Dieter Görrisch

FRANZIS
EXPERIMENTE

2. Auflage

Störsender

von VHF bis Mikrowelle

Inhalt

Inhalt

Inhalt

1 Einleitung

Der Begriff „Störsender“ (engl. „Jammer“) wird seit jeher mit unglaublichen Geschichten und Verschwörungstheorien verbunden. Kaum jemand kennt eigentlich die verschiedenartigen Facetten dieses Themas.

Ob eine Sendeeinrichtung als Störsender bezeichnet werden darf, hängt nicht zuletzt auch von den Absichten seines Eigentümers ab. Als Beispiel sei hier der Mittelwellensender Osterloog in Ostfriesland genannt. In den 30er Jahren als Mittelwellen-Grundnetzsender für das damalige Deutsche Reich gebaut, diente er in den nachfolgenden Kriegsjahren gleichermaßen als Rundfunksender, Störsender und Peilbake für zurückkehrende deutsche Bombenflugzeuge (bis heute ermöglichen die in alle Flugzeuge eingebauten NDB-Peilempfänger übrigens die Navigation mit Hilfe gewöhnlicher Mittelwellen-Rundfunksender). Natürlich kann man jeden Rundfunksender auch als Störsender gegen andere Rundfunksender einsetzen. Oft genügt der Austausch einer einzigen Baugruppe (sog. „Wobbeleinschub“) innerhalb der Sendeanlage und der Rundfunksender wird zum Störer. Störungen können aber auch mit regulären Radioprogrammen bewusst verursacht werden: So wurde der Empfang von RIAS-Berlin bis 1978 von Rundfunksendern der DDR gestört, sie wurden frequenzmäßig einfach knapp neben die RIAS-Frequenz gesetzt und strahlten ein ganz gewöhnliches Rundfunkprogramm aus. Der Empfang der RIAS-Sendungen in der DDR war damit weitgehend unterbunden. Somit ist es also keinesfalls nur eine Frage der Technik, ob ein Sender zum Vor- oder Nachteil seines „Hörers“ betrieben wird. Allerdings gibt es auch reinrassige Störsender, die ausschließlich für diesen Zweck gebaut werden und eine Nutzung zur Kommunikation gar nicht erst zulassen.

Die zahlenmäßig meisten Störeinrichtungen besitzt und betreibt das Militär. Damit werden im Ernstfall die gegnerische Kommunikation, Radareinrichtungen und Waffensysteme gestört. Die größte, jemals bekanntgewordene militärische Einzelaktion war der Abwurf von sog. Aluminiumstreifen im Rahmen der folgenschweren Bombardierung Hamburgs im Juli 1943. 92 Millionen dieser Streifen wurden von den britischen Flugzeugen abgeworfen und „blendeten“ die deutschen Funkmessgeräte. Über 50.000 Schuss der Flak gingen ins Leere, nur drei Zufallstreffer wurden erzielt! Parallel zu kriegerischen Auseinandersetzungen läuft meist eine Propagandaschlacht an, in deren Verlauf die mediale Infrastruktur (TV- und Rundfunksender) des Gegners ganz ausgeschaltet oder zumindest nachhaltig gestört wird. Als Beispiel sei hier der Irak-Krieg genannt. Die amerikanischen Truppen

schalteten zunächst die gegnerischen Sendeanlagen aus und strahlten dann eigene Programme über dem Irak ab. Propagandasendungen (Radio und TV) wurden teilweise über Sender ausgestrahlt, die in großen Flugzeugen eingebaut, stundenlang im Luftraum über dem Irak kreisten. Daran kann man den großen Aufwand erkennen, der heute von den Militärs in der „elektronischen Kriegsführung“ betrieben wird.

Ganz neue Aspekte treten in Zusammenhang mit der weitverbreiteten Konsumelektronik zu Tage. Drahtlose Anwendungen sind heute ganz selbstverständlich geworden. Handys, drahtlose Kfz-Funkschlüssel oder Funkfernsteuerungen gehören zum Inventar eines jeden Haushaltes. Hier eröffnen Störsender völlig neue Möglichkeiten, für groben Unfug und für Kriminelle!

Die nachfolgenden Kapitel ermöglichen einen Einblick in die Technik, Einsatz und die grundlegende Problematik beim Einsatz von Störsendern. Zahlreiche Schaltungen bieten einen Eindruck aktueller Schaltungstechnik.

An dieser Stelle sei darauf hingewiesen, dass der Betrieb von Sendeeinrichtungen in jedem Staat grundsätzlich gesetzlich geregelt ist. Beachten Sie daher die in Ihrem Land geltenden Vorschriften. Wer darüber hinaus durch seine Aussendungen das öffentliche Leben und die allgemeine Sicherheit gefährdet, macht sich in besonderem Maße strafbar! Nachbau und Betrieb der angegebenen Schaltungen geschieht auf eigenes Risiko und eigene Gefahr. Experimente mit hohen Spannungen und Hf-Ausgangsleistungen bergen ein erhebliches gesundheitliches Risiko für Anwender und Mitmenschen. Auf Versuche mit Magnetrons muss aus Sicherheitsgründen generell verzichtet werden!

2 Theoretische Grundlagen

Alle Theorie ist grau und dennoch notwendig. Gerade zum Thema Funkwellen herrschen die abenteuerlichsten Vorstellungen und die in den letzten Jahren angelaufenen Diskussionen zum Thema Elektrosmog haben auch nicht gerade zur Versachlichung beigetragen.

2.1 Grundlegende Eigenschaften elektromagnetischer Schwingungen

Ein elektronischer Schwingungserzeuger (Oszillator) erzeugt zunächst einmal eine Wechselspannung einstellbarer Frequenz. Dadurch kommt es zum zyklisch wechselnden Stromfluss in seinem Schwingelement (Spule, Quarz, dielektrischer Resonator dgl.). Wird der so erzeugte hochfrequente Wechselstrom in eine (möglichst resonante) Antenne eingespeist, entsteht dort ein elektromagnetisches Wechselfeld, das sich abschnürt und in einiger Entfernung noch wirkt. Die Reichweite dieses elektromagnetischen Kraftfeldes hängt von verschiedenen Dingen ab:

– Sendeleistung des Oszillators/Senders
– Freiraumdämpfung und Effekte (Reflexionen, Abschattung dgl.)

Wie das nachfolgende Diagramm zeigt, nimmt die abgestrahlte Sendeleistung mit dem Abstand zur Sendeantenne sehr schnell ab!

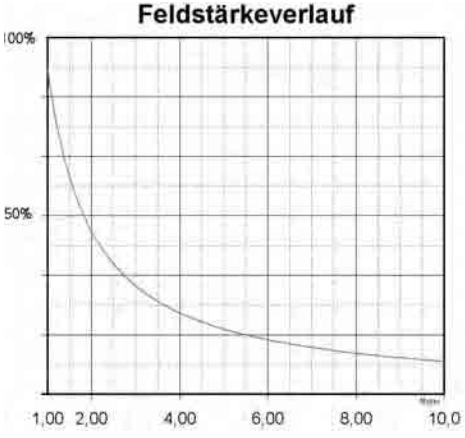

Abb. 2.1 Feldstärkeverlauf

Während sich in unmittelbarer Umgebung der Sendeantenne sogar Energie übertragen lässt (RFID-Chips gewinnen aus dieser hohen Feldstärke ihre Betriebsspannung!), ist in einigen Metern Abstand von der eingespeisten Sendeleistung nur noch ein winziger Bruchteil übrig geblieben. Einerseits verteilt sich die Sendeleistung mit wachsendem Abstand in ein immer größer werdendes Raumvolumen, andererseits tragen

Luftmoleküle und Wasserdampf zusätzlich zur Dämpfung der elektromagnetischen Felder bei. Das bedeutet aber auch, dass in unmittelbarer Nähe der Sendeantenne sehr große Feldstärken herrschen, die sich kaum durch einen weiter entfernten Störsender überdecken lassen.
Ohne die Berücksichtigung der verwendeten Antennen gilt die Formel:

Freiraumdämpfung [dB] = 32,45 +
20 log d [km] + 20 log f [MHz]

d. h. mit steigender Frequenz und steigender Entfernung wird die Dämpfung immer höher, die übertragene Hf-Leistung zum Empfangsort immer kleiner.

Die Freiraumdämpfung bewirkt, dass sich die Sendeenergie in einer bestimmten Entfernung schließlich ganz aufgezehrt hat, der Sender ist dann nicht mehr empfangbar. In der Praxis kann man die unvermeidliche Signaldämpfung durch erhöhte Sendeleistung wieder ausgleichen, wie nachfolgendes Beispiel zeigen wird. Doch hier sind Grenzen gesetzt, ein Sachverhalt der in ganz besonderem Maße bei Störsendern deutlich wird.

Beispiel:
Eine ISM-Funkanwendung mit einer Leistung von 1 mW Sendeleistung auf 433 MHz, erzeugt in einem Abstand von 500 Metern einen Pegel von -79 dBm am Empfänger. Um am Empfangsort den gleichen Signalpegel aus einer Entfernung von 2 km zu erzeugen, sind bereits 16 mW Sendeleistung erforderlich! Bei einer Entfernung von 5 km sind es bereits 100 mW!

Drastischer werden die Unterschiede, wenn zwischen einem der Sender und dem Empfänger kein nennenswerter Abstand besteht. Das ist tägliche Praxis bei Anwendung der weitverbreiteten Kfz-Funkschlüssel. Erst unmittelbar am Fahrzeug wird der Funkschlüssel betätigt, der Abstand zum Fahr-

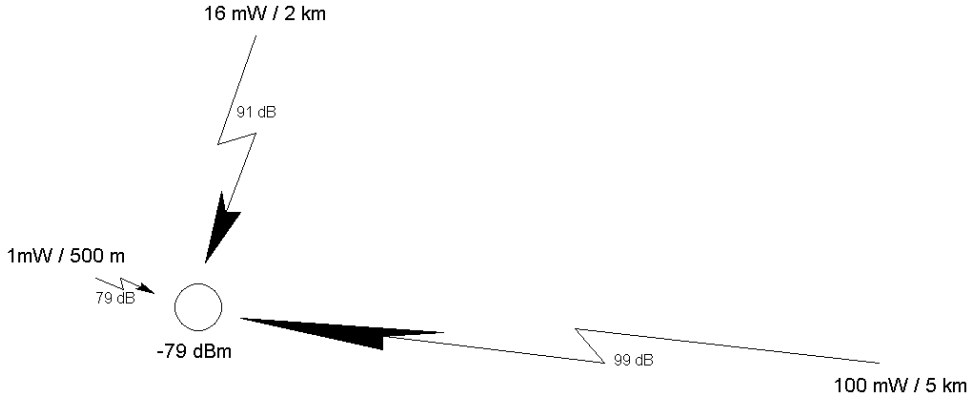

Abb. 2.2 Pegelvergleich 1

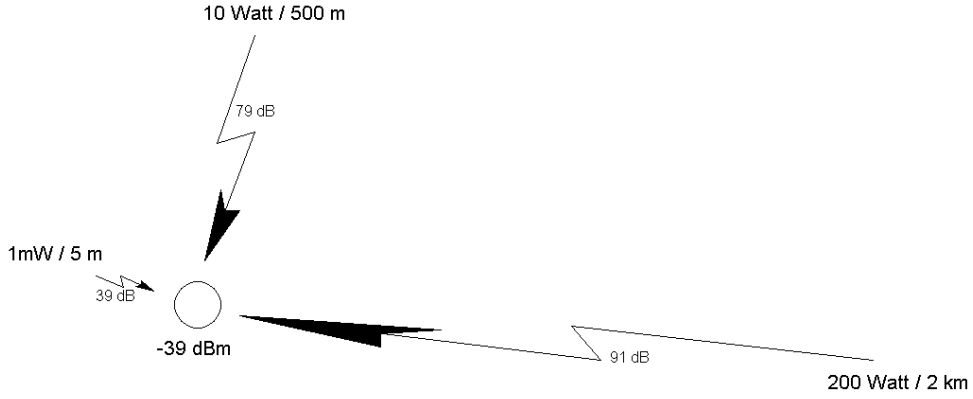

Abb. 2.3 Pegelvergleich 2

zeug beträgt oft nur wenige Meter. Im nachfolgenden Pegelplan erzeugt der Sender 1 mW, in 5 Metern Entfernung einen Empfangspegel von -39 dBm, die Streckendämpfung ist also sehr gering. Um den gleichen Pegel zu erzeugen, sind in 500 Metern Entfernung 10 Watt und in 2 km bereits 200 Watt an Hf-Leistung erforderlich.

Man erkennt deutlich, welchen Stellenwert die Entfernungen zwischen Sender und Empfänger haben.
Das sind natürlich rein theoretische Überlegungen, ohne Berücksichtigung von zusätzlichen Hindernissen im Funkweg, Reflexionen und den Einfluss richtstrahlender Antennen.
Um einen nachhaltigen Störerfolg zu erzielen, muss der Störsender zudem einen deutlich stärkeren Pegel am Empfänger erzeugen als das Nutzsignal. Nur dann wird das Nutzsignal sicher „zugedeckt“ und unwirksam. Wie groß dieser Pegelabstand zwischen Nutz- und Störsignal tatsächlich sein muss, ist ein Erfahrungswert. Geht man von 20 dB Pegelabstand aus, liegt man auf der sicheren Seite. Leider ist das in der Praxis nicht immer erreichbar.

Obiges Beispiel zeigt auch, dass der Einsatz eines Störsenders grundsätzlich umso effektiver ist, je näher er am Empfänger positioniert ist. Eine Erhöhung der Störleistung gleicht die wachsende Entfernung nur sehr uneffektiv aus! Es kann also durchaus auch Sinn machen, mehrere Störsender kleiner Leistung in unmittelbarer Umgebung der Empfänger zu platzieren. Der Empfang des RIAS-Rundfunksenders wurde auf dem Gebiet der DDR zeitweise mit zahlreichen, örtlich verteilten 50 Watt-Mittelwellensendern gestört. Eine weitere Möglichkeit besteht darin, Störsender mit Richtantennen auszustatten und so den Feldstärkepegel am Empfangsort wirksam zu steigern.

Reflexionen und Mehrwegeempfang
Speziell auf kurzen Wellenlängen (>30 MHz) wirkt sich noch ein weiterer Effekt

besonders aus, der hier kurz angesprochen werden soll. Das Sendesignal erreicht den Empfänger in der Praxis nicht nur auf dem direkten Wege, sondern auch über Reflexionen (beispielsweise an Häusern oder Bergen). Durch diese Umwege bedingt, kommt das reflektierte Sendesignal mit einiger Verzögerung beim Empfänger an und überlagert sich mit dem direkt empfangenen Sendesignal. Unter bestimmten Bedingungen (180 Grad-Phasenverschiebung der beiden Signale) kann es hier zur Signalauslöschung (Fading) kommen. Das macht sich in der Praxis durch flackernde Feldstärken bemerkbar. Schlimmstenfalls kommt es geographisch bedingt sogar zur Ausbildung eines stehenden Wellenfeldes und der Sender ist trotz guter Feldstärke an bestimmten Positionen gar nicht mehr zu empfangen. Diesen Fall erlebt man oft im Kraftfahrzeug, wenn beim Anhalten der empfangene UKW-Sender plötzlich im Rauschen untergeht. Rollt man einige Meter weiter, ist der Sender wieder glasklar empfangbar. Das bedeutet für einen Störsender, dass er unter beschriebenen Umständen trotz ausreichender Sendeleistung am Zielort nicht empfangbar ist. Dann hilft nur ein Positionswechsel.

2.2 Störprinzipien

Die Aufgabe eines Störsenders ist es schlichtweg, am Empfänger ein stärkeres Antennensignal zu erzeugen als der Nutzsender. Dann kommt es zur Beeinträchtigung oder völligen Unterdrückung des Nutzsignales. Die mindestens erforderliche Sendeleistung des Störsenders ist von zahlreichen Faktoren abhängig, wobei im Zweifel immer die Formel „viel Leistung hilft viel“ gilt. Die Arten der Störung sind unterschiedlich und hängen vom „Angriffsziel“ ab. Grundsätzlich kann jede drahtlose Übertragung gestört werden, egal ob Rundfunkprogramme, Sprechfunk oder digital codierte Daten. Während Störungen klassischer Betriebsarten (AM oder FM) für den Höhrer mehr oder minder hörbar sind, reagieren digitale Übertragungen unterschiedlicher. Intelligente Funksysteme versuchen die Störung durch Kanalwechsel zu umgehen, was sich beispielsweise durch lautes Knacken im Lautsprecher bemerkbar macht. Auch extrem breitbandige Übertragungsverfahren (Spread Spectrum-Technik), wie sie u. a. vom GPS-Navigationssystem verwendet werden, sind keinesfalls so übertragungssicher, wie immer behauptet wird.

Punktstörung

Bei der Punktstörung handelt es sich um die effektivste Art der Beeinflussung, die auch auf größere Entfernung zum Empfänger eingesetzt werden kann. Bei altgedienten Funkern ist sie unter der Bezeichnung „Trägern“ bekannt und berüchtigt. Das Störsignal wird dazu genau auf das Nutzsignal gelegt, die Frequenzbandbreite des Störers muss größer sein als die des Nutzsignals. Eine klassische Anwendung ist beispielsweise die Störung eines AM-Rundfunksenders. Der Störsender wird mit seiner Frequenz genau auf die Arbeitsfrequenz des Radiosenders gesetzt. Ist der Störsender ausreichend stark, wird der Radiosender am Empfangsort stark gestört. In der Praxis ist

das allerdings nicht ganz so einfach. Da bei Amplitudenmodulation die Empfangsfeldstärke von der Modulation abhängig ist, hört man das Nutzsignal immer wieder „durch“. Auch durch Fading (physikalisch bedingte Signalschwankungen durch Laufzeitunterschiede der Funkwellen) wird eine dauerhafte und vollständige Signalüberdeckung schwierig. Daher wendete man in der Vergangenheit zahlreiche Tricks an: Auf Mittel- oder Kurzwellen setzte man den Störsender gelegentlich nicht direkt auf das Nutzsignal, sondern knapp daneben, dadurch entsteht im Empfänger ein starkes Interferenzpfeifen der beiden AM-Trägersignale. Um die volle Bandbreite des Nutzsenders zu überdecken, wird der Störsender speziell moduliert oder gewobbelt (engl. to wobble = taumeln, schwanken). Die Störsendermodulation muss so erfolgen, dass der gestörte Nutzsender in seiner gesamten Bandbreite voll überdeckt wird. In der Praxis ist das nicht immer leicht zu lösen. Das menschliche Gehör ist nämlich durchaus in der Lage, die charakteristische Stimme einer Person aus einer Geräuschkulisse herauszuhören. Art und Qualität der Störsendermodulation sind daher von entscheidender Bedeutung für den Störerfolg. Während des letzten Krieges wurden von der damaligen Reichsrundfunkgesellschaft sogar „Volksgemurmel-Schallplatten“ zum Störsendereinsatz erstellt, da dieses Stimmengewirr das menschliche Gehör ziemlich überfordert. Bei frequenzmodulierten Aussendungen ist die Situation etwas einfacher, hier kommt der sog. „Wegdrückeffekt“ zum Tragen. Da frequenzmodulierte Sender unabhängig von ihrer Modulation immer mit ihrer vollen Leistung senden, ist ein „Durchhören“ des gestörten Nutzsignales kaum möglich.

Besonders wirksam und gefürchtet ist die Punktstörung auf Eingabefrequenzen von sog. Funkrelais. Diese Einrichtungen werden hierzulande von Behörden und Amateurfunkern in großer Anzahl eingesetzt. Wird ein Funkrelais durch einen Störträger auf seiner Eingabefrequenz gestört, ist es für alle anderen Funkteilnehmer nicht mehr benutzbar und der komplette Funkverkehrskreis erfolgreich blockiert.

Zur Punkstörung eignet sich grundsätzlich jeder Oszillator (mit entsprechender Frequenzstabilität) oder handelsübliche Funkgeräte. Üblicherweise ist die Bandbreite eines Funkgerätes durch schaltungstechnische Maßnahmen auf Normwerte begrenzt und für Störeinsätze ggf. auf größere Bandbreiten zu modifizieren.

Bandstörer

In vielen Anwendungsfällen sind die Arbeitsfrequenzen der Nutzsignale nicht vorher bekannt. Soll beispielsweise das ferngesteuerte Zünden einer Autobombe verhindert werden, lässt sich die dazu benutzte Übertragungsfrequenz bestenfalls abschätzen. Man ist also gezwungen, alle dafür in Frage kommenden Frequenzen (oder Frequenzbänder) zu stören. Das bewerkstelligt man so, dass ein oder auch mehrere Störsender zyklisch zwischen zwei Eckfrequenzen hin- und herwandern. Die wirksame Störleistung wird dabei natürlich über einen weiten Frequenzbereich „gestreut“ und wirkt entsprechend schwächer. Wird ein

Störsender mit einer Ausgangsleistung von 300 Watt über einen Frequenzbereich von 1 bis 550 MHz gewobbelt, beträgt die erzeugte Störleistungsdichte nur noch 0,5 Watt/MHz und ist damit wesentlich schwächer als bei einer Punktstörung! Diesen unvermeidlichen Effekt kann man auch durch höhere Sendeleistung kaum ausgleichen, weshalb Bandstörer nur im Nahfeld echte Wirkung zeigen. Dennoch werden Bandstörer zur Prävention gerne eingesetzt, auch wenn darüber hinaus noch zahlreiche weitere Probleme mit der Frequenzbandbreite von Verstärker und Antennen auftreten. Denn auch Endstufen und Antennen haben nur einen eingeschränkten Arbeitsfrequenzbereich. Somit kann eine wirksame Bandstörung über einen weiten Frequenzbereich eine echte „Materialschlacht“ werden.

Sender zur Bandstörung müssen in ihrer Arbeitsfrequenz schnell verstimmbar sein, was am besten über einen VCO-Steuerspannungseingang funktioniert. Moderne Funkgeräte steuern ihre Oszillatoren vielfach über interne Datenschnittstellen an (beispielsweise I2C-Bus) und sind damit für Wobbelbetrieb nicht geeignet. Die Datenübertragung ist einfach zu langsam, auch die weitverbreiteten externen Datenschnittstellen (CI-5 von Icom) eignen sich dafür nicht!
Ein ganz wesentlicher Punkt ist die Wobbelfrequenz, d. h. wie schnell läuft der Träger des Störsenders über das Band. Ist er zu langsam, können Nutzsignalanteile zum Empfänger durchkommen, was den Störerfolg in Frage stellt. Die Frequenz das Steueroszillators darf also nicht zu langsam sein. Andererseits gibt es Randeffekte, die sich ggf. nutzen lassen: Zahlreiche Funksysteme lassen sich durch bestimmte Wobbelfrequenzen besonders gut außer Tritt bringen, das sind allerdings wohlgehütete Betriebserfahrungen.

Rauschgeneratoren

Einen ganz besonderen Fall der Bandstörer stellen Rauschgeneratoren dar. Rauschen entsteht durch Elektronenbewegungen und ist in den meisten elektronischen Schaltungen ein Schmutzeffekt, den es zu verhindern gilt. Bei einem Rauschgenerator macht man sich den Effekt aber zunutze und erzeugt so ganz bewusst eine „Rauschglocke“, deren Frequenzbereich von hörbaren Anteilen bis in den GHz-Bereich reicht. Der Vorteil eines Rauschgenerators ist sein relativ einfacher Aufbau und sein unkomplizierter Einsatz. Wegen der enormen Frequenzbandbreite ist die erzeugte Störleistungsdichte und die somit erzielbare Reichweite aber auch entsprechend gering. Da keine Eckfrequenzen eingestellt werden können, stören Rauschgeneratoren immer das komplette Frequenzband. Das ist nicht immer erwünscht, gelegentlich benötigt man ein „Funkfenster“, also ein noch nutzbares Frequenzband für die Einsatzkräfte. Dennoch kommen auch Rauschgeneratoren im Nahfeld zum Einsatz, etwa in kleineren Räumlichkeiten (Zimmer) oder Spezialfällen.

Intelligente Störverfahren

Mit dem Einbau von Mikroprozessoren in die Funktechnik lassen sich wesentlich intelligentere Störverfahren realisieren. Sol-

che Systeme sind in der Lage, Funksignale in festgelegten Frequenzbändern selbständig zu erkennen und automatisch zu stören. Durch kurzzeitiges Abschalten des eigenen Störsignales kann ein intelligenter Störsender das Vorhandensein eines Nutzsignales auch während des Störens weiter beobachten. Mehrere Trägersignale können gleichzeitig gestört, neue Signale entdeckt werden. Das ist heute unumgänglich, wenn ebenso intelligente Funksysteme gestört werden sollen. Hier arbeitet man nämlich sehr gerne mit Frequenzsprungverfahren, d. h. die genutzten Übertragungskanäle werden ständig gewechselt und Störungen durch Dritte automatisch erkannt. Mit Einführung intelligenter Funksysteme („ALE" = Automatic Link Establishing, einem automatischen Verfahren, das selbständig und ohne Funker auskommt) werden auch die Störverfahren zunehmend komplexer werden.

Als Beispiel für einen militärischen Störsender sei hier der „Störsender 33 – Hummel" der deutschen Bundeswehr genannt. Er stört einen Frequenzbereich zwischen 1,6 und 512 MHz mit einer Leistung von 1 (optional 2) Kilowatt! Die Anlagen sind in mobilen Funkkoffern (sog. „Shelter") oder in Fahrzeuge eingebaut. Um mit dem Störsender möglichst auch in Frontnähe arbeiten zu können, steht das System auch als Rüstsatz für den 3-Achs-Transportpanzer „Fuchs" zur Verfügung.

RFID-Störer

Die neueste Errungenschaft der Funktechnik sind Transponderchips, kurz RFID (= Radio Frequency Identification Device). Die Funktion ist einfach zu beschreiben: Gerät ein solcher Chip in das Funkfeld des zugehörigen Abfragesystems, sendet er fest einprogrammierte Daten zurück. Auf diese Weise lassen sich drahtlose Abfragen schnell und automatisch erledigen (beispielsweise RFID-Chips als Preisauszeichnungen in kassenlosen Kaufhäusern). RFID-Systeme arbeiten durchweg auf einem der zahlreichen ISM-Bänder, vorzugsweise auf 13,56 MHz oder 2,54 GHz (neuerdings kommen sogar Dual-Band Chips zum Einsatz).

Diese Schaltkreise bestehen aus einem überdimensionierten Schwingkreis, einem Sende-Empfänger (sog. Transceiver) und einem Mikroprozessor. Diese Chips kann man als „Schläfer" bezeichnen, denn sie werden erst in einem elektromagnetischen Feld bestimmter Frequenz aktiv. Der Schwingkreis des Chips arbeitet dabei nicht nur als Antenne für Sendung und Empfang der Daten, sondern auch als Energieabsorber. Denn ein RFID-Chip besitzt keine eigene Energiequelle, sondern bezieht auch seine geringe Betriebsenergie aus dem elektromagnetischen Feld des Abfragesystems. RFID-Chips sind so klein, dass sie in Preisschilder oder unter Klebeplaketten Platz finden. Tieren werden sie unter die Haut gespritzt, als eine Art elektronische Tätowierung zur eindeutigen Identifizierung. Wie soll es auch anders sein, sogar gegen RFID-Abfragesysteme sind bereits wirksame „Abwehrchips" entwickelt worden. In eine Jute-Einkaufstasche eingenäht, behindern sie das Kassensystem beim Abfragen der RFID-Chips in den Preisauszeichnungen.

Die Störung eines RFID-Chips kann allerdings auch auf andere Art und Weise erledigt werden. Metallfolien oder Ferritabsorber in unmittelbarer Nähe eines solchen Chips verstimmen dessen Antenne. Die notwendige Energie- und Funkübertragung zwischen RFID-Chip und Abfragestation werden dadurch nachhaltig gestört, der Chip gibt in diesen Fällen kein Antwortsignal.

Möglicherweise wird es in Zukunft auch aktive Störsysteme gegen RFID-Systeme geben, die Ladendieben ein Vorbeischmuggeln der Ware an automatischen Kassensystemen ermöglichen.

Sachverzeichnis

Dieter Görrisch

2. Auflage

Störsender

von VHF bis Mikrowelle

Nach einer Welle von Viren, Würmern und trojanischen Pferden auf den PCs stellen Störsender möglicherweise die nächste Bedrohung unseres technologischen Umfelds dar. Drahtlos arbeitende Zutrittssysteme, per Funk abgefragte Preisetiketten oder GPS-gestützte Maut-Systeme sind lohnende Ziele für die Hacker der Zukunft. Das vorliegende Buch soll über Möglichkeiten und Geheimnisse rund um das Thema Störsender aufklären.

Der Begriff „Störsender“ wird seit jeher mit Geheimdiensten und Propaganda in Verbindung gebracht. Es gibt kaum jemand, der über die Anwendung von Störsendern Bescheid weiß. In diesem Buch erfahren Sie, auf welch einfache Weise beispielsweise KFZ-Funkschlüssel, Verkehrsradar, GPS-Empfänger und drahtlose Videokameras gestört werden können. Gepulste Magnetrons können Kraftfahrzeuge stoppen und bringen PCs aus 100 Meter Entfernung noch zum Absturz. Praxiserprobte Schaltungen in Halbleiter- oder Röhrentechnik von 30 MHz bis 2,5 GHz geben einen tiefgehenden Einblick in den Aufbau und die Funktionsweise von Störsendern.

Aus dem Inhalt:

Theorie • Perpetuum Mobile • Störsender im praktischen Einsatz • Störsenderschaltungen mit Halbleitern und Röhren • Magnetrons als HERF-Generatoren • Spezielle Störverfahren • Messgeräte, Antennen und Tipps

ISBN 3-7723-4127-6

9 783772 341274

EUR 19,95 [D]