Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Routing in the Internet of Things

Lotte Steenbrink

Ausarbeitung

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Lotte Steenbrink

Ausarbeitung

Eingereicht am: July 25, 2014

Contents

List of Figures

Glossary

beacon Small, periodically transmitted packet. 3

sink node Node at which most traffic is directed. 6

DIO DODAG Information Object. 6

DODAG Destination Oriented Acyclic Graph. 6

DTN Delay Tolerant Network. 2, 5, 6

ICN Information Centric Network. 3

IoT Internet of Things. 1–3, 5, 6

IRTF Internet Research task Force. 6

LLN Low Power and Lossy Network. 1, 2, 5

MANET Mobile Ad-hoc Network. 2, 5

PRoPHET Probabilistic Routing Protocol using History of Encounters and Transitivity. 6

RPL Routing Protocol for Low Power and Lossy Networks. 5

WSN Wireless Sensor Network. 6

1 Introduction

With vast technological advancements and the growing popularity of digital assistance in everyday life and work environments that goes along with it, technologies are needed to evolve these application domains to the next level. One vision for this is the Internet of Things (IoT): interconnected devices, embedded in all kinds of objects. In order to turn this vision into reality, routing protocols are needed to aid the communication between these *things* in a decentralized, self-organized and changing infrastructure.

1.1 The Internet of Things

The IoT is the vision of machine-to-machine communication between devices embedded in things, so-called *smart objects* [1]. To avoid interference with the usability of the *thing*, IoT devices are small, embedded devices, equipped with only a few hundred kB of ROM. They are powered by batteries, which have to last for months or even years without maintenance.
IoT devices are organized in a mesh network which is connected to the Internet through a gateway router. This sets them apart from traditional Wireless Sensor Networks (WSNs). Traffic is usually connectionless and sparse, with small payloads. The traffic patterns emerging from IoT devices vary with the application area: Building Automation, as described by [2], commonly generates point-to-point-traffic, while centralized Home Automation applications of [3] exhibit a mixture of multipoint-to point and point-to-multipoint traffic. Because interference with foreign signals, fading connectivity, and signal reflection or scattering are often encountered in wireless mesh networks, there is no guarantee for bidirectional connectivity.

1.2 The Network Stack

Because the IoT differs from the "traditional" Internet in crucial aspects, the use of a custom network stack as illustrated in Fig. 1.1 is necessary.
The IEEE 802.15.4 Data Link and Physical layers have been optimized for energy-efficiency and the ability to be deployed on cheap device. Its Maximum Transmission Unit (MTU) is a mere 127 bytes. This limitation conflicts with the minimal MTU of 1280 bytes dictated by IPv6, generating the demand for an adaptation layer: 6LoWPAN. Here, IPv6 headers are compressed; packets exceeding the new 127 byte MTU are fragmented. The fragments produced can be reassembled by all border routers connecting a 6LoWPAN network to the Internet.

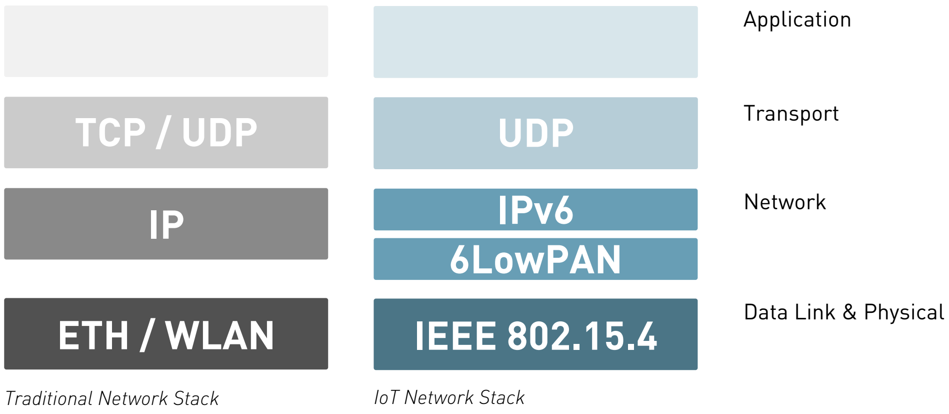

Figure 1.1: Comparison of traditional and IoT Network Stacks.

1.3 Requirements and key challenges for routing protocols

[3], [4] and [2] list requirements for a routing protocol in the differing scenarios of Home Automation, Urban-Low Power and Lossy Networks (LLNs) or Building Automation. Even though these fields may all be categorized as IoT-adjacent, their characteristics differ vastly in terms of traffic flow and patterns, network size, and degree of mobility. Despite these differences, the domains of their requirements can be classified into four categories:

Traffic Patterns: A routing protocol for the IoT has to match the traffic pattern of its area of deployment. Since patterns vary from network to network, as shown in 1.1, there is most likely not *one* protocol to rule them all, but rather at least one appropriate protocol for each subdivision of IoT deployments.

Energy efficiency: The deployment of battery-driven nodes running autonomously for extended periods of time is one of the cornerstones of the IoT. A routing protocol that is resourceful in terms of energy consumption is vital to the functionality of an IoT-based network. Closely tied to these efforts is the topic of energy-*awareness.* A protocol able to communicate its nodes' constraints is able to make more informed routing decisions based on this information.

Scalability: The protocol should scale to a network size ranging from 100 to 1,000,000 nodes, both in terms of performance as well as memory usage: an increase in network size may not lead to an explosion in routing table size.

Mobility: Even though the IoT does not typically experience a lot of movement, a suitable routing protocol should be able to cope with sparse location changes of single nodes.

In addition to the requirements listed above, the nature of the IoT poses unique challenges to any routing protocol serving them.

Bidirectionality: As with all wireless networks, bidirectional connectivity between links is not guaranteed. A routing protocol for the IoT has to be able to recognize and avoid unidirectional links at the least, and may be able to use them in one direction at best.

Transmitter usage: Concerning energy consumption, the transmitter is the most expensive component of a constrained device. It is therefor advisable to use it as sparsely as possible.

1.4 Related research

Because the IoT is a budding field, few research is explicitly tailored to its characteristics. Nonetheless, adjacent fields have produced work which explores problems which are familiar to the IoT, most notably the research fields of Mobile Ad-hoc Networks (MANETs), Delay Tolerant Networks (DTNs) and LLNs.

2 Approaches

In order to meet the constraints of the IoT as described in section 1.3, a routing protocol may employ different strategies. This section lists promising mechanisms and approaches which may form the building blocks if a successful routing protocol for the IoT.

2.1 Protocol characteristics

Each routing protocol exhibits core characteristics which form the very base of its workings. In the following, characteristics which may be most beneficial in an IoT environment will be discussed.

Proactive vs. Reactive

With the exception of hybrid approaches, routing protocols either fall in the category of proactive or reactive.

A proactive protocol gathers routing information proactively, attempting to have an overview of the entire network's topology at all times. Typically, the periodic distribution of beacons provides nodes with insight about the existence and quality of connection to their neighbors. This provides for great performance in terms of latency, but can wreak havoc on the battery lifetime: In networks which experience sparse traffic, most of the topology information exchanged can be considered protocol overhead which will drain a device's batteries unnecessarily.

Reactive protocols search for routes on-demand: only when a transmission towards another node is started, the route discovery process (towards this specific node) is triggered. In consequence, topology information is only exchanged when needed, saving energy. The downside to reactive protocols is their latency: because routes are discovered on-demand, transmissions over unknown or expired routes face delays, for which either the application or the routing protocol has to account by buffering or dropping data.

Hop-by-Hop vs. Source Routing

Packet forwarding may be either carried out hop by hop or through source routing. With the former, each router stores a small part of each route it is participating in: the destination of the route, and over which of its neighbors packets towards this destination should be forwarded. With the latter, the entire path of a route is embedded in its packet header. While this has the benefit of memory-efficiency, it increases header sizes and traffic volumes dramatically. Routes may become stale before the packet carrying them in their header has reached its destination. With the relatively small MTU of IEEE 802.15.4 and the moderate mobility in the IoT, this makes for an unfortunate combination.

Information Centric

Information Centric Networks (ICNs) are not merely a routing protocol, but an entirely new networking paradigm. Oftentimes, it does not matter to the recipient who sends them the data they requested, they are merely interested in receiving the data at all. ICN picks this up: instead of asking single addresses for data, a node will ask the network [5]. Since some IoT use cases, like the evaluation of environmental data, are more focused on the information than its origin as well, ICN may be a suitable solution for some IoT deployments.
Because ICN was designed with large-scale, cabled networks in mind, it exhibits some characteristics problematic for the deployment in the IoT: Connections are assumed to be bidirectional, with no mechanisms to ensure that this assumption holds.
With some ICN protocols, all routers cache the data they forward. Considering that memory is very limited on IoT nodes, this may prove to be problematic. Additionally, data which provides an update for a previous information often doesn't update its predecessor, but is stored as a copy, consuming even more storage space [6].

2.2 Mechanisms

Routing protocols may be equipped with a myriad of mechanisms influencing the way they make routing decisions. In the following, some mechanisms that may be beneficial to IoT protocols will be highlighted.

Energy-aware metrics

Metrics are used to quantify the quality of a link or route under certain aspects. The most commonly deployed metric is Hop Count, with which the route using the fewest hops is chosen. However, this is often less than ideal: not all links are created equal in quality, and long-distance links are especially prone to be lossy. Energy-awareness may be introduced to existing routing protocols with the help of suitable metrics. A metric which takes energy levels on either the node or network level may influence the routing decisions of a protocol in a way which preserves energy resources.
[7] specify several routing metrics for the Routing Protocol for Low Power and Lossy Networks (RPL) protocol, some of which may be interesting for other deployments as well. Notable are:
Node Energy: The energy level of a node may be taken into account in different ways: most intuitively, it may be beneficiary to choose a route over nodes with great residual energy in order to elongate its lifetime and relieve nodes with fewer resources. In doing so, the value of residual energy has to be put into context by the transceiver costs of the individual node as well as its expected lifetime: It may be beneficial to use a node with less battery which is likely to be recharged in the near future (e.g. a mobile device on the nightstand) than one with high residual energy that has to last for a while (e.g. a node in the wall)[1].
Throughput: When the data sent over a router exceeds the amount of throughput it is able to handle, the resulting packet loss will cause retransmissions, wasting energy on redundant communication. Therefor, a router may specify the throughput it is able to handle.
Latency: Different types of information may have different latency constraints, for instance because the data may become stale quickly, is important in case of emergency or may trigger timeouts. By taking these requirements into account, a protocol is able to distribute the network load in a way that supports different traffic requirements.
These approaches can be combined: [8] proposes the use fuzzy logic to merge several relevant characteristics of a route or link into one statement about its quality, in this case *number of hops*, *residual energy* and *Received Signal Strength Indicator*.

[1] Example as published in [7], p. 13

Multipath routing

A protocol employing multipath routing seeks to find and use alternate paths towards every destination. This distributes the cost of forwarding packets among more nodes, saving the energy of individual, highly-frequented nodes. [9]

Probabilistic routing

With probabilistic routing, routing decisions are calculated based on probabilistic values.
The most primitive way to do this is gossiping: Data is flooded through the network like a rumor, but every packet is only forwarded with a probability p. This way, traffic overhead is reduced.
A more elaborate approach is to predict the chance of delivery towards a certain destination through mobility patterns or previous experience and base forwarding decisions on this prediction.

3 Protocols

In the preceding section, the building blocks of an IoT routing protocol, both essential and additional, have been discussed. This chapter provides an overview over routing protocols that are comprised of these building blocks. Each characteristic presented in section 2.1 is represented by at least one protocol.
Each protocol fulfills the criteria listed in section 3.1 and employs at least one of the approaches described in section 2. The protocols are roughly ordered in accordance with the order from section 2. Not all of the protocols presented have been designed with the IoT in mind; most stem from adjacent fields of research such as DTNs or MANETs. Despite this, they exhibit characteristics which may make them suitable for the IoT.

3.1 Criteria

During the past 15 years, an overwhelming amount of routing protocols and protocol modifications for LLNs and MANETs have been published. To sieve through these contributions, a set of criteria has been created and applied to all candidate protocols.

Suitability for the IoT: A routing protocol has to apply to at least one topology and traffic flow scenario common in the IoT. It should be scalable to a certain extent, and be able to cope with unidirectional routes.

Standardization: Protocols which are the result or part of a standardization process are greatly preferred. This ensures the availability of a detailed protocol specification, review by a diverse cast of specialists familiar with the subject and increases the likelihood of adoption in real-world scenarios.

Available implementations: Existing, ideally accessible implementations are an indicator for the maturity and seriousness of a protocol. They allow the evaluation of the protocol through simulation and testbed experiments.

3.2 Overview

Fig. 3.1 provides a feature visualization of the protocols that have been chosen to be presented in the following.

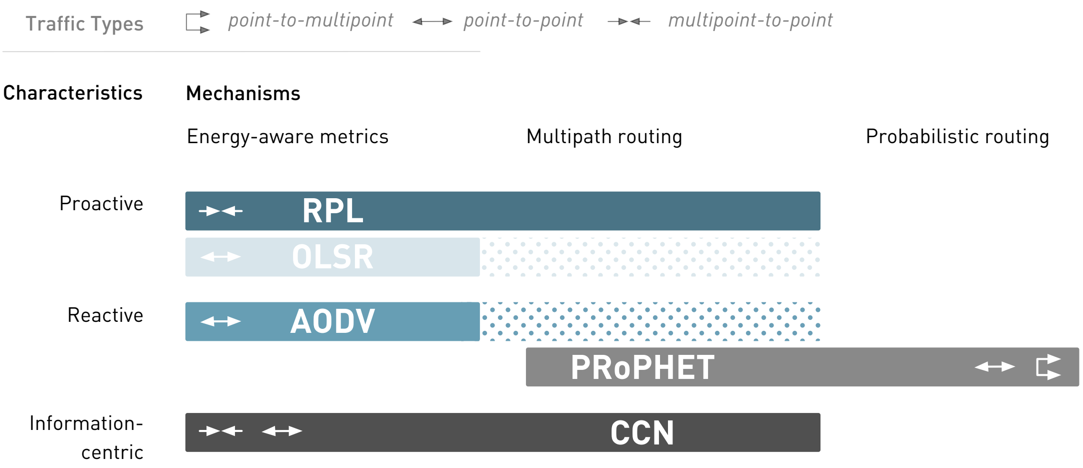

Figure 3.1: Overview over possible routing protocols for the IoT.

3.3 RPL

RPL [10] was designed to be *the* routing protocol for LLN and the IoT. RPL primarily supports *multipoint-to-point* traffic, with reasonable support for *point-to-multipoint* traffic and basic features for *point-to-point* traffic. It operates under the assumption that the network contains a sink node with greater computing ability and energy resources than the rest of the nodes in the network. It constructs a Destination Oriented Acyclic Graph (DODAG) whose root is the sink node, directing all traffic towards the sink node. Each node in the DODAG emits DODAG Information Object (DIO) messages containing information about its identity and rank in the DODAG. Because the DIOs are sent proactively and the network topology is explored in advance, RPL can be classified as a proactive protocol. However, the frequency of DIO decreases over time, reducing unnecessary control overhead once the DODAG has stabilized. When the optional Destination Advertisement Object (DAO) messages are used, RPL is able to perform both bidirectionality checks and multipath routing from the sink node to individual routers. The trade-off for this is an increase in control traffic and memory usage. RPL is the only one of the protocols presented which may also employ source routing. This occurs when it is operating in non-storing mode.

[11] provides a critical evaluation of the RPL protocol. Among others it lists its inflexibility in terms of data traffic flow, especially point-to-point traffic, possible control packet fragmentation and the assumption of bidirectional links as problematic points of the specification. An extension improving the protocol's support for point-to-point communication is presented and evaluated by [12].

3.4 OLSR and OLSRv2

The Optimized Link-State Routing (OLSR) protocol [13] and its successor OLSRv2 [14] are proactive link-state hop by hop routing protocols, both specified by the IETF. They are among the most popular routing protocols for MANETs and thus cannot go unmentioned. OLSRv2 introduces support for alternate metrics as one of its biggest upgrades from OLSR, enabling the use of energy-aware metrics. An extension for OLSRv2 has been proposed by [15] to enable multipath routing, which was studied for OLSR in the past [16]. Both OLSR and OLSRv2 are, however, most likely to be unsuitable for the IoT for the following reasons: Being proactive routing protocols, they periodically broadcast neighbor discovery and topology control packets. They maintain a detailed list about both direct neighbors and routes through the entire network. This generates both protocol overhead on the air, draining batteries through unnecessary transmissions, as well as storage overhead, since information which may never be used is stored in the so-called Information Base.

3.5 AODV, LOADng and AODVv2

Ad hoc On-Demand Distance Vector Routing (AODV) is a reactive hop by hop routing protocol specified by the IETF in 2003 [17]. It makes use of a Route Request (RREQ)- Route Reply (RREP)-cycle, which is triggered every time a packet to an unknown destination has to be sent. During this cycle, a route is discovered and stored Hop-by-Hop: each node only knows which direct neighbor is the next hop towards a certain destination. Whenever a link breaks, this is communicated downstream in the same manner.

Because routes are only stored when necessary, AODV can be described as memory-efficient. In its most minimal configuration, the protocol is likely to be small in terms of code image size because of its simplicity. Multipath extensions to AODV have been proposed by the original author [18] and others [19].

Two successors of AODV have been developed since its specification: The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng) [20] and AODVv2 [21], with the latter having been adopted by the MANET working group of the Internet Engineering Task Force (IETF). While AODV only accepts Hop Count as a metric, both of its successors allow alternate metrics, opening up the possibility for deployment of an energy-aware metric as described in section 2.2.

3.6 CCNx/ CCNLite

CCNx is an implementation of the ICN idea described in section 2.1, created by XEROX PARC.Its lightweight adaption is CCNlite, which has been adopted for the IoT by [22] and [6]. CCN operates on a hop by hop basis. Whenever a node is looking for data, it distributes an *Interest* message. This Interest is forwarded through the network until it can be answered by one of the participating nodes. Each node that received the Interest records it in its Pending Interest Table (PIT). When an Interest is answered with data, all nodes forwarding the data cache it, effectively distributing the data over the network. By doing so, CCN ensures that the data is able to survive even network partitioning. Additionally, subsequent requests for the data may be answered by intermediate nodes, distributing network load among neighbors. CCN is most suitable for multipoint-to-point or point-to-point traffic.

3.7 PRoPHET

The Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) was published in 2012 as an experimental hop by hop routing protocol for DTNs by the Internet Research task Force (IRTF) [23]. It has been described fist in 2003 by [24].

PRoPHET measures a network's movements, both physical and in terms of network traffic. Based on this data, the *delivery predictability* metric stating the probability of a successful data transfer is calculated per neighbor, characterizing PRoPHET as a probabilistic protocol. All data towards a certain route is buffered until a route can be established. This way, PRoPHET is able to handle networks that are never fully connected. Whenever two nodes meet, either through physical movement or a node switching on, they exchange the predictability information they calculated and update their internal data accordingly. Based on this information, each node decides if and which data it may want to forward though the neighbor it just met. A node may send their data through more than one neighbor, making PRoPHET a multipath routing protocol as well.

4 Comparability between protocols

Because there are no widely agreed upon benchmarks for IoT or WSN protocols, the protocols described above can only be evaluated based on their features. [25] discusses routing protocol evaluation considerations which may be used as a basis to construct possible benchmark scenarios. Additionally, the protocols presented have been implemented for different platforms such as Contiki, TinyOS, RIOT, or Linux, most without support for the NS-2 or NS-3 network simulator, complicating evaluation through comparison.

5 Conclusion and outlook

A wide range of approaches for routing in the IoT have been presented. Candidate protocols employing the approaches suggested have been introduced, along with possible criteria a routing protocol may have to match in order to be suitable for the IoT. While none of the protocols may be a one size fits all-solution, they may be suitable for specific IoT scenarios.

However, most proposed solutions have never been tested or even simulated in deployments which match the requirements listed in 1.3. It has been argued that there is a need for testing procedures tailored to IoT environments. The creation and adaption of standardized benchmarks for routing in the Internet of Things may advance the comparison of candidate protocols for the IoT.

Furthermore, the topology and attributes of the IoT complicate experiment and simulation setup: while the former is expensive to set up and maintain, the latter quickly fails to represent the network properties and influences correctly. [26] provides an overview of publicly accessible testbeds suitable for the IoT which may be used for future research and discusses their challenges and application areas.

Wrapping up, it can be concluded that there already are many existing approaches which may prove to be suitable for the IoT. Their direct comparison in both simulation and realistic testbed scenarios could provide further insight into their suitability for distinct IoT scenarios and reveal optimization potential.

Bibliography

[1] S. Gusmeroli, S. Haller, M. Harrison, K. Kalaboukas, M. Tomasella, O. Vermesan, H. Vogt, and K. Wouters, *Vision and Challenges for Realising the Internet of Things*. European Commission, 2010.

[2] J. Martocci, P. D. Mil, N. Riou, and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks," RFC 5867, IETF, June 2010.

[3] A. Brandt, J. Buron, and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks," RFC 5826, IETF, April 2010.

[4] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, "Routing Requirements for Urban Low-Power and Lossy Networks," RFC 5548, IETF, May 2009.

[5] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," *IEEE Communications Magazine*, vol. 50, pp. 26–36, July 2012.

[6] C. Mehlis, "Information-centric networking in the internet of things: Conceptual & practical challenges," Master's thesis, Freie UniversitÃ¤t Berlin, 2014.

[7] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," RFC 6551, IETF, March 2012.

[8] A. Ortiz, F. Royo, T. Olivares, N. Timmons, J. Morrison, and L. Orozco-Barbosa, "Intelligent routing strategies in wireless sensor networks for smart cities applications," in *Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference on*, pp. 740–745, April 2013.

[9] J. Al-Karaki and A. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[10] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, IETF, March 2012.

[11] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL)," in *Proc. of the 7th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 365–372, Oct. 2011.

[12] E. Baccelli, M. Philipp, and M. Goyal, "The p2p-rpl routing protocol for ipv6 sensor networks: Testbed experiments," in *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*, pp. 1–6, Sept 2011.

[13] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, IETF, October 2003.

[14] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg, "The Optimized Link State Routing Protocol Version 2," RFC 7181, IETF, April 2014.

[15] J. Yi and B. Parrein, "Multi-path Extension for the Optimized Link State Routing Protocol version 2 (OLSRv2)," internet-draft, IETF, July 2014.

[16] J. Yi, S. David, H. A. Adnane, B. Parrein, and X. Lecourtier, "Multipath OLSR: Simulation and Testbed," in *5th OLSR Interop/Workshop*, (Vienna, Austria), Oct. 2009.

[17] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, IETF, July 2003.

[18] P. Sambasivam, A. Murthy, and E. M. Belding-royer, "Dynamically adaptive multipath routing based on aodv," in *In Med-Hoc-Net*, 2004.

[19] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, pp. 92–93, June 2002.

[20] T. Clausen, J. Yi, and A. de Verdiere, "Loadng: Towards aodv version 2," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pp. 1–5, Sept 2012.

[21] C. Perkins, S. Ratliff, and J. Dowdell, "Dynamic MANET On-demand (AODVv2) Routing." Online, 2014. `http://tools.ietf.org/html/draft-ietf-manet-aodvv2`.

[22] S. Oh, D. Lau, and M. Gerla, "Content centric networking in tactical and emergency manets," in *Wireless Days (WD), 2010 IFIP*, pp. 1–5, Oct 2010.

[23] A. Lindgren, A. Doria, E. Davies, and S. Grasic, "Probabilistic Routing Protocol for Intermittently Connected Networks," RFC 6693, IETF, August 2012.

[24] A. Lindgren, A. Doria, and O. Schelén, “Probabilistic routing in intermittently connected networks,” *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, pp. 19–20, July 2003.

[25] M. S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,” RFC 2501, IETF, January 1999.

[26] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A survey on facilities for experimental internet of things research.,” no. 11, pp. 58–67.

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, July 25, 2014 Lotte Steenbrink