Thomas Solzbacher*, Ralf Heynicke und Gerd Scholl

Parallelverarbeitung von RSSI-Signalen für ein lückenloses Monitoring des HF-Spektrums im 2,45 GHz ISM-Band

Parallel processing of RSSI signals for gapless monitoring of the 2.45 GHz ISM band

DOI 10.1515/teme-2018-0047

Zusammenfassung: WirelessHART und speziell an industrielle Bedingungen adaptierte WLAN- und Bluetooth-Systeme sind Beispiele für drahtlose Kommunikationssysteme, die sich für die Vernetzung von Sensoren und Aktoren im industriellen Umfeld etabliert haben. Im April dieses Jahres wurde ein zusätzlicher drahtloser Standard IO-Link Wireless [6] für die diskrete Fertigungsautomatisierung verabschiedet. Aufgrund der weltweiten Verfügbarkeit, was wiederum zu einer hohen Verfügbarkeit von kostengünstigen HF-Kommunikationskomponenten führt, wird häufig das lizenzfreie ISM-Band im 2,45 GHz-Bereich intensiv für die Kommunikation genutzt. Um Koexistenzprobleme zwischen den unterschiedlichen Systemen zu vermeiden, wurden bislang im wesentlichen Listen-Before-Talk, Frequency-Hopping und Blacklisting-Verfahren eingesetzt. Spektrumanalysatoren werden in der Regel offline als Monitoring- und Diagnose-Werkzeuge genutzt. In diesem Beitrag wird vorgeschlagen, diese zukünftig auch online in den laufenden Prozess zu integrieren, um eine mögliche Interferenz zwischen den um den Funkkanal konkurrierenden Kommunikationssystemen rechtzeitig zu erkennen bzw. vorherzusagen. Dazu müssen diese in der Lage sein, alle bekannten drahtlosen Systeme schnell und zuverlässig zu detektieren und zu klassifizieren. Ferner muss das Preisniveau dieser Spektrumanalysatoren erheblich unter dem von Labormessgeräten liegen, so dass diese im Sinne eines zusätzlichen Sensors einfach über bekannte Engineering-Werkzeuge in die Kommunikation eingebunden werden können.

Schlüsselwörter: Monitoring, Sensor/Aktor-Netzwerke, Online-Spektralauswertung.

***Korrespondenzautor:** Thomas Solzbacher, Professur für elektrische Messtechnik, Helmut-Schmidt-Universität Hamburg, Holstenhofweg 85, 22043 Hamburg, E-Mail: thomas.solzbacher@hsu-hh.de

Ralf Heynicke, Gerd Scholl, Professur für elektrische Messtechnik, Helmut-Schmidt-Universität Hamburg, Holstenhofweg 85, 22043 Hamburg

Abstract: WirelessHART and WLAN and Bluetooth systems specially adapted to industrial conditions are examples of wireless communication systems that have become established for the networking of sensors and actuators in the industrial environment. In April of this year, an additional wireless standard IO-Link Wireless for discrete manufacturing automation has been introduced. Due to the global availability, which in turn leads to a high availability of low-cost RF communication components, the license-free ISM band in the 2.45 GHz range is frequently used extensively for communication. In order to avoid coexistence problems between the different systems, essentially listen before talk, frequency hopping and blacklisting methods have usually been employed. Spectrum analyzers have so far been used essentially offline as monitoring and diagnostic tools. This article proposes to integrate these online into the ongoing process in order to detect and predict possible interference between the communication systems competing for the radio channel. For this, they must be able to quickly and reliably detect and classify all known wireless systems. Furthermore, the price level of these spectrum analyzers must be considerably lower than that of laboratory measuring devices, so that they can be integrated in the sense of an additional sensor easily via known engineering tools in the communication.

Keywords: Monitoring, sensor/actuator networks, online spectral analysis, secure wireless communication.

1 Einleitung

Sollen drahtlose Sensor/Aktor-Netzwerke mit einer Paketfehlerwahrscheinlichkeit betrieben werden, die derjenigen von drahtgebundenen Systemen entspricht, ist die Auslastung der Frequenzbänder im jeweiligen Fertigungsbetrieb vorort zu planen. In der Regel lassen sich im 2,45 GHz-Band gleichzeitig drei WLAN-Kanäle überlappungsfrei parallel betreiben. Kommen zusätzliche drahtlose Kommunikationssysteme hinzu, müssen sich diese

die noch freien Frequenzkanäle teilen. Aufgrund der systembedingten Hopping-Sequenzen über das komplette 80 MHz-Band ist deshalb die Wahrscheinlichkeit einer Störung durch Bluetooth-Systeme für anderer Funkteilnehmer relativ hoch, auch deshalb weil kein Listen-Before-Talk (LBT)-Mechanismus in Bluetooth implementiert ist. Erst nach der Auswertung der Paketfehlerraten einer Bluetooth-Übertragung werden diese von den verfügbaren Frequenzkanälen ausgenommen, die zu einer erhöhten Paketfehlerrate geführt haben. Dies hat zur Folge, dass bereits bei den ersten Übertragungen von Bluetooth-Paketen andere Teilnehmer gestört werden können. Speziell beim Einsatz von Funktechnologien für die Sensor-Aktor-Kommunikation, bei der definierte Latenzzeiten im Bereich von wenigen Millisekunden eingehalten werden müssen, um Anlagensteuerungen zu realisieren, wird eine Überwachung des Frequenzbands als sinnvoll erachtet. Durch die am Markt vorhandenen Spektrumanalysatoren kann das Spektrum zwar dargestellt werden, allerdings handelt es sich dabei um Messgeräte, die sowohl von der Geschwindigkeit der Signalverarbeitung als auch von den Schnittstellenfunktionalitäten her nicht für einen automatisierten, in die Kommunikation eingebetteten Betrieb, vorgesehen sind. Die Interpretation der Anzeigeergebnisse wird im Allgemeinen durch den Benutzer des Messgeräts durchgeführt. Derartige Labor-messgeräte sind in ihren Anschaffungskosten üblicherweise deutlich höher als die Kosten des gesamten Sensor/Aktor-Netzwerkes einschließlich der angebundenen Sensoren und Aktoren, so dass eine dauerhafte und flächendeckende Implementierung nicht wirtschaftlich wäre. Das nachfolgend vorgestellte Konzept eines Online-Spektrumanalysators mit einer modularen und deshalb skalierbaren Hardware-Architektur soll dies zukünftig ermöglichen. Im handelsüblichen Segment der Messgeräte wird diese Aufgabe typisch durch schnelle Analog-Digital-Wandler (ADC) gelöst. Realtime-Spektrum-Analysatoren (RSA) ermöglichen die Aufnahme von Bandbreiten mit mehreren 100 MHz bei einer gleichzeitigen Auflösung der einzelnen Frequenzen im kHz-Bereich. Dazu werden die HF-Signale mit Hilfe der schnellen Fourier-Transformation (FFT) in den Spektralbereich umgerechnet. Eine automatische Klassifikation der gemessenen Signale ist im Gegensatz zu militärischen Anwendungen im industriellen Bereich nicht vorgesehen. Die Leistungsfähigkeit von PC-gestützte Technologien wie Messkarten und Messboxen liegt in der Regel deutlich unter der Leistungsfähigkeit der Technologien, die in Spezialmessgeräten eingesetzt werden. Durch ihre geringe Messbandbreite von typisch 20 MHz müssen diese das Frequenzband schrittweise in mehreren Frequenzintervallen vermessen, wodurch wiederum zeitliche Lücken entstehen.

Somit ist auch damit eine zeitlich lückenloses Monitoring des gesamten ISM-Bandes nicht möglich.

2 Hardware

Die Grundidee des nachfolgend dargestellten Ansatzes ist, wie in Abb. 1 skizziert, die Messung der Signalstärke auf möglichst allen Frequenzkanälen des 2,45 GHz ISM-Bandes (2,400 GHz bis 2,484 GHz) mit Hilfe von parallel geschalteten HF-Transceivern bzw. der Nutzung der von diesen Transceivern ausgegebenen RSSI-Werten (RSSI = Radio Signal Strength Indicator). Bei den nachfolgend beschriebenen Versuchen wird der CC2400[9] von Texas Instruments genutzt. Da die Messung direkt im Spektralbereich stattfindet, entfällt die relativ aufwändige Umrechnung in den Spektralbereich. Jeder CC2400 vermisst über eine Dauer von 20 μ s einen 1 MHz breiten Frequenzkanal mit einer spezifizierten Genauigkeit von ± 4 dB. Anschließend erfolgt der Wechsel auf eine andere Arbeitsfrequenz. Durch Kalibriermessungen, die in bestimmten Zeitintervallen durchgeführt werden, kann die Genauigkeit deutlich gesteigert werden. Mittels einer speziellen Ansteueroutine können mit dem CC2400 innerhalb von 272 μ s die RSSI-Werte von 8 benachbarten Frequenzkanälen bestimmt werden. Darin eingeschlossen sind die Zeiten für den Frequenzwechsel auf den jeweils nächsten Frequenzkanal von 14 μ s. Durch die Verwendung eines FPGA Spartan6 werden alle Transceiver synchronisiert und die Daten können mit Taktraten von bis zu 1 GHz verarbeitet werden.

Die gemessenen RSSI-Werte der einzelnen Kanäle werden in einem Dual-Port-Memory (DPM) gespeichert. Der ARM9-Microcontroller liest über eine 32 Bit breite externe Busschnittstelle (EBI) die Daten direkt aus dem DPM mit einer Datenrate von bis zu 200 MByte/s. Die

Abb. 1: Blockschaftbild des Low-Cost Spektrumanalysator.

Auswertungs und Klassifikationsalgorithmen werden im ARM-Prozessor durchgeführt und anschließend über das LAN-Modul an eine Softwareanwendung übertragen.

3 Spektralanalyse

Die ursprüngliche Implementierung [7] mit 10 Transceivern sah zur Analyse der verschiedenen Funksysteme zwei verschiedene Modi vor. Zur Erkennung von Funksystemen, die Frequenzsprungverfahren nutzen, wie z. B. Bluetooth (IEEE 802.15.1) wurde die Auswertebandbreite auf 30 MHz reduziert. D. h. mit 10 Transceivern, die jeweils den RSSI-Wert über ein 3 MHz breites Band überwachen kann innerhalb von 32 μ s die Signalstärke über ein 30 MHz breites Signalband bestimmt werden. Mit der Wahl der Messdauer von 32 μ s gegenüber der minimal möglichen Messdauer konnte die Messunsicherheit deutlich reduziert werden. Zur Erkennung von Funksystemen ohne Frequenzsprungverfahren wie z. B. WLAN (IEEE 802.11 b/g/n) oder Zigbee (IEEE 802.15.4) wurde ein Sweep-Modus über das gesamte Frequenzband von 80 MHz mit einer Sweep-Dauer von 1,2 ms implementiert.

Durch die Implementierung eines schnellen Frequenzwechsel nur innerhalb eines Bandes von 8 MHz ohne die Kalibrierung zu verlieren ist es jetzt möglich, das gesamte 2,45 GHz ISM-Band innerhalb von 272 μ s mit 10 Transceivern abzutasten. Ein Bluetooth-Gerät nutzt beim Paging-Vorgang kurze Nachrichten von 68 μ s Dauer. Diese werden auf 16 der 80 verfügbaren Frequenzkanälen gesendet [1]. Innerhalb von 68 μ s werden von jedem HF-Transceiver die RSSI-Werte von 2 Frequenzkanälen gemessen, so dass bei einer Paketwiederholungsrate von 1600 Paketen pro Sekunde und 3200 Paketen eines Paging-Vorgangs insgesamt alle 16 Frequenzkanäle innerhalb von 2 Sekunden ermittelt werden können. Der Paging-Vorgang kann bis zu vier Mal auf verschiedenen Frequenzkanälen wiederholt werden. Zudem ist es jetzt nicht mehr notwendig unterschiedliche Messmodi zu implementieren. Ein WLAN-Beacon-Frame mit einer Dauer von 432 μ s wird ebenfalls vollständig erfasst, so dass eine deutlich genauere Auswertung der Signale möglich ist. Die Signalerkennung und Klassifizierung wurde aufgrund der höheren Geschwindigkeit modifiziert, um die Signale spezifischer vermessen und nach eigenen bekannten Systemen und Störern unterscheiden zu können. Mit Hilfe des 2D-LAD-Algorithmus (Localization Algorithm Based on Double-Thresholding) [2–4] wird ein oberer und unterer Schwellwert für den Rauschpegel berechnet, welcher als Basis für die weitere Signalerkennung verwendet wird. Die durch den Algorith-

Abb. 2: Überlappung der Funkkanäle der verschiedenen Funkstandards im 2,45 GHz ISM-Band.

Abb. 3: Programmablauf-Diagramm zur Erkennung und Klassifizierung von Signalen und Störern.

mus gefilterten Signale werden anschließend die in [5] beschriebenen Algorithmen klassifiziert. Die ersten drei Klassen ergeben sich durch die standardisierten Signale wie WLAN (IEEE 802.11 b/g/n), ZigBee (IEEE 802.15.4) und Bluetooth (IEEE 802.15.1) (vgl. Abb. 2). Die vierte Klasse beinhaltet alle nicht erkannten Signalformen. Darunter zählen auch proprietäre Funksysteme, welche zwar unter die zuvor genannten Standards fallen, aber nicht eindeutig als solcher erkannt werden konnten, wie zum Beispiel IO-Link Wireless, welches dem Bluetooth-Standard entspricht, jedoch ein anderes Zeitverhalten und andere Paketlängen aufweist. Durch die vom Benutzer vorgegebenen A-Priori-Informationen von bekannten bzw. eigenen Funksystemen ergibt sich die fünfte Klasse (vgl. Abb. 3).

Zur Klassifizierung des IEEE 802.11 b/g/n-Standards wird aus der Sendespektralmaske eine Übertragungsform abgeleitet, welche mit den 13 Funkkanälen des gemessenen RSSI-Spektrums korreliert wird. Durch eine dy-

namische Schwellwertanpassung können auch schwache Signale bereits nach kurzer Zeit erkannt werden. Eine ähnliche Vorgehensweise wird bei der Klassifizierung des IEEE 802.15.4-Standards verwendet. Zur Erkennung eines IEEE 802.11.1 (Bluetooth)-Systems werden die RSSI-Messwerte von 3000 Sweeps mit Hilfe eines Histogramms ausgewertet. Dies bedeutet, dass Standard-Funksysteme typisch mit weniger als einer Sekunde mit der Information der verwendeten Frequenzkanäle ermittelt werden können. Durch Vergleichen der bekannten Signale mit den klassifizierten Signalen ist so eine mögliche Vorhersage für die Störung eigener Funkssysteme möglich. Diese können weiter in verschiedene Kategorien bezüglich der verwendeten Frequenzkanäle, Bandbreite und mittlerer Signalstärke sowie nach Zeitpunkt und Dauer des Auftretens kategorisiert werden. Sollte ein Störer erneut auftreten, kann daraus ein Profil abgeleitet werden. Daraus ergeben sich regelmäßige und unregelmäßige Störer. Die Informationen zu den regelmäßigen auftretenden Störern, welche bei jedem Auftreten die gleichen Frequenzkanäle und Bandbreite nutzen, können dann an die Basisstationen gesendet werden. Diese können daraufhin frühzeitig einen Frequenzwechsel durchführen, um die Übertragung auf anderen, nicht genutzten Frequenzkanäle des Störers durch zu führen.

4 Auswertung

Die Auswertung des Spektrums und die Klassifizierung der Signale ist derzeit mit 10 Transceivern mit einer Erkennungsrate von 72,3 % bei dem IEEE 802.11 b/g/n-Standard und 56,2 % für IEEE 802.15.4-Standard möglich. Jedoch können nicht alle Frequenzkanäle lückenlos überwacht werden, da durch die Frequenzwechsel zwischen den RSSI-Messungen eines Transceivers die Frequenzkanäle 252 μ s nicht überwacht werden. Hier gehen die kurzen Pakete im Paging-Verfahren von Bluetooth häufig verloren, so dass es für ein IEEE 802.15.1-System nur eine Erkennungsrate von 16,9 % für jedes Paket besteht. Dies kann jedoch durch ein 2 Sekunden andauerndes Auswerten kompensiert werden so dass die durch den Funkstandard belegten Frequenzkanäle dennoch ermittelt werden können. Die in Abbildung 4 gezeigte Aufnahme eines Bluetooth-System im Paging-Modus mit dem RSA6100 [8] (oben) gegenüber dem Low-Cost-Spektrumanalysator (unten) macht dies deutlich. Um jedoch einen reaktionsschnellen Frequenzwechsel eines Sensor/Aktor-Funknetzwerks auf eine ungestörte Frequenz zu erreichen, ist es nötig, alle Übertragungen von anderen Funksystemen zu erkennen und

Abb. 4: Vergleich eines Bluetooth-Signals aufgenommen mit dem RSA6100A (oben) und dem Spektrumanalysator (unten).

innerhalb einer Millisekunde eine mögliche nicht gestörte Frequenz zu finden und an die Basisstationen zu senden.

Aus diesem Grund wurde zur lückenlosen Überwachung das Konzept des modularen Aufbaus dahin gehend weiter entwickelt, dass alle 84 Frequenzkanäle des 2,45 GHz ISM-Band innerhalb von 2 μ s gemessen werden können. Zur Messung der RSSI-Werte werden 84 synchronisierte CC2650-Module [10] mit 1 MHz Bandbreite und einer Messdauer von weniger als einer Mikrosekunde eingesetzt (vgl. Abb. 5). Dabei ist bei gleicher Genauigkeit von ± 4 dB die Dynamikbereich mit 100 dB um 30 dB größer als die des CC2400. Zur Einbindung in Sensor/Aktor-Netze sind auch weitere Kommunikationsschnittstellen nötig. Die Steuerung und Auswertung des neuen Spektrumanalysators wird durch ein Xilinx Zynq SoC-Modul (System-on-a-Chip) mit einem mit Dual-Core ARM Cortex-A9 und Artix-7 FPGA realisiert. Die beiden ARM-Kerne arbeiten mit einer Geschwindigkeit von 766 MHz. Zur Verarbeitung der Daten ist ein 1 GByte großer DDR3-RAM mit einem Speichertakt bis zu 1066 MHz am SoC angeschlossen. Durch den Dual-Core-Prozessor des CC2650 und die

Abb. 5: Systemaufbau des neuen Spektrumanalysators.

dadurch bedingte Synchronisierung der beiden Kerne können die RSSI-Werte jetzt alle $2\ \mu\text{s}$ ausgelesen werden. Um die RSSI-Daten nach jeder Messung schnell zu verarbeiten, werden diese zu je 32 Bit in Schieberegistern zusammengefasst und mit bis zu 50 MHz Datenübertragungsrate zum SoC übertragen. Hier werden die Daten im SoC durch synchronisierte VHDL-Module verarbeitet. Zur Auswertung und Einbindung in Sensor/Aktor-Netze können neben der kabelgebundenen Gigabit Ethernet-Schnittstelle auch verschiedene Funkschnittstellen und -standards genutzt werden. Hierzu sind neben einem WLAN- und einem Zigbee-Modul noch vier weitere CC2650-Module vorgesehen. Zur einfachen Analyse können die gemessenen Spektraldaten direkt über die HDMI-Schnittstelle visualisiert werden. Durch die höhere Geschwindigkeit der Messung, die höhere Rechengeschwindigkeit der beiden ARM-Kerne für Auswertung wird eine Erkennungsrate für Bluetooth-Systeme deutlich über 95 % erwartet.

5 Zusammenfassung und Ausblick

Das aktuelle System bietet bereits die Möglichkeit, Standards mit und ohne Frequenzsprungverfahren sicher zu erkennen. Jedoch ist die Bestimmung gestörter Frequenzen zu langwierig und zeitlich nicht genau genug aufgelöst, so dass ein Sensor/Aktor-System auf die Informationen der gestörten Frequenzen nicht rechtzeitig reagieren kann. Mit dem neuen wird eine vollständige Messung des Spektrums in $2\ \mu\text{s}$ jegliche Übertragungen eines Funkstandards erfassen. Bereits nach wenigen Übertragungen eines Störers

können so Aussagen zu den gestörten Frequenzkanälen, der Bandbreite und das zeitliche Verhalten bestimmt werden. Die Auswertungszeit wird so unter einer Millisekunde betragen. Damit wird es möglich, den neuen Spektrumanalysator mit einem Sensor/Aktor-Netzwerk zu koppeln um so die Nutzung von gestörten Frequenzkanälen durch das Sensor/Aktor-Netzwerk zu vermeiden. Dieses schnelle, reaktive Verhalten des Sensor/Aktor-Netzwerks auf einen Störer kann so zu einer weiteren Senkung der Paketfehler-rate im Netzwerk führen und die Übertragungssicherheit erhöhen.

Literatur

- [1] IEEE Std 802.15.1™- IEEE Standard for Information technology - Specific requirements - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), New York, 2005.
- [2] J. Vartianinen. Concentrated Signal Extraction Using Consecutive Mean Excision Algorithm, Academic dissertation, Oulu, Mai 2010.
- [3] J.J. Lehtomäki, J. Kokkonen. Spectrum Occupancy Measurements and Analysis Methods on the 2.45 GHz ISM Band. 7th International ICST Conference, CrownCom2012, Stockholm, Juni 2012.
- [4] J.J. Lehtomäki, R. Vuontoniemi, K. Umebayashi, J.P. Mäkelä. Energy Detection Based Estimation of Channel Occupancy Rate with Adaptive Noise Estimation. 6th International ICST Conference, CrownCom2011, Yokohama, Juni 2011.
- [5] L. Van Sang. Algorithmen zur Analyse von Spektralmessung im 2,45 GHz ISM-Band zur Bestimmung von temporär auftretenden Funkstandards, Studienarbeit, Mai 2018.
- [6] R. Heynicke, D. Krush, C. Cammin, G. Scholl, B. Kaercher, J. Ritter, P. Gaggero, M. Rentschler. IO-Link Wireless enhanced factory automation communication for Industry 4.0 applications, Journal of Sensors and Sensor Systems, Vol. 7, 131-142, 2018.
- [7] R. Hornung. Low-Cost Spectrum Analyzer for Cognitive Radio Applications and Coexistence Management in the 2.4 GHz ISM-Band. SENSOR 2013, 2013.
- [8] Tektronix Inc. RSA6100A Series Real-Time Spectrum Analyzers Printed Help Document, Benutzerhandbuch, Mai 2010.
- [9] Texas Instruments Inc. CC2400 2.4 GHz Low-Power RF Transceiver, 2008. URL <http://www.ti.com/lit/ds/symlink/cc2400.pdf>.
- [10] Texas Instruments Inc. CC2650 SimpleLink™ Multistandard Wireless MCU, 2015. URL <http://www.ti.com/lit/ds/symlink/cc2650.pdf>.