - einen Raum bzw. die Beschallungsanlage „einzumessen“, Bühnen – Monitore zu entzerren oder aber auch die Mischung der Musiksignale von verschiedenen Positionen aus zu evaluieren und ggf. zu korrigieren. Eine Reduzierung des erforderlichen Personals kann somit auch den finanziellen Aufwand einer Produktion minimieren.

Um dem Leser die soeben genannten Aspekte möglichst verständlich nahe zu bringen, werden in diesem ersten Kapitel – schematisch - zu ausgewählten Steuerungsvarianten praxisnahe Anwendungsbeispiele vorgestellt. Hierbei wird bereits auf die Stärken und Schwächen der verschiedenen Steuerungsvarianten eingegangen, um dem Interessenten bereits im Vorfeld die Entscheidung bei der Wahl der passenden Funksteuerung zu erleichtern. In Kapitel 2 wird ein theoretischer Überblick über die allgemeine Netzwerktechnik, Wireless LAN und den verschiedenen Steuerungsmedien gegeben. Bereits vorhandene bzw. für diese Arbeit entwickelte Systeme werden in Kapitel 3 vorgestellt. Dem Thema Sicherheit, besonders im Live - Betrieb, wird in Kapitel 4 aufgrund der Wichtigkeit dieses Aspektes, große Beachtung geschenkt. Für die Umsetzung wird auf eine passende Step-by-Step Anleitung in Kapitel 5 verwiesen. Diverse Maßnahmen zur Erhöhung der Sicherheit und Stabilität der vorgestellten Setups in Kapitel 6 runden die Arbeit ab.

1.2 Verbindungsarten

Die nachfolgende Abbildung soll die in dieser Arbeit vorgestellten Möglichkeiten der Funksteuerung von digitalem, audioelektronischen Equipment verdeutlichen. Als Steuergeräte kommen Laptops, Tablet-PC´s oder aber auch sogenannte Smartphones zum Einsatz. Über ein WIFI-Netzwerk werden Steuerungsdaten an Rechnern oder Geräte Servern gesendet, welche die Übersetzung auf das jeweilige Endgerät vornehmen, hier symbolisch dargestellt als ein digitales Mischpult.

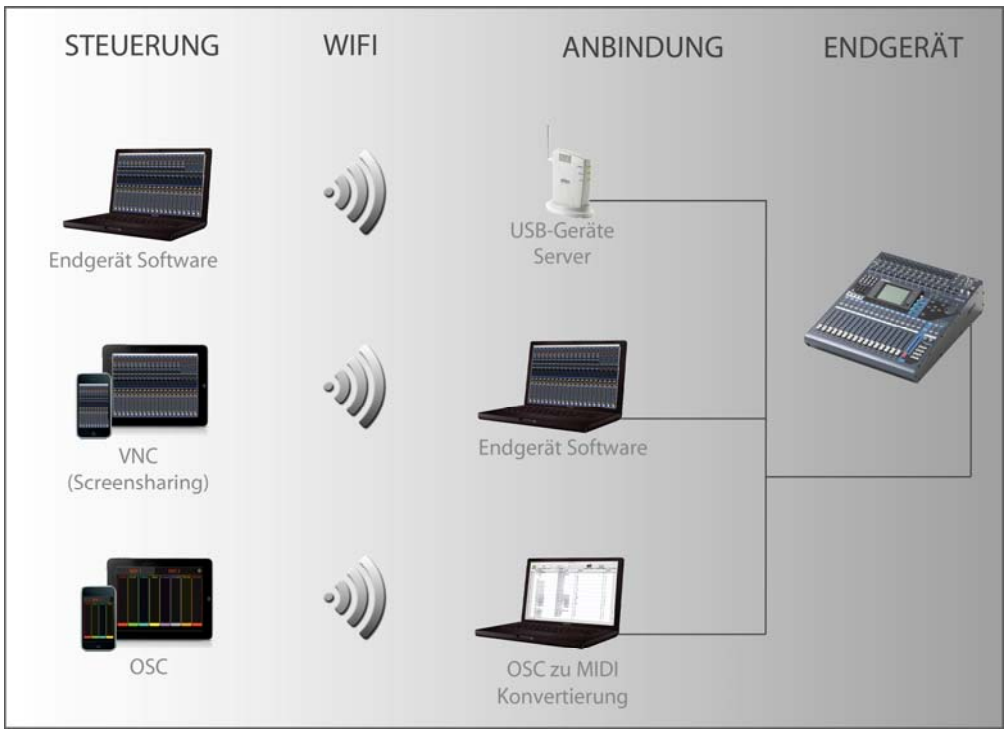

Abb. 1.1: Verbindungsarten

Jede dieser Steuerungsmedien hat seine Vor- und Nachteile. Diese werden in der nachfolgenden Tabelle dargestellt:

VERBINDUNG	***MINDEST – ANFORDERUNG***	***VORTEILE***	***NACHTEILE***	***EMPFOHLENE VERWENDUNG***
Geräte-Server	- PC/Laptop - USB Geräteserver - Steuerungs-Software	- Zugriff auf ALLE Steuerungsparameter - sehr stabil (besonders unter Windows) - keine bemerkbare Latenz	- Zugriff von nur 1 User möglich - diverse Komplikationen bei Verwendung unter Mac OSX - Anschaffungskosten Geräteserver - nur mit vollwertigem Betriebssystem nutzbar (kein Tablet/Smartphone)	- Professionelle Anwendungen in der Beschallungstechnik (FOH und Monitor Mix, Lautsprecherentzerrung, Delay Lines etc.)
Virtual Network Computing (VNC)	- PC/Laptop - 2ter PC/Laptop, Tablet, Smartphone - VNC Software - Steuerungs-Software	- Zugriff auf ALLE Steuerungsparameter - auch Überwachung zusätzlicher Anwendungen möglich (z.B. Recording) - Verwendung Smartphone denkbar → einfaches Handling	- bemerkbare Latenz, besonders bei Verwendung mehrerer Applikationen gleichzeitig	- Professionelle Anwendungen in der Beschallungstechnik (Korrektur voreingestellter Parameter im Bereich FOH und Monitor Mix, Lautsprecherentzerrung, Delay Lines etc.)
Open Sound Control (OSC)	- PC/Laptop - 2ter PC/Laptop, Tablet, Smartphone - TouchOSC Software - OSC auf MIDI Konverter	- Zugriff auf bestimmte Parameter einstellbar - Erstellung eigener Bedienoberflächen je nach Anwendungsart - keine bemerkbare Latenz - jegliches OSC/MIDI fähige Gerät steuerbar	- höherer Konfigurationsaufwand, besonders für große/umfangreiche Oberflächen (jeder Parameter muss einzeln eingestellt werden) - keine Pegel anzeigbar	- Steuerungsoberflächen für Musiker z.B. für Monitoring-Anwendungen (nur Zugriff auf voreingestellte Parameter) - Verwendung von Software-Instrumenten im Livebetrieb - Steuerung von Effektparametern

Abb. 1.2: Tabelle Vor-/Nachteile

1.3 Mögliche Szenarien

Die nachfolgenden Abbildungen sollen mögliche Anwendungsbeispiele der in dieser Arbeit vorgestellten Funksteuerungen - schematisch - verdeutlichen. Bereits vorhandene bzw. für diese Arbeit entwickelte Systeme, welche auf diesen Konzepten beruhen, werden in Kapitel 3 vorgestellt.

Die folgende Abb. 1.3 stellt ein Szenarium im Live-Betrieb dar. Mittels Funksteuerung kann von jeder beliebigen Position aus die verschiedenen Parameter eines digitalen Mischpultes adjustiert werden.

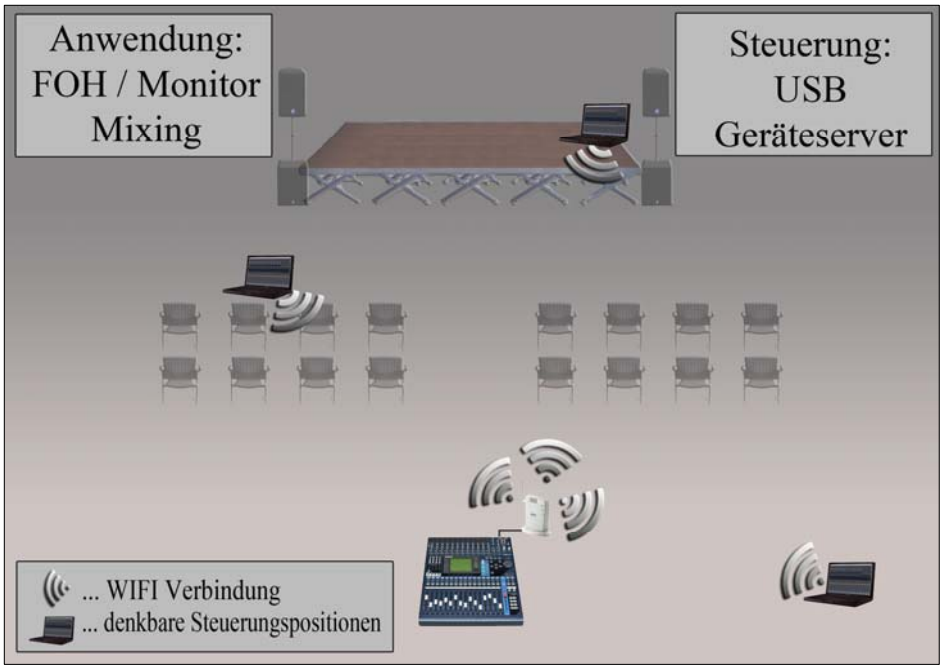

Abb. 1.3: Anwendung: FOH / Monitor Mixing: Steuerung eines Digitalmischpultes mittels Laptop

Abb. 1.4. veranschaulicht einen weiteren Anwendungsfall im Bühnenbetrieb. Hierbei wird es dem Musiker ermöglicht seine persönlichen Monitoring-Einstellungen über vorkonfigurierte, persönlich angepasste Steuerungsoberflächen für dessen Smartphone zu verändern.

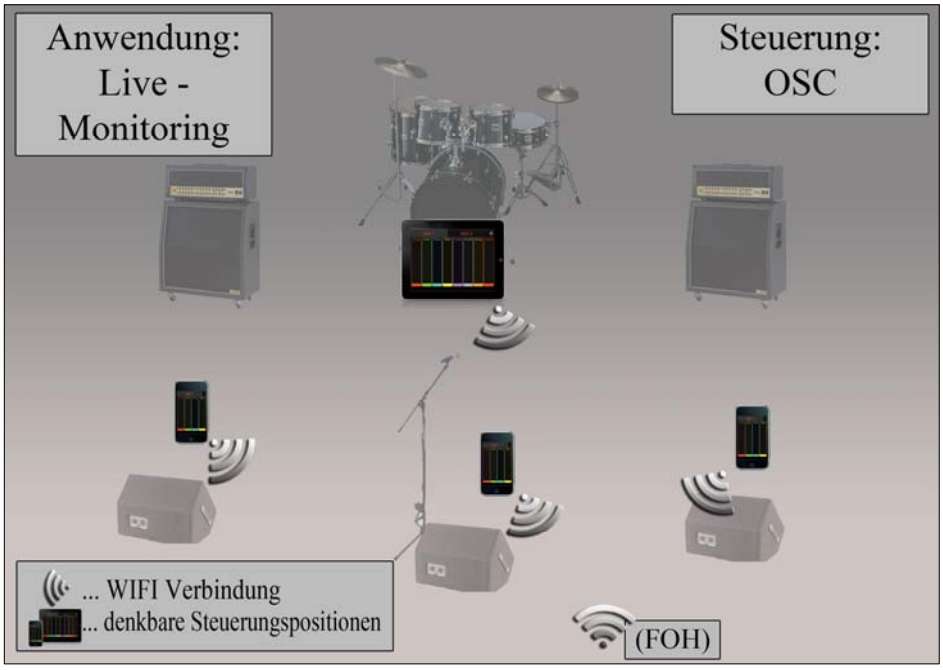

Abb. 1.4: Anwendung: Live-Monitoring: Steuerung der verschiedenen Monitor-Mischungen einer Band mittels Smartphones / Tablet

Auch eine Steuerung von Effekten für das Gesangssignal eines Sängers auf der Bühne ist denkbar, wie Abb. 1.5. zeigt. Hierbei verändert der Musiker verschiedenste Parameter von Software-Effekten z.B. Tap-Delay oder Hall. Aufgrund der Funksteuerung ist der Sänger nicht wie bei den weit verbreiteten Boden-Effektgeräten an eine bestimmte Position gebunden, er kann sich frei auf der Bühne bewegen.

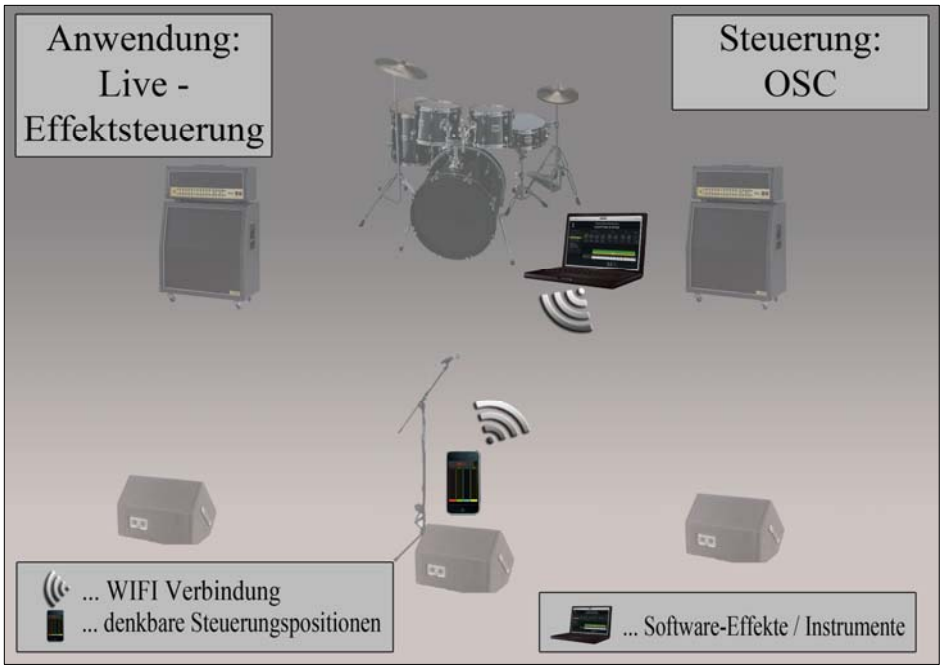

Abb. 1.5: Anwendung: Live-Effektsteuerung: Steuerung diverser (Effekt-) Parameter eines Software-Sequenzers mittels Smartphone

Weiters ist eine Anwendung im Studio-Betrieb denkbar. In Abb. 1.6. wird gezeigt, wie ein Musiker z.B. die Lautstärke-Verhältnisse des Playbacks für die Aufnahme selbst steuert. Somit kann er das Monitoring individuell an seine Bedürfnisse anpassen. Ein weiterer positiver Aspekt kommt zum Tragen: der ausführende Toningenieur gibt einen Teil seiner Arbeit an den Musiker ab, und kann sich auf seine Hauptaufgabe - der Aufnahme - konzentrieren.

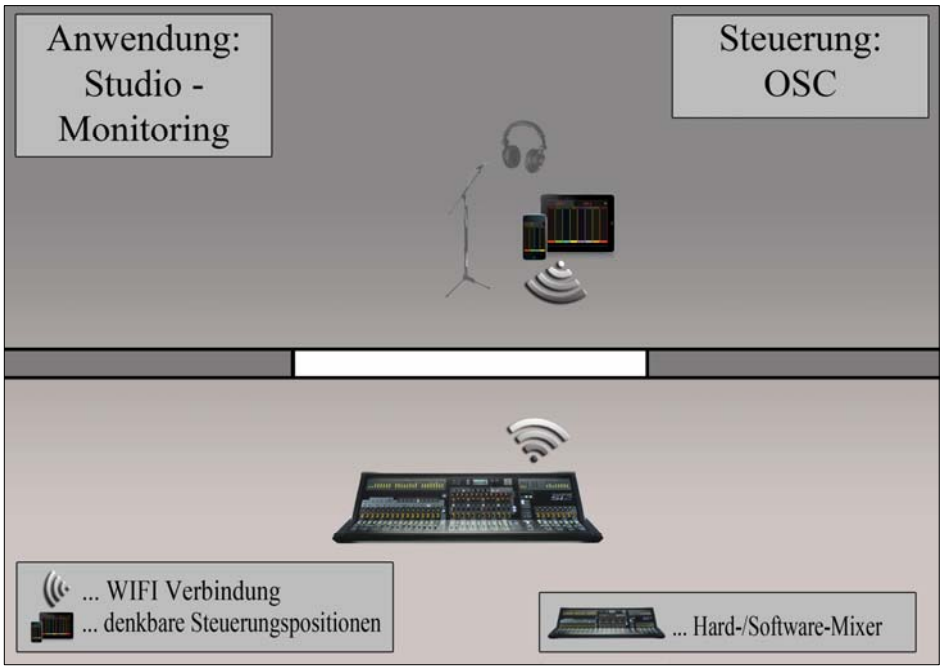

Abb. 1.6: Anwendung: Studio-Monitoring: Steuerung der Monitor-Mischung im Studiobetrieb mittels eines Smartphones / Tablet

2 Theoretische Grundlagen

2.1 Netzwerktechnik

Um die Hintergründe der in dieser Arbeit vorkommenden Konfigurationsvorschläge verstehen zu können, wird im folgenden Kapitel eine kurze Einführung in die Netzwerktechnik gegeben. Ziel ist es, ein grundlegendes Verständnis für die zum Einsatz kommenden Protokolle auf den jeweiligen Schichten zu bekommen, um auch den Sinn und Zweck diverser Techniken für die Netzwerk-Konfiguration bzw. Sicherung nachvollziehen zu können. Im Speziellen werden die sogenannte „Internetschicht“ und die „Transportschicht“ behandelt, da diese fundamentale Bedeutung z.B. im Bereich der Fernwartung (VNC, siehe Kap. 2.3.1.) haben.

2.1.1 Netzwerkaufbau

Im Jahre 1979 wurde das ISO/OSI-Schichtenmodell („International Organization for Standardization / Open Systems Interconnection“) eingeführt, welches die Netzwerk-Kommunikation verschiedener Systeme in sieben Schichten beschreibt:

7	Anwendungsschicht/Application Layer
6	Darstellungsschicht/Presentation Layer
5	Sitzungsschicht/Session Layer
4	Transportschicht/Transport Layer
3	Netzwerkschicht/Network Layer
2	Sicherungsschicht/Data Link Layer
1	Bitübertragungsschicht/Physical Layer

Abb. 2.1: Das ISO/OSI-Schichtenmodell ([5], S. 1)

Jede Schicht steht für sich alleine und wird unabhängig von den anderen ausgeführt.

Für den praktischen Einsatz ist jedoch eher das TCP/IP Referenzmodell heranzuziehen, welches die Schichten des ISO/OSI-Modells zu insgesamt vier Schichten zusammenfasst:

4	Anwendungsschicht
3	Transportschicht
2	Internetschicht
1	Netzzugangsschicht

Abb. 2.2: Das TCP/IP-Schichtenmodell ([1] S.3)

Schicht 1: Netzzugangsschicht:

Diese Schicht fasst die Schichten 1 und 2 des ISO/OSI Modells zusammen. Hier sind die verschiedensten Protokolle angesiedelt, wie z.B. Ethernet, FDDI und Wireless LAN. Seitens der Hardware kommen hier Repeater, und Bridges zum Einsatz (näheres dazu siehe Kap. 6.1). [5]

Schicht 2: Internetschicht:

Auf der Internetschicht werden über das IP-Protokoll Datenpakete weitergeleitet (Routing). Hierbei werden vorwiegend Router verwendet. [5]

Schicht 3: Transportschicht:

In dieser Schicht wird eine sogenannte „Ende-zu-Ende“ Verbindung zweier Systeme hergestellt, also eine direkte Verbindung ohne Zwischenstationen. Zum Einsatz kommen die Protokolle TCP („Transmission Control Protocol“) und UDP („User Datagram Protocol“). [5]

Schicht 4: Anwendungsschicht:

Diese Schicht fasst die Schichten 5 bis 7 des ISO/OSI Modells zusammen und behandelt das, was die eigentliche Anwendung betrifft. [5]

2.1.2 Die Internetschicht: IP

Das „Internet Protocol“ (IP) und seine Nebenprotokolle stellen die Basis des Internets und somit moderner Netzwerke dar. Da IP ein unzuverlässiges, verbindungsloses Protokoll ist, können IP-Pakete versendet werden, ohne dass eine direkte Verbindung zum Empfänger besteht. Mit anderen Worten: Der Sender erhält keine Information darüber, ob das losgeschickte Paket auch beim Empfänger angekommen ist. Geht dieses auf dem Weg durch das Netzwerk verloren, wird es nicht nochmals übertragen.

Aufbau der Adresse:

Die IP-Adresse hat genau zwei Bestandteile: Sie enthält Informationen über das Netzwerk, und dient der Identifizierung des Rechners im Netzwerk. Hierfür verwendet es 4-Byte lange IP-Adressen, welche dezimal notiert und zwischen den Bytes mit Punkten getrennt sind, wie zum Beispiel 129.163.82.207.

Die folgende Tabelle gibt Aufschluss über die Bedeutung dieser Zahlen, welche allgemein in sogenannte Klassen gegliedert sind:

Erste Zahl	Klasse	Erläuterung
0-127	A	Die erste Zahl identifiziert das Netzwerk
128-191	B	Die letzten zwei Zahlen identifizieren den Rechner
192-223	C	Die letzte Zahl identifiziert den Rechner
224-239	D	Reserviert für Multicast
240-255	E	Reserviert für Erweiterungen

Abb. 2.3: Übersicht über IP-Adressen und Netzwerkklassen ([11], S. 427)

Somit würde es sich bei der obigen Adresse um den Rechner 82.207 im Netzwerk 129.163 handeln.

Die Klassen geben in weiterer Folge auch Aufschluss über die Größe des Netzwerkes. So kann ein Netzwerk der Klasse A maximal etwas mehr als 16 Millionen Rechner beinhalten (3 Bytes: 255 x 255 x 255), Klasse B etwa 65000 (2 Bytes: 255 x 255) und Klasse C genau 255. [11]

Klasse D und E dürfen grundsätzlich nicht verwendet werden, da diese für besondere Zwecke reserviert sind.

IPv4 / IPv6:

Seit seiner Einführung 1981 stellt das IP-Protokoll der Version 4 (IPv4) den Standard im Bereich des Internets dar. Jedoch weist dieses Protokoll Mängel auf, da es zum einen über einen (aus heutiger Sicht) zu kleinen Adressraum verfügt, zum anderen ist die Mobilitäts-Unterstützung unzureichend. Aus diesem Grund wurde im Jahre 1995 das IP-Protokoll der Version 6 (IPv6) eingeführt, welches sich jedoch bis heute nicht durchgesetzt hat, da die Schwächen von IPv4 relativ zufriedenstellend ausgeglichen worden sind. Da jedoch aufgrund des begrenzten Adressraums von IPv4 in den nächsten Jahren keine neuen Adressen mehr zur Verfügung stehen, wird eine Umstellung auf IPv6 nicht zu vermeiden sein. [4]

Vorerst ist jedoch nur Version 4 relevant.

Erstellen privater IP-Adressen:

Natürlich gibt es auch Adressen, welche zur lokalen Nutzung außerhalb des Internets gedacht sind. Diese können innerhalb eines lokalen Netzwerkes beliebig vergeben werden. Die nachfolgende Tabelle veranschaulicht den zur Verfügung stehenden Adressbereich:

Adressbereich	Netzmaske	CIDR-Schreibweise
10.0.0.0 – 10.255.255.255	255.0.0.0	10.0.0.0/8
172.16.0.0 - 172.31.255.255	255.240.0.0	172.16.0.0/12
192.168.0.0 - 192.168.255.255	255.255.0.0	192.168.0.0/16

Abb. 2.4: Private IP-Adressen nach [RFC 1918] ([UNI])

Die Kommunikation eines Rechners mit einer privaten IP-Adresse ist nicht direkt möglich, da diese Adressen nicht im Internet auftreten dürfen (global gesehen nicht eindeutig aufgrund der mehrfachen Benutzung). Grundsätzlich werden Daten, die an private Adressen gesendet werden, nicht in andere Netzwerke weitergeleitet. [4][11]

Routing unter IP:

Unter „Routing“ versteht man die Vorgehensweise, wie Daten in Netzwerken weitergeleitet werden. Somit wird bestimmt, ob Daten z.B. ins Internet geleitet werden, oder für einen anderen, ebenfalls ans lokale Netz angeschlossenen Rechner bestimmt sind. Geräte, die diese Funktion erfüllen, werden als *Router* bezeichnet, stellen also sozusagen „Zwischenstationen“ dar. Mittels sogenannter *Routingtabellen* wird entschieden, wer die Daten erhält. [11]

Subnetze

Bei Verwendung größerer Netzwerke ist oft eine weitere Unterteilung in Subnetzwerke notwendig, da z.B. eine Firma an zwei Standorten angesiedelt ist. Mit Hilfe von Teilnetzmasken ist dies realisierbar. Die so entstandenen Teilnetzwerke sind von außerhalb nicht erkennbar, sie erwecken den Anschein eines einzelnen Netzwerkes. [11]

Teilnetzmaske

Wird das Netzwerk als Ganzes verwendet, also nicht zerteilt, verwendet man (für die jeweilige Klasse) die entsprechende Maske.

Klasse	Maske
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Abb. 2.5: Teilnetzmasken ohne Unterteilung eines Netzwerkes ([11], S. 431)

Um ein Netzwerk zu unterteilen sind lediglich folgende Teilnetzmasken möglich:

Zahl	Definierte Teilnetze
128	2
192	4
224	8
240	16
248	32
252	64
254	128

Abb. 2.6: Zulässige Zahlen in der Teilnetzmaske und deren Bedeutung ([11], S. 431)

Möchte man zum Beispiel das Netzwerk der Klasse C in 2 Teilnetze unterteilen, so verwendet man die Teilnetzmaske: 255.255.255.128.

Für einen Rechner, dessen IP-Adresse 198.100.13.14 betragen würde, wären alle Rechner von 198.100.13.1 bis 198.100.13.128 in seinem Subnetzwerk ansprechbar. Andere Rechner müssen über den Router geleitet werden.

Eine Zweiteilung eines B-Klasse Netzwerkes würde mit einer Teilnetzmaske der Form 255.255.128.0 geschehen. [11]

Default-Gateway:

Wird in der Routingtabelle kein passender Eintrag gefunden, werden die Daten an das Default-Gateway gesendet. Dieses dient als Zwischenstation, die alle Netzwerke miteinander verbindet, und ist somit als Router mit mehreren Interfaces zu verstehen. [4]

Broadcast Adresse:

Wird die IP-Adresse mit einem Host-Teil von 255 festgelegt, also z.B. 192.164.0.255, dann wird die Adresse als sogenannte „Broadcast Adresse“ gehandhabt. Gesendete Daten werden somit an alle Rechner im gleichen Netzwerk versendet und müssen auch entgegengenommen werden. Je nach Inhalt wird entschieden, was mit den Daten geschieht. [11]

Automatische Konfiguration der IP-Adresse:

Erreicht ein Netzwerk eine bestimmte Größenordnung, kann eine selbstständige Konfiguration sehr umständlich und zeitintensiv werden. Aus diesem Grund wurde das sogenannte „Dynamic Host Configuration Protocol“ (DHCP) entwickelt, welches diese Aufgaben der Netzwerkadministration übernimmt.

Während seines Startvorganges sendet ein unter DHCP konfigurierter Rechner einen Rundruf (Broadcast) in das Netzwerk. Erreicht dieser einen DHCP-Server, antwortet dieser und sendet dem anfragenden Rechner eine entsprechende Netzwerkadresse bzw. Konfiguration zu, welche eine freie IP-Adresse, die IP-Adresse des Routers sowie eine Teilnetzmaske beinhaltet. Teilnetzmaske und Router-IP-Adresse können somit nicht verändert werden. [11]

2.1.3 Die Transportschicht: TCP / UDP

„Transmission Control Protocol“ (TCP)

Das „Transmission Control Protocol“ ermöglicht einen zuverlässigen, verbindungsorientierten Transport von Daten. Als Netzwerk-Protokoll kommt IP zum Einsatz. Die übertragen Dateneinheiten werden als „Segmente“ bezeichnet. Über IP besteht die Möglichkeit, dass diese Segmente beim Transport vermischt werden oder gar verloren gehen. In diesem Fall sortiert TCP die Pakete, detektiert den Übertragungsfehler und sendet fehlende Daten erneut. Hat der Empfänger nach einer gewissen Zeit den Erhalt der korrekt übermittelten Daten nicht bestätigt, schickt der Sender die Daten erneut. Weiters wird einer Überlastung des Empfängers im Vorfeld entgegengewirkt. [4]

„User Datagram Protocol“ (UDP):

TCP ist - wie bereits erwähnt - ein sicheres und zuverlässiges Protokoll, die Verwendung oben genannter Kontroll-Mechanismen verlängert jedoch die Übertragungszeit. Stellt es für die Applikation kein Problem dar, dass gelegentlich Daten verloren gehen und generell eher wenig Daten transportiert werden, ist besonders für Echtzeitanwendungen das sogenannte „User Datagram Protocol“ (UDP) vorzuziehen.

UDP gilt im Gegensatz zu TCP als verbindungslos und nicht zuverlässig. Das von der Applikation übergebene Datagramm mit der maximalen Länge von 64 kB wird ohne Verzögerung losgeschickt. Geht ein Datagramm infolge der Übertragung verloren, wird es nicht nochmals versendet. [4]

Vergleich TCP/UDP:

Nachfolgende Tabelle veranschaulicht erneut in übersichtlicher Weise die Eigenschaften beider Protokolle und dient dem direkten Vergleich:

Merkmal	TCP	UDP
IP-Protokollnummer	6	17
Verbindung	Verbindungsorientiert. Aufbau einer Verbindung vor der Datenübertragung durch sog. Three-Way-Handshake, Abbau der Verbindung nach Beendigung.	Verbindungslos. UDP-Datagramme können ohne Verbindungsaufbau einfach abgeschickt werden.
Zuverlässigkeit	TCP überträgt verlorengegangene Segmente nochmals und bringt die Daten in die richtige Reihenfolge, bevor sie dem Empfänger übergeben werden. „Was reingeht, kommt auch raus.“	UDP-Datagramme werden bei Verlust durch UDP nicht nochmals übertragen, Datagramme werden nicht in die richtige Reihenfolge gebracht.
Schnittstelle zur Anwendung	Aus Sicht von Sender/Empfänger steht ein Bytestrom zur Verfügung. Sender kann durch den Strom beliebige Datenmengen verschicken, evtl. Segmentierung erfolgt durch das TCP-Protokoll.	Anwendung muss UDP jeweils ein Datagramm zum Senden übergeben. Maximale Kapazität festgelegt durch max. UDP-Datagrammgröße. Aufteilung größerer Datenmengen in mehrere Datagramme muss durch die Anwendung erfolgen.
Sende-/ Empfangsverhalten	Von der Anwendung an TCP übergebene Daten müssen durch das TCP Protokoll beim Sender nicht sofort zum Empfänger geschickt werden. Wenn TCP-Segmente beim Empfänger ankommen, müssen sie nicht sofort an die empfangende Anwendung weitergegeben werden.	UDP sendet übergebenes Datagramm direkt ab und stellt empfangene Datagramme empfängerseitig sofort zur Verfügung.

Abb. 2.7: TCP und UDP im Vergleich ([4], S.124)

Zusammenfassung:

Aus vorheriger Tabelle ist ersichtlich, dass TCP ein sehr zuverlässiges und sicheres Protokoll darstellt. Im Falle eines Verlustes von Datenpaketen während der Verbindung werden diese erneut gesendet, bis der Empfänger mit einem positives Feedback über den Erhalt des Pakets antwortet. Dies erscheint sehr vorteilhaft, jedoch erhöhen die dafür notwendigen Kontrollmechanismen maßgeblich die Übertragungszeit. Da für eine wirkungsvolle Funksteuerung eine möglichst geringe Latenz notwendig ist (z.B. eine Veränderung der Frequenz des Filters eines Equalizers am Steuerungsgerät soll möglichst schnell das entsprechende akustische Ereignis hervorrufen), ist jedoch das UDP – Protokoll vorzuziehen. Es verzichtet auf diese Kontrollmechanismen, sendet und empfängt ohne Umwege, und verkürzt somit die Übertragungszeit erheblich.

2.2 Wireless LAN

Diese Grundlagen der Netzwerktechnik und deren Protokolle gelten sowohl für draht-gebundene Netzwerke (LAN) als auch für drahtlose Netzwerke (WLAN). Im folgenden Kapitel wird nun auf Drahtlosnetzwerke (WLAN) genauer eingegangen. Es werden grundlegende Probleme der Wellenausbreitung (Reflexion, Abschattung, Dämpfung, etc.) erläutert und anschließend werden die verschiedenen WLAN-Standards (802.11 b/g/n) und die beiden Netzwerkformen (Ad-Hoc / Infrastruktur) behandelt.

2.2.1 Wellenausbreitung

WLAN-Systeme arbeiten mit Frequenzen im Bereich von 2,4 GHz bzw. 5,5 GHz. Dies ergibt Wellenlängen im Bereich von ca. 12cm bzw. 5,5cm. Da diese Wellenlängen meist relativ klein gegenüber der Größe von Hindernissen sind, werden diese Wellen kaum um Hindernisse gebeugt, sondern Abschattung und vor allem Reflexion treten in Erscheinung.

Da die verwendeten Antennen meist in alle Richtungen abstrahlen und in realen Räumen die Wellen von den Wänden oft mehrmals reflektiert werden, kommt am Empfänger die Überlagerung aller reflektierten Wellen an. Gegenüber dem direkten Signal weisen jedoch Reflexionen unterschiedliche Phasenlagen und Polarisationen auf. Da am Empfänger so auch destruktive Interferenz auftreten kann, und somit ein zu schwaches Signal ankommt, arbeiten die meisten Geräte mit dem sog. Diversity-Prinzip.

Hier haben die WLAN-Komponenten zwei Antennen eingebaut und ein Umschalter wählt immer diejenige Antenne aus, auf der das beste Empfangssignal ansteht. Durch die internen Antennen kann die Diversity-Funktion allerdings nur zu einem gewissen Grad realisiert werden, da die Antennen räumlich sehr eng zueinander stehen. Ein weit höherer sog. Diversity-Gewinn kann durch externe Antennen erreicht werden, da hier ein größerer Abstand zwischen den beiden Antennen erreicht werden kann [6].

Reichweiten:

Im WLAN-Bereich ist die erzielbare Distanz entscheidend, die zwischen den kommunizierenden Stationen vorhanden sein darf, damit noch eine fehlerfreie Datenübertragung gewährleistet werden kann. Die maximale Reichweite erzielt man bei einer Quasi-Sichtverbindung, die vorliegt, wenn keine Hindernisse zwischen den Verbindungspartnern stehen.

Um die Reichweiten in Abhängigkeit von der Umgebung in etwa abschätzen zu können, hat man bestimmte Richtwerte veröffentlicht, mit denen man die Hindernisse zwischen den Stationen bezüglich ihrer Dämpfung beurteilen kann.

Ein sehr wichtiges Kriterium für die erzielbare Reichweite ist die Art der Umgebung:

Datenrate	**Reichweite in Abhängigkeit von der Umgebung**		
Verbindung	**Flach und offen**	**Halb offen**	**Geschlossen**
11 MBit/s	160 m	50 m	25 m
5,5 MBit/s	270 m	70 m	35 m
2 MBit/s	400 m	90 m	40 m
1 MBit/s	550 m	115 m	50 m

Abb. 2.8: Erzielbare Reichweiten (ohne spezielle Zusatzantenne) ([6], S. 378)

„Flach und offen“ bedeutet, dass kein Hindernis zwischen Sender und Empfänger liegt (z.B. im Freigelände, in großen Hallen, etc.).

„Halb offen“ bedeutet, dass sich Materialien mit geringer oder mittlerer Dämpfung zwischen den beiden Stationen befinden (z.B. in Großraumbüros, in Räumen mit Trennwänden, etc.).

Und als „geschlossen“ werden Umgebungen bezeichnet, in denen Materialien mit hoher Dämpfung zwischen Sender und Empfänger liegen (z.B. Privathaus, Gebäude mit massiven Wänden, etc.) [6].

In nachfolgender Tabelle sind typische Dämpfungseigenschaften angeführt:

Material	Dämpfung	Beispiel
Gips	Gering	Zwischenwände
Holz	Gering	Möbel, Zwischenwände, alte Decken
Glas	Gering	Fensterscheiben
Mauersteine	Mittel	Wände
Wasser	Mittel	Aquarien, feuchte Materialien
Beton	Hoch	Außenwände
Metall	Sehr hoch	Stahlbetonkonstruktionen, Aufzugschächte

Abb. 2.9: Dämpfung verschiedener Materialien ([6], S. 379)

Freiraumdämpfung:

Im Freiraum ist die Dämpfung vor allem von der Entfernung und von der Wellenlänge abhängig.

In folgender Tabelle sind die Werte für die Freiraumdämpfung angegeben:

Distanz	2,4-GHz-Band	5-GHz-Band
1 m	40,2 dB	47,16 dB
10 m	60,2 dB	67,16 dB
100 m	80,2 dB	87,16 dB
200 m	86,22 dB	93,18 dB
400 m	92,24 dB	99,2 dB
1000 m	100,2 dB	107,16 dB

Abb. 2.10: Freiraumdämpfung bei 2,4 GHz und 5 GHz ([6], S. 304)

Aus dieser Tabelle ist ersichtlich, dass sich bei Verdoppelung des Abstandes die Dämpfung um 6 dB erhöht, bei einer Verzehnfachung des Abstandes (d.h. pro Dekade) erhöht sich die Dämpfung um 20 dB [6].

2.2.2 IEEE 802.11 Standard

Im hier vorliegenden Kapitel wird nun genauer auf den WLAN-Standard und dessen verschiedenen Typen und Übertragungsraten eingegangen.

Bedingt durch die Tatsache, dass das Netzwerkprojekt im Jahr 1980 (80) im Monat Februar (2) ins Leben gerufen wurde, wurde als Oberbegriff aller kommenden Netzwerkstandards der Name 802 gewählt. So erhielt beispielsweise der Ethernet-Standard die Bezeichnung 802.3 und der WLAN-Standard die Bezeichnung 802.11. All diese 802-Standards haben gemeinsam, dass sie auf den unteren zwei Schichten des OSI-Referenzmodells angesiedelt sind (siehe Abb. 2.1).

Für die Standardisierung des WLANs griff das IEEE (Institute of Electrical and Electronical Engineers) auf den Ethernet-Standard (802.3) zurück, somit haben diese beiden Standards große Ähnlichkeiten (z.B. Zugriffsverfahren, etc.).

Der 802.11-Grundstandard wurde 1997 definiert und mit ihm waren Datenraten von 1 und 2 MBit/s im 2,4-GHz-Frequenzband möglich.

Da man im WLAN-Bereich stetig höhere Datenraten anstrebte, wurde der IEEE-802.11-Grundstandard stetig erweitert bzw. modifiziert. Im Laufe der Jahre entstanden so neue Standards mit immer höheren Datenraten, unterschiedlichen Übertragungsverfahren und verschiedenen Frequenzbändern [6].

Folgende Tabelle zeigt verschiedene Standards der 802.11-Familie, deren erreichbare Datenraten und die verwendeten Frequenzen:

Standard	Datenrate	Nettodatenrate	Frequenzband
IEEE 802.11	1 MBit/s	0,82 MBit/s	2,4 GHz
IEEE 802.11	2 MBit/s	1,59 MBit/s	2,4 GHz
IEEE 802.11b	5,5 MBit/s	3,44 MBit/s	2,4 GHz
IEEE 802.11b	11 MBit/s	5,8 MBit/s	2,4 GHz
IEEE 802.11b/g	54 MBit/s	14,4 MBit/s	2,4 GHz
IEEE 802.11g	54 MBit/s	24,4 MBit/s	2,4 GHz
IEEE 802.11a	54 MBit/s	24,4 MBit/s	5 GHz
IEEE 802.11n	Bis zu 600 MBit/s	Bis zu 320 MBit/s	2,4 oder 5 GHz

Abb. 2.11: WLAN-Standards und deren theoretisch erzielbare Datenraten ([6], S.164 u. 409)

2.2.3 Netzwerkformen: Ad hoc / Infrastruktur

Da nun die Grundlagen der drahtlosen Netzwerke behandelt wurden, ist nun interessant, wie man mehrere Geräte verbinden kann, welche Netzwerkformen es gibt und wo deren Vor- und Nachteile liegen.

Ad-hoc-Netzwerk:

Abb. 2.12: Ad-hoc-Netzwerk (Quelle: [TECH])

Die einfachste Form eines WLANs besteht aus zwei Rechnern, in denen jeweils ein WLAN-Adapter eingebaut ist (z.B. zwei Notebooks oder auch ein Notebook und ein Smartphone). Jeder dieser Rechner bildet eine sog. Zelle, Funkzelle oder Basic Service Set (BSS). Jede Zelle definiert sich durch den von einer Station ausgeleuchteten Bereich. Solange sich die Computer in derselben Zelle aufhalten, können sie miteinander kommunizieren. Voraussetzung dafür ist, dass die Stationen innerhalb einer bestimmten Reichweite zueinander stehen und auf demselben Kanal arbeiten.

Da so ein Netzwerk keiner Planung bedarf und schnell umgesetzt werden kann, wird es laut IEEE-802.11-Standard auch als Ad-hoc-Netzwerk bezeichnet.

Das Ad-hoc-Netzwerk ist die erste Betriebsform, die im WLAN auftreten kann. Möchte man einen direkten Datenaustausch zwischen zwei oder mehreren Stationen ermöglichen, so muss man auf den WLAN-Stationen den Betriebsmodus „Ad-hoc-Modus“ auswählen. Die Reichweite eines Ad-hoc-Netzwerkes ist innerhalb von Gebäuden auf zirka 30 bis 50m und außerhalb von Gebäuden auf etwa 300m begrenzt [6].

Infrastruktur-Netzwerk:

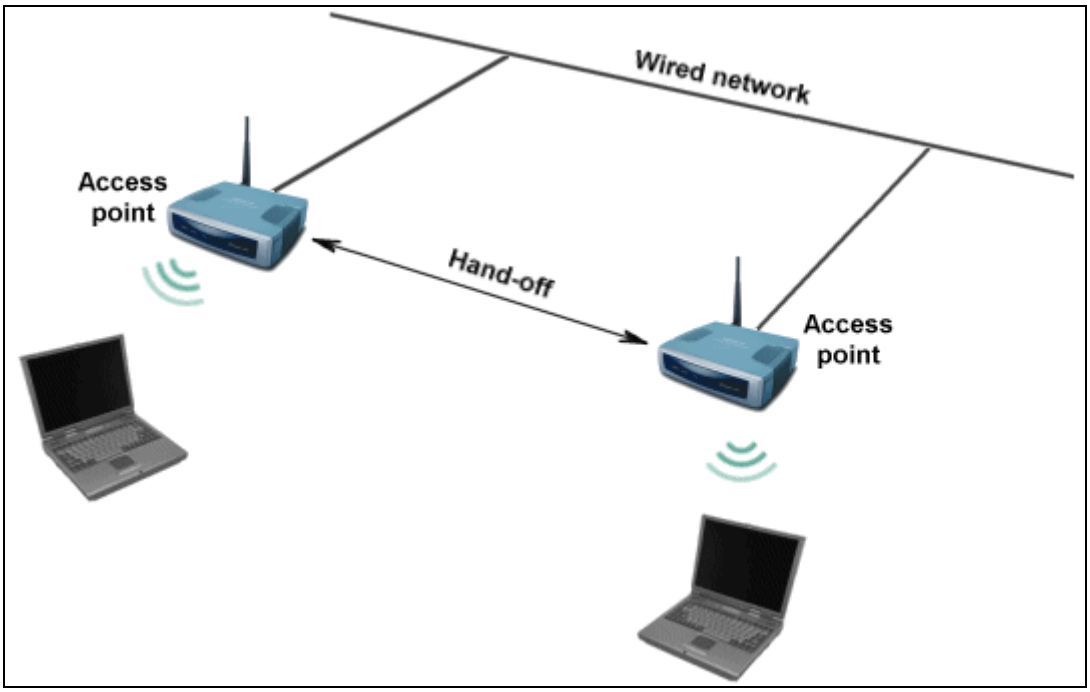

Abb. 2.13: Infrastruktur-Netzwerk (Quelle: [TECH])

Für viele Netzwerke ist es notwendig, eine größere Reichweite zu erzielen. Dazu können über ein Verteilungssystem, das auch als „Distribution System (DS)“ bezeichnet wird, mehrere Zellen miteinander verbunden werden, um eine größere Fläche abzudecken.

Für die Bildung eines Distribution Systems kann entweder ein drahtloses oder ein drahtgebundenes (z.B. Ethernet) Übertragungsmedium zum Einsatz kommen.

Um jetzt einen größeren Bereich (z.B. ein Firmengebäude) abzudecken wird meist auf die vorhandene Netzwerkinfrastruktur zurückgegriffen, um einzelne Wireless Access Points zu verbinden.

Ein Wireless Access Point (kurz: AP) ist eine spezielle Form einer Wireless-Station, die einen Zugang zu einem Distribution System bietet. Müssen Daten von der Wireless-Seite auf die Seite des Distribution Systems übertragen werden, so leitet sie der Access Point weiter. Er erfüllt somit die Aufgabe einer sog. Bridge, die zwei Netzwerke verbindet.

Mit Hilfe eines Access Points lässt sich nicht nur die Ausdehnung eines Funknetzes erhöhen, sondern auch der Übergang zu einem bestehenden drahtgebundenen LAN bewerkstelligen. Dadurch können Ressourcen des LANs, wie z.B. Datenbankserver, Print-Server oder Internetzugang für die Stationen eines WLANs bereitgestellt werden.

Eine Gruppierung aus Verteilungssystem und Access Point wird laut IEEE 802.11 als Infrastruktur-Netzwerk bezeichnet.

Der Infrastruktur-Netzwerkmodus ist die zweite Betriebsform, mit der man innerhalb eines WLANs konfrontiert werden kann. Soll ein Datenaustausch innerhalb eines Infrastruktur-Netzwerks realisiert werden, muss auf den WLAN-Stationen der Infrastruktur-Modus ausgewählt werden. Innerhalb eines solchen Netzwerks wird es den Stationen auch ermöglicht, zwischen verschiedenen Funkzellen zu wandern, ohne dass der laufende Verbindungsaustausch abbricht. Dieser automatische Funkzellenwechsel wird als „Roaming“ bezeichnet [6].

Da nun bekannt ist, wie die drahtlose Übertragung funktioniert, stellt sich nun die Frage was übertragen werden soll. Im folgenden Kapitel 2.3 werden nun die in Frage kommenden Steuerungsmedien (VNC, OSC, MIDI) behandelt und deren Vor- und Nachteile erläutert.

2.3 Steuerungsmedien

2.3.1 Virtual Network Computing (VNC)

Virtual Network Computing ist eine Remote Control Software, die es erlaubt, von einem Rechner (dem „VNC-Client" oder „Viewer") auf einen anderen Rechner (den „VNC-Server") über das Internet zuzugreifen. Hierzu wird der Bildschirminhalt vom Server auf den Client übertragen und der Client sendet Tastatur- und Mausbefehle zurück. Somit entsteht der Eindruck als säße man direkt am Server. Diese Technik ist komplett unabhängig von den jeweiligen Plattformen, d.h. auf Client und Server darf durchaus ein anderes Betriebssystem laufen. Es gibt sogar Java Viewer, bei dem man direkt aus einem (Java-fähigen) Browser auf einen VNC-Server zugreifen kann, ohne ein Client-Programm installieren zu müssen [7].

Jede Implementierung von VNC basiert auf dem sog. Remote Framebuffer Protocol (RFB) [8].

Remote Framebuffer Protocol (RFB):

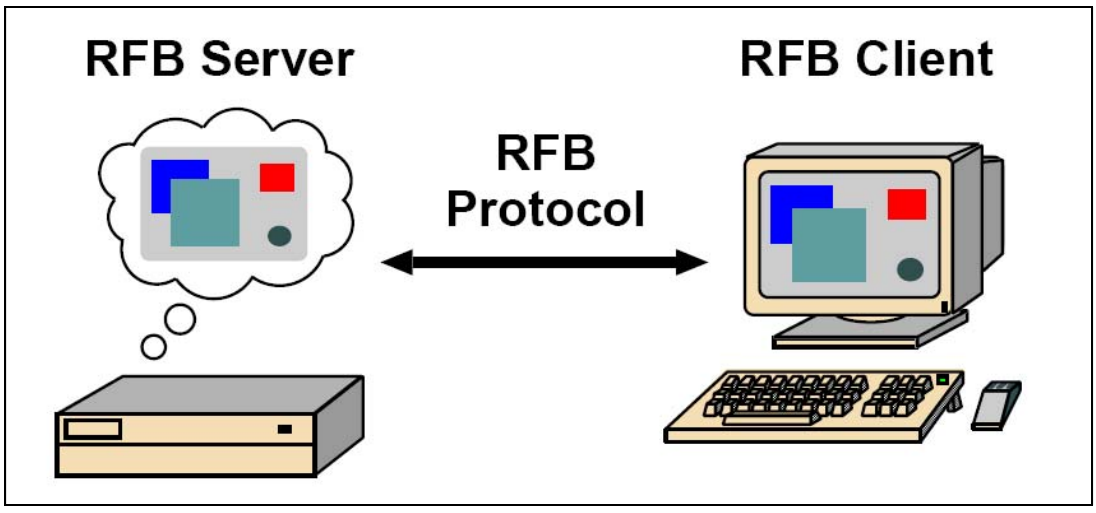

Abb. 2.14: Struktur einer Kommunikation über das RFB Protokoll [8]

RFB ist ein einfaches Protokoll das verwendet wird, um Bildschirminhalte eines sog. RFB-Servers auf einen RFB-Client zu übertragen und Ereignisse wie Tastatureingaben, Mausbewegungen und Mausklicks des Clients zum Server zu senden. Das RFB Protokoll ist netzwerkfähig und wird über TCP (Transmission Control Protocol) übertragen.

Da es auf der Ebene des Grafikspeichers („framebuffer“) arbeitet, werden alle Fenstersysteme wie Unix, Windows oder Macintosh unterstützt. Diese Plattformunabhängigkeit erlaubt es, dass z.B. von einem Windows-Client auf einen Macintosh-Server zugegriffen wird.

Das RFB Protokoll ist ein sog. „Thin Client“ Protokoll, d.h. es wurde so entwickelt, dass an den Client nur minimale Anforderungen gestellt werden. RFB macht den Client zustandslos, d.h. wenn die Verbindung unterbrochen wird, oder sich ein anderer Client mit dem Server verbindet, wird immer der aktuelle Zustand des Servers angezeigt. Somit ist egal von welchem Punkt der Erde aus man sich mit dem Server verbindet, es wird immer das Graphical User Interface (GUI) des Servers angezeigt und man hat immer den Eindruck direkt am Server zu arbeiten [8].

Der Bildschirminhalt wird auf eine einfache Weise übertragen. Die Vorschrift hierfür lautet: „Nimm ein Rechteck von Pixeldaten und schreibe es auf Position x,y“. Dies macht es möglich, nur Bildschirmänderungen in einem bestimmten Bereich des Bildes übertragen zu müssen, und nicht die Verbindung mit einem durchgehenden Stream von ganzen Bildschirminhalten auszulasten. Außerdem kann die Qualität der Anzeige vom Client eingestellt werden. So kann zum Beispiel die Farbtiefe in 24-bit, 16-bit oder 8-bit gewählt werden. Dies kann bei einer langsamen Verbindung oder einem „langsamen Client“ Ressourcen sparen.

Bei der Initialisierung der Verbindung einigen sich Client und Server auf die verwendete Protokollversion (hierbei wird die neueste Version genommen, die BEIDE unterstützen) und auf die Sicherheitseinstellungen (z.B. Passwortschutz bei VNC-Verbindungen). Auch die Kodierung und das Format der Pixeldaten wird festgelegt [8].

Die Eingabe-Seite dieses Protokolls basiert auf einem Standard-Arbeitsplatz mit einer Tastatur und einem Zeigegerät (z.B. Maus, Trackball, Touchpad, Touchscreen). Vom Client werden also einfach nur Eingabeereignisse wie Tastatureingaben, Mausklicks und -bewegungen an den Server gesendet [8].

Hier sei noch zu erwähnen dass das RFB-Protokoll unverschlüsselt übertragen wird. Das heißt, dass auch die Tastatureingaben unverschlüsselt gesendet werden, was bei sensiblen Daten wie Passwörtern die Gefahr der Ausspähung birgt.

Um dieses Sicherheitsproblem zu lösen ist es oft ratsam zwischen Client und Server eine VPN-Verbindung aufzubauen und die Daten zu verschlüsseln.

2.3.2 Open Sound Control (OSC)

Eine weitere vielseitig einsetzbare Steuerungsmöglichkeit bietet das Protokoll „Open Sound Control“.

OSC ist ein nachrichtenbasiertes Protokoll, das für die Kommunikation zwischen Computern, Sound-Synthesizern und anderen Multimedia-Geräten entwickelt wurde. Es ist unabhängig von der verwendeten Plattform und auch unabhängig vom Transportprotokoll. Jedoch wird meist UDP (User Datagram Protocol) oder TCP (Transmission Control Protocol) verwendet [12], [13]. OSC ist durch seine implementierten Datentypen sehr flexibel einsetzbar und bietet eine hohe numerische Auflösung. Die unlimitierte hierarchische Adressstrukur und eine spezielle „Pattern-Matching“-Syntax machen es möglich einer Nachricht mehrere Empfänger zuzuordnen. Die Verwendung von präzisen Zeitstempeln und die Möglichkeit, Nachrichten zu gruppieren, erlauben es, diese Gruppe von Befehlen an den Empfängern gleichzeitig auszuführen. Außerdem gibt es eine spezielle Syntax, um Informationen vom Empfänger abzufragen, wie z.B. den Adressraum, den aktuellen Wert eines Parameters oder die Dokumentation zu einem bestimmten Objekt [13].

OSC wird eingesetzt um Steuersignale von Hardware (z.B. Keyboards, gestengesteuerte Eingabegeräte, JazzMutant Lemur, etc.) oder Software (z.B. Pure Data, Max/MSP, TouchOSC, Logic Pro, Traktor, etc.) zu einem Empfänger (Hard- oder Software) zu übertragen.

Datentypen:

Mit OSC können diese fundamentalen Datentypen übertragen werden:

Int32: 32-bit Integerzahl (vorzeichenbehaftet)

Float32: 32-bit Gleitkommazahl nach IEEE 754

OSC-timetag: 64-bit Zeitstempel. Die ersten 32bit sind dabei die Sekunden seit dem 1.1.1900, die zweiten 32bit definieren die Sekundenbruchteile. Dies entspricht dem Network Time Protocol (NTP) und macht eine Zeitauflösung von ungefähr 0,23 Nanosekunden möglich.

OSC-string: Eine ASCII-Zeichenkette, an die bei Bedarf Nullen angehängt werden um die 32bit-Blockgröße zu erreichen.

OSC-Blob: „Blob“ steht für „Binary Large Object“ und besteht aus einer 32bit Integerzahl, die die Anzahl der Bytes angibt, anschließend kommen die zu übertragenden Bytes und bei Bedarf werden auch hier wieder Nullen angehängt um die vorgegebene Blockgröße von 32bit zu erfüllen [12].

Übertragung

Das Open Sound Control Protokoll ist transportunabhängig, d.h. OSC kann über eine Vielzahl von Verbindungsarten übertragen werden (z.B. USB, IEEE-1394 „Firewire“, PCI, Ethernet, Fast Ethernet, etc.) [13].

Die Übertragungsrate beträgt bei OSC mehr als 10 Mbit/s (zum Vergleich: MIDI überträgt mit 31,25 kbit/s, also ungefähr um den Faktor 300 langsamer).

Die kleinste Einheit, die übertragen wird, nennt man ein OSC-Paket. Dieses besteht aus einem Byte, das seine Länge beschreibt und den zu übertragenen Daten. Die Größe eines OSC-Pakets ist immer ein Vielfaches von 4Byte. Wie schon bei den Datentypen erwähnt beträgt die Blockgröße somit immer 32bit.

Eine sog. OSC-Message besteht aus der Adresse des Parameters der geändert werden soll (als ASCII-Zeichenkette), danach kommen die Anzahl und die Art der Parameter wiederum als Zeichenkette, und schließlich der Wert des Parameters [12], [13].

Mehrere OSC-Messages können zusammengefasst und als sog. OSC-Bundle übertragen werden. Bei einem OSC-Bundle wird ein Timestamp mitgesendet, der definiert, wann der Befehl ausgeführt werden soll. Somit können alle OSC-Messages die im gleichen Bundle sind beim Empfänger gleichzeitig abgearbeitet werden (z.B. mehrere Töne eines Akkordes werden gleichzeitig angespielt).

Weiters können sogar mehrere OSC-Bundles in größere OSC-Bundles zusammengefasst werden [12].

Die folgende Abbildung zeigt wie OSC-Messages in OSC-Bundles zusammengefasst werden:

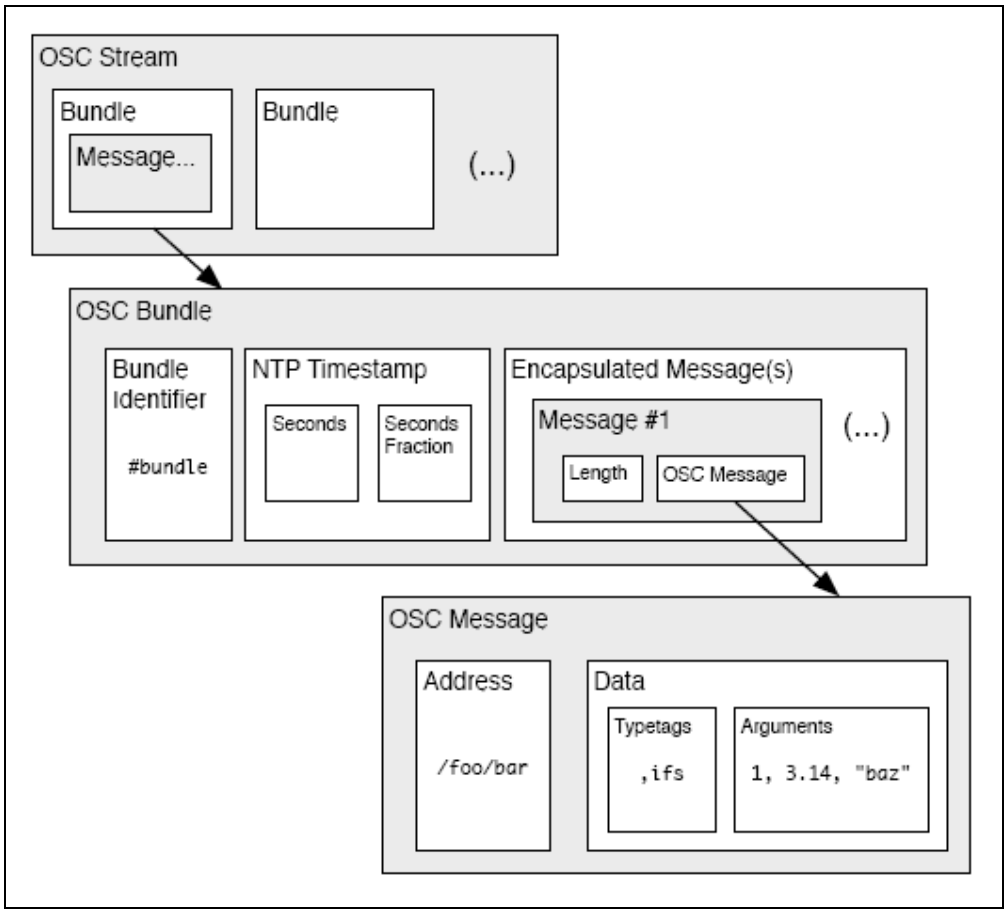

Abb. 2.15: Struktur vom OSC-Format [9]

Adressierung

Die Adressierung in OSC erfolgt innerhalb einer hierarchischen Objektstruktur. Sie ist nicht limitiert, d.h. man hat keinen definierten Adressraum sondern kann individuelle Adressen vergeben in einer Schreibweise ähnlich URLs (z.B.: "/resonators/3/frequency").

In diesem Beispiel würde man also auf die Frequenz des Resonators 3 zugreifen. Diese Baumstruktur von Gruppen und Objekten erlaubt auch die Adressierung von ein oder mehreren Objekten. Außerdem können mithilfe vom sog. „Pattern Matching“ mehrere Adressen den gleichen Befehl empfangen. Dazu braucht man nur eine OSC-Message mit einer speziellen Syntax zu adressieren, die dann vom Empfänger auf die jeweiligen Objekte aufgeteilt wird [12], [13].

Zusatzfunktionen für den Programmierer:

Durch spezielle OSC-Messages kann man bestimmte Informationen vom Empfänger anfordern. Zum Beispiel kann der Adressraum abgefragt werden, indem man einer Adresse einen abschließenden Schrägstrich hinzufügt. Als Antwort erhält man dann eine Liste von Adressen in diesem Verzeichnis. Außerdem kann man mit der reservierten Adresse „/current-value“ aktuelle Parameterwerte abfragen und mit „/documentation“ erhält man eine Zeichenkette mit der Dokumentation des Objektes oder der Funktion, oder ggf. einen Internetlink dazu [13].

Vorteile / Nachteile

Die größten Vorteile von Open Sound Control sind:

+ flexible Adressierung,

+ hohe Auflösung dank seiner Datentypen,

+ präziser Timestamp,

+ Netzwerkfähigkeit,

+ hohe Datenrate,

+ Pattern Matching um eine Nachricht an mehrere Empfänger zu senden,

+ ASCII-Zeichenketten können übertragen werden,

+ sogar beliebig große Bitfolgen (z.B. Audio/Videos) können übertragen werden.

Nachteile:

- Bei OSC gibt es keine einheitliche Adressierung, somit kann jeder Hersteller andere Adressnamen vergeben, was zu Inkompatibilitäten führen kann.

2.3.3 Musical Instrument Digital Interface (MIDI)

Eine nach wie vor sehr beliebte Steuerungsart bietet MIDI. Im Vergleich zu OSC (siehe Kap. 2.3.2) ist MIDI zwar langsamer und ungenauer, aufgrund seiner Standardisierung jedoch noch weit verbreitet. Deshalb wird im hier vorliegenden Kapitel genauer auf MIDI und dessen Vor- und Nachteile eingegangen.

Musical Instrument Digital Interface (kurz: MIDI) ist ein Protokoll zur Kommunikation zwischen Synthesizern, Samplern, Rhythmusmaschinen, Bandmaschinen, Computern, Mischpulten, etc. Es wurde 1983 vorgestellt und gilt als eine der erfolgreichsten Innovationen in der Geschichte der Musikelektronik. Es ist ein Protokoll mit dem Steuerungsdaten von einem MIDI-Gerät (z.B. einem MIDI-Keyboard) zu einem anderen MIDI-Gerät (z.B. einem Klangerzeuger) übertragen werden. Bei einem Tastendruck werden also keine Audioinformationen übertragen, sondern nur Informationen wie Tonhöhe, Anschlagstärke, usw. Der eigentliche Ton wird dann erst beim Empfänger erzeugt.

Neben der einfachen Übertragung von Tasteninformationen bietet die MIDI-Norm umfangreiche Möglichkeiten zusätzliche Steuerdaten wie z.B. Klangfarbenänderungen (mit sog. Program-Changes) oder z.B. Pedalstellungen (mit sog. Controller-Daten oder Control Changes) zu senden. Diese sog. Control Changes (kurz: CC) werden auch teilweise benutzt um z.B. Kanal-Fader bei Digitalmischpulten zu steuern (z.B. mit der Software „Osculator“, siehe Kap. 5.3.2).

Besonders wichtig für die Kommunikation zwischen Digitalmischpulten und einem Rechner sind aber vor allem die sog. Systemexclusiven Meldungen (kurz SysEx). Da diese SysEx-Messages die höchste Flexibilität aufweisen und Daten herstellerspezifisch auf ein bestimmtes Gerät übertragen werden können, basieren auch viele Mischpultfernsteuerungssysteme (z.B. Yamaha Studio Manager) auf diesen Nachrichten.

Obwohl MIDI schon 1983 entwickelt wurde, und es technisch eigentlich schon überholt sein sollte (z.B. bei der Datenrate), ist es nach wie vor einer der wichtigsten Standards. Die MIDI-Autoren entwickelten eine äußerst flexible Sprache, die besonders an eine kontinuierliche Weiterentwicklung angepasst war. Wenn wir einen Vergleich mit unserem eigenen Sprachvokabular herstellen, können wir sagen, dass es jederzeit möglich ist, das MIDI-Wörterbuch um neue Ausdrücke zu erweitern. Dies ermöglichte die Erweiterungen der Norm Zug um Zug, den Bedürfnissen entsprechend, wobei eine ausbaufähige Kompatibilität beibehalten wurde [1].

Aufbau einer MIDI-Message:

Die MIDI-Norm unterteilt Informationen (Bytes) in zwei Kategorien: Status-Bytes und Daten-Bytes. Im Allgemeinen ist es die Aufgabe des Status, die vom Musiker ausgeführte Handlung anzuzeigen (z.B. das Anschlagen oder Loslassen einer Taste oder eines Sustain-Pedals, das Verändern eines Pitch Bend- oder Modulationsrades, etc.). Dennoch erfordert diese Handlung in den meisten Fällen zusätzliche Präzisierungen (z.B. Nummer und Anschlagdynamik der angeschlagenen Taste, etc.). Die Daten-Bytes, die den Status ergänzen, übernehmen diese Aufgabe. Alle MIDI-Informationen beruhen ausnahmslos auf einer Struktur des Typs „Status + Daten“, die unter dem Oberbegriff Befehl (Message)

zusammengefasst sind. Die Anzahl der in einem Befehl enthaltenen Daten richtet sich nach der Funktion des Statustyps (von 0 bis n).

Um ein Status-Byte von einem Daten-Byte zu unterscheiden, benutzt die MIDI-Norm das Most Significant Bit (MSB). Je nachdem ob dieses Bit 0 oder 1 ist, wird das Byte als Status-Byte (1xxxxxxx) oder Daten-Byte (0xxxxxxx) eingestuft [1]. (siehe Abb. 2.16)

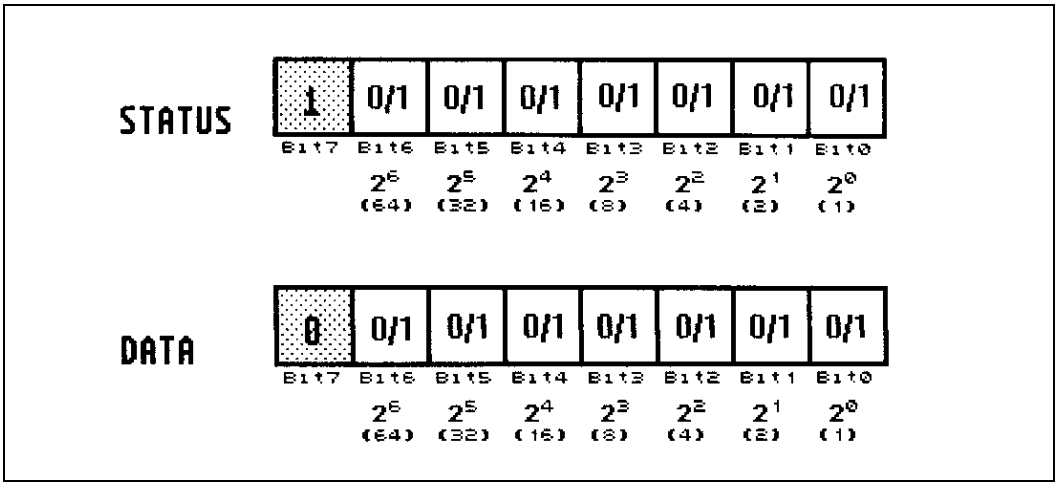

Abb. 2.16: Unterscheidung der Bytes in Status-Bytes und Daten-Bytes [1]

Folglich bleiben der MIDI-Sprache nur 7 freie Bits um eine Information darzustellen. Dies entspricht 128 verschiedenen Werten. Bezüglich der Daten kann diese Beschränkung auf 128 Werte leicht umgangen werden, indem mehrere dieser Daten demselben Status-Byte zugeordnet werden. Demgegenüber ist die Anzahl der Status-Bytes auf 128 beschränkt. Dies ist jedoch mehr, als man für die Verschlüsselung musikalischer Handlungen benötigt.

Kurz gesagt wird jeder MIDI-Befehl aus einem Status-Byte unter 128 möglichen Werten gebildet und ist dazu bestimmt, eine Ordnung oder eine Handlung darzustellen (1xxxxxxx), gefolgt von 0 bis n Daten-Bytes (0xxxxxxx), die den Inhalt dieser Handlung präzisieren [1].

Der MIDI-Kanal:

Jeder Befehl der in einem MIDI-Netz ein Ausgabegerät verlässt, durchläuft das gesamte MIDI-Netz. Damit jetzt nicht z.B. bei einem Tastendruck jeder Tongenerator diese Note spielt, wurde ein logischer Adressraum geschaffen. Um beispielsweise nur auf dem Tongenerator 1 diese Note zu spielen, stellt man die Tastatur und den Tongenerator auf dieselbe Adresse. Alle übrigen Geräte mit einer anderen Adresse, empfangen zwar diese Nachricht, ignorieren aber alle Befehle die nicht für sie bestimmt sind. Dieser Zuordnungsbefehl ist in das Status-Byte integriert und nennt sich MIDI-Channel (MIDI-Kanal) [1]. (Siehe Abb. 2.18)

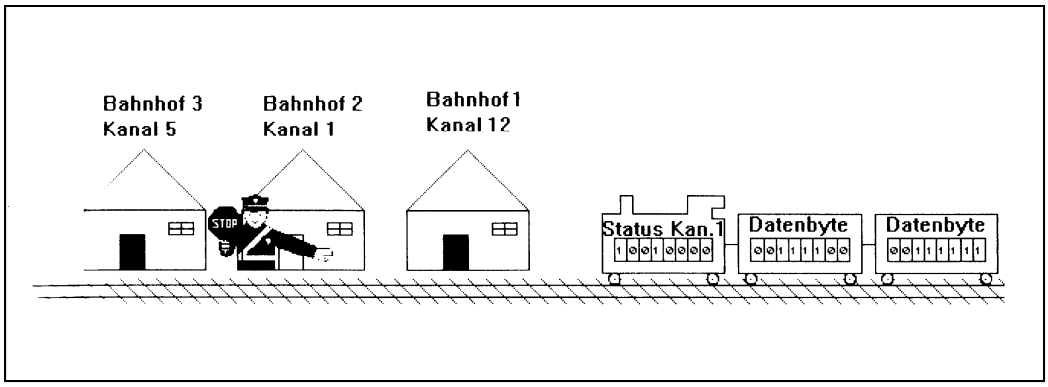

Abb. 2.17: Beispiel eines MIDI-Befehls an Kanal 1 in einer Kettenverbindung [1]

In Abb. 2.17 wird diese Adressierung noch mal verdeutlicht. Während der MIDI-Befehl (hier ein Zug bestehend aus Status- und 2 Datenbytes) auf der Strecke jedes Gerät (hier jeden Bahnhof) passieren muss, hält dieser Zug aber nur an den Bahnhöfen, wo der Empfangs-Kanal mit dem Kanal des Befehls übereinstimmt.

Das bedeutet, damit ein Dialog zwischen zwei MIDI-Instrumenten stattfinden kann, ist es unerlässlich das Ausgabeinstrument und das Empfangsinstrument über eine identische Kanalnummer zu regeln. Da die Bits 0 bis 3 des Statusbytes die Kanalnummer bilden, sind insgesamt 16 verschiedene Kanäle adressierbar.

(Achtung: im Binärcode werden die Kanäle 1 bis 16 von 0 bis 15 durchnummeriert) [1].

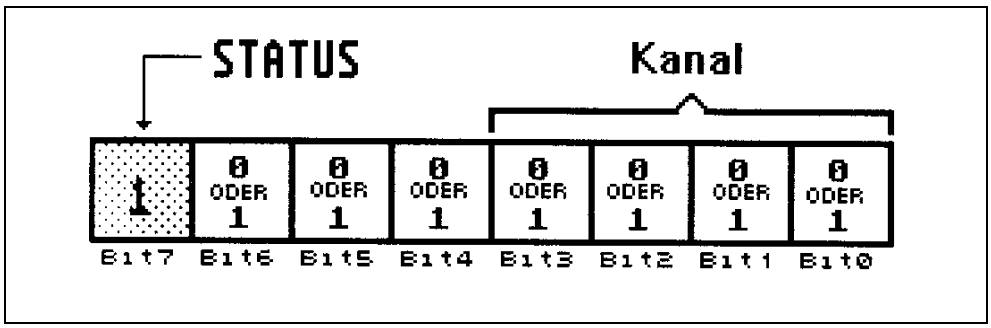

Abb. 2.18: Aufbau eines Statusbytes. Die Bits 0 bis 3 stellen die Kanalnummer dar [1].

Arten von MIDI-Messages:

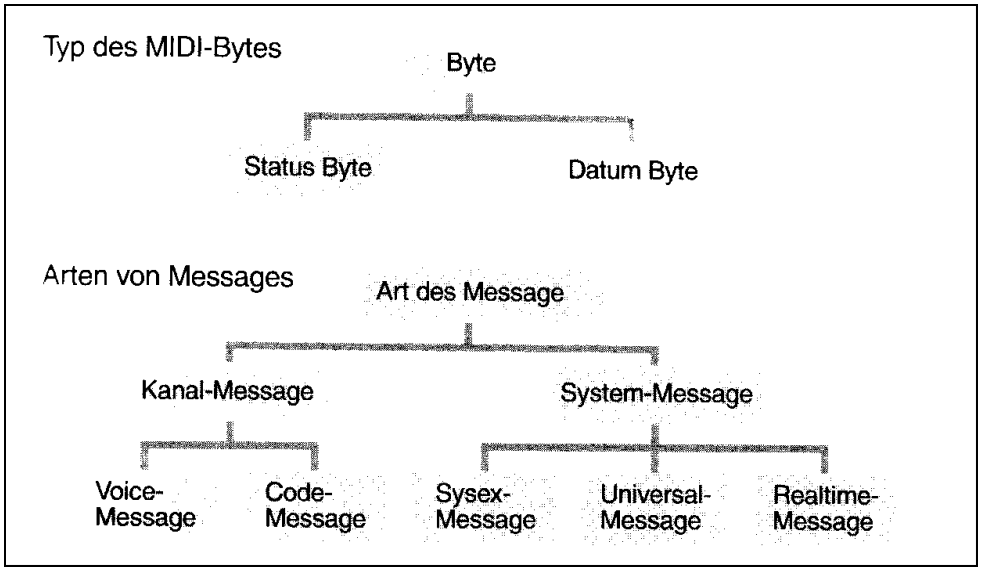

Abb. 2.19: Verschiedene Typen von MIDI-Bytes und MIDI-Messages [1]

Die Kanal-Messages:

Die sog. Kanal-Messages, die an einen der 16 Kanäle adressiert sind, werden durch die Bits 4 bis 6 des Statusbytes weiter spezifiziert (siehe Abb. 2.18). Mit diesen 3 Bits ist es nun möglich die sieben verschiedenen Statustypen, die einer Kanal-Message zugeordnet sind, zu unterscheiden. In aufsteigender numerischer Ordnung finden wir jeweils den Statustyp der losgelassenen Taste (Note Off, 000), der angeschlagenen Taste (Note On, 001), polyphoner Druck (Polyphonic Aftertouch, 010), Kontrollwechsel (Control Change, 011), Programmwechsel (Program Change, 100), Kanaldruck (Channel Aftertouch, 101) und Tonhöhenvariation (Pitch Bend, 110) [1].

Die System-Messages:

Im Gegensatz zu den Kanal-Messages integrieren System-Messages keine Kanal-Kennzeichnung, da sie für das gesamte MIDI-Netz bestimmt sind. Die linke Hälfte des Status-Bytes einer System-Message entspricht immer 1111 (entspricht „F“ in hexadezimaler Darstellung). Die Bits 0 bis 3 des Status-Bytes (welche Kanalinformationen hätten enthalten können), können nun acht Nachrichten in Echtzeit (System Real Time Messages) und zwei herstellerspezifische Befehle (System Exclusive Messages) bilden [1].

System Exclusive Messages:

Die systemexternen Befehle (System Exclusive Messages, kurz: SysEx) sind für Steuerungen und insbesondere Funkvernetzungen wahrscheinlich die wichtigste Art von MIDI-Befehlen. Diese Befehle sind dazu gedacht, Informationen „außerhalb der Norm“ zu übertragen.

Alle bisherigen MIDI-Befehle hatten allgemeine Bedeutung. So ist das Format eines Befehls über eine angeschlagene Taste (Note On) immer das gleiche, ob die Taste nun bei einer Yamaha-, Roland- oder Korgtastatur angeschlagen wird. Dies ist eine normfähige Information, da alle Tastaturen die Aufgabe haben, Noten zu spielen. Auf gleiche Weise akzeptieren es alle Tongeneratoren, auf diese Notenbefehle zu reagieren. Dagegen können zwei dieser Generatoren, die auf unterschiedlichen Syntheseprinzipien beruhen (z.B. Frequenzmodulation bei Yamaha, LA-Synthese bei Roland), auf keinen Fall ihre Tonparameter (ihre Speicher) austauschen. Andererseits: Zwei Yamaha-, Roland-, oder Korg-Synthesizer, die identisch oder ähnlich sind, können sich gegenseitig diese Parameter übermitteln. Und dies funktioniert dank System Exclusive Messages.

Im Allgemeinen haben die SysEx-Messages die Aufgabe, jegliche gerätespezifische Information an ein MIDI-Gerät zu übertragen [1].

Das Format einer System Exclusive Message sieht folgendermaßen aus:

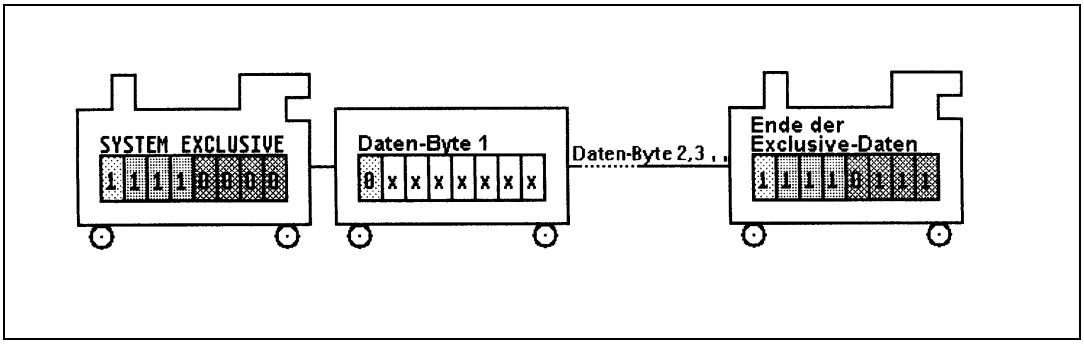

Abb. 2.20: Aufbau einer System Exclusive Message [1]

Eine System Exclusive Message beginnt also immer mit dem Byte 11110000 (entspricht 0xF0), dann kommen beliebig viele Daten-Bytes (wobei deren MSB immer 0 ist) und abgeschlossen wird die Nachricht mit dem Byte 11110111 (entspricht 0xF7). Da beliebig viele Daten-Bytes übertragen werden können ist es am einfachsten, das Ende der Nachricht mit diesem „End Of Exclusive“-Befehl anzuzeigen [1].

Herstellerspezifische Befehle:

Das erste Datenbyte einer System Exclusive Message definiert den Gerätehersteller (z.B. 0x43 für Yamaha). Wie bei jedem Datenbyte ist die Anzahl der möglichen Werte auf 128 begrenzt. Angesichts der wachsenden Anzahl der Firmen, die einen Identifikations-Code zugeteilt haben möchten, wurde entschieden, die Anzahl der Werte zu erhöhen, und sie so auf 16.384 zu bringen und ein System mit variabler Größe zu entwickeln.

Wenn also das erste Datenbyte 0x00 ist, so identifizieren die nächsten 2 Bytes den Gerätehersteller des Empfängers [1].

Dieser Firmen-Code ist eindeutig, wird von der MIDI Manufacturers Association vergeben und ist unter http://www.midi.org/techspecs/manid.php veröffentlicht.

Somit sieht z.B. eine SysEx-Nachricht an ein Yamaha-Gerät folgendermaßen aus:

0xF0	Beginn der SysEx-Message
0x43	Hersteller-ID Yamaha
…	
…	
…	beliebig viele Datenbytes (wobei das MSB jeweils eine 0 sein muss)
0xF7	Ende der SysEx-Message

Übertragung:

Das MIDI-Interface arbeitet gerichtet (ein Kabel pro Übertragungsrichtung), seriell, asynchron und mit einer Geschwindigkeit von 31.250 Bit/s. Es arbeitet nicht spannungsgesteuert, sondern mit einer 5mA-Stromschleife. Um elektrische Störgeräusche zu vermeiden, insbesondere Massenschleifen, ist jeder MIDI-Eingang mit einem Optokoppler ausgestattet. Somit findet eine galvanische Trennung statt [1].

Will man MIDI über ein Computernetzwerk (z.B. LAN oder WLAN) übertragen, wird meist das Real-Time Transport Protocol (RTP) [10] verwendet. Lazzaro und Wawrzynek haben in „RTP Payload Format for MIDI“ [4] ein Format spezifiziert, MIDI über RTP zu übertragen. Dieses Format macht es möglich, sowohl musikalische Interaktionen über das Internet zu übertragen (z.B. für Internet-Jams, etc.), als auch z.B. größere Daten zu versenden (file streams). Es definiert auch Werkzeuge, um Übertragungsfehler zu korrigieren [4].

Zusammenfassung:

Jede der hier behandelten Steuerungsarten (VNC, OSC und MIDI) hat seine Vor- und Nachteile und bietet verschiedene Einsatzmöglichkeiten. Im folgenden Kapitel 3 werden nun Anwendungsbeispiele vorgestellt und deren Stärken bzw. Schwächen behandelt.

3 Anwendungsbeispiele

In Kapitel 1 wurden – schematisch - zu ausgewählten Steuerungsvarianten praxisnahe Anwendungsbeispiele vorgestellt. Hierbei wurde bereits auf die Stärken und Schwächen der verschiedenen Steuerungsvarianten eingegangen, um dem Interessenten bereits im Vorfeld die Entscheidung bei der Wahl der passenden Funksteuerung zu erleichtern.

Bereits vorhandene bzw. für diese Arbeit entwickelte Systeme werden im hier vorliegenden Kapitel 3 vorgestellt. Ziel ist es, einen noch tieferen Einblick in die Möglichkeiten einer Funksteuerung im Beschallungsbereich zu vermitteln, indem entsprechende Systeme recherchiert und evaluiert werden.

3.1 Steuerung raumakustischer Parameter

Hier wird die Einsatzmöglichkeit einer Funksteuerung als „Effektsteuerung“ vorgestellt (siehe Kap. 1.3.). Hierbei wurde über das Akustik System „Constellation“ der Firma „Meyer Sound“ recherchiert, welches zur künstlichen Nachverhallung in einem Konzertsaal des „Hauses für Musik und Musiktheater“ der Kunstuniversität Graz Verwendung findet. Eine ständige Veränderung von raumakustischen Parametern wie z.B. der Nachhallzeit passen den Raum an die jeweilige Szene einer Aufführung an. Dies kann ein außergewöhnliches Erlebnis für den Besucher darstellen.

Kurzüberblick:

Steuerungsbasis:	WI-FI
Verwendungszweck:	Steuerung raumakustischer Parameter
Systemaufbau:	- Akustik-System: „Constellation“ der Firma „Meyer Sound“ - WLAN-Hausnetzwerk - Windows-Rechner mit Steuerungsoberfläche: „Explorer“

Im hier dargestellten Praxisbeispiel handelt es sich um die professionelle Steuerung diverser raumakustischer Parameter eines Akustik-Systems über ein WLAN-Netzwerk während einer Veranstaltung. Darbietungs- bzw. Durchführungsort ist das Haus für Musik und Musiktheater (kurz „MUMUTH“) der Kunstuniversität Graz, unter der Leitung von Dipl. Tonmeister Ulrich Gladisch, seines Zeichens zuständiger Tonmeister.

Abb. 3.1: Haus für Musik und Musiktheater der Kunstuniversität Graz

Details zur Verwendung:

Mit Hilfe des Akustik-Systems „Constellation“ der Firma „Meyer Sound“ ist es möglich, die akustische Wahrnehmung des Raumes manuell festzulegen. Als Ausgangspunkt dient hier die natürliche Nachhallzeit des Raumes, welche für einen Konzertsaal sehr kurz ist. Es besteht die Möglichkeit, die Raumempfindung an das Stück bzw. den jeweiligen (fiktiven) Aufführungsort anzupassen.

Der Grundgedanke dieser Technik war, je nach Stilistik der Darbietung den Raum anpassen zu können. Jedoch lag es auch nahe, diese Technik dynamisch zu verwenden, also einen Wechsel der Raumempfindung *während* des Stückes herbeizuführen. Dies wurde bereits in einigen Theater- und Opernaufführungen umgesetzt, wobei der ausführende Tonmeister anhand der Partitur mit Hilfe eines Laptops und eines WI-FI-Netzwerkes die Akustik inmitten des Publikums steuern konnte. Spielt das Stück z.B. in der einen Szene in einem Wohnzimmer mit relativ „trockener“ Akustik, kann der Raum in der nächsten Szene plötzlich (als Extrembeispiel) in eine Tropfsteinhöhle verwandelt werden.

Hierbei sei anzumerken, dass es zu Zeiten der Entstehung dieser Arbeit nicht möglich war, exakte Werte für die natürliche Nachhallzeit, bzw. die infolge des Systems entstehenden Nachhallzeiten des Raumes anzugeben. Einige Zeit nachdem der Raum von Akustik-Spezialisten eingemessen wurde, wurden bauliche Veränderungen (Entfernung von Absorbermaterial) gemacht, welche den natürlichen Raum und somit auch das Gesamtsystem beeinflussen. Eine Aktualisierung der Parameter wird jedenfalls erwogen.

Abb. 3.2: „György-Ligeti-Saal“ des „MUMUTH“ Graz

Details zum Systemaufbau:

Herz des Systems sind 64 Mitten- / Hochtonlautsprecher und 8 Subwoofer des Akustik-Systems, welche zum Teil dezent in die Wandarchitektur eingearbeitet wurden, zum Teil an der Decke des Raumes positioniert wurden. 24 Mikrofone (Bezeichnung: „DPA 4022 M“) sind im diffusen Schallfeld positioniert, nehmen den Schall auf und wandeln diesen in die elektrische Domäne. Nach erfolgreicher Analog-Digital-Wandlung werden die Daten an die Software weitergegeben, in welcher die digitale Signalverarbeitung geschieht. Anders gesagt ist eine komplizierte Verschaltung bzw. Matrizierung von Mikrofonen und Lautsprechern hierbei implementiert.

Dies erfolgt in zwei unabhängigen Zonen, welche den vorderen und den hinteren Teil des Raumes beinhalten. Eine detailliertere Beschreibung der Verarbeitung an dieser Stelle würde aber eindeutig den Rahmen dieser Arbeit sprengen.

Die Verschaltung ist das Resultat einer mehrere Tage andauernden akustischen Einmessung des Raumes durch ein Team von Akustikern der Firma Meyer Sound.

Im Allgemeinen sind in der Software sechs fixe Presets gespeichert, welcher mit der Software „Explorer“ geladen werden können. Jedoch besteht auch die Möglichkeit, verschiedenste Parameter wie z.B. „Erste Reflexionen“ oder „Nachhallzeit“ mittels der Software „Cue-Station“ nachzujustieren.

Blockschaltbild / Bilder des Systemaufbaus

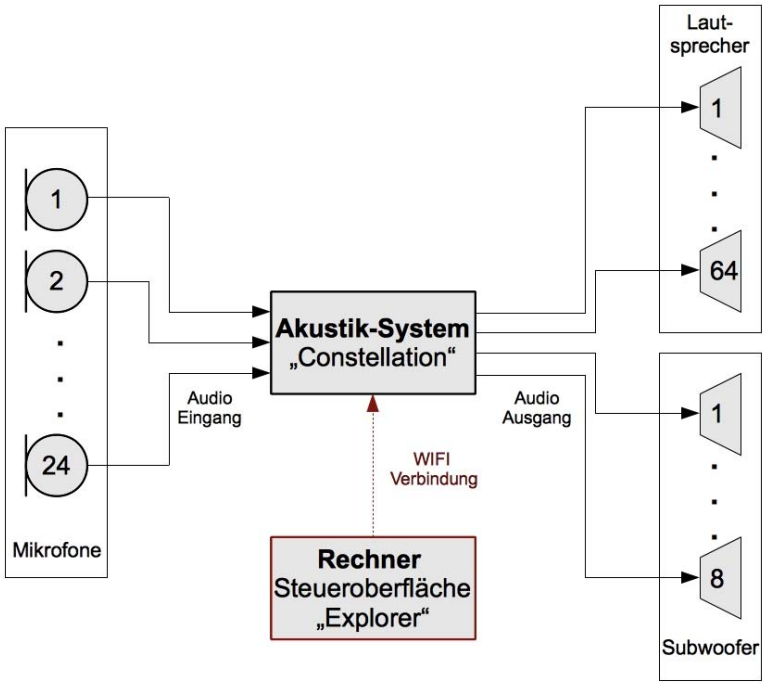

Abb. 3.3: Blockschaltbild Steuerung Mumuth

Abb. 3.4: Lautsprecher Akustiksystem

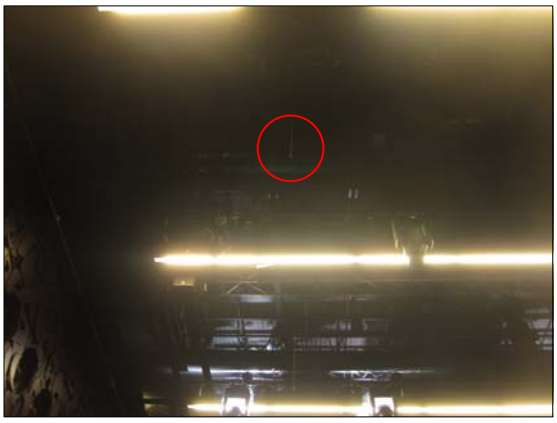

Abb. 3.5: Mikrofon Akustiksystem

Weiteres vorhandenes System:

Ein weiteres im Konzertsaal installiertes System wird für die direkte elektroakustische Beschallung des Auditoriums verwendet. Die hierbei verwendeten Lautsprecher können im Raum mittels Pantografen in Höhe, Neigung und Winkel positioniert werden. Aufgrund diverser Sicherheitsbedenken seitens des „TÜVs“ musste hierfür jedoch eine drahtgebundene Steuerung installiert werden, um die Sicherheit für das Auditorium gewährleisten zu können. (siehe auch Kap. 4)

Abb. 3.6: Beschallungssystem des MUMUTH Graz

Abb. 3.7: Steuerung des Beschallungssystems des MUMUTH Graz

Zusammenfassung / Erfahrungsbericht:

Bei diesem Verwendungszweck geschieht die technische Umschaltung unhörbar. Auch in Punkto Stabilität konnten bisher keine Probleme der Steuerung beobachtet werden.

3.2 FOH-System: Audio-Interface mit DSP

Im hier dargestellten Praxisbeispiel handelt es sich um die professionelle Steuerung eines Live-Beschallungssystems auf Basis eines digitalen Audio Interfaces mit integriertem digitalen Signalprozessor („DSP“) mittels OSC und VNC. Zum Zeitpunkt der Verfassung dieser Arbeit herrscht eine steigende Verbreitung dieser Geräte. Daher liegt es nahe, diese Form des Systemaufbaus zu erwähnen, besonders auf Hinsicht der Handlichkeit und Flexibilität gegenüber vergleichbarer, rein analoger Systeme. Die Zusammenstellung des Systems geschieht durch Klemens Moser, seines Zeichens Verkaufsberater für Studiotechnik des Musikhauses „KeyWi“ in Puch bei Hallein, Land Salzburg.

Kurzüberblick:

Basis:	VNC / OSC
Verwendungszweck	Live Beschallung und Monitoring, Effekt-Steuerung
Systemaufbau:	– High-End Audio Interface der Firma Metric Halo (Mobile I/O 2882 Expanded 2D) – Apple Mac Book mini 13Zoll – Apple´s „Mainstage“: dem Sequenzer „Logic“ ähnliche, ressourcenschonende Software zur Einbindung von Effekten und Software-Instrumenten in den Live-Betrieb

Details zum Verwendungszweck:

Das Metric Halo Mobile I/O 2882 Expanded 2D ist ein High-End Audio Interface mit integriertem DSP, und ist somit mit einem Digitalmischpult vergleichbar. Da ein angeschlossener Rechner lediglich als Steuerungsoberfläche dient, ist es dementsprechend auch als stabil und zuverlässig zu bezeichnen, da ein Ausfall des Rechners die Funktionalität des Interfaces nicht beeinflusst. Diesem Ansatz folgte Klemens Moser und stellte für ihn und seine Coverband einen kleinen und sehr flexiblen FOH Mixer zusammen. Da die Steuerung, wie bereits erwähnt, die CPU wenig beansprucht, ist es weiters möglich, Studioeffekte wie z.B. den Faltungshall „Space Designer“ des Sequenzers „Logic“ über die Software „Mainstage“ einzubinden, ohne dass die Stabilität maßgeblich darunter leidet. Das ganze System wird für FOH Anwendungen per VNC gesteuert. Für Pausen der Band, in der selbige von der Veranstaltung kurz abwesend ist, erhält der Veranstalter/Moderator ein Smartphone (iPhone) mit einer OSC Oberfläche, durch welche es ihm möglich ist, die Lautstärke seines Ansage-Mikrofons und der Hintergrundmusik zu steuern. Für alle anderen Funktionen des Interfaces bleibt der Zugriff verwehrt. Weiters beinhaltet die Steuerung einen Not-Aus Knopf (z.B. im Falle eines Feedbacks) und die Telefonnummer des Technikers, falls Probleme auftreten.

Details zum Systemaufbau:

Beim Metric Halo Mobile I/O 2882 Expanded 2D handelt es sich um ein Interface mit 8 analogen Mikrofon-Vorverstärkern, 8 digitalen Eingängen im ADAT-Format und weiteren Eingängen in High-End Studioqualität. Die Input-Kanäle sind digital steuerbar. Über Firewire sind bis zu 4 Geräte kaskadierbar. Die Anzahl der Misch-Kanäle ist unbegrenzt. Die interne DSP umfasst neben Standard-Mischpult Funktionen auch eine breite Palette digitaler Effekte in Studioqualität. Über die Software „Mainstage“ der Firma Apple lassen sich weitere digitale Effekte in das Setup einbinden, wie z.B. Faltungshall und Delay-Effekte, aber auch Software-Instrumente. Gesteuert wird das gesamte System über einen handelsüblichen Laptop der Firma Apple, ein MacBook mini 13 Zoll. Für die Funksteuerung wird weiters ein Smartphone mit der Bezeichnung iPhone, ebenfalls ein Produkt der Firma Apple, verwendet.

Blockschaltbild / Bilder des Systemaufbaus:

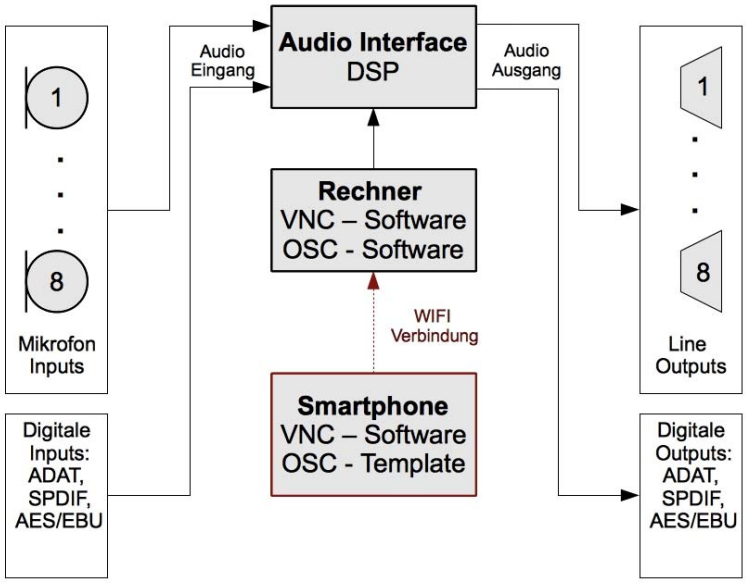

Abb. 3.8: Blockschaltbild Steuerung Audio-Interface

Abb. 3.9: Metric Halo Mobile I/O 2882 Expanded 2D

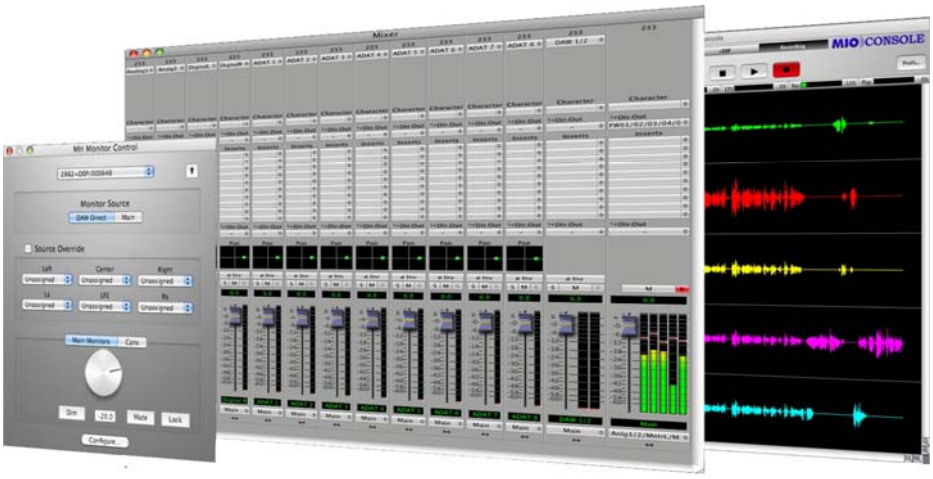

Abb. 3.10: Mixoberfläche „MIO-Console“

Zusammenfassung / Erfahrungsbericht:

Aufgrund der extrem guten Qualität der Mikrofon-Vorstufen und Wandler, sowie der digitalen Effekte des Interfaces, und der Möglichkeit, jederzeit beliebige Einstellungen auch während der Show abzurufen (Total Recall), kann man behaupten, das Gerät bringt „das Studio auf die Bühne“. Arbeitet die Band mit Click (Metronom), ist es auch möglich, Sample-Einspielungen bzw. eine Lichtshow per MIDI einzubinden. Die Mixoberfläche ist sehr Sequenzer-nahe aufgebaut, somit selbsterklärend für erfahrene Tontechniker, und ermöglicht tolle Routing-Möglichkeiten.

Im Falle eines Ausfalls der Stromversorgung stellt sich das Gerät unmerklich auf „Bus-Powered“, also Stromversorgung über den Firewire Port bzw. den Akku des Rechners um, wodurch wenigstens kurzzeitig ein Zeitfenster für Handlung entsteht (die Veranstaltung kann unmerklich weitergeführt werden, ca. 20 bis 40 Minuten, natürlich Akku bzw. Last-abhängig).

In Tests bei Volllast belief sich die CPU Belastung des Rechners auf ca. 5 bis 6 %. Die WLAN-Verbindung geschieht über ein Ad-Hoc Netzwerk, somit ohne Access-Point/Router, was laut Angaben einen Steuerungsradius von 20 bis 30 Meter ermöglicht. Die Verwendung von VNC bzw. OSC geschieht völlig unkompliziert, jedoch muss man bei OSC für die mehrfache Konvertierung, sprich OSC → MIDI, MIDI → MCU („Mackie Control Universal“) im Hintergrund laufende Programme verwenden.

Weiters positiv zu erwähnen ist der maßgebliche Sound- und auch Preisunterschied im Vergleich zu kommerziellen Digitalmischpulten dieser Preiskategorie.

Laut Angaben ist das System seit März 2008 bei ca. 80 Shows im Jahr in Verwendung und läuft ausgezeichnet. Lediglich drei Ausfälle sind zu verzeichnen, was jedoch auf Transportschäden, Problemen bei der Stromversorgung, sowie einem Produktionsfehler zu Beginn zurückzuführen ist.

3.3 FOH-System: Digitalmischpult

Im hier dargestellten Praxisbeispiel handelt es sich um die professionelle Steuerung eines Digitalmischpultes im Live-Betrieb. Das System ist ein fixer Aufbau und wird von der Musikgruppe „Meissnitzerband“ auf verschiedensten Bühnen im deutschsprachigen Raum eingesetzt. Die Zusammenstellung des Systems geschieht durch die FOH- und Monitoring Techniker der Band Sebastian Mandl und Blasius Buchegger.

Kurzüberblick:

Steuerungsbasis:	USB Geräte Server
Verwendungszweck:	FOH und Monitoring-Einstellungen
Systemaufbau:	- Yamaha 01V96 Digitalmischpult - M-Audio PROFIRE 2626 - Silex SX-2000 WG + , Wireless USB Geräte Server - Yamaha „Studiomanager“, Steuerungssoftware - MacBook Pro

Details zum Verwendungszweck:

Die hier genannte Folk-Rock-Band namens „Meissnitzerband“ ist auf vielen Bühnen im gesamten deutschsprachigen Raum zu finden. Oftmals, besonders bei Veranstaltungen im kleinen Rahmen, entfällt jedoch leider die Möglichkeit, einen optimalen FOH-Mischplatz inmitten des Raumes aufzubauen. Auch bei Verwendung von sogenannten „Delay Lines“, einer bestimmten Art von Mehrzonenbeschallung, erweisen sich zum Beispiel gängige Einmessverfahren oftmals also sehr unhandlich, da eine Regelung bzw. Korrektur der Signale ortsgebunden am Mischplatz erfolgen muss. Daher haben sich die zuständigen Techniker für eine Funksteuerung eines Digitalmischpultes der Firma Yamaha mit der Bezeichnung 01V96 entschieden. Mit Hilfe der Software-Applikation der Firma Yamaha namens „Studio Manager“ und einen Wireless USB Geräteserver ist es nun möglich, auf nahezu alle relevanten Parameter der Konsole über einen Laptop überall im Raum zuzugreifen. Die so entstandene Flexibilität ermöglicht auch den Einsatz als fixen Monitor-Mischplatz, wie im folgenden Bild erkennbar ist.

Abb. 3.11: Typisches Szenario während einer Show

Details zum Systemaufbau:

Wie bereits erwähnt, ist das Herz dieses Systems ein Yamaha 01V96 VCM Digitalmischpult. Als 8 Kanal Mikrofon-Vorstufe und AD-DA Wandler dient ein M-Audio PROFIRE 2626 Firewire Audio Interface mit integrierter DSP, mit welchem über einen Firewire Bus auch spontane Audio-Mitschnitte realisierbar sind. Um eine WLAN Steuerung zu ermöglichen, kommt ein „Silex SX-2000 WG + " Wireless USB Geräteserver zum Einsatz. Die Geräte sind allesamt in einem vier Höheneinheiten hohen 19-Zoll-Trible Door-Birkenmulitplex Case verbaut. Um den Empfang des Geräteservers möglichst wenig zu beeinflussen, wird eine externe Antenne verwendet. Alle relevanten Ein- und Ausgänge des Systems sind über eine Patchbay erreichbar, welche sich an der Oberseite des Cases befindet.

Als Steuerung dient ein Apple „Mac Book Pro", auf welchem die Software „Studiomanager" installiert ist.

Blockschaltbild / Bilder des Systemaufbaus

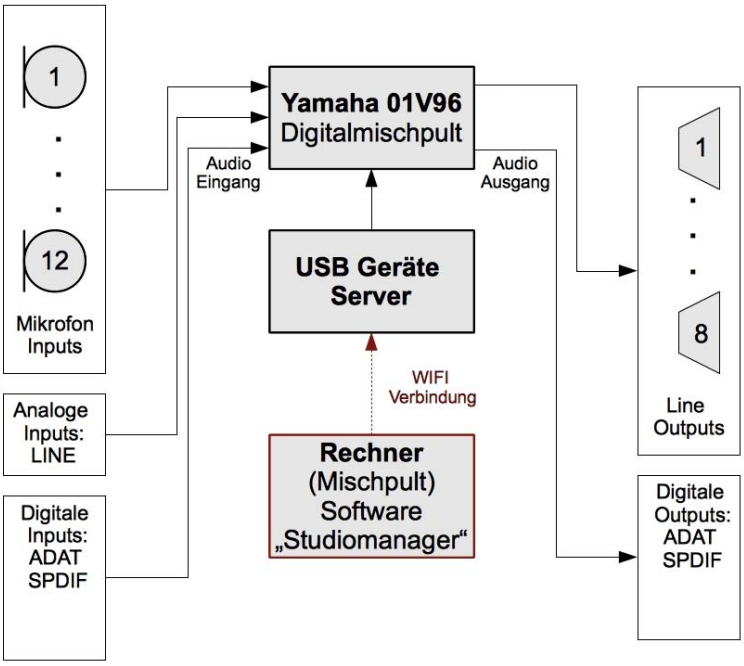

Abb. 3.12: Blockschaltbild Steuerung FOH Mischplatz

Abb. 3.13: FOH-Mischplatz

Zusammenfassung / Erfahrungsbericht:

Die Verwendung einer Funksteuerung für FOH Zwecke ist allgemein sehr empfehlenswert, jedoch sollte man die in Kap. 4 erörterten Sicherheitshinweise beachten. Der Zugriff auf alle Parameter des Mischpultes von einer beliebigen Position im Raum erweist sich als sehr nützlich, besonders bei Verwendung für Monitoring Anwendungen und bei Mehr-Zonen-Beschallung. Ein weiterer Vorteil ist die mögliche und relativ unkomplizierte Kombination mit einem anderen Steuerungssystem wie zum Beispiel „Virtual Network Computing“ (siehe Kap. 5.2). Hierbei wird es dem Techniker ermöglicht, im Falle einer stark besuchten Veranstaltung, bei der im Auditorium Platzmangel herrscht, anstatt des - im Vergleich - relativ großen Laptops sein Smartphone zur Steuerung zu benutzen.

Zu beachten bei diesem Setup bei Verwendung als parallel zum FOH laufenden Monitor Mischplatz ist die mögliche gegenseitige Beeinflussung der Techniker bei der Bedienung. Konkret gesagt: Justiert gerade der FOH Techniker einen Parameter am Mischpult, und betätigt währenddessen der Monitor-Techniker den Kanal-Auswahl Knopf eines anderen Mischkanals, verändert der FOH Techniker unabsichtlich einen ungewollten Parameter (den des nun ausgewählten Kanals). Weiters zu beachten ist, dass sich mit dem verwendeten USB-Geräteserver nur *eine* Verbindung herstellen lässt. Eine Verwendung von mehreren Rechnern parallel ist somit *nicht* möglich.

3.4 In-Ear-Monitoring System: Audio-Interface mit DSP

Im hier dargestellten Praxisbeispiel handelt es sich um die Steuerung eines kompletten In-Ear-Monitoring Systems für eine Rockband. Einsatz findet dieses System vor allem im Live-Betrieb, es wird jedoch auch für Probe-Zwecke verwendet. Die Zusammenstellung des Systems erfolgte durch die Musiker der Band, Florian Ainhirn, DI Franz Schober, und Blasius Buchegger.

Kurzüberblick:

Steuerungsbasis:	OSC
Verwendungszweck:	Live-Monitoring
Systemaufbau:	- Motu 828 Mk3, Firewire Audio-Interface mit integrierter DSP - Motu 8Pre, 8-Kanal Mikrofon-Vorstufen mit AD Wandlung - 3 x LD Systems Mei 1000, UHF In-Ear System - Cue Mix FX, Motu Mixing Software für Interfaces - Mac Book mini 13 Zoll - Smartphones mit Applikation „TouchOSC“

Details zur Verwendung:

Um eine gute und gleichmäßige Monitoring-Situation im Proberaum wie auch im Live-Betrieb zu gewährleisten, haben sich die Musiker der Rockband „Gainful Experience“ zu einer Kombination von Monitor-Lautsprechern und einem eigenständigen In-Ear System entschlossen. Dieses System ermöglicht jedem Einzelnen der Musiker sich einen eigenständigen Stereo-Mix für sein UHF- In-Ear System zu erstellen, welche mittels ihres Smartphones über eine WLAN Steuerung veränderbar ist. Eine Basis-Mischung, welche zu gleichen Teilen *allen* Monitor-Lautsprecher zugeführt wird, sorgt für die notwendige Lautstärke bzw. das Spielgefühl, welches für diese Art von Musik unentbehrlich ist. Aufgrund der kompletten Eigenständigkeit dieses Systems ermöglicht es den Musikern, die im Proberaum eingestellte und gewohnte Monitoring-Situation auf die Bühne zu bringen. Hierfür wird die Basis-Mischung (1 bis 2 Kanal) einfach an den FOH bzw. Monitor-Mischplatz geleitet, es muss lediglich der Pegel der Lautsprecher eingestellt werden.

Details zum Systemaufbau:

Mittelpunkt des Systems ist ein Motu 828 Mk3 digitales Audio-Interface mit integrierten Effekten. Dieses Gerät ist aufgrund der internen DSP als Digitalmischpult verwendbar, und mittels der Software „Cue Mix FX“ über einen Rechner steuerbar. Die 8 analogen Eingänge des Motu 828 und die 8 analogen Eingänge des Motu 8 Pre werden mit den Signalen der einzelnen Instrumente gespeist und sind im Digitalmischpult für alle Mischungen einzeln in Pegel und Panorama justierbar. Als Signale dienen: Bass Drum, Snare Drum, 3 x Tom, 2 x Overheads, Bassgitarre, Leadgitarre (Stereo), Rhythmusgitarre, Gesang (Stereo). Mit Hilfe der integrierten Dynamikbearbeitung des Motu 828 Mk3 kann die Dynamik der Instrumente derart eingegrenzt werden, dass sie eine gleichmäßige Lautstärke für die einzelnen Monitor Mischungen ermöglicht. Es werden insgesamt über die analogen Outputs der Geräte fünf Stereo-Mischungen erstellt, drei für die eingebauten UHF In-Ear Systeme, eine für ein externes UHF In-Ear System und eine für einen kabelgebundenen Kopfhörer-Ausgang (Schlagzeug). Um die Signale „Bass Drum“ und „Snare Drum“ für das In-Ear-Monitoring zu optimieren, kommt ein „SPL Transient Designer“ zum Einsatz, welcher in das Zeitverhalten des Signals eingreift und den „Attack“, also den Anschlag der Trommel erhöht (näheres siehe Produktspezifikation).

Blockschaltbild / Bilder des Systemaufbaus

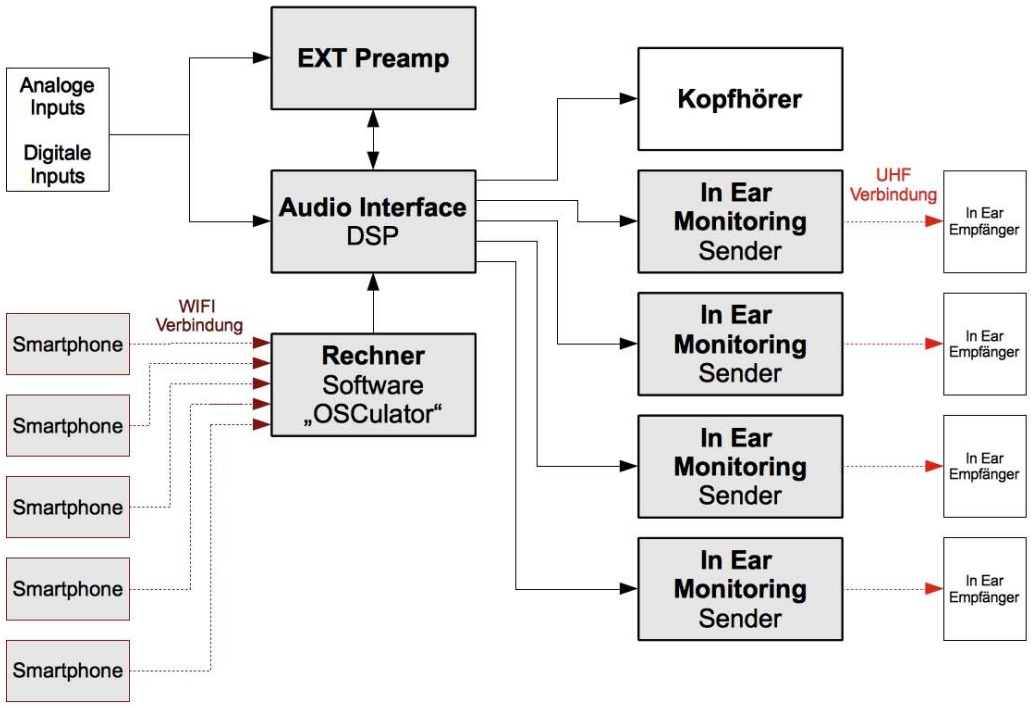

Abb. 3.14: Blockschaltbild Steuerung In-Ear-Monitoring

Abb. 3.15: Vorderseite Monitoring-System

Abb. 3.16: Rückseite Monitoring-System

Zusammenfassung / Erfahrungsbericht:

Dieses System ist nach einer Eingewöhnungsphase aufgrund der ungewohnten Handhabung bzw. Verwendung eines In-Ear Systems besonders für Sänger sehr empfehlenswert. Wie bereits erwähnt ermöglicht es dem Musiker, seine Monitor-Einstellungen direkt vom Proberaum auf die Bühne zu bringen. Lange Einstellproben entfallen, aufgrund des Funk-In-Ear Systems hat der Musiker eine (annähernd) homogene Monitoring-Situation überall auf der Bühne, was die Bewegungsfreiheit enorm erhöht. Im Falle kleiner Korrekturen kommt die WLAN Steuerung ins Spiel: Anstatt dem Monitor-Mischer Anweisungen während des Konzertes geben zu müssen, kann der Musiker die Mischung einfach über sein Smartphone anpassen. Dieses lässt sich z.B. mittels einer Halterung an seinem Mikrofonstativ befestigen, ist somit jederzeit erreichbar.

Das System ist jedoch sehr kostenintensiv und erfordert einen erfahrenen Tontechniker unter den Musikern. Weiters ist In-Ear-Monitoring nicht für Musikgruppen zu empfehlen, welche eine gewisse Mindestlautstärke auf der Bühne wie im Proberaum fordern (Rock bzw. Metalbands). Die Handhabung eines In-Ear Systems erfordert eine gewisse Disziplin, da zu hohe Lautstärken auf den Kopfhörern sehr schnell zu schweren Gehörschädigungen führen können.

Die alternative Verwendung der WLAN Steuerung für Bodenmonitore ist natürlich auch denkbar. Hierbei ist jedoch zu beachten, dass eine unerfahrene Handhabung insbesondere von Mikrofonsignalen auf Lautsprechern sehr schnell ein Feedback auslösen kann. Daher sollte der Regelbereich im Vorhinein eingegrenzt werden, bzw. diverse Lautsprecher ausreichend entzerrt werden.

4 Sicherheit

In den vorherigen Kapiteln wurden mögliche Einsatzmöglichkeiten für eine Funksteuerung beschrieben und theoretische Einführungen über relevante Themengebiete gegeben. Verschiedene Systeme, welche in der Praxis bereits Verwendung finden, wurden vorgestellt. Das nun folgende Kapitel widmet sich dem Aspekt der Sicherheit, da dies eine sehr wichtige und zentrale Thematik darstellt.

4.1 Allgemeine Überlegungen:

Um die in den nachfolgenden Kapiteln erörterten Funksteuerungen in der Praxis effektiv und verantwortlich einsetzen zu können, ist es unerlässlich und beinahe verpflichtend für den ausführenden Toningenieur, sich mit dem Aspekt der Sicherheit zu befassen. Die größtmögliche Ausfallsicherheit, also einen störungsfreien Ablauf der Veranstaltung sowie insbesondere der Schutz des Auditoriums vor etwaigen Gesundheitsschäden setzen eine gründliche Auseinandersetzung mit den möglichen Manipulationsmöglichkeiten der Netzwerkthematik voraus.

Das Internet als globales Netzwerk ist heutzutage in vielen Bereichen kaum mehr wegzudenken. Vielfach sind auch firmeninterne Netzwerke über das Internet erreichbar. Auch im Consumer-Bereich nimmt die Nutzung vor allem im Mobilfunk von Tag zu Tag zu. Somit verbreiten und vereinfachen sich auch die Techniken von Tag zu Tag, sich Zugang zu diversen Computernetzwerken zu verschaffen.

Unter vielen Tontechnikern herrscht die allgemeinen Meinung vor, eine mechanische Manipulation der Veranstaltung, also jemand unterbreche zum Beispiel die Stromversorgung, sei viel wahrscheinlicher als eine Sabotage über solch ein WI-FI-Netzwerk. Aufgrund dieser Annahme wird dann häufig auf einfache Sicherheitsmechanismen wie z.B. eine Verschlüsselung der Verbindung via WPA (siehe Kap. 4.3.) verzichtet, und somit auf die „Gutmütigkeit“ des anwesenden Publikums vertraut. Jedoch ist es heutzutage bereits möglich, mit einem der zurzeit sehr verbreiteten Smartphones und der passenden „App“ (Application = Programm für Smartphones) WLAN Netzwerke auszuspähen und weiterführend zu missbrauchen.

Die folgenden Punkte dienen rein als Gedankenanstoß, daher wird gebeten, dies nicht wortwörtlich zu nehmen:

- Eigentlich kann man ein WLAN-Netzwerk umdeuten als ein Netzwerk von beliebig vielen, frei zugänglichen „Kabelverbindungen“ (= Funkwellen). Um Zugriff zu erhalten, muss lediglich der „Stecker“ (= Passwort) passen.

- Oftmals erzählen Tontechniker von Veranstaltungen, bei denen Gäste versucht haben, Einstellungen am Pult zu verändern. Die Verwendung eines ungesicherten Netzwerkes wäre gleichbedeutend mit der Vorstellung, man biete einem potentiellen Saboteur einen Platz neben dem Mischpult an. In diesem Fall ist natürlich nicht 100% sicher, dass etwas passiert, jedoch ist die *Möglichkeit* gegeben.

- Weiters zu bedenken ist, dass sich der Techniker dank der Funksteuerung nicht mehr permanent am Pult aufhalten muss. Dies hätte natürlich maßgeblichen Einfluss auf die Reaktionsgeschwindigkeit im Falle einer Panne: bei etlichen Kilowatt Leistung an der PA kann eine immense Gefahr für das Auditorium entstehen. Somit ist der Betrieb einer Fernsteuerung ohne entsprechende Schutzmaßnahmen unverantwortlich. Daher sollte sich bei Verwendung einer Funksteuerung während einer größeren Veranstaltung stets jemand beim Pult befinden. (Bsp. siehe Kap. 3.1., kabelgebundene Steuerung für Beschallungsanlage von TÜV gefordert)

Aus diesem Grund erscheint es den Autoren dieser Arbeit besonders wichtig, sich in einem eigenständigen Kapitel diesem Thema zu widmen, um dessen Wichtigkeit zu betonen. Es wird an künftige Nutzer appelliert, den Aspekt der Sicherheit ernst zu nehmen und vor den Nutzeffekt zu stellen.

Zuallererst werden kurz einige gängige Manipulationsarten in der Netzwerktechnik erläutert:

4.2 Gängige Manipulationsarten netzwerkseitig:

Grundsätzlich gibt es vier Möglichkeiten, wie ein Angreifer die Kommunikation zwischen zwei Stationen stören kann:

- Abfangen: Ein Angreifer liest die Nachricht mit, somit kann er Zugriff auf den Inhalt erlangen.
- Manipulieren: Ein Angreifer manipuliert und verfälscht die bei der Kommunikation ausgetauschte Nachricht
- Täuschen: Ein Angreifer täuscht eine falsche Identität vor, wodurch er mit dem Opfer kommuniziert. (Opfer = Sender, Empfänger oder beides gleichzeitig)
- Unterbrechen: Ein Angreifer sabotiert die Kommunikationsverbindung zwischen zwei Stationen.

Es gibt nahezu unbegrenzte Möglichkeiten für die Umsetzung solcher Angriffe in die Praxis. Besonders einfach wird es für den Angreifer, wenn er Zugang auf eine der Zwischenstationen erhält. In diesem Fall leitet der Saboteur einfach die Kommunikation zwischen den zwei Stationen auf eine dritte, unter seiner Kontrolle stehende um.

Mithören:

Es ist sehr einfach, den gesamten Datenverkehr im Netzwerk mitzuhören. Dieser Vorgang wird im Allgemeinen als „Packet Sniffing“ bezeichnet und ist, falls keine Protokolle zur Verschlüsselung verwendet werden, auf allen Schichten (siehe Kap. 2.1.1) möglich. Jedes Paket auf jeder Schicht ist somit *komplett* lesbar.

Ein Beispiel hierfür wäre das Open Source Programm „Wireshark“ (früher „Ethereal“) [WIRE] welches für die Netzwerkanalyse verwendet wird. Es beinhaltet Funktionen, welche die Nutzdaten einer TCP-Verbindung (siehe Kap. 2.1.3) auszulesen und darzustellen vermögen. Somit können alle übertragene Informationen (Daten und auch Passwörter (!)) dargestellt und aufgezeichnet werden. Dies gilt auch für UDP Verbindungen und Kommunikation mittels zusätzlicher Protokolle. Auch verschlüsselte Verbindungen können relativ einfach entschlüsselt werden, diverse Software ist ebenfalls im Internet frei zugänglich, z.B. die Sniffing und Netzwerk-Analyse Applikation „Ettercap“. [ETTER]

Einzige Vorraussetzung für den Angreifer für diese Art der Manipulation ist, im Besitz von Zugriffsrechten auf einen Rechner im Netzwerk zu stehen, was z.B. in einem ungesicherten WLAN-Netzwerk beinahe ein Kinderspiel ist. Durch eine Vielzahl von Sniffing-Programmen auch für Smartphones lassen sich somit in solch einem Netzwerk einfach diverse Passwörter für VNC Verbindungen oder detaillierte OSC-Konfiguration erkennen und mittels einer Version der verwendeten Steuerungssoftware für Manipulationen reproduzieren. [3]

Manipulation:

Es gibt auch eine Vielzahl von Möglichkeiten, die über die Netzwerkverbindung übertragenen Daten direkt zu manipulieren, wie z.B. bei der „Network Address Translation“ (NAT). Hierbei werden IP-Adressen verändert, es können aber auch TCP und UDP-Portnummern umgeformt werden.

Manipulation beim Routing:

Eine Kernfunktion im Netzwerk übernimmt das Routing (siehe Kap. 2.1.2). Ist es einem Angreifer möglich, den Datenverkehr über seinen Rechner umzuleiten, hat er volle Kontrolle über diese. Auch durch gezielte Fehlinformationen kann der Saboteur das Routing verfälschen oder sogar komplett unterbrechen.

Beim dynamischen, aber auch beim statischen Routing kann mittels Falsch-Information dem zuständigen Router vorgetäuscht werden, die Verbindung über den Rechner des Angreifers wäre besonders vorteilhaft.

Weiters bietet das IP-Protokoll als Option das sogenannte „Source Routing“ an, welches die Erstellung einer Liste für die erlaubten Zwischenstationen im Netzwerk ermöglicht. Auch hier ist ein potentieller Angriffspunkt denkbar.

Eine weitere Möglichkeit, Zugang zum Netzwerk zu erhalten, ist eine Vortäuschung von falschen Adressen. Dies wird im Allgemeinen als „Address-Spoofing“ bezeichnet und wird in den folgenden Punkten kurz erläutert:

MAC-Adressen-Spoofing

Eine MAC-Adresse („Media-Access-Control“) ist die Hardware-Adresse eines Netzwerkgerätes und ist somit global eindeutig. Daher werden diese teils auch für die Authentifikation und Identifikation bestimmter Systeme verwendet. Die MAC-Adresse wird bei der Kommunikation im Klartext, also unverschlüsselt, übertragen. Jedoch ist die Verwendung von gefälschten Mac-Adressen bzw. deren Klonung ohne Probleme möglich, wodurch man vollen Zugriff erhält. Daher sind Schutzverfahren, die eine Identifikation anhand der MAC-Adresse nutzen, aus dem Aspekt der Sicherheit nutzlos. [3]

IP-Adressen-Spoofing

Natürlich lässt sich auch ganz einfach die IP-Adresse (siehe Kap. 2.1.2) fälschen, diese jedoch kann zumeist nur für unidirektionale Angriffe verwendet werden. Unidirektional heißt hier, der Angreifer schränkt einen Dienst ein bzw. unterbricht diesen (sogenannte „Denial-of-Service“ Angriffe).

TCP-Sequence Number Attack

Für den Datenaustausch über TCP wird ein Verbindungsaufbau vorausgesetzt, was aber mit einer gefälschten IP-Adresse aufgrund der einseitigen Kommunikation nicht möglich ist. Der Verbindungsaufbau geschieht über einen sogenannten Three-Way-Handshake, bei dem vereinfacht gesagt der Client anfragt, der Server antwortet und der Client den Erhalt der Antwort bestätigt. Im zweiten Schritt ist die sogenannte „Anfangssequenznummer" erforderlich, welche man auch erraten kann (z.B. durch vorherige Analyse). Somit kann unter Umständen der Handshake vorgetäuscht werden.

DNS-Spoofing

Da sich der User nicht für jede Internetadresse eine IP-Adresse merken kann, bzw. dies sehr umständlich wäre, wurde das „Domain Name Service" eingeführt. Dies hat die Aufgabe, Domainnamen und Hostnamen in IP-Adressen umzusetzen.

Durch Fälschen einer Website und somit deren DNS ist es z.B. dem Angreifer möglich, an die Kontodaten eines Bankkunden zu kommen. (Kunde öffnet von Angreifer kontrollierte Website und gibt Daten ein).

Das hier genannte Beispiel ist natürlich eher Internetbezogen, der Grundgedanke dahinter, eine falsche grafische Oberfläche zu generieren und damit an Passwörter zu kommen, ist aber auch in lokalen Netzwerken denkbar.

In den folgenden Punkten wird nun auf Sicherungsmechanismen in für unsere Zwecke relevante Schichten eingegangen.

4.3 Sicherheit Netzwerkschicht (WEP, VPN)

4.3.1 „Wired Equivalent Privacy" (WEP)

WEP steht für „Wired Equivalent Privacy" und stellt einen symmetrischen, kryptographischen Schlüssel dar, welcher dazu dient, WLAN-Verbindungen zu schützen.

Als Standard-Sicherheitsmechanismus von 802.11b-Netzwerken sollte hiermit die sicherheitsrelevanten Themen „Authentifizierung" und „Vertraulichkeit" abgedeckt werden. Jedoch wurde WEP niemals umfassend von unabhängigen Experten getestet, was zu erheblichen Sicherheitsmängeln führte.

WEP gilt heute als gebrochen. Oft herrscht die allgemeine Meinung, der Mechanismus reiche z.B. für kleine Büro oder Heimnetzwerke, aufgrund seiner Schwächen und der Vielzahl an Manipulationsarten muss dem jedoch widersprochen werden. Im folgenden Teil wird kurz der Aufbau und dementsprechend die Schwächen dieses Sicherheitsmechanismus aufgezeigt. [5]

Verschlüsselung

Die Verschlüsselung erfolgt zwischen dem Client und dem Access Point. Beide Seiten haben Schlüssel zur symmetrischen Ver- und Entschlüsselung der Kommunikation, welcher zuvor ausgetauscht wurde („shared Key"). Die Länge dieses Schlüssels betrug zu Anfangszeiten des Mechanismus 40 bit, heutzutage sind eher Längen von 128 bit üblich.

Der sogenannte „RC4 Algorithmus" wandelt diesen Schlüssel in einen einzigartigen Schlüsselstrom für genau eine Übertragung. Für jedes Datenpaket wird der gleiche Schlüssel verwendet, wodurch jedes Mal ein identischer Chiffretext entsteht.

Dadurch kann dieser sehr leicht gebrochen werden. Folge dessen wurde eine Zufallskomponente, der sogenannte „Initialization Vector" (IV) eingeführt, welcher eine Länge von 24 Bit beträgt und dem Schlüssel angehängt wird. Aufgrund der Kürze des IV tritt nach ca. 5000 gesendeten Paketen eine wiederholte Verwendung auf. Weiters muss auf der Gegenseite der IV zur Entschlüsselung bekannt sein, daher wird er mit den (verschlüsselten) Paketen mitgeschickt. Er kann sich jedoch nicht im verschlüsselten Teil befinden, daher wird er im Klartext übertragen. [3]

Schwächen des WEP-Sicherheitsmechanismus

Wie zuvor erwähnt, ist der Initialization Vector mit 24 Bit eindeutig zu kurz, wodurch nach kurzer Zeit eine wiederholte Verwendung geschieht. Bei wiederholten IV und konstantem WEP Schlüssel, sowie weiterer konstanter Komponenten in der Nachricht, wie z.B. IP-Adressen, kann nach und nach der Schlüsselstrom berechnet werden.

Dementsprechende Software ist z.B. im Internet frei zugänglich, bzw. teilweise sogar als „Open Source" Programme zu finden. Aus diesem Grund ist der Verwendung von WEP definitiv abzuraten. [3]

4.3.2 WPA / WPA2

Aufgrund oben genannter Sicherheitsrisiken wurden neue Sicherheitsmechanismen dem WEP Standard hinzugefügt, welche durch die sogenannte „Robust Security Network Association" (RSNA) im Standard „IEEE 802.11i spezifiziert wurde.

Die „Wi-Fi Alliance“, ein Zusammenschluss verschiedenster Hersteller zur Förderung der Kompatibilität von IEEE 802.11 Produkten, hat unter WPA („Wi-Fi Protected Access“) und WPA2 Teile des IEEE 802.11i Standards ausgewählt.

Hierbei stellt WPA den Nachfolger von WEP dar. Das hier verwendete sogenannte „Temporal Key Integrity Protocol“ basiert auf WEP, und dient sozusagen als Übergangslösung, wird daher an dieser Stelle nicht näher behandelt.

Den aktuellen Standard stellt WPA 2 dar. Im Gegensatz zu WEP und WPA basiert WPA 2 auf dem sogenannten „Counter Mode with Cipher Block Chaining with Message Authentication Code Protocol“ (CCMP). Diese ist von WEP komplett unabhängig und basiert wiederum auf dem „Advanced Encryption Protocol“ (AES) welches z.B. auch in den USA für die Verschlüsselung geheimer Dokumenten von Behörden eingesetzt wird.

CCMP schützt zuverlässig die Vertraulichkeit und Integrität der übertragenen Frames. In weiterer Folge ist es möglich, Replays zu erkennen. (Replay = nochmaliges Absenden von übertragenen Paketen durch Angreifer)

In Punkto Authentifikation kommen zwei Verfahren zum Einsatz:

- Die Verwendung eines bereits bestehenden gemeinsamen Schlüssels, des sogenannten „Pre-Shared-Key“ (PSK)

- Die Verwendung von IEEE 802.1X. Dies stellt eine Zugangskontrolle der einzelnen Zugangspunkte zu einem Netzwerk dar. Hierfür ist ein sogenannter Authentication Server notwendig, welcher den Client authentifiziert und in weiterer Folge einen Anschlusspunkt (Port) zuteilt.

Während des Aufbaus der RSNA wird ein symmetrischer kryptographischer Schlüssel ausgehandelt, der später zur Verschlüsselung verwendet wird.

In kleineren Netzwerken bietet sich die Verwendung des PSK an, da hier der Betrieb eines IEEE 802.1X Authentifikations-Servers zu aufwendig wäre.

Zusammenfassend kann man sagen, dass mit WPA 2 die Schwachstellen im ursprünglichen Standard zufriedenstellend geschlossen wurden. Es sind auch bisher weitgehend nur Passwortangriffe auf diesen Sicherheitsmechanismus bekannt. [3]

Zusammenfassung:

Abschließend wird nochmals darauf hingewiesen, dass natürlich keine 100%-ige Sicherheit in einem Netzwerk herstellbar ist. Jedoch einige mit Bedacht eingesetzte Sicherheitsmechanismen können es potentiellen Angreifern sehr schwer machen, das Netzwerk zu stören, und sind somit unerlässlich.

5 Step-by-Step Anleitungen

In den vorangegangenen Kapiteln wurden verschiedene Anwendungsmöglichkeiten für eine Fernsteuerung beschrieben und theoretische Einführungen über die vorkommenden Themengebiete gegeben. Verschiedene Systeme, welche in der Praxis Verwendung finden, wurden vorgestellt. In diesem Kapitel werden nun für die in Kap. 1 vorgestellten Verbindungsarten (vgl. S. 7, Abb.1.1) detaillierte Schritt-für-Schritt-Anleitungen gezeigt um solche Systeme zu realisieren, außerdem wird auf etwaige Probleme und Besonderheiten eingegangen. Da oft große Unterschiede zwischen Windows- und Macintosh-basierten Systemen bestehen, wurden diese teilweise getrennt betrachtet.

Kapitel 5.1 beschreibt nun eine Verbindung zu einem USB-Geräteserver, wobei die Steuerung des Endgerätes über die Hersteller-Software (hier: Yamaha Studiomanager) geschieht.

5.1 USB Geräte Server

5.1.1 WI-FI-Netzwerk

Der hierfür verwendete USB Geräteserver der Firma Silex mit der Bezeichnung „SX-2000 WG“ gilt als äußerst einfach zu konfigurieren. Da das beiliegende Benutzerhandbuch sehr detailliert ausgeführt ist, wird an dieser Stelle auf dieses Manual verwiesen.

5.1.2 Beispiel: Software „Studiomanager“ (Yamaha)

Die hierbei verwendete Software „Studiomanager“ der Firma „Yamaha“ gilt ebenfalls als einfach zu konfigurieren. Aus diesem Grund wird an dieser Stelle auf Website der Herstellerfirma, bzw. auf die Installationsanleitung verwiesen.

5.2 Virtual Network Computing (VNC)

In diesem Kapitel wird eine Screensharing-Anwendung (VNC-Verbindung) vorgestellt, bei der man das Endgerät entweder mit einem Rechner oder mit einem Smartphone drahtlos steuert.

5.2.1 WI-FI-Netzwerk

Um eine drahtlose Screensharing-Anwendung zu benutzen, muss als erstes gewährleistet sein dass die beiden Geräte miteinander kommunizieren können. Die folgende Anleitung beschreibt den Aufbau einer WLAN-Verbindung.

5.2.1.1 Konfiguration unter Windows XP

Die einfachste Möglichkeit zwei Geräte drahtlos zu verbinden ist eine sog. Ad-Hoc-Verbindung. Um so eine Verbindung unter Windows herzustellen gehen Sie folgendermaßen vor:

1.) START→ VERBINDEN MIT → DRAHTLOSE NETZWERKVERBINDUNG wählen.

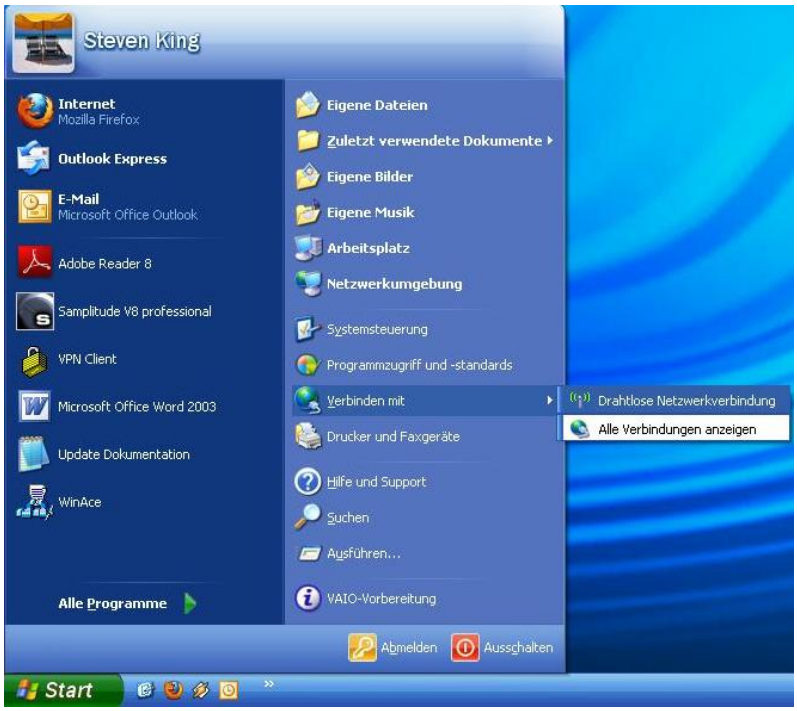

Abb. 5.1: Startmenü

2.) Wählen Sie ERWEITERTE EINSTELLUNGEN ÄNDERN

Abb. 5.2: Verfügbare Drahtlosnetzwerke anzeigen

3.) Wählen Sie in der Registerkarte „DRAHTLOSNETZWERKE“ „HINZUFÜGEN“

Abb. 5.3: Eigenschaften von Drahtlose Netzwerkverbindung

4.) Vergeben Sie jetzt einen Netzwerknamen, wählen Sie eine Datenverschlüsselung, einen Netzwerkschlüssel (Passwort), und aktivieren Sie das unterste Kontrollkästchen. Bestätigen Sie mit OK.

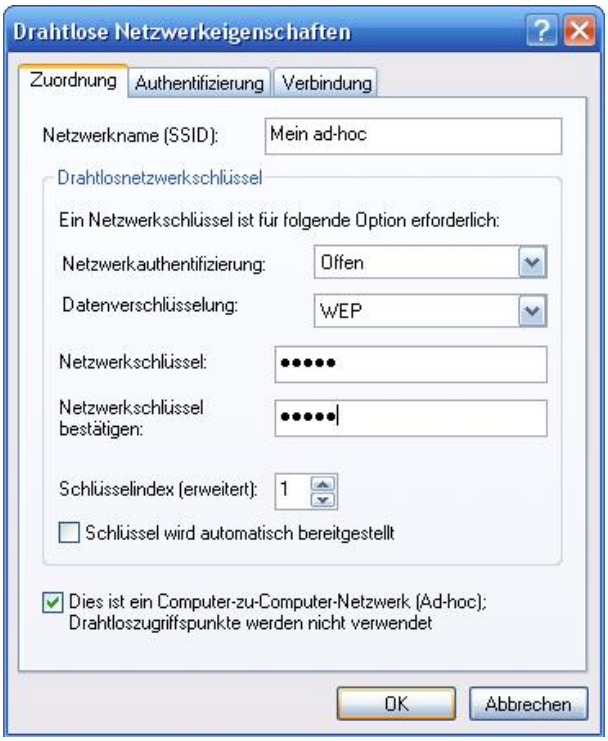

Abb. 5.4: Drahtlose Netzwerkeigenschaften

5.) Diese Verbindung müsste jetzt in der Liste der Bevorzugten Netzwerke angezeigt werden. Bestätigen Sie mit OK.

Abb. 5.5: Drahtlosnetzwerke

6.) Jetzt müsste Ihre Verbindung in den verfügbaren Drahtlosnetzwerken sichtbar sein. (Möglicherweise auch nur bei anderen Rechnern)

Abb. 5.6: Verfügbare Drahtlosnetzwerke

Falls Probleme auftreten sollten, könnte dies an Ihrer Firewall liegen. Versuchen Sie Ihre Firewall vorübergehend zu deaktivieren. Falls Sie die Windows-Firewall benutzen, können Sie diese folgendermaßen deaktivieren:

START→ VERBINDEN MIT → DRAHTLOSE NETZWERKVERBINDUNG wählen, ERWEITERTE EINSTELLUNGEN ÄNDERN wählen, auf die Registerkarte „ERWEITERT“ klicken (hier können Sie auch einstellen, ob jemand Ihre Internetverbindung mitbenutzen darf), auf „EINSTELLUNGEN“ klicken und die Windows-Firewall vorübergehend auf INAKTIV setzen.

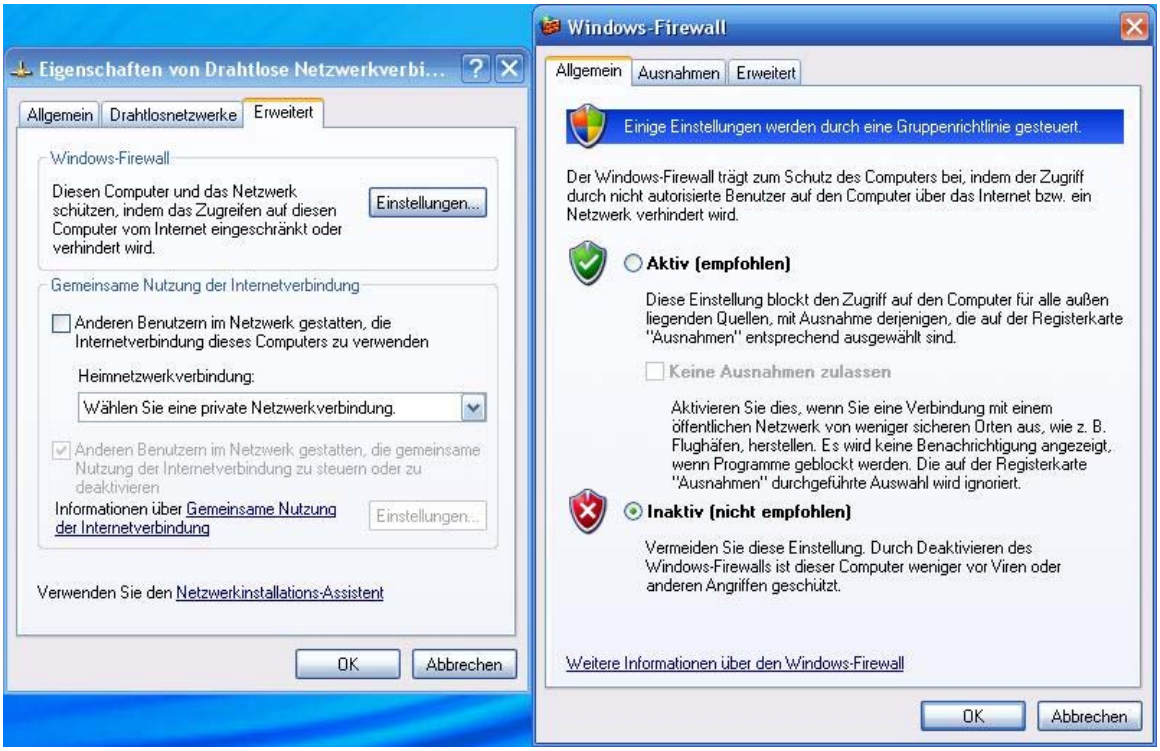

Abb. 5.7: Windows-Firewall

5.2.1.2: Konfiguration unter Mac OSX Snow Leopard:

Ad Hoc Netzwerk:

Mit Hilfe eines Ad Hoc Netzwerkes können Sie einfach und schnell ein Netzwerk anlegen.

Vorgehensweise:

Öffnen Sie zunächst den „SYSTEMEINSTELLUNGEN“ Dialog, und wählen Sie den Eintrag „NETZWERK“. Es erscheint das folgende Fenster:

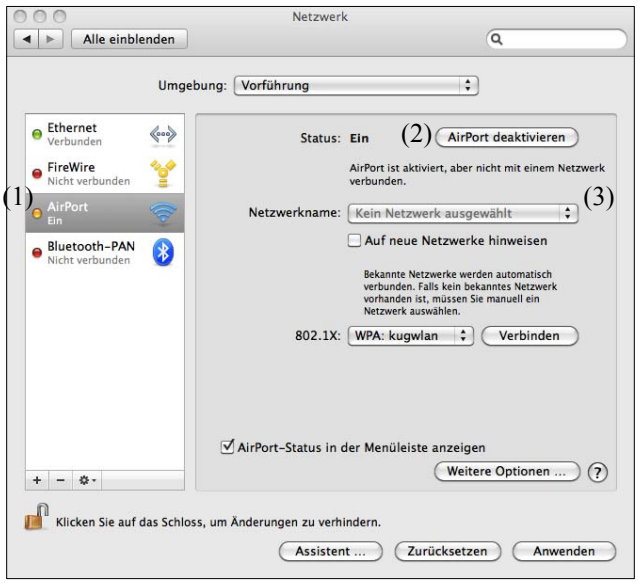

Abb. 5.8: Netzwerk

Wählen Sie links den Eintrag „AIRPORT“ aus (1). Falls Ihr Airport deaktiviert ist, aktivieren Sie ihn (2). Im Ausklappmenü „NETZWERKNAME“ (3) ist die Option: „NETZWERK ANLEGEN“ zu finden:

Abb. 5.9: „Computer-zu-Computer“-Netzwerk erstellen

Wählen Sie einen geeigneten Namen für Ihr Netzwerk (1). Sie sollten unbedingt die Option „KENNWORT ERFORDERLICH“ anwählen, um ein Passwort für das Netzwerk zu vergeben (2). Klicken Sie auf „OK“.

Haben Sie auf diese Weise ein Netzwerk angelegt, erscheint dieses bei allen Rechnern und Geräten, welche sich in Reichweite Ihres Mac´s befinden. [11]

Bei dieser Art von Netzwerk müssen Sie jedoch einige Dinge beachten:

- Sollte beim Erstellen des Netzwerkes nach dem Administrator-Kennwortes verlangt werden, Sie dies jedoch nicht wollen, können Sie diese Funktion ausschalten. Gehen Sie hierbei unter: SYSTEMEINSTELLUNGEN → NETZWERK → AIRPORT → WEITERE OPTIONEN → AIRPORT und wählen Sie den Eintrag „Administratorkennwort erforderlich für: Computer-zu-Computer-Netzwerke erstellen“ ab (1):

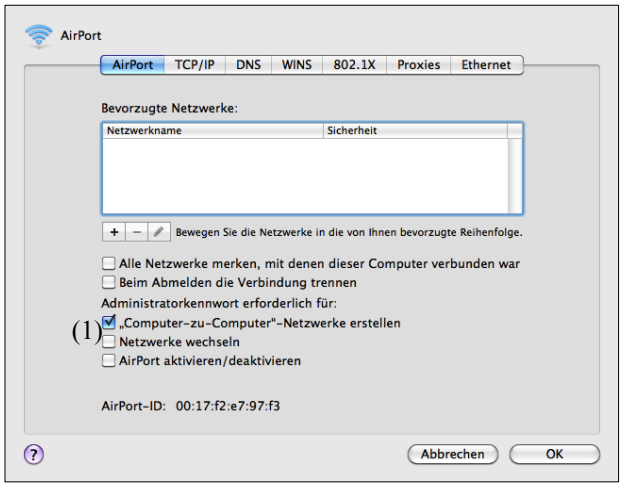

Abb. 5.10: Airport

- sollte sich der Rechner nach einer gewissen Zeit in den Ruhezustand schalten, ist es möglich, dass die Verbindung zum Endgerät abbricht und evtl. das Netzwerk neu aufgebaut werden muss. Passen Sie aus diesem Grund die Einstellungen im Dialog: „SYSTEMEINSTELLUNGEN - ENERGIE SPAREN“ Ihren Anforderungen an.

- sobald die Verbindung getrennt wird, steht das Netzwerk nicht mehr zur Verfügung, da es leider unter Mac OS X nicht möglich ist, diese Einstellungen zu speichern.

Da das Netzwerk nicht gespeichert wird, muss es jedes Mal erneut angelegt werden. Alternativ ist es möglich, das Anlegen des Netzwerkes mittels eines „AppleScriptes“ zu automatisieren.

Beim AppleScript handelt es sich um eine eigenständige Programmiersprache unter OS X. Sein Hauptverwendungszweck besteht in der Steuerung anderer Programme mittels einer sehr einfachen Programmiersprache, somit ist der User in der Lage, eigenständige Applikationen zur Automatisierung verschiedenster Arbeitsabläufe zu erstellen: [11]

Gehen Sie in Ihr PROGRAMME-Verzeichnis und öffnen Sie unter DIENSTPROGRAMME → APPLESCRIPT-EDITOR den Editor.

Geben Sie folgenden Code in den Eingabe-Bereich ein: [HARD]

```
property NetworkName : "C-zu-C-Netzwerk"
property NetworkPassword : "dreizehnZeich"
property CreateMenuName : "Netzwerk anlegen …"

-- Airport aktivieren
do shell script "networksetup -setairportpower en1 on"
--
try
do shell script "/usr/sbin/scselect " & NetworkName
delay 2

end try
tell application "System Events"
tell process "SystemUIServer"
tell menu bar 1
set menu_extras to value of attribute "AXDescription" of menu bar items
repeat with the_menu from 1 to the count of menu_extras
if item the_menu of menu_extras contains "Airport" then exit repeat
end repeat
tell menu bar item the_menu
perform action "AXPress"
delay 0.2
perform action "AXPress" of menu item CreateMenuName of menu 1
end tell
end tell
repeat until exists window 1
delay 0.5
end repeat
tell window 1
keystroke NetworkName
click checkbox 1
keystroke tab
keystroke NetworkPassword
keystroke tab
keystroke NetworkPassword
click pop up button 2
click menu item 2 of menu 1 of pop up button 2
delay 0.5
click button 1
end tell
end tell
end tell
```

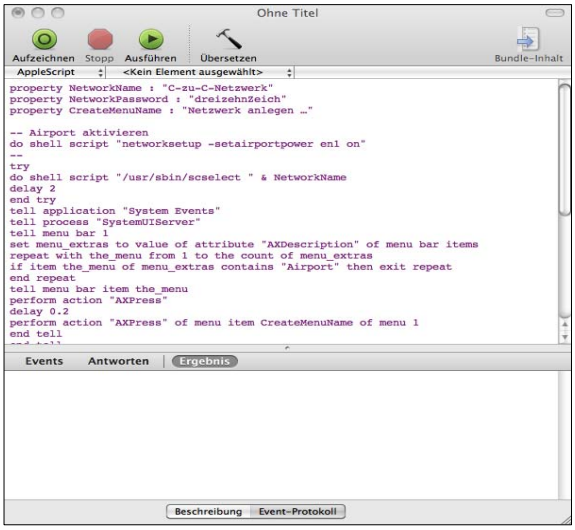

Abb. 5.11: Apple Script

Unter „property NetworkName“ geben Sie den gewünschten Netzwerk-Namen ein, unter „property NetworkPassword“ das gewünschte Passwort.

Unter ABLAGE → SICHERN UNTER können Sie nun ein eigenständiges Programm erstellen. Geben Sie einen Titel (1) für das Programm ein, und wählen Sie unter DATEIFORMAT (2) den Eintrag PROGRAMM. Nachdem Sie einen geeigneten Zielordner ausgewählt haben, klicken Sie auf SICHERN.

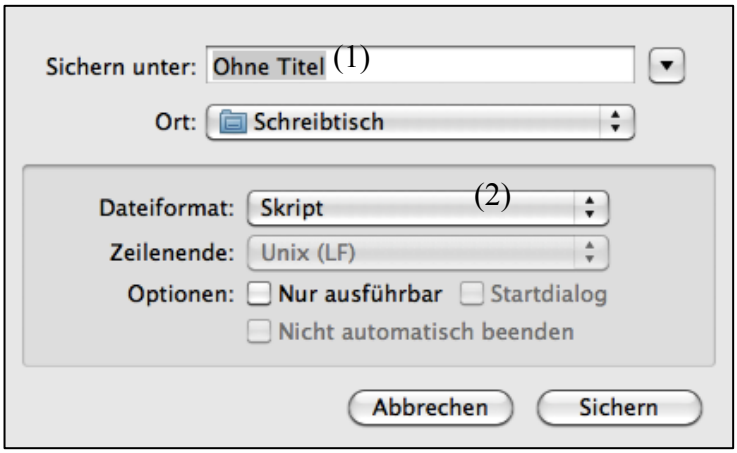

Abb. 5.12: Skript speichern

Nun haben Sie ein kleines Programm erstellt, welches ihnen die manuelle Konfiguration erleichtert. Sobald Sie es öffnen, erstellen Sie automatisch das gewünschte Netzwerk. [11]

Sollte ihnen diese Vorgehensweise umständlich erscheinen, da Sie ein solches Netzwerk öfters benötigen, gibt es auch noch eine weitere Möglichkeit:

Erstellung eines dauerhaften Ad-Hoc Netzwerkes

Über Umwege ist es auch möglich, ein dauerhaftes Ad-Hoc Netzwerk zu erstellen, das für folgende Anwendungen im Vergleich zu vorher genannten Möglichkeiten stabiler ist und bei welchem sich nach erfolgreicher Konfiguration auch alle beteiligten Geräte automatisch verbinden.

Gehen Sie folgendermaßen vor:

Öffnen Sie SYSTEMEINSTELLUNGEN → FREIGABEN, und wählen Sie den Eintrag INTERNETFREIGABEN aus, es erscheint folgendes Fenster:

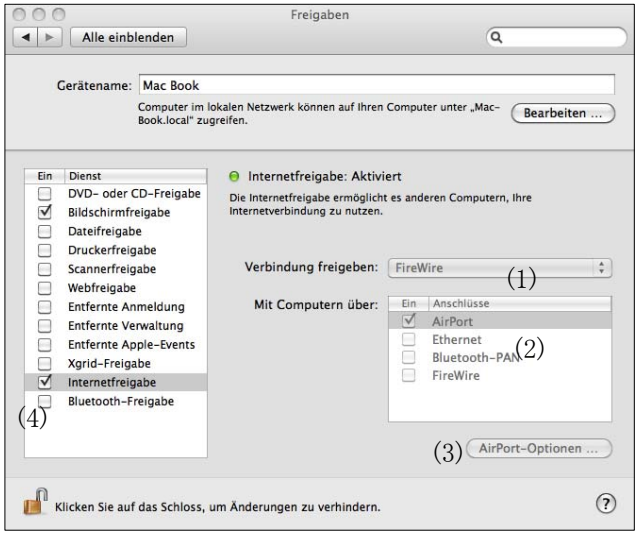

Abb. 5.13: Internetfreigaben

Wählen Sie bei „Verbindung freigeben“ den Eintrag FIREWIRE (1). Im Bereich „Mit Computern über“ setzen Sie ein Häkchen bei AIRPORT (2). Im Eintrag „Airport-Optionen“ (3) können Sie das Netzwerk wie weiter oben bereits beschrieben, konfigurieren. Nun ist es möglich, die Internetfreigabe frei zu schalten, indem Sie ein Häkchen bei INTERNETFREIGABE (4) setzten und den darauffolgenden Dialog mit START bestätigen.

Die Funktion „Internetfreigabe“ ist eigentlich dafür gedacht, den Rechner als Router zu nutzen und eine bestehende Internetverbindung mit anderen Geräten / Usern zu teilen, der Rechner fungiert als DHCP-Router. Daher wird empfohlen, z.B. eine Firewire-Verbindung freizugeben, welche nicht mit anderen Rechnern oder mit dem Internet verbunden ist, um unerwünschte Nebeneffekte zu vermeiden. [11]

Vorteil dieser Verbindung ist, dass Sie sich mit keinem anderen WI-FI Netzwerk (versehentlich) verbinden können, es permanent besteht und Sie es einfach über den Airport ein und ausschalten können.

Beachten Sie jedoch, dass falls Sie eine Internet-Sharing Anschluss verwenden, welches tatsächlich mit dem Internet verbunden ist, Sie Probleme bei der Konfiguration bekommen können, da DHCP die IP-Adresse wechseln kann (wodurch z.B. eine gespeicherte VNC Einstellung sich nicht verbinden kann).

Access-Point

Sollten Sie dauerhaft das gleiche Netzwerk benötigen, wird ein eigenständiger Access-Point empfohlen. Hierbei können Sie ein Netzwerk erstellen, und die Geräte, also Rechner/Tablets/etc. automatisch mit diesem Verbinden lassen.

Eine Konfigurationsanleitung für das Einrichten eines Access-Points (Router) erscheint an dieser Stelle trivial, verwenden Sie hierzu bitte die Bedienungsanleitung des entsprechenden Gerätes.

Für die automatische Verbindung unter OS X öffnen Sie folgenden Dialog: SYSTEMEINSTELLUNGEN → NETZWERK → AIRPORT → WEITERE OPTIONEN → AIRPORT und wählen Sie unter BEVORZUGTE NETZWERKE Ihr Netzwerk aus.

5.2.2 VNC: Rechner → Rechner

Da nun eine funktionierende WLAN-Verbindung zwischen den Geräten besteht, können wir nun beginnen die VNC-Verbindung zu konfigurieren.

5.2.2.1 VNC-Konfiguration unter Windows XP

Um eine VNC-Verbindung zwischen zwei Rechnern herzustellen, muss auf beiden Rechnern eine VNC-Software installiert werden. Wir haben uns hier entschieden, RealVNC 4.1.3 zu verwenden, da hier Client- und Serverversion kostenlos erhältlich sind.

Laden Sie sich dazu von der Hersteller-Homepage http://www.realvnc.com/ die Installationsdateien herunter.

VNC-Server-Konfiguration

Den Rechner, den man fernsteuern will, nennt man VNC-Server. Um auf diesem Rechner die VNC-Server-Software einzurichten gehen Sie folgendermaßen vor:

1.) Führen Sie die Installationsdatei aus, und folgen Sie den Anweisungen.

ACHTUNG: Wenn Sie nicht wollen, dass der Service-Modus bei jedem Systemstart automatisch startet, sondern den VNC-Server lieber manuell starten, deaktivieren Sie bei der Installation in folgendem Fenster bitte die unteren beiden Kontrollkästchen:

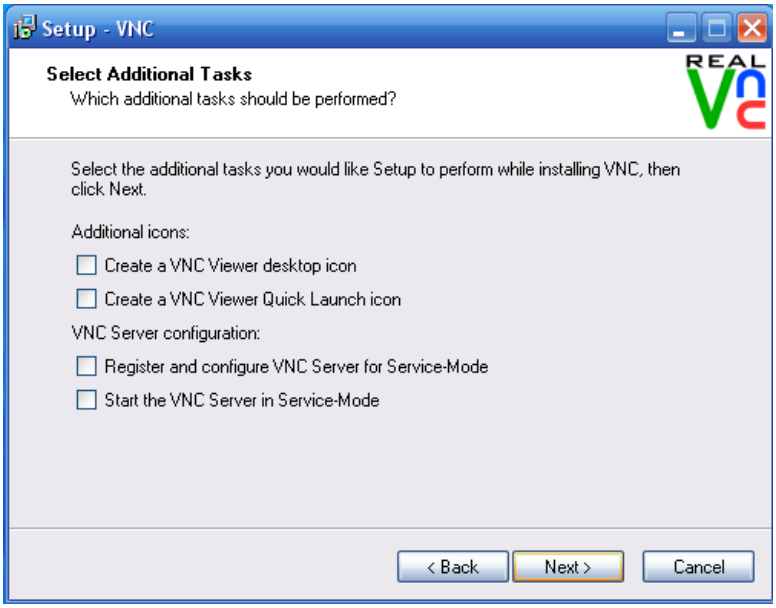

Abb. 5.14: Service-Mode-Einstellungen

2.) Nach der Installation können Sie den VNC-Server manuell starten, indem Sie „START→PROGRAMME→RealVNC→VNC Server 4 (User Mode)→Run VNC Server“ auswählen.

3.) Auf „START→PROGRAMME→RealVNC→VNC Server 4 (User Mode)→Configure User-Mode Settings“ können Sie jetzt ein Passwort vergeben. Klicken Sie dazu in der Registerkarte „AUTHENTICATION“ auf „CONFIGURE“:

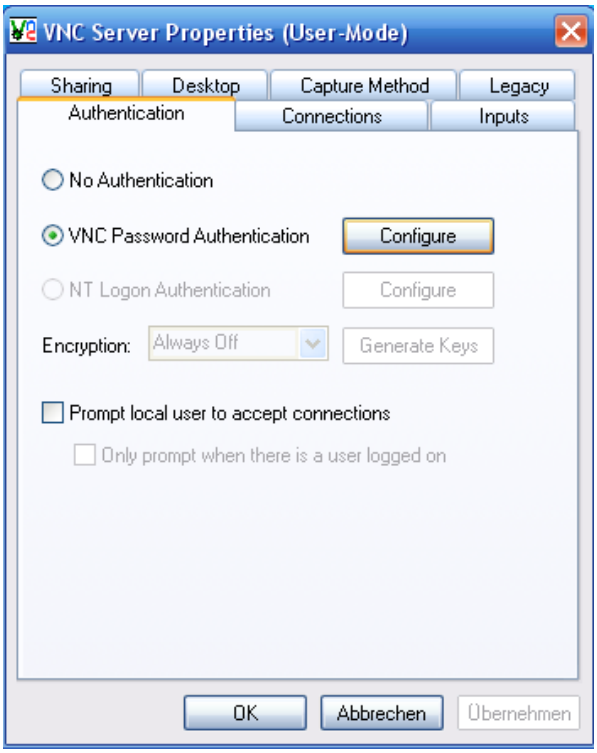

Abb. 5.15: Erstellen eines Passwortes

VNC-Client-Konfiguration an einem Rechner

Die Installation am VNC-Client (also dem Rechner, mit dem man fernsteuern will, auch „Viewer“ genannt) ist sehr simpel. Man installiert die VNC-Client-Software und wählt „START→PROGRAMME→RealVNC→VNC Viewer 4→Run VNC Viewer“ um ihn zu starten.

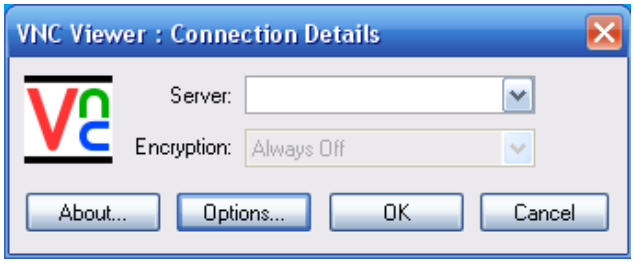

Abb. 5.16: VNC-Viewer-Oberfläche

Unter „OPTIONS“ kann man z.B. einstellen, in welcher Farbqualität man den Bildschirm-Inhalt des VNC-Servers dargestellt haben will, oder welche Ereignisse an den VNC-Server übertragen werden:

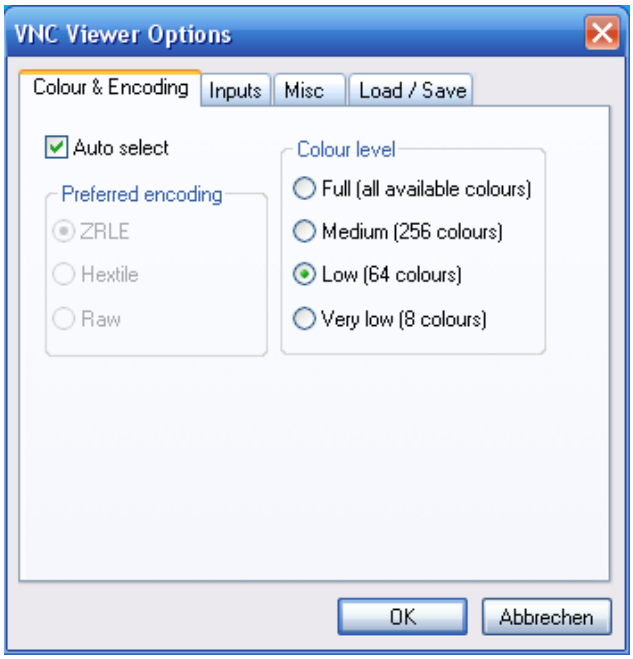

Abb. 5.17: Optionen im VNC Viewer

Falls Probleme auftreten, könnte eine Firewall dafür verantwortlich sein. Sie müssen ggf. in Ihrer Firewall-Konfiguration den TCP/IP bzw. UDP Port 5900 freischalten.

Sollten dennoch Probleme auftreten, versuchen Sie die Firewall vorübergehend zu deaktivieren.

5.2.2.2 Konfiguration unter Mac OS X

Konfiguration zu steuernder Rechner:

Mac OS X hat bereits einen entsprechenden VNC-Server im Betriebsprogramm integriert, welcher sehr einfach zu konfigurieren ist.

Gehen Sie wie folgt vor:

Öffnen Sie: SYSTEMEINSTELLUNGEN → FREIGABEN; es erscheint folgendes Fenster:

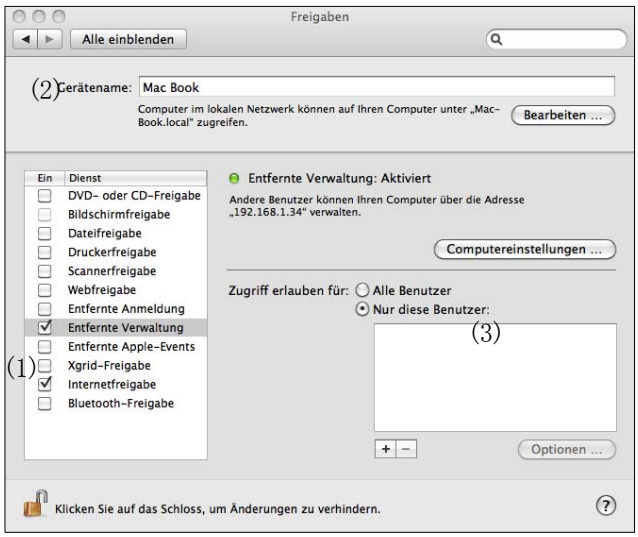

Abb. 5.18: Freigaben

Wählen Sie in der linken Spalte den Eintrag ENTFERNTE VERWALTUNG aus und setzten Sie davor ein Häkchen (1). Nun ist die Fernsteuerung über VNC (Windows) bzw. über „Apple Remote Control" (OS X) aktiv. Unter „Gerätename" können Sie eine Bezeichnung wählen, mit der die VNC Verbindung im Netzwerk sichtbar ist (2). Unter „Zugriff erlauben für" (3) können Sie definieren, welche Benutzer Zugriff auf Ihren Rechner haben dürfen (4).

Sollten Sie öfters ausschließlich mit zwei Apple-Rechnern arbeiten, empfiehlt sich die Anschaffung des Programms „Apple Remote Desktop“. Dieses ist optimiert für die Fernverwaltung unter OS X und bringt einige nützliche Features mit sich. In diesem Fall kommt (fast) analog zur oben beschriebenen Vorgehensweise statt des Menüpunktes „Bildschirmfreigabe“ der Menüpunkt „Entfernte Verwaltung“ zur Verwendung.

Näheres dazu entnehmen Sie bitte dem entsprechenden Manual bzw. der Website der Firma Apple.

5.2.3 Smartphone / Tablet → Rechner

Konfiguration zu steuernder Rechner:

Mac OS X hat bereits einen entsprechenden VNC-Server im Betriebsprogramm integriert, welcher sehr einfach zu konfigurieren ist.

Gehen Sie wie folgt vor:

Öffnen Sie: SYSTEMEINSTELLUNGEN → FREIGABEN; es erscheint folgendes Fenster:

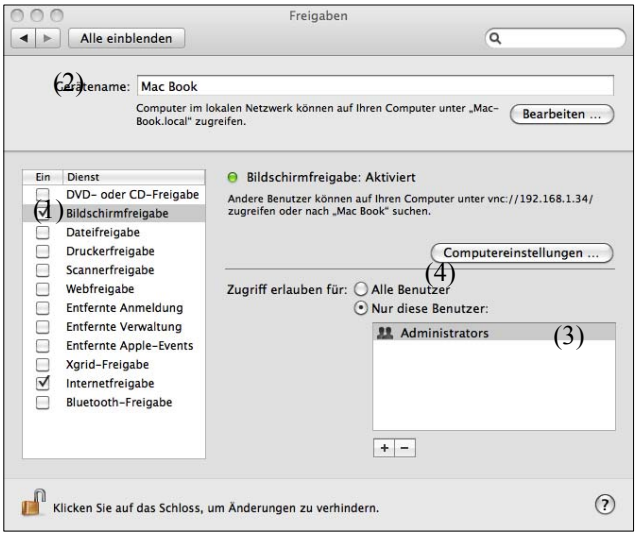

Abb. 5.19: Freigaben

Wählen Sie in der linken Spalte den Eintrag BILDSCHIRMFREIGABE aus und setzten Sie davor ein Häkchen (1). Nun ist die Fernsteuerung über VNC aktiv. Unter „Gerätename“ können Sie eine Bezeichnung wählen, mit der die VNC Verbindung im Netzwerk sichtbar ist (2). Unter „Zugriff erlauben für“ (3) können Sie definieren, welche Benutzer Zugriff auf Ihren Rechner haben dürfen (4).

Im Nächsten Schritt wählen Sie den Eintrag COMPUTEREINSTELLUNGEN (5). Es erscheint folgendes Fenster:

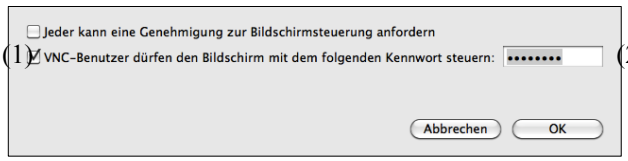

Abb. 5.20: Passwort

Setzen Sie unter „VNC-Benutzer dürfen den Bildschirm mit folgendem Kennwort steuern:“ ein Häkchen (1). Nun können Sie ein Passwort definieren, mit welchem der Rechner gesteuert werden kann (2). Mit OK bestätigen Sie die Eingabe. Schließen Sie die Fenster.

Nun haben Sie den Rechner für eingehende VNC-Verbindungen konfiguriert. Ist eine solche Verbindung aktiv, wird dies in der oberen Menüleiste mit einem Monitor und einem Fernglas gekennzeichnet. [1]

Konfiguration Smartphone:

Netzwerk-Konfiguration: (iOS)

(alle nachfolgenden Konfigurationen wurden mit einem Apple iPod 2G durchgeführt)

Zuallererst ist es erforderlich, dass sich das entsprechende Steuerungsgerät im gleichen Netzwerk wie der zu steuernde Rechner befindet.

Öffnen Sie: EINSTELLUNGEN → WIFI. Es erscheint folgendes Fenster:

Abb. 5.21: WIFI Smartphone

Falls der integrierte Wireless LAN ausgeschaltet ist, schalten Sie diesen ein (1) Wählen Sie nun unter (2) Ihr zuvor erstelltes Netzwerk aus. Mit einer Betätigung des blauen Pfeils neben dem Netzwerknamen (3) öffnen Sie den Einstellungs-Dialog zu Ihrem Netzwerk. Es erscheint folgendes Fenster:

Abb. 5.22: automatische Netzwerkverbindung

Um eine automatische Verbindung mit Ihrem Netzwerk herzustellen, betätigen Sie den entsprechenden Schieberegler beim Eintrag „Autom. Verbinden“ (1). Im Bereich „IP Adresse“ können Sie nochmals Ihre Netzwerk-Einstellungen kontrollieren. Beachten Sie ggf. die Verwendung privater IP-Adresse (Siehe Kap. 2.1.2.)

Nun besteht eine Verbindung zwischen Ihrem iOS Gerät und Ihrem Rechner, somit sind beide bereit für die entsprechenden Steuerungskonfigurationen.

Steuerungs-Konfigurationen für VNC Viewer (iOS/Android)

Es gibt verschiedenste Möglichkeiten bzw. Software-Lösungen, mit denen eine VNC Verbindung herzustellen ist. Näheres entnehmen Sie bitte den Kapiteln 2.3.1 bzw. Anhang A.

In verschiedensten Versuchen im Laufe dieser Arbeit hat sich die Software „VNC Viewer“ der Firma „RealVNC“ als äußerst stabil und einfach zu bedienen erwiesen. Zwar befinden sich etliche Freeware-Lösungen auf dem Markt, die Investition in dieses „App“ lohnt sich jedoch in jedem Fall. Alternativ können Sie auch Lösungen aus Anhang A versuchen.

Die nachfolgende Anleitung wurde unter iOS erstellt. Da die Software auch für Android erhältlich ist, sind die Schritte 1 zu 1 übertragbar:

Nach erfolgreichem Kauf und Installation der Software, öffnen Sie das Programm über den Icon und betätigen Sie im unteren Rand des Bildschirmes den Eintrag „Available“. Nun werden alle möglichen VNC Verbindungen nach ihren Namensgebungen gelistet:

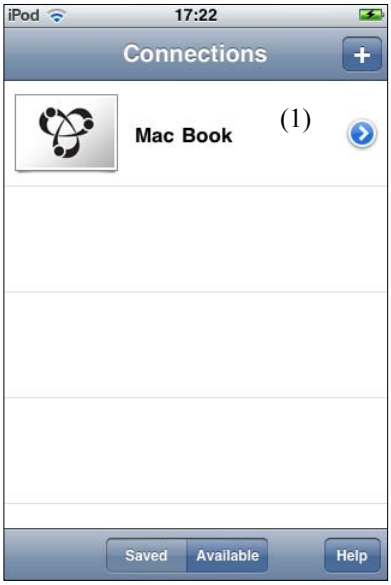

Abb. 5.23: Connections

Wählen Sie das zuvor konfigurierte Netzwerk aus (1) und geben Sie im folgenden Fenster das entsprechende Passwort ein. Der Bildschirm des Rechners erscheint nun auf Ihrem Gerät:

Abb. 5.24: Desktop des Rechners

Um die Geschwindigkeit zu optimieren, verwenden Sie das Programmeinstellungen Menü, dieses erreichen Sie unter dem Icon „i“ (1). Wählen Sie den Eintrag „Picture Quality“. Es erscheint folgendes Fenster:

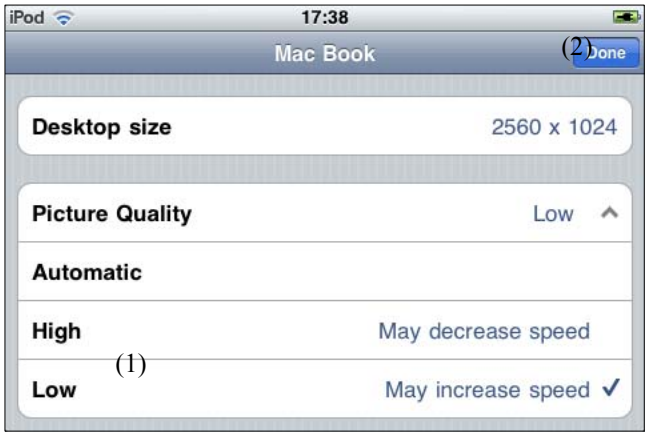

Abb. 5.25: Picture Quality

Wie bereits in Kap. 2.3.1. erläutert, hängt die Geschwindigkeit der Steuerung mit der Darstellungsauflösung zusammen. Da für den Zweck der Steuerung die grafische Darstellung sekundär ist, wählen Sie den Eintrag: „Low“ (1). Weiters können Sie diesem Menüpunkt diverse interessante Informationen entnehmen, wie z.B. über Desktop Größe und Übertragungsrate. Bestätigen Sie Ihre Wahl mit „Done“ (2).

Die Konfiguration ist nun erfolg und Sie haben die Möglichkeit, Ihren Rechner, bzw. die gewünschte Software zu steuern.

Speicher einer dauerhaften Verbindung

Die soeben erläuterte Konfiguration ermöglicht eine sehr schnelle und einfache Steuerung einer beliebigen VNC Verbindung. Verwenden Sie jedoch oftmals die gleiche Konfiguration, liegt es nahe, diese auf Ihrem Gerät zu speichern, um z.B. nicht bei jeder Verbindung das Passwort eingeben zu müssen.

Zu diesem Zweck öffnen Sie das Programm und wählen im Startbildschirm den Eintrag „+“ am rechten, oberen Rand. Es erscheint folgendes Fenster:

Abb. 5.26: Details

Geben Sie nun die IP Adresse (1) bzw. den Namen der VNC Verbindung (2) Ihres Rechners ein. Diese entnehmen Sie entweder dem Netzwerk-Menü Ihres Rechners oder Sie notieren sich einfach die Daten der oben genannten Verbindung unter „Available“. Betätigen Sie den Schieberegler um das Passwort permanent zu speichern (3) und setzen Sie die Bildqualität aufgrund der zuvor genannten Argumente auf „Low“ (4).

Bestätigen Sie zum Abschluss Ihre Eingaben mit „Connect“ (5) und geben Sie im folgenden Fenster das Passwort ein.

Ihre Konfiguration ist nun gespeichert; wollen Sie die Verbindung später erneut herstellen, wählen Sie einfach den entsprechenden Eintrag im Startbildschirm.

Detaillierte Steuerungshinweise und Bedienung entnehmen Sie bitte dem entsprechenden Manual bzw. Hilfe Foren, da Ausführungen darüber den Rahmen dieser Arbeit sprengen würden.

5.3 OSC Konfiguration unter Mac OS X

Wie zuvor erwähnt, kommunizieren die Geräte im Netzwerk mit Hilfe des Protokolls „Open Sound Control“ (siehe Kapitel 2.3.2). Leider besteht zum Zeitpunkt der Verfassung dieser Arbeit eine mangelhafte Unterstützung dieses Protokolls auf Seiten entsprechender Hard- und Software. Aus diesem Grund ist eine Konvertierung auf das weit verbreitete und standardisierte „Musical Instrument Digital Interface“ (MIDI) (siehe Kap. 2.3.3) von Nöten, welches in folgenden Schritten erläutert wird. Zur Verwendung kommt das Programm „OSCulator“. Herstelleradresse bzw. Downloadhinweise sind im Literaturhinweis-Verzeichnis angeführt.

Zuallererst ist die Herstellung eines WLAN Netzwerkes notwendig:

5.3.1 Wi-Fi Netzwerk

Für die Konfiguration des Wireless LAN Netzwerkes beachten Sie bitte das vorhergegangene Kapitel (5.2.1), da die Konfiguration hierfür analog geschieht.

5.3.2 Erstellen einer geeigneten Mix-Oberfläche: [TOUCH]

Nach erfolgreichem Download und Installation des Programms „TouchOSC-Editor“ vergewissern Sie sich zuallererst, dass Sie die aktuellste Version besitzen. Falls nicht, updaten Sie die Applikation, da gewisse Konfigurationsmenüs in älteren Versionen nicht vorhanden sind. [2]

Um eine Mix-Oberfläche erstellen zu können öffnen Sie zuallererst das soeben genannte Programm. Es öffnet sich folgendes Fenster:

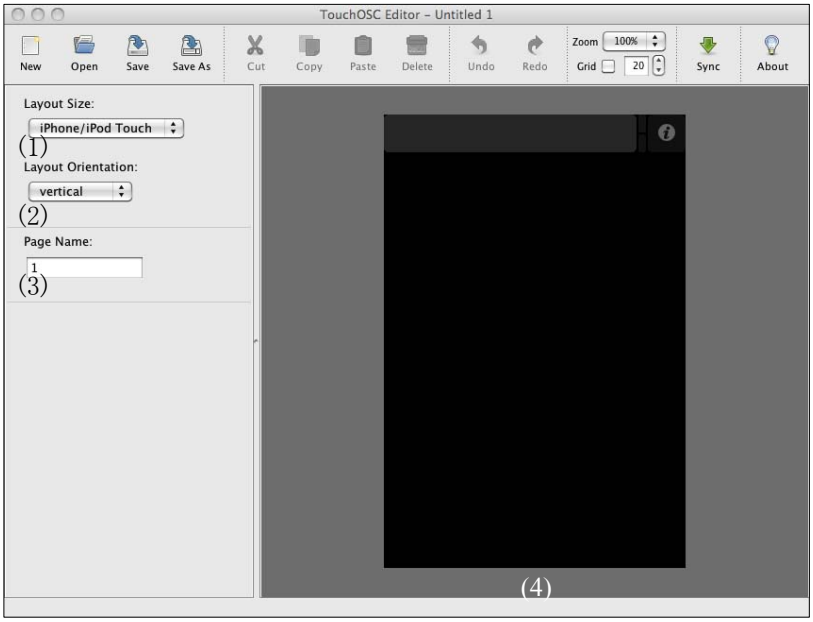

Abb. 5.27: TouchOSC Editor

Wählen Sie im linken, oberen Abschnitt unter dem Menüpunkt „Layout Size“ (1) Ihr entsprechendes Gerät aus. Wählen Sie die gewünschte Orientierung (2) und geben Sie der Seite, welche Sie bearbeiten, einen Namen (3). Es ist zu empfehlen, das Raster einzuschalten, da dies die Konfiguration enorm erleichtert. Wählen Sie eine geeignete Auflösung für das Raster. Ein Rechtsklick auf der Seitenoberfläche (4) öffnet die Bedienelemente-Bibliothek.

Eine Ausführung über die einzelnen Bedienelemente erscheint an dieser Stelle nicht sinnvoll, aus diesem Grund wird auf das entsprechendes Manual bzw. diverse Foren verwiesen. In der nachfolgenden Anleitung werden zum Zwecke der Verdeutlichung lediglich ein vertikaler Schieberegler und ein ON/OFF Button konfiguriert. Die Erstellung mehrerer Bedienelemente geschieht analog dazu.

Fügen Sie die Elemente „Fader V“ und „Toggle Button“ der Oberfläche hinzu und benennen Sie sie gegebenenfalls. Wählen Sie nun den Schieberegler aus, es erscheint folgendes Fenster:

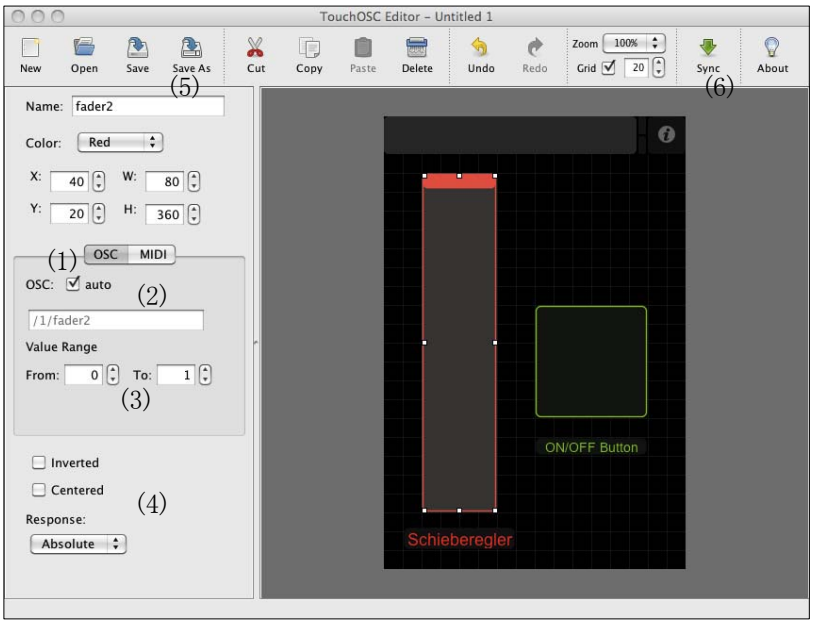

Abb. 5.28: Erstellen einer Oberfläche

Nach erfolgreicher Benennung und Farbgebung wählen Sie OSC als Übertragungsprotokoll aus (1) und stellen Sie sicher, dass OSC auf „auto“ gestellt ist (2). Wählen Sie einen gewünschten Wertebereich (3). Im folgenden Bereich (4) können Sie die Daten invertieren (umkehren), mittels Centered den Fader in Mittenposition stellen und auf absolute oder relative Empfindlichkeit stellen.

Es ist auch möglich, als Übertragungsprotokoll „MIDI“ zu verwenden. Dies hat jedoch einige Einbußen in Punkto Stabilität zur Folge.

Wiederholen Sie diese Schritte für den ON/OFF Button.

Sie haben eine Oberfläche erstellt. Um diese nun auf Ihr Gerät zu exportieren, speichern Sie zuallererst die Vorlage unter einem geeigneten Namen (5). Stellen Sie sicher, dass Ihr WLAN

Netzwerk aktiv ist (obere Menüleiste). Wählen Sie den Icon „Sync“ (6). Das Programm ist nun für eine Synchronisation mit Ihrem Gerät bereit.

Nach erfolgreichem Download und Installation des Programms für Ihr Gerät, stellen Sie sicher, dass sich Ihr Gerät im gleichen Netzwerk befindet wie der Rechner. Öffnen Sie die Applikation. Es erscheint folgendes Fenster:

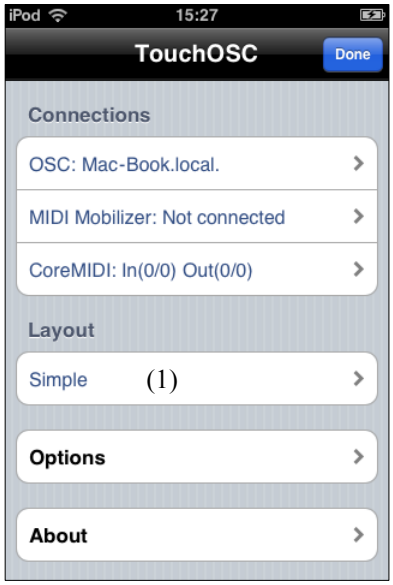

Abb. 5.29: TouchOSC am Smartphone

Wählen Sie den Menüpunkt „Layout“ (1) und im nachfolgenden Fenster den Menüpunkt „Add“. Wählen Sie Ihren Rechner aus, es erfolgt die Synchronisation. Ihre Oberfläche ist nun im Menüpunkt „Layout“ zu finden und auszuwählen.

Nun erfolgt die Konfiguration Ihres Gerätes.

5.3.3 Konfiguration am Smartphone / Tablet (iOS/Android)

(Alle nachfolgenden Konfigurationen wurden mit einem Apple iPod Touch 2G erstellt)

Über das Startfenster des Programms „TouchOSC“ können Sie alle notwendigen Konfigurationen durchführen:

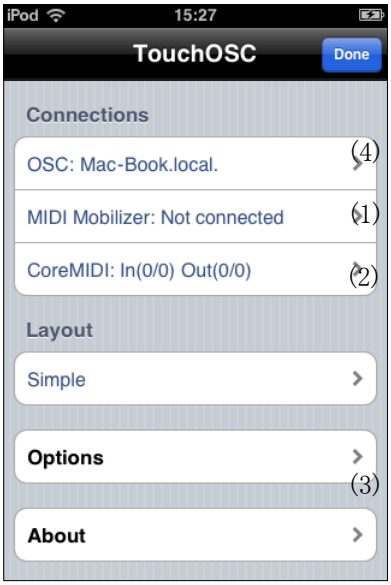

Abb. 5.30: Konfiguration TouchOSC

Sind Sie im Besitz eines „MIDI Mobilizers“ der Firma Line6 (MIDI Interface für Apple iOS Geräte), dann können Sie diesen unter dem Menüpunkt „MIDI Mobilizer“ konfigurieren. (1)

Es ist auch möglich, anstatt das OSC Protokoll MIDI zu verwenden, vorausgesetzt die Oberfläche wurde unter MIDI konfiguriert. Aufgrund diverser Stabilitätsprobleme (näheres siehe Kap. 6: Anhang A) ist dies jedoch nicht ratsam. Falls doch gewünscht, können Sie unter dem Menüpunkt „CoreMIDI“ Ihren MIDI-Port konfigurieren. (2)

Im Menüpunkt „Options“ können Sie verschiedenste Programmfeatures einstellen, näheres entnehmen Sie bitte dem Manual bzw. entsprechenden Foren. (3)

Für die Netzwerk-Konfigurationen wählen Sie den Menüeintrag OSC (4) und betätigen Sie den nachfolgenden Schiebebutton. Es erscheint folgendes Fenster:

Abb. 5.31: Einstellen der Ports

Unter „Host“ wählen Sie Ihr Netzwerk. (1)

Unter „Port (outgoing)“ wählen Sie den OSC Port, auf dem Ihr Gerät sendet. (2)

Unter „Port (incoming)“ wählen Sie den OSC Port, auf dem das Gerät empfängt. (3)

Ist Ihr Netzwerk korrekt konfiguriert, erscheint die IP-Adresse des Rechners. (4)

Kehren Sie ins Startmenü zurück und bestätigen Sie Ihre Einstellungen im rechten oberen Bereich mit „Done“. Es erscheint Ihre zuvor erstellte Oberfläche, welche nun für Steuerungsoperationen bereit ist.

Konfigurieren Sie nun Ihren Rechner mittels folgender Anleitung:

Rechnerkonfiguration unter Max OS X („OSCulator“) [OSC]

Nach erfolgreichem Download und Installation des Programms „OSCulator“ öffnen Sie es. Unter FILE → NEW erstellen Sie eine neue Datei. Es erscheint folgendes Fenster:

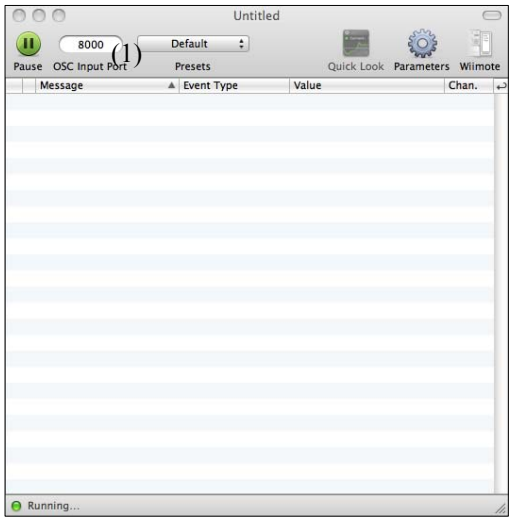

Abb. 5.32: OSCulator

Geben Sie im Feld „OSC Input Port“ (1) den zuvor bei Ihrem Steuerungsgerät eingestellten OSC Port ein. Versichern Sie sich, dass sich das Gerät und Ihr Rechner im gleichen Netzwerk befinden.

Sobald Sie am Gerät einen der beiden Regler betätigen, erscheint unter „Message“ die Bezeichnung des Eingabeelements:

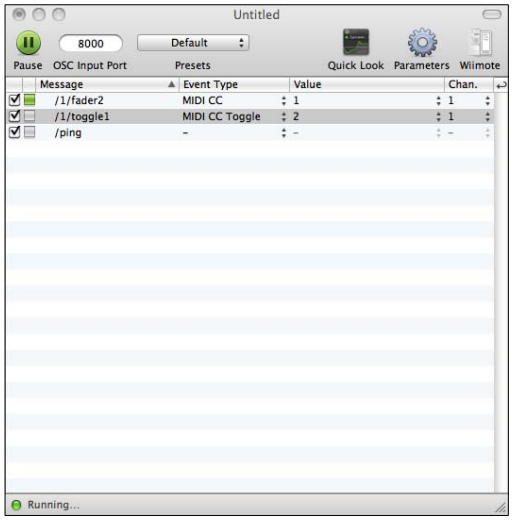

Abb. 5.33: empfangene Messages im OSCulator

Unter „Quick Look“ können Sie die Detektion der OSC Message durch das Programm verfolgen.

Klicken Sie neben einem dieser Regler in den Bereich „Event Type“ und definieren Sie die Art der Konvertierung, z.B. MIDI CC (näheres siehe Kap. 2.3.3), weisen Sie unter „Value“ einen MIDI Wert und unter „Chan.“ einen MIDI Kanal zu. Wiederholen Sie diese Schritte bei jedem Ihrer Regler.

Betätigen Sie den Icon „Parameters“ und wählen Sie den Eintrag „I/O“. Es erscheint folgendes Fenster:

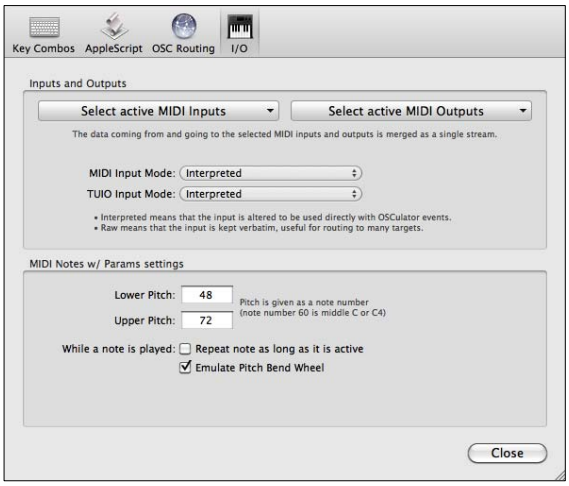

Abb. 5.34: Input/Output-Konfiguration

In diesem Dialog können Sie die MIDI Ports konfigurieren.

Unter SELECT ACTIVE MIDI INPUT können Sie den Input Port definieren. Dieser ist besonders für Feedback-Nachrichten für die Synchronisation des zu steuernden Gerätes und Ihrer Oberfläche wichtig.

Unter SELECT ACTIVE MIDI OUTPUT können Sie den Output Port definieren. Dieser ist für die Steuerung zuständig, somit definieren Sie hier den Input Port Ihres MIDI Gerätes.

Alternativ können Sie bei beiden Menüpunkten den Eintrag „OSCulator In“ bzw. „OSCulator Out“ wählen, in diesem Fall müssen Sie auch in Ihrem zu steuernden Gerät/Software diesen Eintrag auswählen.

Mit CLOSE kehren Sie zum Hauptmenü zurück.

Nun sollte bei Betätigung eines Reglers am Gerät bei Ihrem zu steuernden Gerät / Software eine MIDI Detektion zu erkennen sein. Falls nicht, wiederholen Sie bitte oben genannte Schritte bzw. kontrollieren Sie Ihr MIDI Routing.

Weisen Sie nun in Ihrem zu steuernden Gerät / Software den ankommenden MIDI Nachrichten die entsprechenden Regler und Buttons zu. Näheres dazu entnehmen Sie bitte dem Kapitel 2.3.3. bzw. der Bedienungsanleitung Ihres Gerätes / Software.

6 Setup Erweiterungen zur Erhöhung der Sicherheit und Stabilität

6.1 Access Points, Repeater

Wie schon in Kapitel 2.2.3 erwähnt, erlaubt die Kombination von Access Points und eines Distribution Systems den Aufbau eines WLANs mit beliebiger Ausdehnung und Komplexität.

Somit ist es möglich dass man z.B. im ganzen Gebäude eine gute Empfangsqualität realisiert. Und dies wirkt sich natürlich auf die Geschwindigkeit und Stabilität der Übertragung aus.

Es ist auch möglich mehrere Access Points ausschließlich drahtlos miteinander zu verbinden. Hierbei werden die Datenframes erst komplett eingelesen, an den nächsten Access Point umadressiert und danach ausgesendet. Dieses Verfahren entspricht einer einfachen Repeater-Funktion. Bei diesem Repeater-Modus entstehen natürlich Latenzzeiten, woraus sich logische Grenzen in der Anzahl der Access Points ergeben, die quasi hintereinander geschaltet werden können, um größere Distanzen zu überbrücken [6].

6.2 Antennen

Antennenprinzip

Den Grundbaustein einer Antenne stellt ein Parallelschwingkreis dar, in dem die Energie zwischen Spule und Kondensator hin- und herpendelt. Verkleinert man nun die Spule auf eine Windung und zieht die Platten des Kondensators so weit auseinander, dass sich die Kondensatorplatten an den Enden des Leiters (bzw. der Spule) befinden, so erhält man einen sog. offenen Schwingkreis. Dieser stellt die Grundform jeder Antenne dar. Der Strom erzeugt dabei um die Antenne ein ringförmiges Magnetfeld und die Spannung ein elektrisches Feld zwischen den Enden der Antenne.

Beide Felder werden im Raum abgestrahlt, wobei die magnetischen und elektrischen Wechselfelder senkrecht zueinander stehen und die elektromagnetische Strahlung einer Antenne bilden [6].

Antennengewinn

Mit dem sog. Antennengewinn (in engl. Literatur als „gain“ bezeichnet) wird angegeben, in welcher Höhe die Antenne in der Hauptabstrahlrichtung ihre Leistung abgibt bzw. aufnimmt. Dabei stellt man einen Vergleich zu einem isotropen Kugelstrahler her und beschreibt, wie viel Leistung man diesem zufügen muss, damit er dieselbe Strahlungsleistung in dieser Hauptabstrahlrichtung abgibt.

Ein isotroper Kugelstrahler ist ein Modell einer idealen, verlustlosen Antenne, die elektromagnetische Leistung in alle Richtungen gleichmäßig abstrahlt.

Für den Empfangsfall ist der Antennengewinn definiert als Verhältnis der in Hauptabstrahlrichtung empfangenen Leistung zur Empfangsleistung des isotropen Kugelstrahlers.

Um darzustellen, dass bei der Angabe des Antennengewinns der isotrope Kugelstrahler als Vergleich zugrunde gelegt wird, gibt man den Antennengewinn in dBi (dB isotrop) an [6].

Wie auch bei der Richtcharakteristik eines Lautsprechers oder Mikrofons, wird die Abstrahlcharakteristik einer Antenne in Polardiagrammen dargestellt. Hier wird jeweils für die horizontale und die vertikale Ebene ein Polardiagramm angegeben. Wobei je nach Darstellungsart entweder der äußere Kreis die richtungsabhängige Maximalleistung repräsentiert (0dB-Linie) und nach innen der relative winkelabhängige Abfall der abgestrahlten Leistung in dB aufgetragen ist, oder (wie in den folgenden Abbildungen) die Gesamtleistung den 0dB-Kreis definiert, und man somit den Antennengewinn direkt ablesen kann.

Also unterscheidet sich nur die Skalierung. Bei der ersten Darstellungsart ist die Maximalleistung die Bezugsgröße, in der zweiten Darstellungsart wird die Gesamtleistung als Bezugsgröße herangezogen.

Omnidirektionale Antenne

Omnidirektionale Antennen haben in der horizontalen Ebene einen Öffnungswinkel von 360°, weshalb man auch von Rundstahlern spricht. Auch interne Notebookantennen haben annähernd eine Rundstrahlcharakteristik.

Eine Dipol-Antenne gehört zu der Gruppe der Omni-Antennen und weist einen typischen Antennengewinn von 2 bis 2,2 dBi auf, wobei der vertikale Öffnungswinkel 70° bis 80° beträgt [6].

In Abb. 6.1 ist die Richtcharakteristik einer Dipol-Antenne dargestellt:

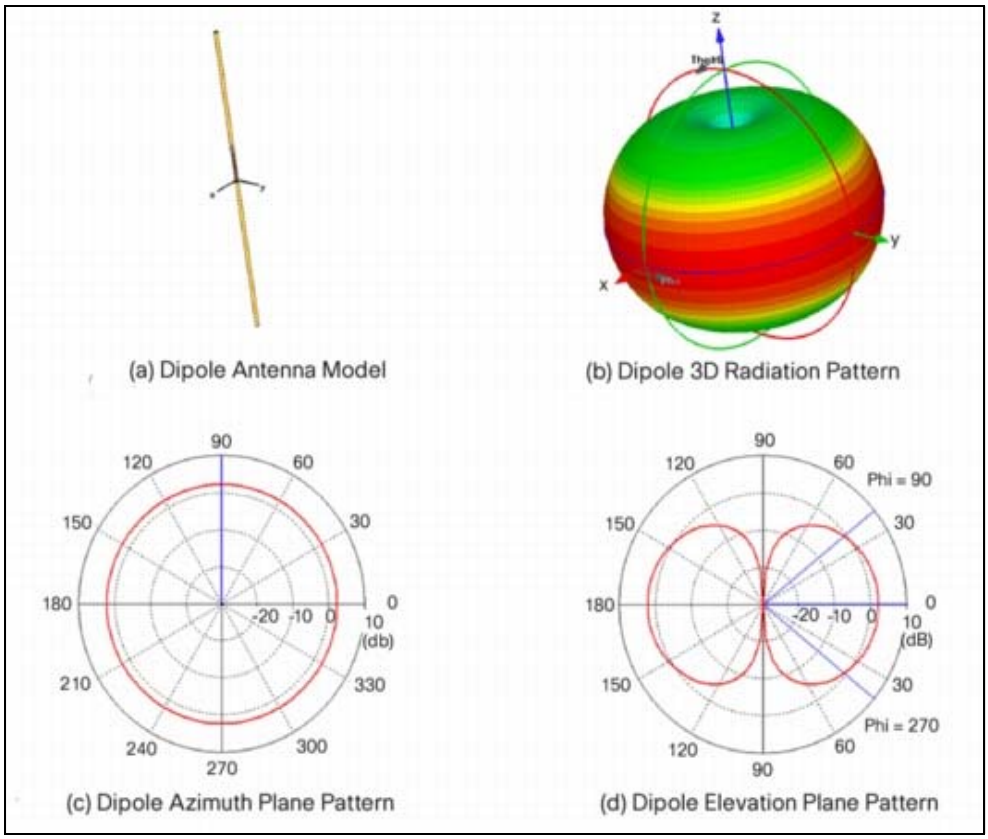

Abb. 6.1: Richtcharakteristik einer Dipol-Antenne (Quelle: [CISCO])

Omni-Antennen können durch ihre Bauweise auch einen größeren Antennengewinn erzielen. Indem man mehrere Dipole zusammenschaltet und übereinander anordnet, kann eine stärkere Richtwirkung erzielt werden. Je größer die Anzahl dieser Dipole ist, desto mehr Antennengewinn wird erreicht, und desto kleiner wird der vertikale Öffnungswinkel. Diese Antennen werden auch als Gewinnrundstrahler bezeichnet.

Hier sei noch zu erwähnen, wie der Antennengewinn mit dem Öffnungswinkel zusammenhängt.

Der Öffnungswinkel ist der Winkel zwischen jenen zwei Punkten, an denen die Leistung gegenüber dem Maximum auf die Hälfte (-3dB) abgesunken ist. Deshalb spricht man auch von der Halbwertsbreite oder 3-dB-Breite [6].

Mehr Antennengewinn bedeutet jetzt, dass die Hauptkeule schmäler wird und somit wird auch der Öffnungswinkel kleiner. Z.B. verfügt eine Omni-Antenne mit 12 dBi Gewinn über einen Öffnungswinkel von gerade einmal 7°. Deshalb muss immer ein Kompromiss zwischen Reichweite und Strahlungsbreite gefunden werden.

Abb. 6.2 zeigt eine Omni-Antenne mit einem Antennengewinn von 5,8 dBi:

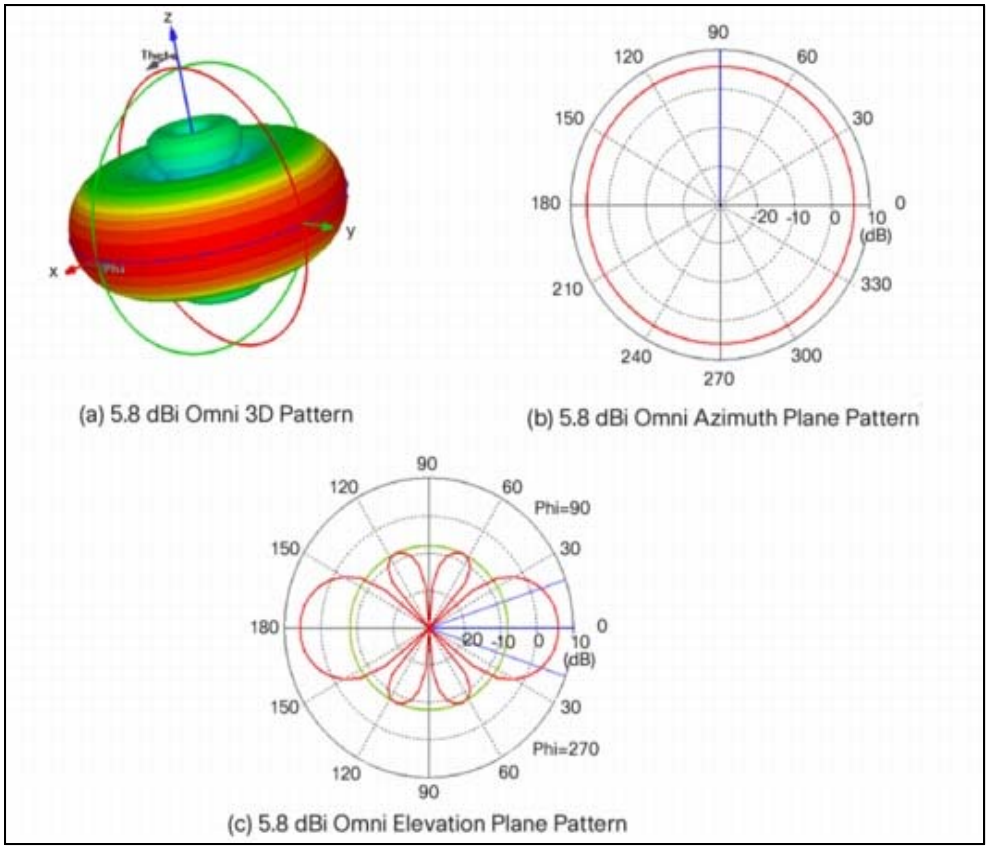

Abb. 6.2: Richtcharakteristik einer omnidirektionalen Antenne mit Gewinn (Quelle: [CISCO])

Patch-Antennen

Patch-Antennen sind durch ihre flache Bauweise sehr gut für die Wandmontage geeignet. Sie erzielen sowohl in vertikaler als auch in horizontaler Ebene eine Richtwirkung.

Durch Bildung eines Arrays von mehreren solchen Patch-Antennen lässt sich die Richtwirkung noch erheblich verstärken. Diese Arrays werden auch Panel-Antennen genannt und bieten einen typischen Antennengewinn von 12 bis 14 dBi [6]. (Siehe Abb. 6.3 und 6.4)

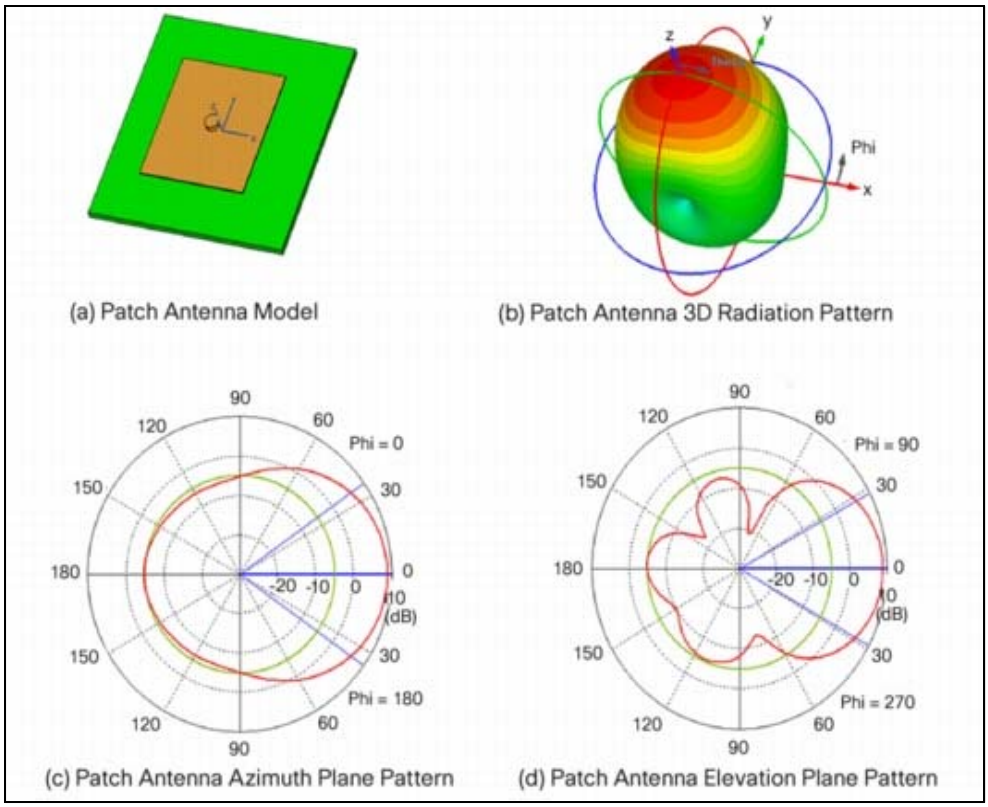

Abb. 6.3: Richtcharakteristik einer Patch-Antenne (Quelle: [CISCO])

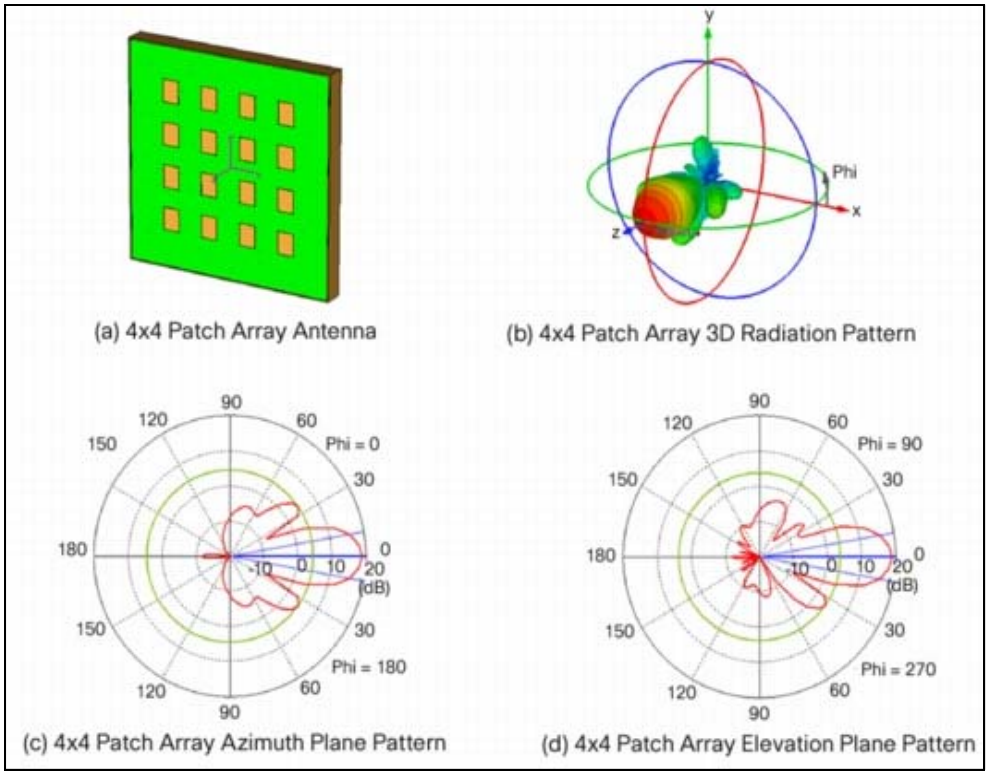

Abb. 6.4: Richtcharakteristik eines Arrays von 16 Patch-Antennen (Quelle: [CISCO])

Yagi-Antenne

Yagi-Antennen sind Richtfunkantennen die aus mehreren Dipolen gebildet werden. Der Aufbau ist charakterisiert durch einen Längsstrahler, der die Vorzugsrichtung definiert und einer Reihe von parasitären Dipolen. Der Gewinn einer solchen Yagi-Antenne ist von der Anzahl und der Länge der Dipole und deren Abstand zueinander abhängig. Wegen ihrer einfachen und preiswerten Bauweise sind diese Antenne in der Nachrichtentechnik sehr verbreitet (z.B. terrestrische Fernsehantenne) [6].

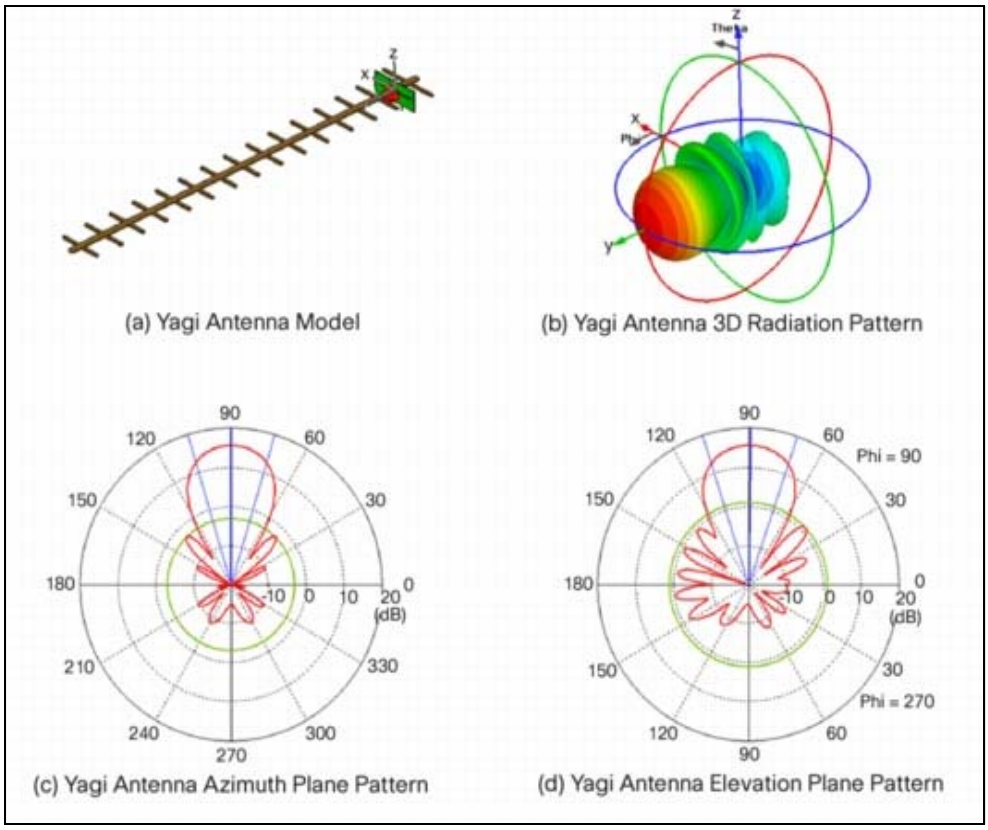

Abb. 6.5: Richtcharakteristik einer Yagi-Antenne (Quelle: [CISCO])

Sektorantenne

Wie der Name schon sagt, sind Sektorantennen in erster Linie dazu gedacht, ein Kreissegment in der horizontalen Ebene auszuleuchten. In der Praxis kommen Sektorantennen mit einem horizontalen Öffnungswinkel zwischen 60° und 120° zum Einsatz, die einen Antennengewinn von bis zu 12 dBi aufweisen [6].

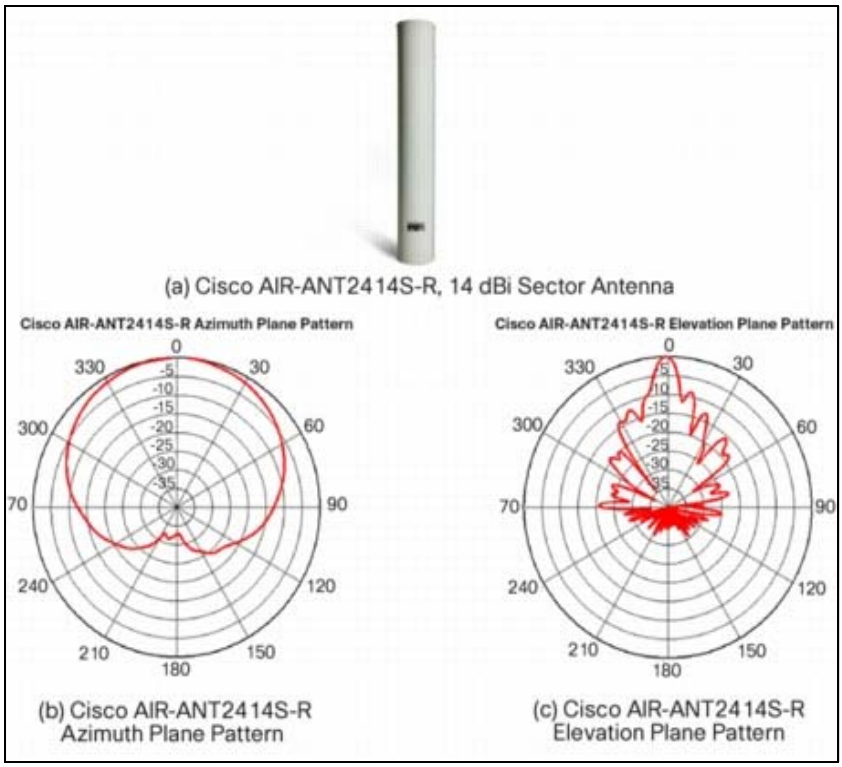

Abb. 6.6: Richtcharakteristik einer Sektorantenne (Quelle: [CISCO])

Parabolantennen

Parabolantennen arbeiten mit einem Reflektor in Form eines Rotationsparaboloids. Sie bieten einen sehr hohen Antennengewinn im Bereich von 10 bis 25 dBi, bei einem Öffnungswinkel von 70° bis 10°, wobei der Durchmesser etwa 12 bis 82cm beträgt.

Parabolantennen werden im WLAN-Bereich zur Errichtung von Richtfunkstrecken eingesetzt um z.B. zwei entfernte Gebäude zu verbinden. Mit Parabolantennen können je nach Bauweise Übertragungen von mehreren Kilometern erreicht werden [6].

Eigenbau-Lösungen

Im Internet findet man zahlreiche Anleitungen, mit denen man Richtantennen oder simple Reflektoren mit einfachsten Mitteln selbst nachbauen kann. Z.B. auf http://www.wlan.org.uk/antenna-page.html findet man verschiedenste Antennentypen mit unterschiedlichen Charakteristiken und unterschiedlichem Antennengewinn.

Folgende Abbildung zeigt eine Bauanleitung für eine 2,4-GHz-Antenne:

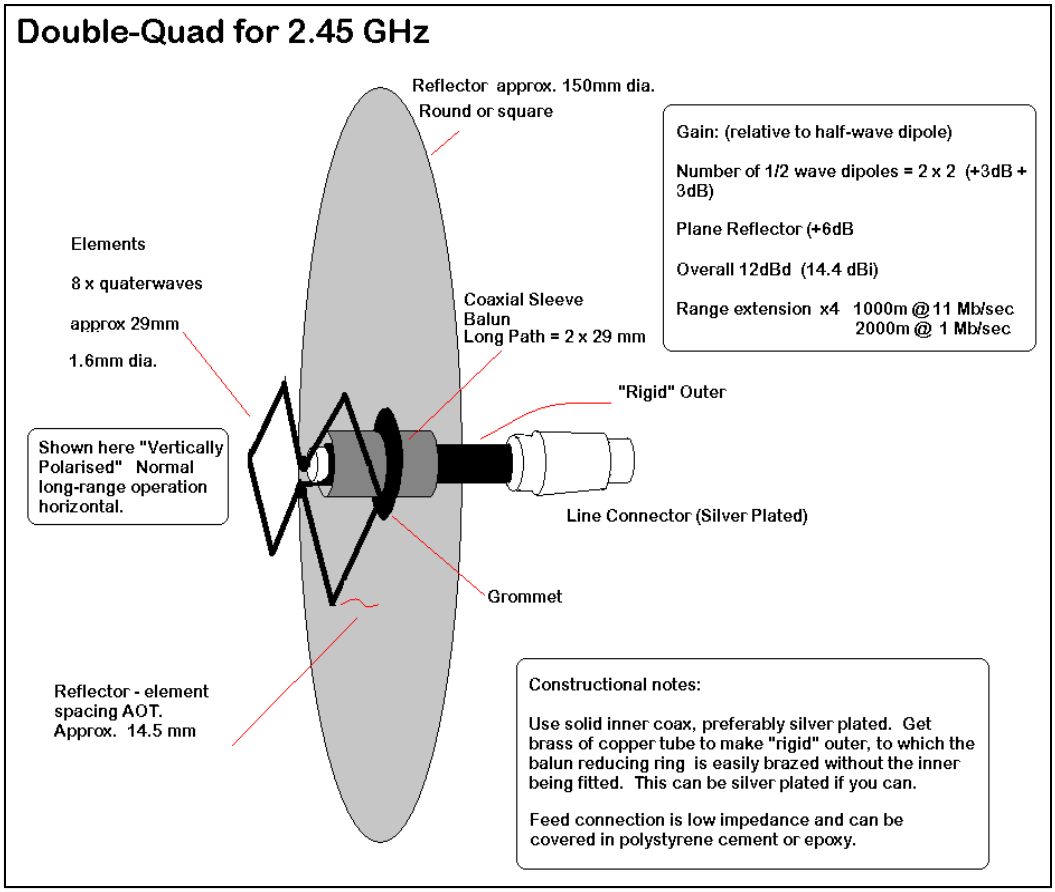

Abb. 6.7: Eigenbau-Richtantenne (Quelle: http://www.wlan.org.uk/g8ota%20double-quad.gif)

Dabei sei aber zu erwähnen, dass es hier wenige bis gar keine wissenschaftlichen Informationen, Messprotokolle oder sonstiges gibt. Somit haben solche Lösungen zwar im privaten Bereich durchaus ihre Berechtigung, da sie sehr kostengünstig und einfach herzustellen sind, und sehr wohl eine Performance-Steigerung bringen können.

Für professionelle Anwendungen ist es jedoch ratsam, eine andere Lösung anzustreben.

6.3 Verwendung öffentlicher Netzwerke

6.3.1 Vorteile / Risiken

Vielerorts werden in der heutigen Zeit sogenannte „Hotspots“ verwendet. Hierbei handelt es sich um öffentliche WLAN Netze wie z.B. in Schulen, auf Universitäten, Restaurants, teils öffentlichen Plätzen, aber auch etwa in Kongresshäusern, welche frei zugänglich sind. Der Vorteil an diesen Netzen ist, dass sie (zumeist) professionell durch diverse Firmen installiert werden, somit an die Räumlichkeiten / das Areal angepasst werden. Durch diverse Einmessverfahren kann ein großer Bereich mit WLAN konstanter Stabilität abgedeckt werden.

Aufgrund der Stabilität und Reichweite solcher Netzwerke liegt es nahe, im Falle einer Veranstaltung diese für eine Funkvernetzung der Beschallungsanlage zu verwenden, da für den Nutzer die Erstellung eines eigenen Netzwerkes nicht mehr von Nöten ist.

Da diese Netzwerke jedoch - wie bereits erwähnt - frei zugänglich sind, können andere Nutzer Einfluss auf ihre Tätigkeiten nehmen (siehe Kap. 4.2).

Daher ist es notwendig, zusätzliche Sicherheitsvorkehrungen zu ergreifen, um die Sicherheit des Auditoriums gewährleisten zu können.

Eine sehr effiziente Möglichkeit, sich in solch einem Netzwerk vor Manipulationen zu schützen, ist die Verwendung von sogenannten „Virtual Private Networks“.

6.3.2 Virtual Private Network (VPN)

Mittels eines „Virtual Private Networks“ wird ein verschlüsselter Tunnel zwischen der Station und dem Server aufgebaut, über den die gesamte Kommunikation erfolgt. Die kryptographischen Schlüssel für die Verbindung jeder Station zum VPN-Server sind individuell, wodurch der Datenverkehr der so verbundenen Stationen hinsichtlich Vertraulichkeit und Integrität geschützt sind.

Das VPN ermöglicht somit das Betreiben einer sicheren, scheinbar direkten Punkt-zu-Punkt Verbindung zwischen zwei Stationen, und ist somit mit einer direkten Leitung vergleichbar. VPNs können über Software, aber auch über Hardware realisiert werden.

Vielfach werden heutzutage VPNs z.B. von Firmen verwendet, um ihren Mitarbeitern einen sicheren Zugang zum firmeninternen Netzwerk und somit deren Daten von zuhause aus über das Internet zu ermöglichen. [3]

Verbindungsaufbau / Datenübertragung

Auf dem Rechner A läuft eine spezielle Software, der VPN Client, welcher über das Netzwerk eine Verbindung zum VPN-Server auf Rechner B aufbaut. Rechner A hat die IP-Adresse x, Rechner B die IP-Adresse y. Nachdem sich der VPN-Client authentifiziert hat, werden Schlüssel vereinbart, mit denen die Verbindung kryptographisch geschützt wird. Die Kommunikation erfolgt über eine abweichende IP-Adresse z, also nicht über die tatsächlichen Adressen der beiden Rechner.

Der VPN-Client übernimmt die Datenpakete von der Anwendung und „tunnelt“ diese verschlüsselt an den VPN-Server. Dieser empfängt die Datenpakete, entschlüsselt, überprüft und entkapselt sie und sendet dann die ursprünglich von der Anwendung erzeugten Pakete mit den eigentlichen IP-Adressen weiter.

6.3.2.1 Konfiguration unter Windows XP

Um eine sichere VPN-Verbindung zwischen zwei Rechnern unter Windows herzustellen, wird hier auf die Support-Seiten von Microsoft verwiesen. Hier sind ausführliche Anleitungen für die Client- und Serverkonfiguration sowie Problemlösungen zu finden.

Z.B. für Windows XP auf: http://support.microsoft.com/kb/918663/de

6.3.2.2 Konfiguration unter Mac OS X Snow Leopard

Um eine sichere VPN-Verbindung zwischen zwei Rechnern unter Mac OS X herzustellen, wird eine externe Software-Lösung benötigt, da das Betriebssystem in seiner Standard-Version keine VPN- Server Funktion bereitstellt.

Hierbei kommen eine Fülle von Programmen in Frage. Nachfolgend werden kurz zwei Möglichkeiten erwähnt:

iVPN

iVpn ist eine einfach zu handhabende VPN-Server Lösung. Auf eine detaillierte Beschreibung bzw. Konfiguration wird aufgrund des guten Software Support an dieser Stelle verzichtet.

Downloadbar ist dieses Programm unter:

http://macserve.org.uk/projects/ivpn/

Tunnelblick

Eine weitere Möglichkeit wäre die Verwendung der Software-Lösung „Tunnelblick“. Diese Open-VPN Lösung ist etwas komplizierter zu handhaben, ist jedoch als Freeware erhältlich. Hier erscheint eine detaillierte Konfiguration ebenfalls trivial.

Downloadbar ist dieses Programm unter:

http://code.google.com/p/tunnelblick/

Zusammenfassung

Zusammenfassend kann man sagen, dass die Ergreifung von diversen Maßnahmen zur Erhöhung der Sicherheit und Stabilität bei der Verwendung von Funksteuerungen besonders bei größeren Veranstaltungen zu empfehlen bzw. unumgänglich ist. Jederzeit sollte die Sicherheit des Auditoriums an erster Stelle stehen. In diesem Kapitel wurde gezeigt, dass man bereits mit einfachen Mitteln gezielt die Stabilität verbessern kann, und mittels eines VPN – Tunnels einen Zugriff von dritten vermieden werden kann.

7 Zusammenfassung / Ausblick

Allgemein kann man sagen, dass die hier vorgestellte Thematik derzeit einen sehr dynamischen Verlauf erfährt. Bereits während der Erstellung dieser Arbeit machte sich oftmals ein Umschwung im Bereich der Funksteuerungen bemerkbar. Immer wieder wurden neue Applikationen für Apple Geräte (iPad/iPod/iPhone) veröffentlicht, besonders nachdem diese Geräte ab der Version 4.2 des Betriebssystems iOS (Veröffentlichung Nov 2010) mit Einschränkungen MIDI-fähig wurden. Nach der Markteinführung des Betriebssystems „Android“ für Smartphones und Tablets anderer Hersteller, war man nicht mehr nur auf Apple-Geräte beschränkt, die Mehrheit der am Markt erhältlichen Geräte wurden für diese Zwecke verwendbar.

Mit der steigenden Verbreitung von digitalen, audioelektronischen Geräten, besonders im Bereich der Mischpulte wurden daher die Rufe von ausführenden Toningenieuren nach neuen Möglichkeiten der Steuerung via Funk immer lauter.

Einige wenige Hersteller wie z.B. Yamaha erkannten die Nachfrage und stellten Steuerungs-Applikationen für Apples „iPad“ zur Verfügung, leider jedoch nur für vereinzelte Mischpult-Konsolen wie z.B. der „M7CL“. [YAM]

Da eine Verwendung solcher Steuerungen viele Vorteile mit sich bringt, wurde diese Thematik aufgegriffen und aus verschiedensten Gesichtspunkten betrachtet. Das Ziel war es, mithilfe kommerziell erhältlicher Geräte, also Laptops, Tablets und Smartphones, möglichst einfach aber effektiv solche Steuerungen realisieren zu können. Zumindest temporär sollte die Lücke zwischen fehlenden Systemen gefüllt werden und eine Steuerung möglichst Hersteller-unabhängig umsetzbar gemacht werden. Die Vorzüge der Verwendung von Funksteuerungen sollten nicht nur einer Hand voll erfahrenen Toningenieuren mit entsprechendem Equipment vorbehalten sein.

Das Ergebnis der Arbeit sind 3 Systeme, allesamt einfach zu realisieren, unter Windows und Mac OS X verwendbar, und beliebig kombinierbar. Die Einsatzmöglichkeiten sind sehr vielfältig, so kann beinahe jedes Midi – fähige Gerät, bzw. jedes Gerät, das über eine Steuerungs-Software verfügt, über ein WLAN Netzwerk gesteuert werden. Neben den Vorteilen wurden natürlich auch diverse Nachteile diskutiert.

Ausblick

Auf der sogenannten „Namm“, eine der weltweit größten und renommiertesten Musikmessen (Anaheim, Kalifornien, USA), wurden im Jänner 2012 bereits erste Komplettlösungen von Herstellern wie Mackie oder Line 6 vorgestellt. Nicht nur die nahtlose Einbindung eines Apple „iPads“ über Funk wird ermöglicht, teils wird sogar komplett auf diverse Hardware-Steuerungseinheiten wie Fader oder Potentiometer verzichtet. Lediglich das „iPad“ dient der Steuerung. [MACK] [LINE6]

Somit kann man sagen, dass in der nächsten Zeit die Möglichkeiten der Funksteuerung von entsprechenden Geräten sicherlich eine steigende Verbreitung erfährt. Es ist anzunehmen, dass die oben genannten innovativen Schritte von „Mackie“ und „Line6“ auch andere Hersteller motivieren werden, hier nachzuziehen und in neue Ansätze und Produkte zu investieren.

8 Literaturverzeichnis

[1] Braut, C., “Das MIDI Buch”, 2., überarbeitete Auflage, SYBEX-Verlag, 1993

[2] Freed, A., Schmeder, A., “Features and Future of Open Sound Control version 1.1 for NIME”, NIME Conference, 2009

[3] Kappes,M., “Netzwerk- und Datensicherheit, eine praktische Einführung”, *Teubner*, 1.Auflage, 2007

[4] Lazzaro, J., Wawrzynek, J., “RTP Payload Format for MIDI**”**. RFC 4695, IETF Proposed Standard Protocol, 2006

[5] Hofherr, M., “WLAN-Sicherheit, Professionelle Absicherung von 802.11-Netzen”, *Heise*, 1. Auflage, 2005

[6] Rech, J., “Wireless LANs”, *Heise*, Auflage 3, 2008

[7] Richardson, T., Stafford-Fraser, Q., Wood, K., Hopper, A., "Virtual Network Computing", *IEEE Internet Computing*, Vol.2 No.1, Jan/Feb, 1998

[8] Richardson, T., „The RFB Protocol“, RealVNC Ltd., Version 3.8, (http://www.realvnc.com/docs/rfbproto.pdf), 2010

[9] Schmeder, A., Freed, A., Wessel, D., „Best Practices for Open Sound Control“, Linux Audio Conference, Utrecht, The Netherlands, 2010

[10] Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V., “RTP: A transport protocol for real-time applications”, RFC 3550, 2003

[11] Surendorf, K., “Mac OS X Snow Leopard, das umfassende Handbuch”, *Galileo Design,* Auflage 1, 2010

[12] Wright, M., “The Open Sound Control 1.0 Specification” (http://opensoundcontrol.org/spec-1_0), 2002

[13] Wright, M., Freed, A., “Open Sound Control: A New Protocol for Communicating with Sound Synthesizers", International Computer Music Conference, Thessaloniki, Greece, 1997

Internetlinks:

[CISCO]
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.html

[ETTER] http://ettercap.sourceforge.net/

[HARD] http://hardbitrocker.de/block_leser/items/wlan-netzwerk-via-apple-script-anlegen.html

[LINE6] http://line6.com/stagescape-m20d/

[MACK] http://www.mackie.com/products/dl1608/

[OSC] http://www.osculator.net/

[TECH] http://www.technologyuk.net/telecommunications/networks/wireless_networks.shtml

[TOUCH] http://hexler.net/software/touchosc

[UNI] http://www.uni-protokolle.de/Lexikon/Private_IP-Adresse.html

[WIRE] http://www.wireshark.org/

[YAM]
http://www.yamahaproaudio.com/global/en/products/peripherals/applications/m7clstagemix/

9 Anhang: Abkürzungsverzeichnis

AD	Analog-Digital
AP	Access Point
BSS	Basic Service Set
CC	Control Change
DS	Distribution System
DSP	Digital Signal Processing
FOH	Front Of House
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronical Engineers
IT	Informations-Technik
LAN	Local Area Network
MCU	Mackie Control Universal
MIDI	Musical Instrument Data Interface
MSB	Most Significant Bit
NTP	Network Time Protocol
OSC	Open Sound Control
OSI	Open Systems Interconnection
PA	Public Address
PCI	Peripheral Component Interconnect
RFB	Remote Framebuffer Protocol
RTP	Real-Time Transport Protocol
SysEx	System Exclusive Message
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UHF	Ultra High Frequency
URL	Uniform Resource Locator
USB	Universal Serial Bus
VNC	Virtual Network Computing
WI-FI	Synonym für Wireless LAN
WLAN	Wireless Local Area Network
XOR	exclusive OR