



White Paper

Routing und Netzwerktopologien

Im Standard für 802.15.4 Low Power Geräte

Verfasser

Manuel Pietschmann

dresden elektronik ingenieurtechnik gmbh

Juli 2012



Abstract

In diesem Whitepaper werden die Routingverfahren und damit verbundene Netzwerktopologien vorgestellt, die im IEEE 802.15.4 Funkstandard und auf diesem aufbauende Protokolle Verwendung finden. Der IEEE 802.15.4 Funkstandard wurde entwickelt für Geräte mit niedrigem Energieverbrauch und kleinen Datenraten im unterem Preissegment (100,- € abwärts). Im Standard sind die physikalische Schicht (PHY) und die Medienzugriffsschicht (MAC) definiert, darauf aufbauende Netzwerk und Routing Schichten werden unter anderem von der ZigBee Allianz und der 6LoWPAN Arbeitsgruppe veröffentlicht.

Einführung

Netzwerke im Lowpower Bereich stellen besondere Herausforderungen an die zugrunde liegenden Routingverfahren und Topologien. Zu diesen gehören unter anderem schlafende Knoten und nicht statische Umgebungen mit beweglichen oder zeitweise nicht erreichbaren Geräten. Die folgende Tabelle zeigt verschiedene Kriterien, die zur Entscheidung für eine bestimmte Topologie oder eines Protokolls hilfreich sein können.

Topologie	Reichweite	Mutihop	Robustheit ³	Gängige Protokolle
Stern	gering ¹	nein	APC ³	proprietär, 6LoWPAN
Peer-to-Peer	gering ¹	nein	APC, P2P ³	proprietär, 6LoWPAN
Cluster Tree	groß ²	ja	APC, PC ³ , SHN ³	6LoWPAN, ZigBee
Mesh	groß ²	ja	APC, PC, P2P, SHN, AR ³	6LoWPAN, ZigBee

¹ Ergibt sich aus direkter Punkt zu Punkt Verbindung, z.B. 50 – 200m

² Die Reichweite kann prinzipiell mit jedem Hop um dessen Funkreichweite erweitert werden, z.B. bei 10 Hops 500 – 2000m.

³ Die Abkürzungen spiegeln Faktoren wieder, die zur Robustheit und Sicherheit des Routings beitragen (sie sind im Glossar erläutert).



Glossar

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

Begriff	Beschreibung
AODV	Advanced Ad-hoc On-Demand Distance Vectoring; Populärer Mesh Routing Algorithmus.
APC	Alternate PAN coordinator; Koordinator, der fähig ist, den PAN Koordinator zu ersetzen, falls dieser ausfällt. Es kann mehrere davon im Netz geben, aber nur einen aktiven PAN Koordinator.
AR	Alternative Routes; Diese Routen können als Reserve gewählt werden, falls ursprüngliche Routen nicht erreichbar sind.
FFD	Full Function Device; Ein Gerät, das Koordinator-Fähigkeiten hat. FFD Geräte sollten dauerhaft mit Strom versorgt werden.
Hop	Zwischenstationen einer Route sowie der Weg (Funk) von einem Knoten zum nächsten.
Koordinator	FFD Gerät, das Pakete weiterleitet und neue Knoten in das Netz integrieren kann.
PAN Koordinator	Hauptverwalter eines Netzes. Hat die Aufgabe, ein Netz mit geeigneten Parametern zu eröffnen und zu verwalten.
PC	Die Kommunikation zwischen Eltern/Kind Knoten, der Elternknoten muss ein FFD Gerät sein. Ermöglicht Multihop Routing (Baumstruktur).
P2P	Peer-to-Peer; 1-Hop Kommunikation zwischen FFD Geräten in gegenseitiger Funkreichweite.
RFD	Reduced Function Device; Ein einfaches Gerät, das kein Koordinator sein kann. Meist Batterie betriebene Geräte mit geringen Ressourcen, die schlafen können.
Route	Der Weg eines Paketes von der Quelle bis zum Ziel mit allen Zwischenstationen.
RPL	Routing Protocol for Low power and Lossy Networks; Ein eng an 6LoWPAN geknüpftes Routing Protokoll, das von der IETF Arbeitsgruppe ROLL erstellt wird.
SHN	Self-healing network; Automatische Regenerierung der Topologie bei Nicht-Erreichbarkeit eines Knotens.
TTL	Time to Live; Haltbarkeitszeit eines Paketes.

Routing und Netzwerktopologien

Beim Routing in Netzwerken wird dafür gesorgt, dass Datenpakete von einer Quelle zum Ziel gelangen. Die Herausforderung besteht darin, optimale Wege (die sogenannten Routen) zu finden. Weiterhin soll die Zuverlässigkeit in Netzen mit dynamischen Eigenschaften, wie z.B. bewegliche oder zeitweise nicht erreichbare Knoten, gesichert werden. Dazu müssen unter anderem bestehende Routen gewartet und wenn nötig Alternativen gefunden werden. Die gängigen Routingverfahren unterscheiden sich dabei grundlegend und sollten für den jeweiligen Anwendungszweck geeignet gewählt werden.

Stern

In einem Stern kommunizieren alle Teilnehmer über einen zentralen Vermittler, den PAN Koordinator [1] [5]. Die Netzabdeckung ist dabei sehr begrenzt, da selbst dann, wenn sich mehrere Nachbarn in Reichweite befinden, die Kommunikation zwischen diesen stets über den zentralen Knoten geschieht. Dies hat auch zur Folge, dass, wenn kein alternativer PAN Koordinator zur Verfügung steht, bei Ausfall des PAN Koordinators das gesamte Netz zum Erliegen kommt.

Die Stern Topologie zeichnet sich durch minimalen Aufwand bei Installation und Wartung aus, sie eignet sich für räumlich begrenzte Anwendungen sowie Anwendungen, die geringe Latenzen voraussetzen.

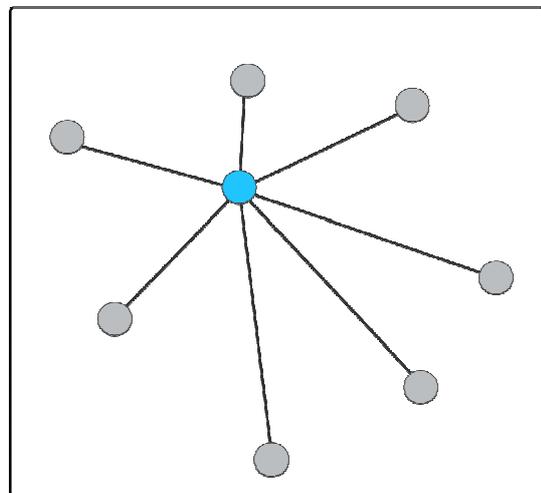


Abbildung 1: Stern Topologie

Peer-to-Peer

In dieser Topologie existiert ebenfalls ein PAN Koordinator, in dessen Funkreichweite sich jeder Teilnehmer befinden muss. FFD Knoten können, im Gegensatz zur Stern Topologie, direkt untereinander kommunizieren, ohne über eine zentrale Stelle gehen zu müssen. Voraussetzung dafür ist, dass diese sich in Funkreichweite befinden.

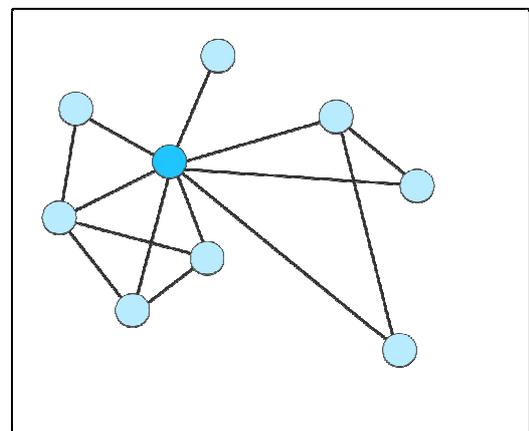


Abbildung 2: Peer-to-Peer Topologie



Dadurch ergeben sich wesentlich flexiblere Kommunikationsstrukturen und eine gesteigerte Netzwerkperformance. Routing über mehrere Hops hinweg kann mit Peer-to-Peer als Basis in höheren Protokollschichten umgesetzt werden [1] [5]. Peer-to-Peer Kommunikation ist ein fester Bestandteil aller Mesh Routingverfahren.

In Funknetzen eignet sich reines Peer-to-Peer Routing für räumlich begrenzte Anwendungen, in denen Knoten fortlaufend mit direkten Nachbarknoten kommunizieren müssen. Im Gegensatz zum Stern entstehen bei hohen Teilnehmerzahlen keine Engpässe beim Zustellen der Pakete über den PAN Koordinator.

Cluster Tree

Diese Topologie definiert sich durch ihre Eltern-Kind Verbindungen in einer Baumstruktur, deren Wurzel der PAN Koordinator bildet. Das Verfahren baut auf der Stern Topologie auf und erweitert diese um zusätzliche Hops.

Jeder FFD Knoten, der bereits einem Baum angehört, kann als Einstiegspunkt für neu hinzukommende Knoten dienen. Damit können auch Geräte, die sich außerhalb der Funkreichweite des PAN Coordinators befinden, dem Netz beitreten [1] [2].

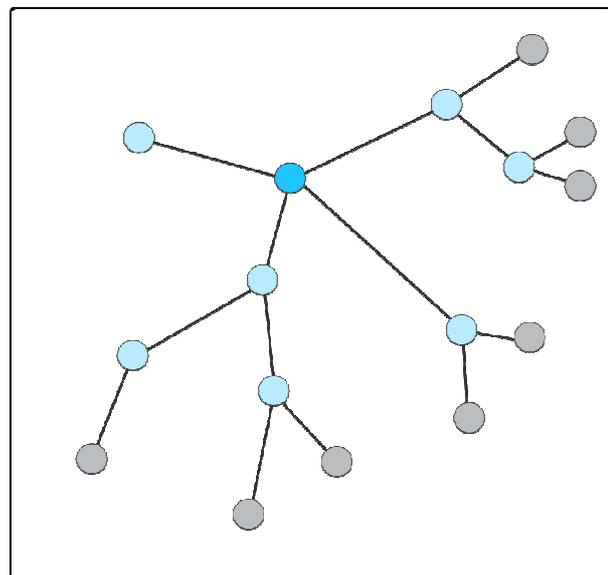


Abbildung 3: Cluster Tree Topologie

FFD Knoten agieren als Repeater, die die Reichweite des Netzwerks erheblich erweitern können. Dadurch können Daten zwischen Knoten ausgetauscht werden, die keine direkten Nachbarn sind. Das Routing erfolgt dabei immer der Hierarchie entlang, selbst wenn sich das Ziel in direkter Funkreichweite befindet.

Kindknoten in selbstheilenden Cluster Tree Netzen suchen automatisch nach geeigneten neuen Elternknoten in Funkreichweite, sobald ein Verlust der ursprünglichen Eltern detektiert wird.

Die Cluster Tree Topologie eignet sich für Anwendungen, die größere Distanzen oder Hindernisse überbrücken müssen und deren zeitlichen Anforderungen im Rahmen der der gewählten Verzweigungstiefe des Baumes liegen.

Mesh

In vermaschten Netzen tauschen benachbarte Knoten Informationen über direkte Nachbarn und bekannte Routen zu entfernten Knoten aus. Die Topologie setzt sich aus einer Kombination aus Peer-to-Peer und Cluster Tree Struktur zusammen. Dabei steht keine besondere Hierarchie im Vordergrund, alle Knoten sind untereinander gleichberechtigt.

Es wird zwischen zwei Kategorien von Routingverfahren unterschieden: Proaktives Mesh Routing und Reaktives Mesh Routing.

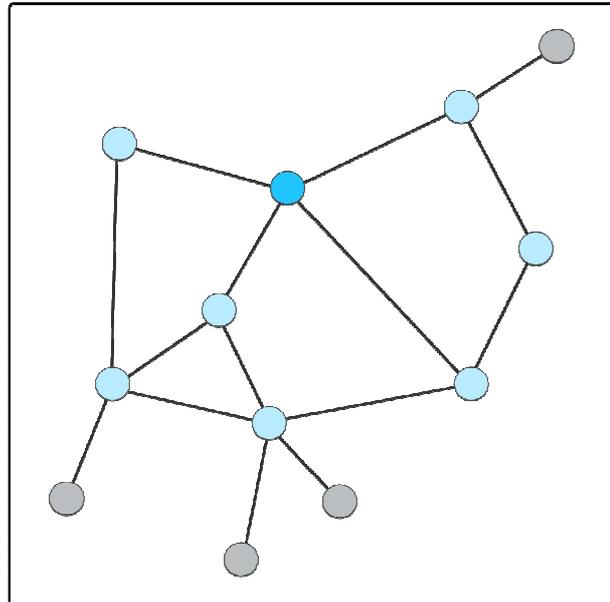


Abbildung 4: Mesh Topologie

Proaktives Mesh Routing

Knoten im proaktiven Routing tauschen Nachbar- und Routingtabellen im vollem Umfang aus. Dies ist für kostengünstige Geräte, die über verhältnismäßig wenig Speicher verfügen, häufig schwer realisierbar. Proaktives Routing wird daher vor allem in industriellen Anwendungen und Geräten mit größeren Speicherkapazitäten genutzt. Der Vorteil pro-aktiver Verfahren besteht darin, dass Routen zwischen Quelle und Ziel in der Regel schneller verfügbar sind. Die dafür benötigten Routingtabellen liegen in jedem Knoten vor und werden periodisch aktualisiert. Problematisch ist dabei der Speicherbedarf, der linear zur Knotenanzahl steigt. Größere Netze mit mehreren hundert oder gar tausend Knoten müssen daher über genügend Ressourcen verfügen.

Reaktives Mesh Routing

Reaktives Routing zeichnet sich dadurch aus, dass Informationen selektiv und nur bei Bedarf angefragt werden, was zu deutlich kleineren Routingtabellen, jedoch auch zu mehr Verwaltungsaufwand führt. Das hat zur Folge, dass Routen, die noch nicht genutzt wurden, erst ermittelt werden müssen. Daher sind zeitkritische industrielle Anwendungen keine Idealkandidaten für reaktives Routing, wenn sich die Routen fortlaufend ändern können. Für zeitunkritische Anwendungen sind reaktive Routing-Protokolle dagegen eine effiziente Lösung. Reaktives Routing skaliert trotz geringer Ressourcen der Geräte sehr gut mit der Netzgröße, selbst wenn viele tausend Knoten verwendet werden.



Selbsteilung und Wartung

Sogenannte selbstheilende Eigenschaften ergeben sich durch den fortlaufenden Austausch der Nachbarinformationen und dem Pflegen der Routingtabellen. Wenn Knoten kurzfristig nicht erreichbar sind oder gänzlich ausfallen, werden alternative Routen genutzt, sofern diese bekannt sind, oder neue Routen angefragt.

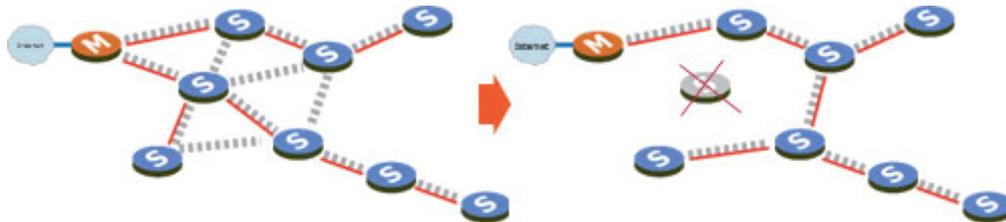


Abbildung 5: Selbstheilung

(Bildquelle: http://www.arrowspan.com/graphics/pop_structure.gif)

Dadurch sind vermaschte Netze auch unter dynamischen Bedingungen sehr zuverlässig. Mesh Routing Algorithmen sind derart aufgebaut, dass performante Routen bevorzugt werden, dabei ist nicht zwingend die Anzahl an Zwischenknoten ausschlaggebend, vielmehr bestimmen Parameter wie die Signalqualität der einzelnen Verbindung die Bewertung und somit die Auswahl der Routen. Sollten für ein Sendeziel keine Routen bekannt sein und das Ziel kein direkter Nachbar sein, kann neben erneuten Routinganfragen alternativ auf Cluster Tree Routing zurückgegriffen werden und die Daten werden über den Elternknoten gesendet [1].

Zu den bekannten Routing-Protokollen, die in 802.15.4 Funkstandard basierten Anwendungen Verwendung finden, gehören:

- **Reaktives Routing**
 - Advanced Ad-hoc On-Demand Distance Vectoring (AODV), verwendet in ZigBee Routing [2]
 - Routing Protokoll for Low Power and Lossy Networks (RPL), empfohlen für 6LoWPAN [6]
 - Dynamic Source Routing (DSR) [7]
 - Dynamic MANET On-Demand for 6LowWPAN (DYMO-low) [9]
 - 6LoWPAN Ad-hoc On-Demand Distance Vector (LOAD) [9]

- **Pro-aktives Routing**
 - Graph Routing, bevorzugt in WirelessHART [8]
 - Optimized Link State Routing (OLSR)

Ad-hoc On Demand Distance Vector (AODV)

Das oft genutzte AODV Routingverfahren gehört zu den reaktiven Verfahren; durch die geringen Ressourcenanforderungen eignet es sich besonders für Geräte welche über relativ wenig Speicherplatz verfügen. Das Erkunden von Routen erfolgt immer nur auf eine direkte Anfrage.

Knoten signalisieren periodisch per Broadcast die eigene Anwesenheit, somit kennt jeder Knoten auch seine direkten Nachbarn.

Wenn Daten an einen nicht bekannten Knoten gesendet werden sollen, versucht der Absender eine Route zum Zielknoten zu ermitteln. Dabei wird per Broadcast ein Route Request (RREQ) Nachricht gesendet, diese enthält neben der Absenderadresse und einer Haltbarkeitszeit der Nachricht (engl. Time to live - TTL) eine Sequenznummer, welche für den Absender eine eindeutige ID darstellt. Ein Empfänger der RREQ

Nachricht kann, falls er selbst der Zielknoten ist oder eine Route zu diesem kennt, mit einer Route Reply (RREP) Nachricht dem Absender antworten. Eine RREQ Nachricht wird solange per Broadcast weitergeleitet bis die TTL abgelaufen ist. Es gilt hierbei, dass jeder Empfänger einer RREQ Nachricht diese nur einmal weiterleitet, daher muss in einer Tabelle temporär die Absenderadresse und Sequenznummer der RREQ Nachricht festgehalten werden. Die Sequenznummer in einer RREP Nachricht erlaubt es allen Knoten, über die diese Nachricht zum Absender zurückgeleitet wird, die eigene Routingtabelle zu aktualisieren. Hierbei gilt, dass eine höhere Sequenznummer eine aktuellere Route darstellt.

Sollte der Absender nach einer bestimmten Zeit keine Antwort auf die Anfrage bekommen, sendet er erneut eine RREQ Nachricht mit einer höheren TTL und einer neuen Sequenznummer aus. Gefundene Routen werden solange gepflegt, solange in Abständen Daten über sie versendet werden [10].

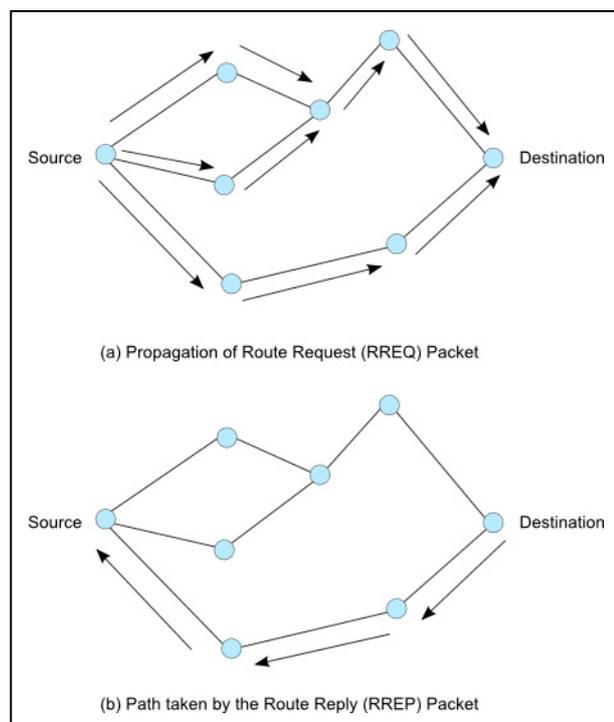


Abbildung 6: AODV routing example

(Bildquelle:
http://www1.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/fig4.gif)

Routing Protocol for Low Power and Lossy Networks (RPL)

Die IETF Arbeitsgruppe ROLL (Routing over Low Power and Lossy Networks) hat bestehende Routingprotokolle wie OSPF, AODV, IS-IS und OLSR analysiert und festgestellt, dass diese Protokolle in ihrer derzeitigen Form nicht den Anforderungen von „low power and lossy networks“ (LLN) Sensornetzen gerecht werden. Infolgedessen hat die Arbeitsgruppe ein für 6LoWPAN Sensornetzwerke geeignetes Protokoll namens RPL spezifiziert. Das RPL Protokoll ist derzeit das verbreitetste Protokoll in 6LoWPAN Implementierungen. Mithilfe von 6LoWPAN werden Sensornetzwerke in die IPv6 Welt integriert und sind darin direkt zugänglich.

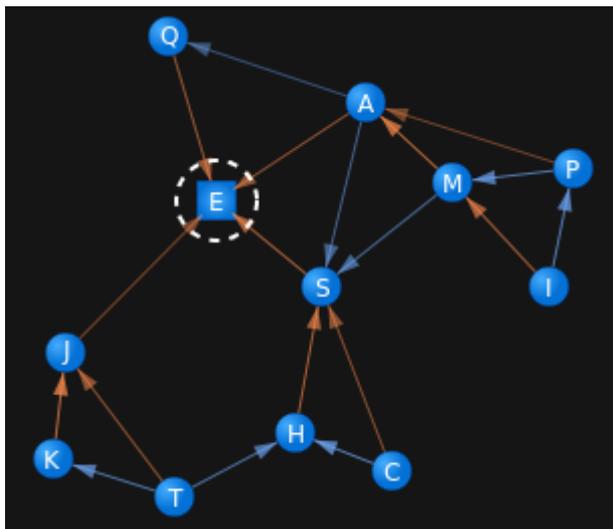


Abbildung 7: RPL example

(Bildquelle: http://de.wikipedia.org/wiki/Routing_Protocol_for_Low_power_and_Lossy_Networks)

Zu den Anforderungen gehören hohe Zuverlässigkeit, Robustheit und Verfügbarkeit bei gleichzeitig niedrigem Energie- und geringen Ressourcenverbrauch. Das Protokoll soll weiterhin für große Sensornetzwerke mit mehreren tausend Knoten geeignet sein [6].

Das Routing basiert auf dem Distanzvektoralgorithmus. Jeder Knoten sendet in regelmäßigen Abständen Pakete, welche unter anderem seine ID und den Rang im Graphen enthalten. Es werden dabei zielorientierte, gerichtete, azyklische Graphen (engl. DODAG - Destination Oriented Directed Acyclic Graph) bei den Empfängern aufgebaut. Die Knoten sind durch die gesammelten Graphinformationen in der Lage, den nächst besten Hop, der zum Ziel führt, zu ermitteln. Bedingt durch mögliche Schlafzeiten einzelner Knoten ist es möglich, die Informationen explizit anzufordern.

Im Vergleich zu alternativen Routing Protokollen wie AODV wurde mit RPL Routing eine höhere Gesamtpformance des Netzwerks erreicht. Besonders bei fragmentierten Daten führt RPL Routing zu signifikant weniger Retransmissions (engl. für erneutes Senden bei Übertragungsfehlern).

Abbildung 7 zeigt einen DODAG mit Zielknoten E, die roten Verbindungen stellen den bevorzugten Verbindungspfad dar, die blauen Verbindungen repräsentieren alternative Verbindungspfade.



Dynamic Source Routing (DSR)

Grundlegend gilt bei diesem Verfahren, dass der Absender (die Quelle) den Weg des Pakets teilweise oder ganz bestimmt. Der Sender eines Pakets legt mindestens den nächsten Hop und maximal alle Hops bis hin zum Ziel fest. Für die restlichen Nutzdaten ist daher weniger Platz vorhanden. DSR gehört wie AODV zu den reaktiven Routingprotokollen. Die benötigten Hop Informationen werden beim sogenannten „Route Discovery“ gewonnen, bei dem involvierte Knoten nur die relevanten Information speichern.

Wenn z.B. ein Knoten noch keine Route zum Ziel kennt, sendet er ein „Route Request“ Paket, das per Broadcast durch das Netz geleitet wird. Zu Beginn hat das Paket nur eine Sequenznummer und die Quelladresse. Alle Empfänger des Pakets, sofern sie nicht das Ziel sind und die „Time to life“ (TTL) des Pakets noch nicht abgelaufen ist, leiten dieses genau einmal weiter (Duplikate sind anhand der Sequenznummer erkennbar). An das Paket wird die Adresse des jeweiligen Empfängers angehängt, es enthält daher den bisher zurückgelegten Weg. Wenn das Paket das erste Mal beim Ziel eintrifft (es können mehrere über verschiedene Routen eintreffen), antwortet der Zielknoten der Quelle über die umgekehrte Route im Paket (Route Reply).

Weiterhin können Knoten Routen über Nachbarn erlernen, die bereits eine Route zum Ziel kennen. In diesem Fall sendet ein Nachbar, der das Ziel kennt, ein Route Reply mit der vollständigen Route zum Initiator des Route Requests [4].

Durch die sogenannte Flow State Erweiterung des Dynamic Source Routings ist es möglich, beim Senden nur noch den nächsten Hop anzugeben.

In Bezug auf 802.15.4, das eine maximale Länge von 127 Byte für die Nutzdaten hat, ist Source Routing nur beschränkt geeignet. Im ZigBee Pro Standard ist Source Routing mit maximal 5 Hops möglich.



Referenzen

- [1] **F. Cuomo, S. Della Luna, E. Cipollone, P. Todorova, T. Suihko**, "Topology formation in IEEE 802.15.4: cluster-tree characterization", Sixth Annual IEEE International Conference on Pervasive Computing and Communications.
- [2] **F. Cuomo, S. Della Luna, U. Monaco**, „Routing in ZigBee: benefits from exploiting the IEEE 802.15.4 association tree“, 2007.
- [3] **Gerald Kupris, Axel Sikora**, „ZigBee: Datenfunk mit IEEE 802.15.4 und ZigBee“, 2007 Franzis
- [4] Dynamic Source Routing, http://en.wikipedia.org/wiki/Dynamic_Source_Routing , Wikipedia 2010
- [5] **IEEE Computer Society**, "IEEE Std 802.15.4-2006", IEEE-SA Standards Board 2006
- [6] **IETF**, „Description of Working Group ROLL“, <http://datatracker.ietf.org/wg/roll/charter/>
- [7] **IETF**, "Dynamic Source Routing", <http://www.ietf.org/rfc/rfc4728.txt>
- [8] **Tomas Lennvall, Stefan Svensson, Fredrik Hekland**, "A Comparison of WirelessHART and ZigBee for Industrial Applications", 2009
- [9] **Vassil Stefanov**, "Mesh routing for IPv6 over 802.15.4 on TinyOS", 2008
- [10] **C. Perkins, E. Belding-Royer, S. Das, I. Chakeres**, "AODV", <http://moment.cs.ucsb.edu/AODV>



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.

Copyright © 2012 dresden elektronik ingenieurtechnik gmbh. Alle Rechte vorbehalten.