dresden elektronik

White Paper

Grundlagen 6LoWPAN

Einführung in das „Internet der Dinge“

Verfasser
Enrico Lehmann
dresden elektronik ingenieurtechnik gmbh

Juli 2012

Abstract

Bisher waren Funknetzwerke, die dem IEEE 802.15.4 Standard folgen, an proprietäre Protokolle gekoppelt. Das bietet aber weder Möglichkeiten der einfachen Erweiterbarkeit noch können diese Netze mit anderen interoperieren. Im Gegensatz dazu steht das Internet, das auf freien Spezifikationen aufbaut, worauf sich auch dessen Erfolg gründet. Mit der nun startenden Einführung des neuen Internet Protokolls in der Version 6 bietet sich nunmehr die Möglichkeit, weltweit nahezu jedem Gerät eine eindeutige Adresse zuzuweisen. Das ließ die Idee entstehen, Sensornetzwerke mit der IPv6 Welt zusammenzuführen. Aus diesem Grund wurde die *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) Arbeitsgruppe der Internet Engineering Task Force (IETF) gegründet, die sich mit dieser Thematik auseinandersetzt.

Die Arbeitsgruppe hat die Grundlagen dafür geschaffen, drahtlose Sensornetzwerke mit dem Internet zu verbinden. In diesem Whitepaper soll die 6LoWPAN Technik näher erläutert, und auf die Funktionsweise und Probleme näher eingegangen werden. Abschließend werden noch einige Einsatzfelder beschrieben und der zukünftige Einsatz weiterer Protokolle erläutert.

Einführung

Abbildung 1 stellt beispielhaft ein Firmennetzwerk mit aufgebautem 6LoWPAN Funknetzwerk dar. Die Anbindung zum Internet geschieht über den Border-Router (auch Edge-Router genannt). An diesem können weitere Netzwerkkomponenten angeschlossen werden. Im dargestellten Fall sind das der Firmen-Server, ein einzelner Arbeitsplatzrechner, ein weiteres Subnetz, das durch den Router SR1 verwaltet wird, und das näher zu erläuternde 6LoWPAN Netzwerk. Der 6LoWPAN Border-Router sorgt zum einen für den Datenaustausch zwischen den Funkknoten und dem Firmennetzwerk, zum anderen für Erzeugung und Verwaltung des Funk-Subnetzes.

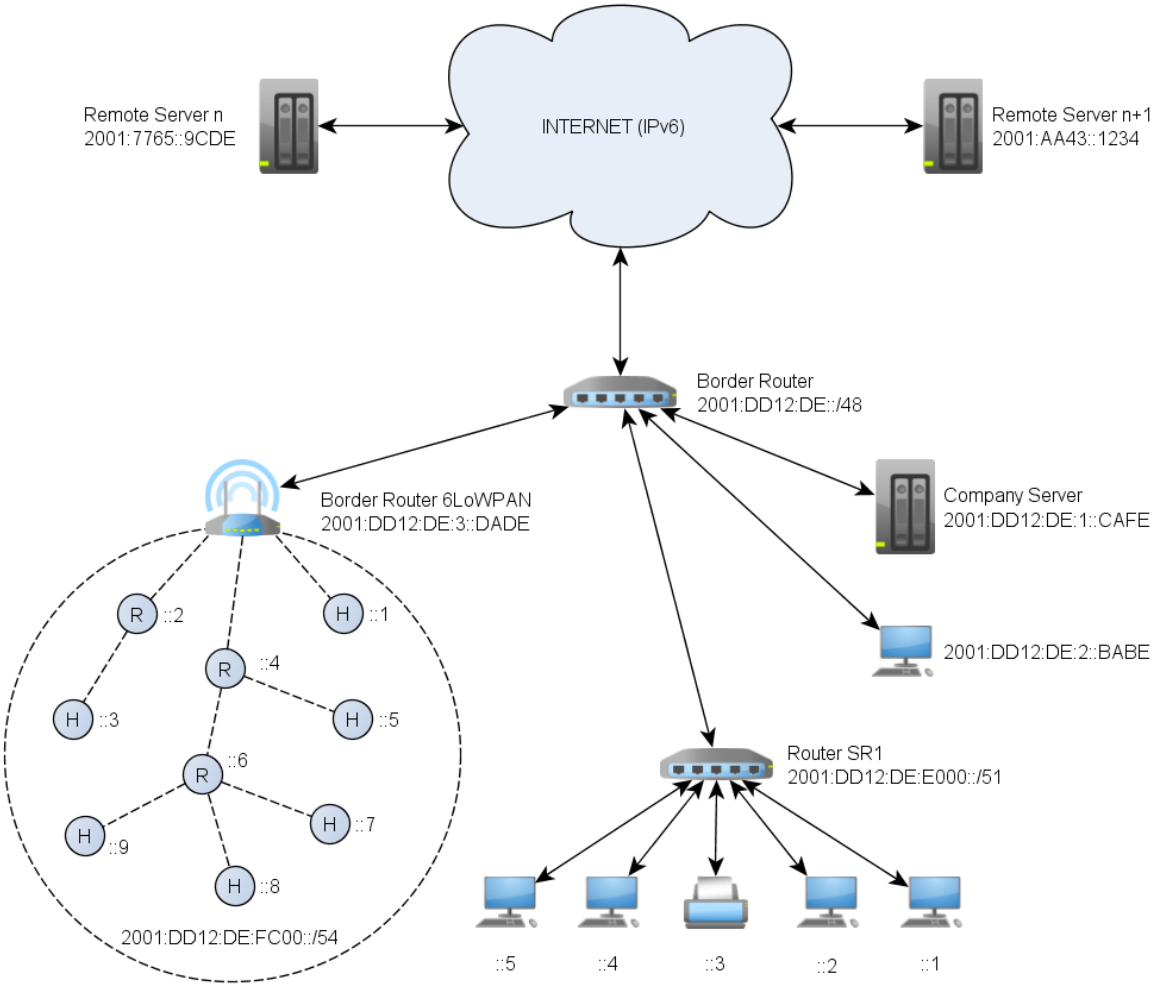


Abbildung 1: IPv6 Netzwerk mit 6LoWPAN Funknetzwerk

Zum besseren Verständnis der 6LoWPAN Funktionsweise führt der nachfolgende Abschnitt in die Grundlagen von IPv6 ein. Es erläutert den Adressaufbau und stellt einige wichtige Adressbereiche sowie Kategorien vor. Um Unterschiede zum IPv4 Protokoll zu verdeutlichen, werden ebenfalls der IPv6 Header und das neue Verfahren der sogenannten Autokonfiguration beschrieben. Der darauf folgende Abschnitt behandelt das eigentliche Thema: 6LoWPAN. Das Verfahren wird vorgestellt und das Protokoll eingehend erläutert.

Glossar

Das Glossar gibt einen Überblick über in diesem White Paper verwendete Begriffe und Definitionen.

Begriff	Beschreibung
802.15.4	IEEE 802.15.4 Standard, geltend für: low-rate wireless Personal Area Network (WPAN)
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
CIDR	Classless Inter-Domain Routing
DAD	Duplicate Address Detection
EUI	Kurzwort für “Extended Unique Identifier” (Bildung von MAC Adressen)
Hop	Zwischenknoten einer Route sowie Weg von einem Netzknoten zum nächsten
HTTP	Hypertext Transfer Protocol
IDD	Interface Identifier
IETF	Internet Engineering Task Force
IPv6	Internet Protocol Version 6, Version des Internet Protokolls (IP) bestimmt zur Nachfolge des IPv4, derzeit meist benutztes Protokoll zur Steuerung fast allen Internet-Verkehrs.
MAC	Medium Access Control ... Schicht, Adresse etc.
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
OSI	Open Systems Interconnection (OSI) Modell, Schichtenmodell als Designgrundlage von Kommunikationsprotokollen in Rechnernetzwerken.
PHY	OSI Modell Schicht 1: Die Bitübertragungsschicht definiert elektrische und physikalische Geräte-Spezifikationen. Sie definiert den Zusammenhang zwischen Gerät und Übertragungsmedium sowie Aufbau aller Hardware-Komponenten.
PSDU	PHY Service Data Unit
RFC	Liste der “Request For Comments” Memoranden (auf der IETF Website verfügbar)
RPL	Routing Protocol for low power and Lossy networks
ROLL	Routing Over Low power and Lossy networks
SOAP	Simple Object Access Protocol, ein Protokoll zum Austausch XML-basierter Nachrichten über ein Computernetzwerk
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WPAN	Wireless Personal Area Network

Internetprotokoll Version 6 (IPv6)

Grundlage des heutigen Internets bildet das Internetprotokoll Version 4 (IPv4). In den 1980er Jahren entwickelt, stellt es mehr als 4 Milliarden Adressen zur Verfügung. Durch den Zuwachs an internetfähigen Geräten gingen Wissenschaftler aber davon aus, dass Ende 2011 keine IPv4 Adressen mehr zur Verfügung stehen **[1]**. An dieser Stelle setzt das 1995 standardisierte Internetprotokoll Version 6 an. Es deckt einen Adressraum von 2^{128} Adressen ab - das wären 6,7 $\cdot 10^{23}$ Adressen pro Quadratmeter Erdoberfläche. Damit kann den neuen Anforderungen auf Jahrzehnte hinaus Rechnung getragen werden.

IPv6 Adressen

Die Darstellung einer IPv6 Adresse erfolgt ähnlich wie auch bei einer IPv4 Adresse nach dem Classless Inter-Domain Routing (CIDR) Verfahren, das die Adresse in einen Netzwerk- und einen Hostteil unterteilt.

```
IPv6 address/prefix length
2001:0CFF:0:CD30::/60
```

Wie ersichtlich, unterscheidet sich bei IPv6, im Gegensatz zu IPv4, aber die Notationsweise. Aufgrund des großen Adressbereiches werden IPv6 Adressen in hexadezimaler Schreibweise dargestellt und in Blöcke von jeweils 16 Bit, durch Doppelpunkte getrennt, zusammengefasst. Führende Nullen können entfernt und Blöcke von aufeinanderfolgenden Nullen einmalig durch '**::**' ersetzt werden. Nachfolgendes Beispiel verdeutlicht das nochmals.

```
AA12:BBFD:0000:0000:0000:0000:CAFE:0011
AA12:BBFD::CAFE:11
```

Eine IPv6 Adresse wird nie an ein System (z.B. PC), sondern nur dessen Schnittstelle (engl. Interface) gebunden. Ein Interface wiederum kann mehrere IPv6 Adressen besitzen. Die Adressen werden kategorisiert, und in Unicast, Anycast und Multicast unterteilt. **Tabelle 1** erläutert die unterschiedlichen Kategorien näher und **Tabelle 2** führt einige wichtige IPv6 Adressen auf. Link Local Unicast Adressen bezeichnen link-lokale Adressen, die nur im eigenen Subnetz erreichbar sind (Router leitet Pakete nicht weiter). Sie bestehen aus dem Präfix (siehe **Tabelle 2**) und dem sogenannten 64 Bit großem *Interface Identifier* (IID). Häufig wird dafür die *Link-Layer* Adresse (auch MAC-Adresse genannt) des Interfaces genutzt. Global Unicast Adressen sind weltweit eindeutige und routbare IPv6 Adressen. Im Allgemeinen bestehen auch sie aus einem 64 Bit Präfix und dem 64 Bit Interface Identifier.

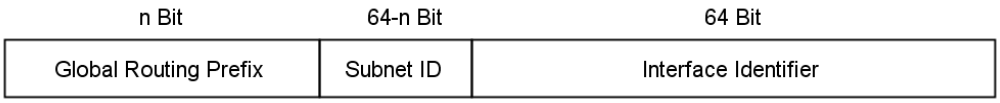
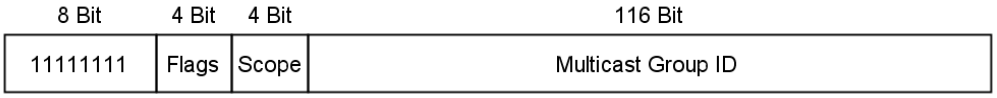
Kategorie	Aufbau / Beschreibung
Unicast	 Ein Paket mit Unicast Zieladresse wird nur an das Interface mit dieser Adresse gesendet.
Anycast	Anycast Adressen werden aus Unicast Adresen gebildet, sind also syntaktisch gleich. Die Anycast Adresse gilt für mehrere Interfaces, das Paket wird aber nur an eines dieser Interfaces gesendet (immer an das nächst-gelegene, abhängig vom Routing-Protokoll).
Multicast	 Pakete mit Multicast Zieladresse werden an alle Interfaces gesendet.

Tabelle 1: IPv6 Adresskategorien

Der Wirkbereich von Multicast Paketen kann über die Adressvariablen *Flags* und *Scope* (siehe **Tabelle 1**) beeinflusst werden (weitere Informationen finden Sie in RFC 4291). So können Multicast Pakete nur innerhalb eines Subnetzes oder, bei richtiger Einstellung, weltweit gesendet und empfangen werden.

Adresstyp	Komprimierte Notation	Ausführliche Notation	Präfix binär
Undefined	::/128	0:0:0:0:0:0:0:0/128	00…00 (128 Bits)
Loopback	::1/128	0:0:0:0:0:0:0:1/128	00…01 (128 Bits)
Multicast	FF00::/8	FF00::/8	11111111
Link Local Unicast	FE80::/10	FE80::/10	1111111010
Global Unicast	All other addresses		

Tabelle 2: Wichtige IPv6 Adressen

IPv6 Header

Der IPv6 Header soll an dieser Stelle näher erläutert werden, da dies zum besseren Verständnis des 6LoWPAN Verfahrens beiträgt.

Abbildung 2: IPv6 Header

In **Abbildung 2** ist der IPv6 Header dargestellt, der aus den nachfolgend kurz erläuterten Feldern besteht: Das erste Feld *Version* gibt, wie der Name schon sagt, die Version des Protokolls wieder. In diesem Fall also die Version 6. Die nachfolgenden Felder *Traffic Class* und *Flow Label* haben in Routern Einfluss auf die Behandlung von IPv6 Paketen (Priorität etc.). *Payload Length* gibt die Länge der nachfolgenden Nutzdaten an. Das nachfolgende Protokoll (z.B. TCP oder UDP) wird über *Next Header* identifiziert. Der Wert in *Hop Limit* definiert die maximale Anzahl an Hops (engl: „Hopser“, Weg von einem Netzknoten zum nächsten), die ein IPv6 Paket passieren darf. In *Source* bzw. *Destination Address* steht die 128 Bit lange Quell- bzw. Zieladresse.

Autokonfiguration

Das Verfahren der Autokonfiguration in IPv6 ist eine der größten Änderungen zu IPv4. Es gestattet einem Knoten das selbstständige Erstellen einer vollständigen IPv6 Adresse, ohne dass manuell eingegriffen werden muss oder Konfigurations-Server notwendig sind. Um eine Adresse zu erhalten, kommuniziert ein Host über das *Neighbor Discovery Protocol* (NDP) mit den Teilnehmern im eigenen Subnetz. Das Verfahren läuft dabei nach dem in Abbildung 3 dargestelltem Schema ab. Zum Einsatz kommen dabei die vier folgenden Nachrichtentypen:

- *Router Solicitation*
- *Router Advertisement*
- *Neighbor Solicitation*
- *Neighbor Advertisement*

Router Solicitation Nachrichten beinhalten, neben weiteren Optionen, den für das Subnetz gültigen Präfix. Die Nachrichten werden von allen Routern periodisch ausgesendet. Möchte ein Host am Netzwerk teilnehmen, weist er sich eine Link-Local Unicast Adresse zu (`FE80::<64 Bit IID>`). Dann sendet er diese Adresse über die Neighbor Solicitation Nachricht an alle anderen Teilnehmer im Subnetz, um zu überprüfen, ob die Adresse nicht schon belegt ist. Erhält der Host innerhalb eines bestimmten Zeitraumes keine Neighbor Advertisement (NA) Nachricht, kann er davon ausgehen, dass die Adresse einmalig ist. Dieses Verfahren wird auch Duplicate Address Detection (DAD) genannt. Um nun das korrekte Netzwerk-Präfix zu erhalten, sendet der Host eine Router Solicitation Nachricht an den Router, um mit der Router Advertisement Nachricht das korrekte Netzwerk-Präfix zu erhalten.

Mittels dieser vier Nachrichten ist ein Host in der Lage, sich eine weltweit gültige IPv6 Adresse zuzuweisen.

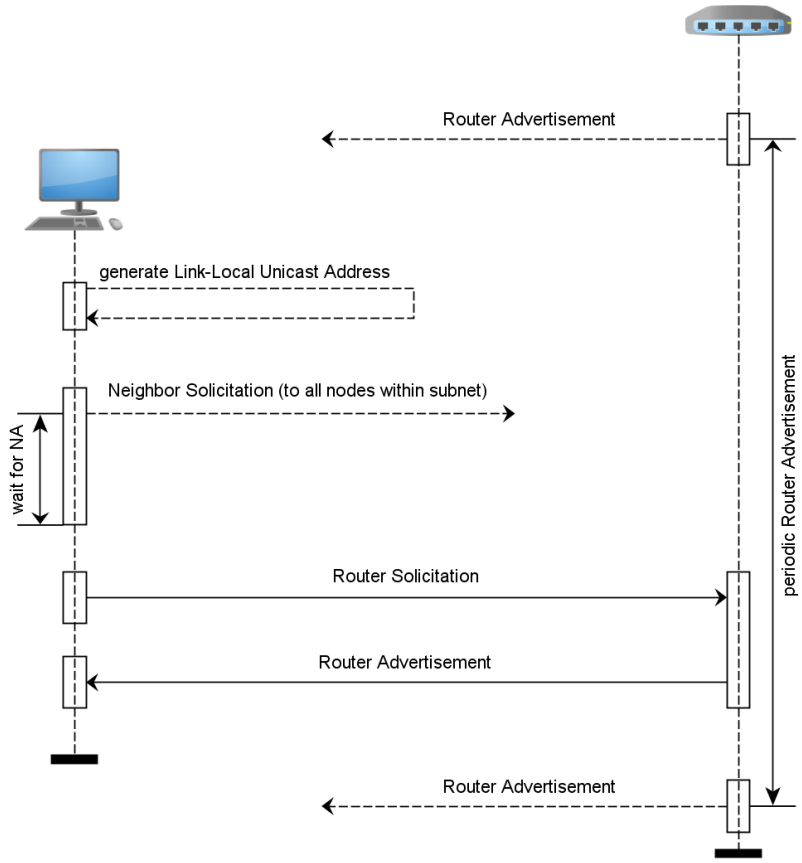


Abbildung 3: Ablauf einer Autokonfiguration

6LoWPAN

Für den Versand von IPv6 Paketen innerhalb von 802.15.4 Netzwerken sind zwei größere Hürden zu nehmen. Erstere ist die maximal zur Verfügung stehende Payloadgröße von 127 Bytes. Von diesem Wert müssen 25 Bytes für den MAC Header selbst, und weitere 40 Bytes für den IPv6 Header abgezogen werden. Damit verbleiben 62 Bytes für Nutzdaten. Kommen außerdem Verschlüsselung und/oder zusätzliche Anwendungsprotokolle (z.B. TCP, UDP,...) hinzu, verringert sich der verfügbare Speicherplatz für Nutzdaten rapide. **Abbildung 4** verdeutlicht diese Problematik bildlich. Um dem entgegenzuwirken, sind Techniken zur Header-Komprimierung entworfen worden [RFC 4919, RFC 4944].

127 Byte			
MAC Header	IPv6 Header	UDP Header	Payload
25 Byte	40 Byte	8 Byte	54 Byte

Abbildung 4: Verhältnis Kopfdaten zu Nutzdaten

Die zweite Hürde stellt die Maximum Transmission Unit (MTU) von IPv6 mit 1280 Bytes dar. Das ist die Größe, welche die MAC Schicht mindestens zur Verfügung stellen muss, um ohne Fragmentierung ein IPv6 Paket senden zu können. Da dies offensichtlich nicht möglich ist, muss eine Fragmentierungs- und Defragmentierungs-Ebene eingeführt werden, die es ermöglicht, IPv6 Pakete auf 802.15.4 Frames aufzuteilen und anschließend wieder zusammenzusetzen.

Die verschiedenen Aufgabengebiete wie Header-Komprimierung, Fragmentierung, Routing und Autokonfiguration, werden unter der Bezeichnung Adaptation Layer (engl. Anpassungs-Schicht) vereint und definieren den Begriff 6LoWPAN.

Routing unter 6LoWPAN

Mittels Routing werden Pakete, mitunter über mehrere Zwischenknoten (engl. hops), von einem Quell- an einen Zielknoten vermittelt. Abhängig von der Schicht, in der das Routing zum Einsatz kommt, werden die Protokolle in zwei verschiedene Kategorien unterteilt: Mesh-Under und Route-Over. Ersteres nutzt die MAC-Adresse bzw. 16 Bit Short Adresse (Schicht 2 Adressen), um Pakete weiterzuleiten, letzteres nutzt dafür die IP Adressierung (Schicht 3). **Abbildung 5** verdeutlicht das Schema der beiden Verfahren.

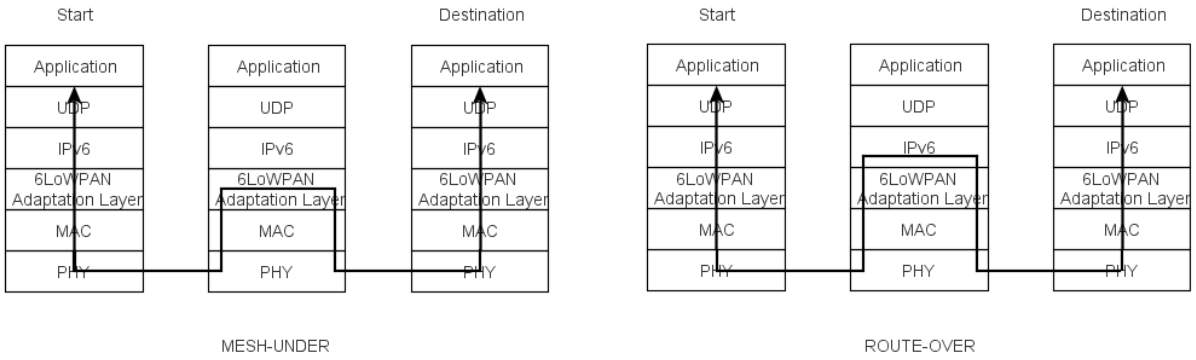


Abbildung 5: Unterschied Mesh-Under vs. Router-Over Routing

Da innerhalb eines Mesh-Under Netzwerkes das Routing für die IP Schicht transparent geschieht, werden Mesh-Under Netzwerke auch als ein einziges IP Subnetz gesehen. Der einzige IP Router innerhalb eines solchen Netzwerkes ist der Border-Router. Dadurch wird für das gesamte 6LoWPAN Funknetzwerk eine Broadcast Domäne aufgebaut, welche die Kompatibilität mit einigen IPv6 Protokollen gewährleistet. So zum Beispiel das oben erläuterte Verfahren zur Sicherstellung, dass keine doppelten Adressen vorhanden sind. Diese Nachrichten müssen an alle Teilnehmer des Netzes gesendet werden, was durch das Routing Schema immer gewährleistet wird. Auf der anderen Seite wird dadurch eine sehr hohe Netzwerklast generiert, da diese Pakete immer an alle Teilnehmer gesendet werden müssen. Mesh-Under bietet sich daher in lokal begrenzten und kleinen Netzwerken an. Auch größere Netzwerke können hiermit realisiert werden, wenn Multicast Pakete vermieden und, soweit möglich, durch Unicast Pakete ersetzt werden.

In Route-Over Netzwerken findet Routing hingegen in der IP Schicht statt, daher stellt jeder Hop einen IP-Router dar **[2]**, **[3]**. Das bedeutet aber auch, dass jeder Hop im Netzwerk die entsprechenden Fähigkeiten eines IP Routers, wie z.B. Neighbor Discovery, mitbringen muss. Das wiederum ermöglicht die Nutzung von IP Funktionalitäten wie IPv6 Routing, Dienste für Management sowie Konfiguration. Die Verwendung von IP Routing bildet auch die Grundlage dafür, unabhängig von unteren Schichten zu sein, und vereinfacht daher die Integration in leistungsfähigere Netzwerke. Zudem werden Nachrichten nicht über Broadcast gesendet, sondern immer nur zu den Knoten innerhalb der Funkreichweite. Das beschränkt aber Protokolle (Neighbor Discovery), die immer an alle Teilnehmer Multicast Pakete versenden. In diesem Fall müssen die Nachrichten über die Router-Grenzen hinweg weitergeleitet werden.

Ein Protokoll für Route-Over Netze, das sich gerade im Standardisierungsprozess befindet, ist das Routing Protocol for Low power and Lossy Networks (RPL). Weitere Informationen dazu sind auf der Arbeitsgruppenseite Routing Over Low power and Lossy networks[1] (ROLL) des IETF zu finden. Anhand dieser Aussage ist schon ein klarer Trend erkennbar, welches Routing-Verfahren Einzug in die Produkte halten wird. Route-Over besitzt gegenüber Mesh-Under den Vorteil, dass die meisten Proto-

[1] http://datatracker.ietf.org/wg/roll/ Stand: 08.07.2011

kolle ohne Änderungen eingesetzt werden können, und die Probleme beim Routing über die Schicht 2 umgangen werden. Denn, werden unterschiedliche Netze untereinander verbunden, und kommen unterschiedliche Routing-Verfahren auf der Schicht 2 zum Einsatz, kann das zu Fehlverhalten führen, das aber in Schicht 3 nicht mehr sichtbar ist.

Fragmentierung

Die Fragmentierung dient zur Aufteilung eines großen Paketes in mehrere kleinere Pakete. Dazu werden in jedem Paket zusätzliche Daten generiert, um die Pakete am Ende wieder in der richtigen Reihenfolge zusammensetzen zu können. Dieser Schritt wird als Defragmentierung bezeichnet. Beim Zusammensetzen werden die zusätzlich erzeugten Daten entfernt und die Pakete wieder zu einem vollständigen Gesamtpaket zusammengeführt.

Das Verfahren ist bei 6LoWPAN offensichtlich notwendig, da ein IPv6 Paket bis zu 1280 Bytes groß sein kann, aber die maximale Paketgröße in IEEE 802.15.4 nur 127 Bytes beträgt.

Auch bei der Fragmentierung muss unterschiedliches Verhalten in Abhängigkeit vom eingesetzten Routing beachtet werden. So werden in Mesh-Under Netzwerken die Fragmente bis zum Zielknoten weitergeleitet und erst dort zusammengesetzt. Route-Over Netzwerke hingegen leiten jedes Fragment nur bis zum nächsten Hop weiter. Dort werden alle Fragmente zusammengesetzt und dann das Gesamtpaket ausgewertet, um den nächsten Zielknoten zu ermitteln. Bei Route-Over Netzwerken muss also jeder Hop alle Fragmente speichern, und deshalb über genügend Ressourcen verfügen. Das entfällt bei Mesh-Under, dafür wird sehr schnell höherer Netzwerkverkehr generiert, da alle Fragmente sofort weitergeleitet werden. Geht dabei ein Fragment verloren, muss das komplette Paket neu angefordert werden **[4]**.

Generell sollte versucht werden, eine Fragmentierung zu vermeiden. Zum einen steigt der Verwaltungsaufwand zur Realisierung des Verfahrens und zum anderen muss immer genügend Speicher (mind. 1280 Bytes) zur Verfügung stehen, um einen sicheren Ablauf zu gewährleisten. Gerade für ressourcenbeschränkte Geräte stellt das in den meisten Fällen einen Engpass dar. Oft können bei näherer Betrachtung die inhaltlich wichtigen Daten auf ein Minimum reduziert werden, so dass alle relevanten Daten in einem Paket Platz finden. Diese Maßnahmen sind weitaus effizienter, senken die Netzwerklast und sorgen für eine längere Lebensdauer bei Geräten mit Batterieversorgung.

Autokonfiguration

Die Autokonfiguration beschreibt das selbständige Erzeugen einer vollständigen IPv6 Adresse. Diese besteht aus dem 64 Bit Präfix mit dem anschließenden 64 Bit Interface Identifier (IID). Letzterer wird vom Knoten selbst generiert. Basiert die Schnittstelle des Gerätes, wie im IEEE 802.15.4 Standard vorgesehen, auf einer EUI-64 Adresse, dann kann zur Erzeugung des IID das modifizierte EUI-64 Verfahren, wie in **Abbildung 6** zu sehen, genutzt werden. Es ist aber auch möglich, die 16 Bit Short Address dafür zu nutzen. Dabei wird eine Pseudo 48 Bit Adresse nach folgendem Schema erstellt:

```
16_Bit_PAN_ID : 16_Bit_Zeros : 16_Bit_Short_Address
```

Der IID wird aus dieser Adresse wiederum mit der Modified EUI-64 Methode erzeugt. Generell sollte aber davon abgesehen werden, die Short Address als IID zu nutzen. Denn die Short Address ist nur solange gültig, wie eine Verbindung mit dem PAN Koordinator besteht. Fällt der PAN Koordinator aus, oder die Verbindung bricht ab (und muss neu gestartet werden), dann kann der Knoten eine andere Short Address erhalten. Das wiederum führt nach außen zu einem ungültigen IID.

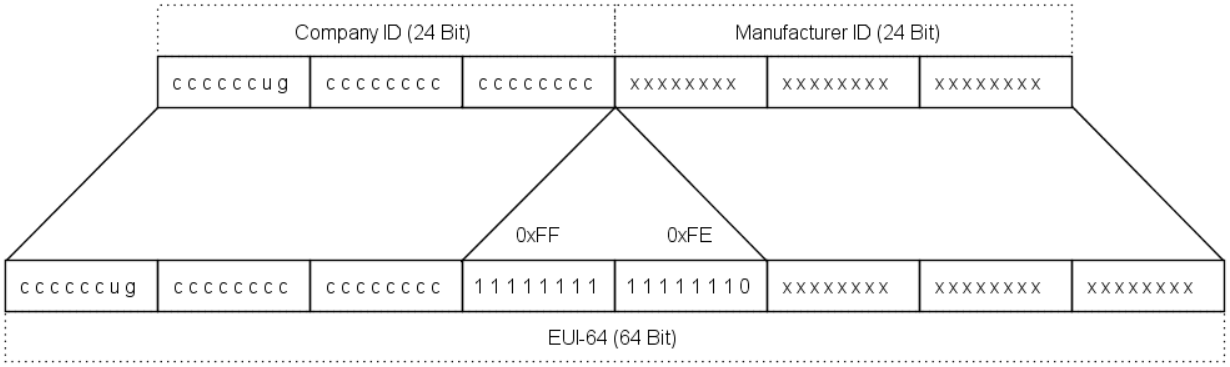


Abbildung 6: Modifiziertes EUI-64 Verfahren

Die Autokonfiguration besteht aus mehreren Nachrichten, hier die Nachrichten des Neighbor Discovery Protocol (NDP). Um diese innerhalb LoWPANs zu nutzen, sind einige Herausforderungen zu meistern. Denn Nachrichten wie Router Advertisement, Router Solicitation und Neighbor Solicitation sind an Multicast Adressen gerichtet. Im Mesh-Under Netzwerk, das einen einzigen IP-Link darstellt, müssen damit alle Knoten im Netz die Nachricht erhalten. Das wiederum flutet das Netzwerk und beeinträchtigt die Bandbreite erheblich. Demgegenüber steht der Vorteil, dass das NDP nahezu unverändert übernommen werden kann, da alle Knoten im Netzwerk erreichbar sind (unter der Annahme, dass alle Knoten aktiv sind).

Anders hingegen im Route-Over Netzwerk. Denn da jeder Hop einen IP Router darstellt, wird der Muticast zu einem Broadcast für alle Knoten in Funkreichweite. Das grenzt zwar die Netzwerklast auf diesen Bereich ein, löst aber genau dadurch nicht die Problematik der notwendigen Duplicate Address Detection (DAD), also der Überprüfung auf doppelte Adressen. Denn die DAD verlangt nach einem transitiven Netzwerk (Knoten A kann Paket an Knoten B senden; Knoten B kann Paket an Knoten C senden; dann kann Knoten A auch ein Paket an Knoten C senden). Im transitiven Netzwerk kann die Eindeutigkeit einer Adresse durch Erreichbarkeit aller Knoten sichergestellt werden. Da ein Route-Over Netzwerk aber nicht transitiv ist, kann die Eindeutigkeit einer Adresse nicht gewährleistet werden **[2]**.

Diese und weitere Problemfälle des Neighbor Discovery Protokolls in Bezug auf LoWPANs werden in dem Internet-Entwurf **[5]** behandelt. Es werden Lösungen vorgeschlagen und auf die entsprechenden Neuerungen und Erweiterungen eingegangen. So ist es das Ziel, Multicast Adressen durch entsprechende Unicast Adressen zu ersetzen. Realisiert wird das durch den erweiterten Einsatz des Border-Router. Dieser kennt die Adressen aller Knoten im Netzwerk und stellt gleichzeitig die Schnittstelle zum Netzwerk außerhalb des LoWPANs dar. Damit senden Knoten zur Duplicate Address Detection keinen Multicast, sondern einen Unicast zum Border-Router. Weitere Informationen in der Anwendung des NDP können **[5]** entnommen werden. Der Internet- Entwurf steht mittlerweile vor der Standardisierung zum RFC.

Header Komprimierung

Header Komprimierungen sind gängige Praxis, es existieren verschiedene Verfahren für den IP Header. Das traditionelle Verfahren ist zustandsbasiert und übermittelt immer nur die Unterschiede zum vorhergehenden Header. Einsatz findet es bei Punkt-zu-Punkt Verbindungen, da es einen Zustand zwischen zwei Endpunkten aufbaut. Bei sich dynamisch ändernden Funknetzwerken ist das Verfahren aber ungeeignet, daher wurden neue Wege gesucht und in **[6]** entwickelt.

Das Verfahren nutzt zur Komprimierung des IPv6 Headers zwei verschiedene Methoden. Erstens entfernt es redundante Informationen, die aus anderen Schichten oder dem Kontext abgeleitet werden können. So hat das Feld *Version* im IPv6 Header immer den Wert ‘6‘, es kann davon ausgegangen werden, dass dieser sich innerhalb eines 6LoWPAN Netzes nicht mehr ändert - daher kann das Feld entfernt werden. Auch können das Längenfeld sowie Adressinformationen aus dem MAC Header (dieser befindet sich vor dem IP Header und logisch eine Schicht unterhalb der IP Schicht) gewonnen werden. Zweitens werden für einige IPv6 Felder bekannte Standardwerte gesetzt und können dadurch kompakter übertragen werden. So sind *Traffic Class* und *Flow Label* immer Null und das *Hop Limit* wird auf die Werte 1, 64 oder 255 gesetzt. Optional kann die Komprimierung beliebiger IPv6 Präfixe vorgenommen werden. Dazu enthält jeder Knoten eine Tabelle mit Präfixen und einer damit verknüpften Nummer. Die Nummer ist auf 4 Bit begrenzt, also kann die Tabelle maximal 16 Einträge enthalten. Ist der Präfix bekannt, wird nur noch die Nummer übertragen, nicht aber der 8 Byte lange Präfix **[3]**. Eine Methode, wie die Tabelle mit Präfixen gefüllt wird, ist aber nicht Bestandteil der Spezifikation **[6]**.

Abbildung 7 stellt das IPv6 Header Komprimierungsverfahren beispielhaft dar. Findet eine Kommunikation innerhalb des 6LoWPAN Netzwerkes statt, kann der IPv6 Header auf zwei Bytes komprimiert werden. Wird die Präfix-Tabelle verwendet, und die Präfixe für das aktuelle Sub- und das externe Netz sind bekannt, kann der IPv6 Header noch auf 12 Bytes komprimiert werden (siehe b.). Sind hingegen die Präfixe nicht bekannt und müssen eingefügt werden, kann immer noch eine Kompressionsrate von 50% erzielt werden. Bei den Beispielen wurde davon ausgegangen, dass die Interface Identifier (IID) aus den Adressfeldern des MAC Header abgeleitet werden können.

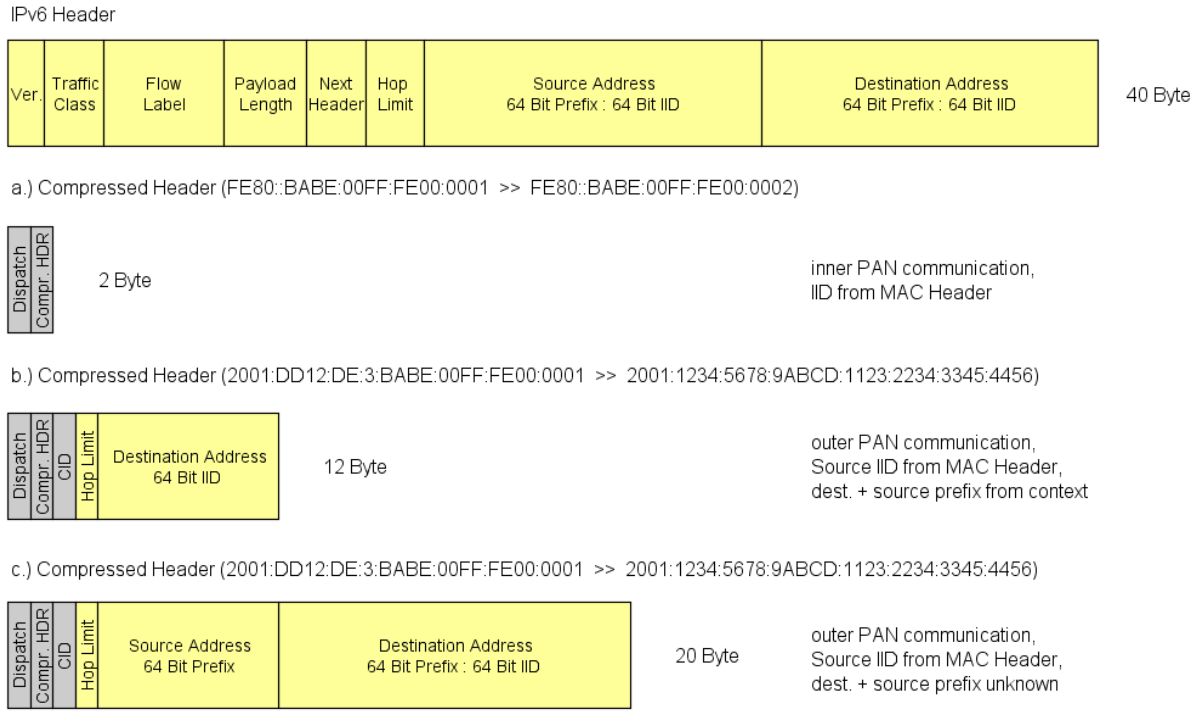


Abbildung 7: Header Komprimierung

Zum Schluss soll noch bemerkt werden, dass in der Spezifikation **[6]** auch ein Verfahren zur Komprimierung des User Datagram Protocol (UDP) Headers dargestellt ist. Damit ist es möglich, den 8 Byte UDP Header auf bis zu 1 Byte zu reduzieren.

Einsatz weiterer Protokolle

Bisher wurde nur das Verfahren beschrieben, um effizient IPv6 Pakete über Funknetzwerke zu übertragen. Interessant sind aber darauf aufbauende Protokolle wie UDP und das bekannte Transmission Control Protocol (TCP), auf dem wiederum das Hypertext Transfer Protocol (HTTP) aufsetzt. Denn erst durch den Einsatz dieser Protokolle können die bereits in der Praxis existierenden und benutzten Anwendungen zum Einsatz kommen. Für das verbindungslose und dadurch anspruchslose Protokoll UDP sind Methoden entwickelt worden, die es ermöglichen, den Header stark zu komprimieren. Das weitaus populärere, allerdings verbindungsorientierte, Transportprotokoll TCP kann bisher mit keinem Verfahren einfach komprimiert werden. Erste Entwicklungen dazu fanden in RFC1144 statt, der TCP für serielle Schnittstellen nutzbar machte. Entwicklungen über RFC 2507 führen zum aktuellen Internet Entwurf **[7]**. Letzterer ist speziell auf die Bedürfnisse von Funknetzwerken ausgelegt. Trotz dieser Entwicklungen hat es noch keinen Einzug in aktuelle Implementierungen gehalten (außer die Berkeley IP Implementierung BLIP[2]).

Weitere Internetprotokolle, wie auch HTTP, sind nicht mit dem Ziel entwickelt worden, kompakt, maschinenlesbar und erweiterbar zu sein, und sind daher nur mit hohem Aufwand für eingebettete Systeme zu bearbeiten. Hinzu kommt die fehlende Unterstützung von Komprimierungsverfahren, die auf eingebetteten Systemen einsetzbar sind. Anwendungen oberhalb von HTTP, wie zum Beispiel SOAP, bringen weitere Schwierigkeiten mit sich. SOAP Anwendungen werden als Web-Services bezeichnet und basieren auf XML. Vorwiegend finden sie Einsatz zur Netzwerkkommunikation von Maschine-zu-Maschine (M2M). Über SOAP können Funktionen zum Zugriff auf bestimmte Eigenschaften einer Maschine realisiert werden. XML als menschenlesbares Format mit hohen Speicheranforderungen ist für Funkknoten mit geringer Bandbreite eher ungeeignet obwohl es Komprimierungsverfahren (WBXML, BXML, EXI) gibt. Diese sind aber für eingebettete Systeme nur begrenzt einsatzfähig.

Beschränkt man sich aber nicht nur auf TCP, sondern betrachtet das UDP Protokoll näher, lässt sich feststellen, dass es eine Reihe nicht zu unterschätzender Anwendungsprotokolle mitbringt. Hier existieren Protokolle zum Transport von Echtzeitdaten, über die Verwaltung von Netzwerken, bis hin zu einfachen Dateiübertragungsprotokollen. Zudem gibt es aktuelle Bestrebungen, Webservices über UDP für 6LoWPAN Netzwerke nutzbar zu machen. So versuchen Entwicklungen, SOAP-over-UDP[3], und dessen Alternative, Representational State Transfer (REST), im Bereich von Funknetzwerken einzusetzen. Letzteres hat in den letzten Jahren enorm an Bedeutung gewonnen und ist ein Architektur-Modell, das es ermöglicht, Web-Services zu beschreiben. In der Constrained RESTful Environments[4] (CoRE) Arbeitsgruppe des IETF werden Spezifikationen erarbeitet, mit Hilfe derer ressourcenbeschränkte Geräte über Web-Services bedient werden können. Dafür ist das Constrained Application Protocol (CoAP) entworfen worden, das genau dieses Aufgabengebiet abdeckt.

[2] http://smote.cs.berkeley.edu:8000/tracenv/wiki/blip
[3] http://docs.oasis-open.org/ws-dd/soapoverudp/1.1/os/wsdd-soapoverudp-1.1-spec-os.html
[4] https://datatracker.ietf.org/wg/core/charter/

Anwendungsfelder

Im Gebäudemanagement kann diese Technologie zur Überwachung von Temperaturen und der damit verbundenen Steuerung der Klimatechnik dienen. Es können Lichtsensoren angebracht werden, anhand derer das künstliche Licht innerhalb des Gebäudes automatisch entsprechend der natürlichen Lichtmenge gesteuert wird. Das kann nicht nur zu hohen Einsparungen führen, auch die zentrale Steuerung über einen Server, die von außerhalb möglich ist, trägt zur komfortablen Bedienung und hohem Nutzen bei.

Abbildung 8: Gebäudeautomatisierung [8]

Das Speditionsgeschäft umfasst Transportwege zu Wasser, zu Lande und in der Luft. Werden dabei verderbliche Lebensmittel transportiert, sind die Umgebungsbedingungen (Temperatur, Luftfeuchte, ggf. Gas-Zusammensetzung, Licht) von immanenter Bedeutung. An dieser Stelle können Kisten mit Sensoren ausgestattet werden, die eben diese Werte überprüfen und aktuelle Messwerte an ein Gateway senden. Das sorgt dafür, dass die Daten an eine Zentrale gesendet werden, von wo aus das Geschehen überwacht und in bestimmten Fällen eingegriffen werden kann.

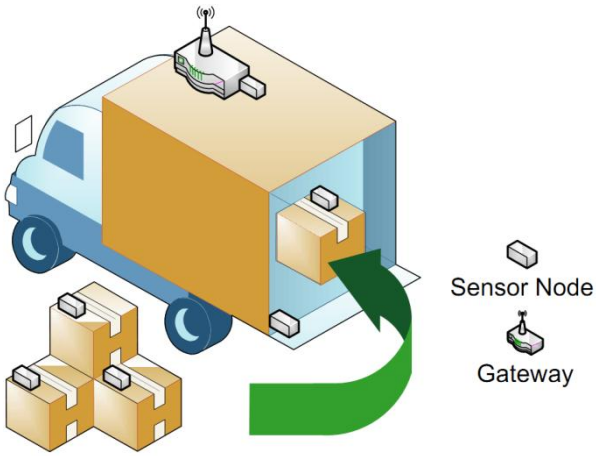


Abbildung 9: Transportwesen [9]

Die Automatisierungstechnik bietet sehr viele Anwendungsfelder aufgrund des breiten Spektrums. Da das Web-basierte Steuern und Regeln schon lange Stand der Technik ist, bietet sich der Einsatz von 6LoWPAN Modulen an, um vorhandene Technologien einzusetzen, und gleichzeitig die Vorteile (z.B. des Mesh-Netzwerkes) zu nutzen. Skeptiker in Bezug auf Echtzeitfähigkeit und Einsatzmöglichkeiten seien darauf hingewiesen, dass das Ethernet ebenfalls nicht echtzeitfähig ist, aber aus der heutigen Automatisierungstechnik nicht mehr wegzudenken ist.

Abbildung 10: Automatisierungstechnik [10]

Eine Teilaufgabe im Bereich des Gesundheitswesens ist die Überwachung von Frühgeborenen, die sehr empfindlich gegenüber Temperaturschwankungen sind. Über in der Kleidung eingenähte Sensoren können zentral alle Werte überwacht werden. Ebenso gilt das für Menschen, deren Vitalfunktionen ständig überwacht werden müssen, ohne ihren Alltag zu sehr einzuschränken. Mit entsprechenden Sensoren und der ständigen Online-Aktualisierung kann sofort auf Veränderungen reagiert und eingegriffen werden. Eine vergleichbare Funktionalität kann für ältere Menschen zum Einsatz kommen.

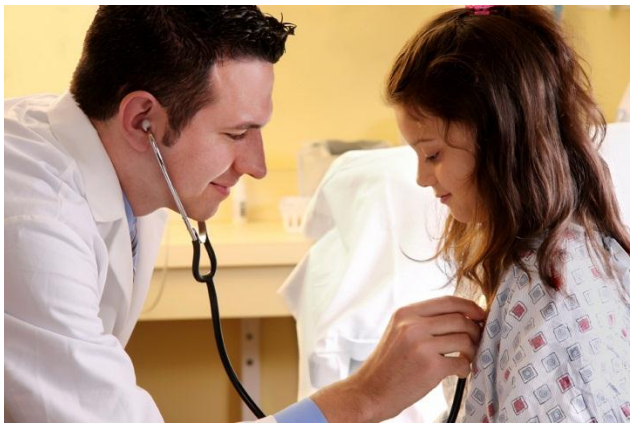


Abbildung 11: Gesundheitswesen [11]

Referenzen

[1] http://www.heise.de/netze/artikel/IPv4-Adressen-werden-knapp-221468.html

[2] **Jonathan Hui/David Culler/Samita Chakrabarti:** 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture. White paper # 3. IPSO Alliance, 2009.

[3] **Jonathan Hui/David Culler:** IPv6 in Low-Power Wireless Networks. Proceedings of the IEEE, 2010.

[4] **Chowdhury, A.H./Ikram, M./Cha, H-S./Redwan, H./Shams,S.M.S/Kim, Ki-H./Yoo, S-W.:** Route-over vs. Mesh-under Routing in 6LoWPAN. International Wireless Communications and Mobile Computing Conference 2009. Seiten 1208-1212.

[5] **Shelby, Z./Chakrabarti, S./Nordmark, E.:** Neighbor Discovery Optimization for Low-power and Lossy Networks. Internet-Draft. 2010. URL: http://tools.ietf.org/html/draft-ietf-6lowpan-nd-17, Stand: 27.07.2011.

[6] **Hui, J./Thubert, P.:** Compression Format for IPv6 Datagrams in6LoWPAN Networks. Internet-Draft. 2010. URL: http://tools.ietf.org/html/draft-ietf-6lowpan-hc-15, Stand: 27.07.2011.

[7] **Ayadi, A./Ros, D./Toutain, L.:** TCP header compression for 6LoWPAN. Internet-Draft. 2010. URL: http://datatracker.ietf.org/doc/draft-aayadi-6lowpan-tcphc/, Stand: 27.07.2011.

[8] http://www.wago.us/ , Stand: 27.07.2011.

[9] **M. Becker/B.-L. Wenning/C. Görg/R. Jedermann/A. Timm-Giel:** Logistic applications with Wireless Sensor Networks. HotEmNets 2010.

[10] http://www.mt-solutions.at, Stand: 09.08.2011.

[11] http://www.negotiationlawblog.com, Stand: 27.07.2011.

dresden elektronik ingenieurtechnik gmbh
Enno-Heidebroek-Straße 12
01237 Dresden
GERMANY

Tel. +49 351 - 31850 0
Fax +49 351 - 31850 10
www.dresden-elektronik.de
E-Mail wireless@dresden-elektronik.de

Markenzeichen

- 802.15.4™ ist ein Markenzeichen des Institute of Electrical and Electronics Engineers (IEEE).
- ZigBee® ist ein eingetragenes Markenzeichen der ZigBee Allianz.

Diese Markenzeichen sind durch ihre jeweiligen Eigentümer nur in bestimmten Ländern eingetragen. Andere Marken und ihre Produkte sind Markenzeichen oder sind eingetragene Markenzeichen ihrer jeweiligen Eigentümer und sollten als solche beachtet werden.

Haftungsausschluss

Inhalt und Gestaltung dieses Dokuments sind urheberrechtlich geschützt. Die Vervielfältigung, Verbreitung und Speicherung der enthaltenen Texte, Bilder und Daten bedürfen der vorherigen schriftlichen Zustimmung der dresden elektronik ingenieurtechnik GmbH.
Die auf diesen Seiten zur Verfügung gestellten Informationen wurden unter Beachtung größter Sorgfalt erarbeitet und ergänzt. Dennoch kann keine Garantie für die Richtigkeit und Vollständigkeit der angegebenen Informationen und Daten übernommen werden, da zwischenzeitlich eingetretene Änderungen nicht gänzlich auszuschließen sind.