Hybrid routing for the Internet of Things

challenges and opportunities

Lotte Steenbrink

Wintersemester 2014/15

With the Internet of Things (IoT), new use cases and requirements for mobile mesh networks have begun to blossom. In order to meet these requirements, routing protocols are needed to manage connectivity and prepare the transport of packets. Traditionally, proactive protocols have been used for environments with more traffic and high constraints in terms of latency, while reactive protocols have been used for sparse, high-mobility networks. IoT networks may exhibit all of the aforementioned characteristics at the same time, or change from one set to another depending on their environment. This is why neither pure proactive or reactive routing may be able to satisfy the IoT's demands: Protocols need to be able to adopt to a rapidly changing environment, and do so autonomously and efficiently. Because traditional approaches to routing may not be feasible for this task, *hybrid roting protocols* have begun to resurface. This paper will introduce existing approaches to hybrid routing and aims to provide suggestions on how to evolve them to make them a better fit for the IoT.

1 Introduction

1.1 What is the Internet of Things?

The IoT envisions autonomous communication between computers installed in everyday objects such as furniture, toys, clothing, or tools with the goal of making them smarter and improving their user experience. Some IoT devices are very constrained, with no constant power supply. Therefor, they need to be resourceful in terms of computation, storage, RAM and energy usage. Other devices may not exhibit one or any of these characteristics. For example, a sensor built into a lamp can tap into the available power supply and is therefor not restricted by battery life concerns. A computer controlling a smart home may have more computation resources than the IoT nodes it manages, and so on. In other words, IoT networks are comprised of hardware which are homogeneous in terms of abilities and requirements, but most nodes are constrained in some way.

To communicate amongst each other, IoT nodes form spontaneous, wireless mesh networks. The vision of the Internet of Things is rapidly becoming reality, and with its rise, environments which cannot be optimally served by either reactive or proactive routing protocols alone are created. Thus, the demand for a new kind of routing protocol is created, too.
One example for this may be the lighting system in a smart home: Each lamp needs to maintain a stable connection to the control center of the house. This means that a substantial amount of control traffic is directed at the sink node that is the central control. Because of its direction, this traffic forms a tree-like topology. In addition to this, lamps may want to communicate spontaneously between each other, for example to create optimal lighting in the study when homeowners sit down at their desk.

1.2 What is hybrid routing?

Hybrid Routing protocols combine two central routing paradigms in one protocol: Reactive and proactive routing. While reactive protocols stay idle until a route is needed and then *react* to this demand, proactive protocols constantly monitor their network for peers and link qualities, (re-)calculating routes as they gather new data. The former class of protocols perform well in sparse, very mobile networks and save energy by generating less control overhead. The latter are

best suited for networks with high demands in terms of throughput, reliability and latency.
Hybrid routing protocols aim to adjust their routing strategy from proactive to reactive and, conversely, from reactive to proactive, depending on the circumstances: Routes or areas that are deemed important or see a lot of traffic require proactive attention, while sparsely, less important or very mobile areas or routes are best served reactively.
In the example of section 1.1, all lamps would maintain a proactive route towards the control center, while inter-lamp communication may be set up reactively.

The rest of this paper is organized as follows. The next section recounts the history and context of hybrid routing research. Subsequently, requirements for hybrid routing protocols will be listed in section 2.1, followed by an introduction to existing hybrid routing protocols and their specific characteristics in section 3. Section 4 then goes into central characteristics which are exhibited by all hybrid routing protocols presented. Following up, section 5 examines existing experimental research and considers how it could be advanced with the use of testbeds. Section 6 then goes on to discuss the findings presented in previous sections with regard to their suitability for the IoT. Finally, section 7 provides a conclusion of the approaches presented and discussed and an outlook towards future work.

2 History of hybrid routing research

Most research on hybrid routing protocols stems from an era where wireless mesh routing was at its very beginning. This meant that the building blocks for hybrid routing, namely proactive and reactive routing protocols, were under construction themselves. While proactive and reactive protocols were developed and examined, research in hybrid routing stalled until a more thorough understanding of proactive and reactive has been reached.
This has since been achieved: The Internet Engineering Task Force (IETF) has standardized Optimized Link-State Routing (OLSR)[1], OLSRv2[2] and Ad hoc On-Demand Distance Vector Routing (AODV)[3], AODVv2[4] is on its way to become a standard, and The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)[5] will be deployed in the large-scale smart grid network of France [6]. The body of experience with both reactive and proactive protocols has grown and created the building blocks needed to pick up hybrid routing protocol research again.

But while this milestone has been reached, the amount of protocols of any kind specifically targeted at IoT-like environments is very small. By the time of this writing, the Routing Protocol for Low Power and Lossy Networks (RPL)[7] is the only dedicated IoT protocol available, and it cannot cover the entire diverse set of requirements that are found under the umbrella term of "Internet of Things". Thus, it is necessary to evaluate protocols designed for environments that share some characteristics with the Internet of Things and may be customized to be a good fit. Suitable environments are as follows:

Delay Tolerant Networks (DTNs) are designed to cope with network partitioning, which my be caused by movement or lossy links.

Mobile Ad-hoc Networks (MANETs) share the characteristic mobility challenges and ad-hoc nature of their infrastructure with the IoT.

Low Power and Lossy Networks (LLNs) match IoT requirements the closest: nodes are expected to be constrained in terms of battery and computation resources, and links are expected to be lossy. One might say that The IoT consists of many LLNs, attached to the big Internet through border routers.

Vehicular Ad-Hoc Networks (VANETs) have seen a lot of research concerning hybrid protocols. Unfortunately, their characteristics differ too drastically from the IoT: node mobility in VANETs is extremely high, with somewhat ordered movement patterns as cars usually only move on streets, which are known beforehand.

The goal of this paper is thus to explore how hybrid routing can be advanced with the IoT in mind, building on the foundation which research on MANET routing of the past 15 years has built. It aims to provide a critical overview over existing work and highlight challenges which might arise in hybrid protocol design for the IoT.

Name	Scope	Architecture	Published
Node-Centric Hybrid Routing [9]	Path	Compositional	2002
SHARP[8]	Area and path	Compositional	2003
P2P extension[10] of RPL[7]	Path	Monolithic	2013
ZRP [11] and extensions [12] [13] [14]	Area	Monolithic	2002/2004
ZHLS[15] and extension [16]	Area	Monolithic	1999/2006
HYMAD[17]	Area	Compositional	2010

Table 1: Overview over existing hybrid protocols. An explanation of the terminology used can be found in section 4

2.1 Requirements for hybrid routing protocols for the IoT

Ramasubramanian et al. [8] list three core properties a hybrid routing protocol needs to have. Although originally written with mobile ad-hoc networks in mind, these principles can be adapted to the IoT.

Adaptivity Because IoT use cases are as numerous as its environments are subject to changes, the protocol should be able to adapt to a wide variety of circumstances. It should adjust its behavior to changes in mobility, traffic patterns, link quality, and other qualities.

Flexibility The protocol should be able to satisfy the requirements of different applications in terms of reliability, latency or throughput.

Efficiency and robustness The protocol should strive to be efficient in terms of energy consumption, traffic and computational overhead, all the while maintaining the ability to reliably find routes through the network. It must perform equally well or better than purely reactive or proactive protocols in the same situation.

3 Existing Protocols

The following section will provide a short introduction to all existing hybrid routing protocols and its characteristic mechanisms for MANETs, LLNs and DTNs. A tabular overview can be found in table 1.

3.1 Zone Routing Protocol (ZRP)

The Zone Routing Protocol was originally developed for MANETs and is one of the most-referenced and -extended hybrid routing protocols to date. It was originally described in an Internet-draft which expired on January 2003[11]. It clusters nodes into so-called *Routing Zones*, which adapt their diameter to the network's degree of mobility and traffic density. Routes inside these routing zones are discovered and maintained in a proactive fashion. In addition to the topology inside their zone, nodes are also aware of topology which all routing zones form. To find routes to nodes in foreign routing zones, the reactive protocol makes use of a technique similar so some multicast routing approaches. The so-called Bordercast Routing Protocol (BRP)[18] constructs an overlay *bordercasting* tree between all routing zones, and forwards the packet along the tree to one *bordercasting node* per routing zone. Each bordercasting node will know if the target of the route discovery is in their routing zone, since the zones are maintained with a proactive protocol. If this is the case, it reports this to the source node, and the data exchange begins. If it is not the case, it forwards the packet. This way, traffic overhead is avoided. An illustration of this clustering can be found in fig. 1.

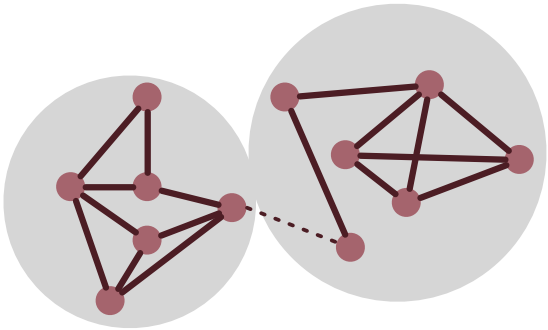


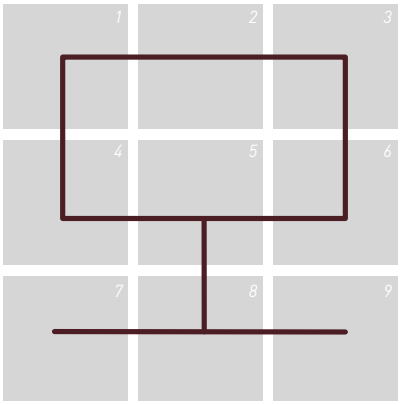
Figure 1: Sketch of area-centered routing, as practiced by ZRP, ZHLS and HYMAD

The draft describes ZRP as a routing *framework*. It introduces its own proactive and reactive

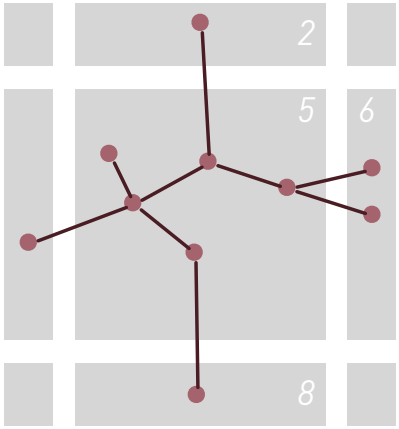
protocol, namely the Intrazone Routing Protocol (IARP)[19] for proactive routing inside routing zones, and the Interzone Routing Protocol (IERP)[20] to discover routes between zones reactively. Because of the modular nature of ZRP, alternate protocols such as OLSR for proactive or AODV for reactive may be used instead of the predefined options (i.e. IERP and IARP).
There are two extensions of ZRP: the Two-Zone Hybrid Routing Protocol (TZRP)[12], the Wireless Ad Hoc Routing Protocol (WARP)[14] and the Independent Zone Routing Protocol (IZR)[13].

3.2 Zone-Based Hierarchical Link State (ZHLS)

ZHLS is a hierarchical, GPS-based roting protocol. It clusters all nodes into non-overlapping routing zones based on their geographical location. This is done with the use of a zone map, "which has to be worked out at the design stage"([15], p. 1416). There is no information provided whether the zone map is determined at the protocol or the network design stage.
Similar to routing mechanisms in peer-to-peer overlay networks, destinations are not just determined by their IP address, but by a (Zone ID, IP Address) tuple. On startup, Each node automatically knows on which zone ID it belongs to based on its GPS coordinates. As usual, route discovery within the zones is done in a proactive fashion, but nodes also maintain information about connections to neighboring zones. These neighboring nodes are called *gateway nodes*. Additionally, an overlay network which connects the routing zones is created. Whenever a connection between two nodes from neighboring zones is known, a route between their zones exists, too. An illustration of the topology of both the routing zone overlay and the connections inside a zone can be found in fig. 2. This protocol design bears the often erroneous assumption that physical proximity guarantees near-optimal, or even any kind of, connectivity, which has been debunked by [21] and [22]. Additionally, GPS localization is known to be imprecise inside buildings or reflecting environments such as narrow streets, which could impact protocol performance even further. Hamma et al.[16] propose to reintroduce gateway flooding to ZHLS.



(a) Topology of routing zone overlay



(b) Detailed view into a routing zone

Figure 2: Overview over ZHLS hierarchy layers

3.3 Node-Centric Hybrid Routing

NCHR[9] serves networks which contain some nodes, called *netmarks*, that offer services to their peers, such as being a DNS server or an Internet Access Point. All nodes in the network maintain proactive routes towards the netmarks, while other connections are established reactively. This introduces an ability-based hierarchy into routing zones which strays from the common assumption that all nodes are equal and routing zones are created by proximity. The draft uses SOAR[23] for this, but maintains that AODV[3] or DSR[24] may be used just as easily.

3.4 Hybrid DTN-MANET Routing for Dense and Highly Dynamic Wireless Networks (HYMAD)

Just like ZRP, ZHLS, and Node-centric Hybrid routing, nodes participating in HYMAD [17] form proactively maintained zones. These zones are maintained by an unspecified distance-vector routing algorithm. The difference to all previously named protocols is that HYMAD borrows its approach to inter-zone roting not from traditional MANET schemes, but from Delay-Tolerant Networks (DTN), where nodes store data until they move and meet other nodes with which they

can communicate (this is called *store-and-forward*).
While amongst the more recent research, there are no peer-reviewed publications about HYMAD.

3.5 Sharp Hybrid Adaptive Routing Protocol (SHARP)

This protocol claims to offer each application the possibility to specify their needs in terms of latency and loss rate in the form of a metric, which is then used to guide the trade-off between proactive protocol overhead and reactive loss of reliability and latency. SHARP combines both area-centered and path-centered paradigms in what could be called a path-centered-in-area-centered approach. Routing zones are established around *hot destinations*, i.e. nodes at which a majority of the traffic is directed. Gateways, nodes that offer a service, or sink nodes which collect sensor data in a Wireless Sensor Network may qualify as such a hot destination. Inside these routing zones, a Destination Oriented Acyclic Graph (DODAG) is formed with the hot destination as root, and proactive routes are kept *only towards the hot destination node*. SHARP claims that this help meet the application requirements stated above, but it comes at the cost of enhanced traffic overhead and uneven battery draining, because nodes closer to the hot destination will forward more traffic than the ones on the outskirts.

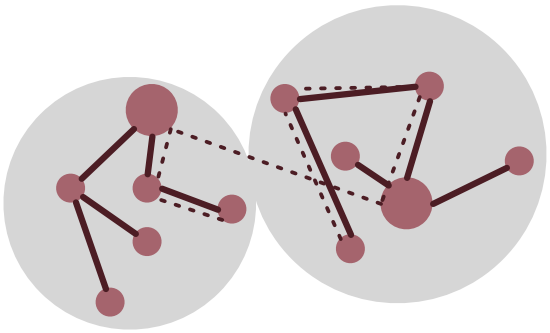


Figure 3: Sketch of the SHARP topology

If the desired destination is outside of the routing zone, a reactive route discovery is initiated. This is similar to ZRP's approach.
SHARP's routing strategy relies heavily on the assumption that only special nodes are the target of traffic, and is likely to fail in environments where all nodes are equal.
SHARP defines its own proactive protocol, the SHARP Proactive Routing protocol (SPR), which is based on DSDV[25] and TORA[26]. Neither of these protocols are relevant in MANET routing as of today. For reactive routing, AODV is used, but may be exchanged for any other reactive protocol.
[8] does not offer a solution as to how hot destinations may be identified by the participating nodes.

3.6 P2P-RPL

The P2P-RPL protocol is an extension of the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL)[7]. RPL itself was designed for IoT-like circumstances, but focus primarily on networks which feature a *sink node* towards which all traffic is directed. RPL constructs a DODAG whose root is the sink node. All traffic is then routed towards the sink node. Parent nodes in the DODAG do not necessarily know about their children, so communication towards any other than the sink node is not possible in all configurations of the RPL protocol. In case it is possible, packets from one leaf node to another will always have to travel to the root node first to be sent back, even if they are in close proximity. In networks with a substantial amount of peer to peer traffic, this leads to battery draining and traffic bottlenecks close to the sink node. This is why [27] suggests to extend the protocol with reactive route request messages which are piggybacked onto regular RPL traffic whenever a node S wants to communicate with a neighbor D, which is not the sink node. As soon as it receives this route request, D answers with a route reply. Through the distribution of these messages, a DODAG originating at S is formed, along which the peer to peer traffic can now be routed.

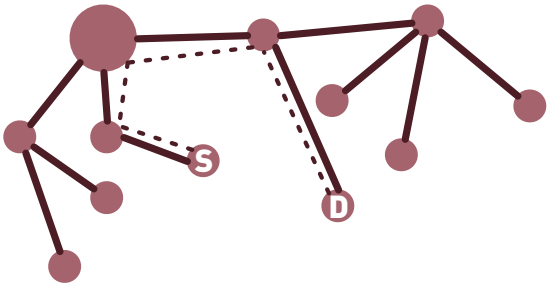
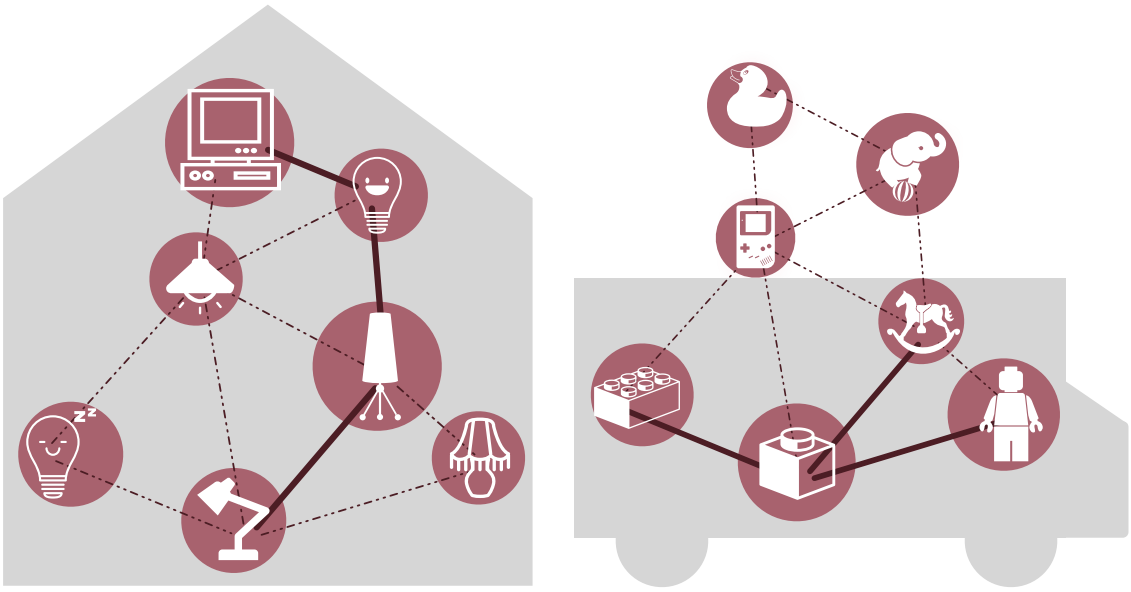


Figure 4: Sketch of the P2P-RPL topology



(a) Example of a path-centered network: lights and control center in a smart home.

(b) Example of an area-centered network: Goods in a delivery truck and warehouse

Figure 5: Application Scenarios for hybrid routing protocols[2]

4 Central aspects of hybrid routing protocols

All hybrid protocols discussed in section 3 share commonalities, some of which fundamentally shape the way a routing protocol sees and serves a network. The goal of this section is to identify these aspects and discuss them with regard to the requirements of IoT environment.[1]

4.1 Scope

Hybrid protocols differ in the way they prioritize routes and decide which of them should be maintained proactively or set up reactively. There are two approaches to this, which this paper dubs the *path-centered* and the *area-centered* approach repectively.

path-centered This approach serves networks in which some nodes, near or far, are more important than others. This is illustrated by the use-case demonstrated in fig. 5a, which shows the different lamps of a house and the house's control center. Each lamp needs a stable connection to this control center, be it to switch on/off occasionally to confuse burglars, or exchange status info and configurations. Thus, this connection is maintained proactively, as indicated in the diagram by the thick straight line. Additionally, they may want to communicate with each other upon user interaction. Because this happens spontaneously and sparsely, the connections amongst all lamps are set up reactively, as indicated by the dotted lines. The most recent publication on hybrid routing, which is also the only publication with a focus on the IoT [10], features a path-centered approach using RPL[7] as a basis, extending it with its own reactive mechanism.

area-centered Protocols relying on this approach assume all nodes are equal in principle, but nearby nodes are more important than nodes which are farther away and know their neighborhood best. They cluster the network into so-called "routing zones". Nodes that are in the same zone maintain their connections among each other proactively, so routes towards other members of a routing zone are always known beforehand. Routes towards nodes from foreign

[1] Note that the taxonomies presented are not common in previous work, but were created by the author due to a lack of naming in other literature.

[2] Computer designed by Ji Sub Jeong, Light bulbs designed by Julien Deveaux, Lamps designed by Renee Ramsey-Passmore, Thomas Le Bas and Becca O'Shea, Rubber Duck designed by Simon Child, Rocking Horse designed by Okan Benn, Circus Elephant designed by Solène Troussé, Lego designed by Okan Benn, Lego designed by Jon Trillana, Game Boy designed by Simon Child, Castle designed by Road Signs.

zones are established reactively. Existing hybrid protocols which rely on routing zones cluster nodes into zones based on their physical or topological proximity. For example, SHARP periodically adjusts the number of hops which make up a routing zone based on changes in link and traffic metrics.
One example use-case for area-centered routing may be a warehouse as illustrated in 5b whose goods (or their packaging) are equipped with IoT hardware. Employees are thus able to tell details about the stock simply by asking their scanner, which communicated with the other IoT devices. In case a truck with new goods arrives, employees can use their scanner to ask for the nearest packaging for information about the entire truckload. Thus, knowledge about their immediate neighbors is vital to these nodes, while none of them has special features which may turn it into a "more important node". Many early attempts at Hybrid routing, most popularly ZRP, but also more recent research such as HYMAD, feature this approach.

Because the IoT is an umbrella term for many different use cases, none of these approaches is necessarily better than the other. Even combinations of both paradigms could be feasible. It may even be argued that Node-Centric Hybrid Routing, as detailed in section 3.3, is such a hybrid-hybrid: While it does cluster nodes into routing zones, the topology of these routing zones is directed towards its most important member, the *netmark*. The suitability of both approaches for a specific environment depends on traffic and mobility patterns (caused by different usage scenarios) and the roles of all nodes involved.

4.2 Architecture

Because hybrid protocols incorporate proactive and reactive protocols as building blocks, the relationship between its reactive and proactive components– how it all goes together– may be more than just a sequence of instructions. All hybrid protocols presented in section 3 can be classified as one of the two following architectural types.

Monolithic protocols have a reactive and a proactive component firmly in place. Oftentimes, these components are variations of well-known proactive and reactive protocols, customized to improve the hybrid protocol's overall performance or decrease traffic- or computational overhead. For example, [27] piggybacks reactive control traffic onto already existing, proactive RPL messages, thus avoiding unnecessary traffic and saving battery life. This bears great potential for optimization, but complicates code re-use and the deployment of updates.

Compositional protocols are organized as a mere *framework* which can be used to combine different proactive or reactive protocols. The choice which proactive and reactive protocols are used is not made the protocol designer anymore, but by the person deploying the protocol for a specific environment.
Some existing hybrid solutions such as SHARP, Node-Centric Hybrid Routing and HYMAD chose this route, but with a twist: one component, for example the reactive protocol, is fixed, while the proactive protocol can be exchanged at will. This architecture allows for a great deal of flexibility: If a new version of a protocol that is in use surfaces, it can be adopted quickly. The same with alternative protocols which prove to serve some or all use-cases better. Existing implementations of well-known proactive or reactive protocols can be integrated and re-used. A compositional protocol bears the possibility to be customized for certain deployments, because the most suitable proactive and reactive protocols for the task may be picked and combined seamlessly. Of course, this comes at the cost of lightweightedness: Approaches which are very flexible usually produce a higher amount of overhead. Additionally, if preexisting specifications and implementations are used, it may be hard to optimize them in terms of size and computational or traffic overhead.

5 Experimental work

Most research concerning hybrid routing protocols stems from a time where large testbeds were technically not feasible and simulations were conducted instead. Thus, publications documenting real-world experience with hybrid deployments are rare.

[28] has evaluated the reactive AODVv2 protocol for IEEE 802.15.4. networks, a technology widely used in IoT deployments, as early as in 2006. However, the "real environment" used consists of 4-7 nodes, arranged in different topologies with a per-node distance of 12 cm. While a careful evaluation of simplified topologies is invaluable when examining new approaches, these findings can not provide us with information on the performance of (NST-)AODV in large scale, production IoT deployments. [27] reports about testbed experiences with P2P-RPL, comparing its performance in comparison to pure RPL in terms of route length and percentage of routes traversing the root node. In [14], WARP is compared to OLSR in experiments with a "real" network, which turns out to consist of 14 unidentified laptops connected to an unspecified number of stationary PCs over ethernet. This research is from 2002, a time when WiFi hardware wasn't necessarily standard in consumer-grade laptops.

While simulations have proven to be useful for protocol design and evaluation, there are three main problems to a simulation-only approach:

1. A simulation is only as good as its model. As shown by [21] and [29], many simulations conducted in wireless network research are based on flawed assumptions about the environment they are trying to model, resulting in drastic deviations from reality. Additionally, as shown by [30], results of the same experiment may vary from simulator to simulator.

2. Without data from "real world" experiments, the verification a model represents real conditions satisfactorily is hard.

3. Especially in wireless networking, a node's environment (i.e. flying bids, surfaces reflecting differently based on time or weather conditions, unforeseeable radio propagation...) is a big and unforeseeable influence. Even when the model is adequately accurate, it can never account for the unforeseen quirks which will be encountered in a real environment. This can be a great benefit when testing specific aspects of a protocol, because it is possible to observe just this aspect. But in order to test if a protocol can cope with the challenges the real world brings, it has to be tested in a lifelike environment.

Of course, even data from testbed experiments or even real-world deployments can never fully reproduce real conditions either: The collected data can never be a complete map of the situation, and by deciding which data to collect, information is prioritized and quantified. This decision, too, is influenced by assumptions about the environment which is monitored. Still, experiences from real-world experiments or deployments are vital to fully understand the challenges of hybrid IoT routing and assess the solutions at hand. Because the opportunity to deploy experimental software on productive systems is rarely given, more and more testbeds have been established in recent years. [31] provides a requirement analysis for IoT-ready testbeds. It concludes that in order to be suitable for meaningful research, testbeds need to offer the following features to their users:

Experimentation: The ability to specify, interact with, monitor, and repeat an experiment in a straightforward way. Additionally, the ability to run an experiment through simulation, with conditions similar to the testbed, should be given.

Hardware Features: The hardware provided should be heterogeneous, with various capabilities and sensor types. The number of available devices should be possibly in the hundreds, with the possibly to add more recent devices in the future. In case of testbeds that span across several sites, the possibility of federating them into a big network should be given. The hardware should be subject to regular maintenance.

Mobility: Devices of the testbed should be able to move around in various patterns with the help of robotic and automation systems.

Software management & tools: Simulation scenario configuration, may it be mobility patterns, hardware configurations, or low-level device control, should be easily accessible.

Based on this analysis, it provides an overview over existing facilities and their features. The two biggest testbeds, IoT-Lab[3] and smartsantander[4] feature between 2,728 and 20,000 nodes and, even though their primary target are Wireless Sensor Networks (WSNs), provide mobility through toy trains (IoT-Lab) or public buses (senslab). The latter has an impact on the reproducibility of experiments and limits the influence an experiment designer has on mobility patterns.

6 Suitability for the IoT

Because most of the discussed hybrid protocols have not been designed for the IoT, not all of their characteristics may be suitable for such a deployment. This section discusses common pitfalls and possibilities on how to advance the propositioned hybrid protocol solutions towards suitability for the IoT. However, experience with both hybrid protocols and IoT environments is rare, as detailed in section 5, so all statements about suitability have to be taken as educated guesses rather than hard truths.

As discussed in section 4, routing protocols can be categorized to be either path- or area-centered in terms of scope, and either composite or monolithic protocols in terms of architecture.
All proposed area-centered protocols cluster nodes into routing zones either by geographical or topological proximity. For the IoT, this approach to clustering could be extended with regard to communication patterns: Nodes may be more likely to communicate frequently based on their abilities (all nodes with a constant power source), their purpose (all kitchen appliances), or their activity (all nodes which require periodic updates), to name only a few.
The scope of a routing protocol heavily depends on the kind of network it serves: are there sink nodes, or are all nodes created equal? Which routes are considered most important, and how are they determined? All answers to these questions are valid, but produce very different requirements a protocol must fulfill. Therefore, none of the discussed approaches is necessarily better than the other. Time may tell which kind of use case and thus which kind of scope is more common. Alternatively, it might be discovered that this clear distinguishment may not be found in the wild, and that a hybrid protocol has to serve both (or even more) kinds of networks. One way of implementing this may involve defining all n-hop neighbors of a node in a path-centered protocol as sink nodes, thus artificially creating routing zones.
Ideally, a hybrid protocol for the IoT would be able to identify the kind of environment it is operating in and adjust to its needs, but building such a protocol likely depends on the development of more use-case oriented protocols first.

6.1 Assumptions about the protocols' environment

Some of the protocols presented in section 3 are based on assumptions which have since been proven to be problematic, or exhibit characteristics which may be unsuitable for the IoT. The reliance on geographic neighborhood as employed by ZHLS, while intuitive at first, has been shown to be inadequate by [21] and [22].

6.2 Increased complexity to avoid routing loops

One of the main problems in protocol design is guaranteeing loop-freeness. A routing protocol has to ensure that no routes are created which form a circle rather than a path, so-called routing loops. Routing protocol have their own protection mechanism against this, which are often proven to be correct in complex theoretical procedures. When two routing protocols serve the same network, the probability of routing loops increases. What protects one protocol from routing loops might not apply to the other protocol, or, in the worst case, might counter the other protocol's loop prevention mechanisms. This is even bigger a challenge if the hybrid protocol to be designed is not of the monolithic kind, but a composition of two interchangeable base protocols. In this case, the proactive and reactive protocols which are used cannot be modified statically. Instead, a flexible solution which applies to any and unknown protocol combinations has to be created. Because the components are not known beforehand, this solution has to be sound even without

[3] `https://www.iot-lab.info`
[4] `http://www.smartsantander.eu`

the possibility to prove the correctness of collective loop-free prevention mathematically. Alternatively, a way to prove loop-freeness for a protocol combination whenever necessary has to be found.

6.3 Long- vs short term solutions

Provided there are ways to slim down the code to a manageable size and control overhead, frameworks for hybrid protocol composition appear to be the more appealing approach, as they are likely to be more future-proof and flexible. As mentioned in section 3, many of the protocols that were the basis for modifications are considered outdated now. While this took decades in this instance, the IoT may be considered to be just as established a field as MANETs were at the turn of the millennium. Thus, it is not unlikely it will be subject to changes and paradigm shifts, too, and a hybrid routing protocol for the IoT should be able to account for this to a certain extent. However, it might also take many more years and failed attempts at IoT hybrid routing until the subject is understood well enough to create such a framework. this includes, but is not limited to, handling the increased complexity of avoiding routing loops, as sketched above.

Thus the, creation, evaluation and optimization of monolithic protocols with a clear use case and mission may help gaining the knowledge which is necessary to develop more flexible and capable hybrid routing frameworks.

7 Conclusion and Outlook

In conclusion, there is ground work in hybrid routing research to build on, but this body of work has been created before the rise of the IoT. Most of it has to be updated to not only to suit the IoT, but also to respect the leaps MANET, DTN and LLN routing research has made. The fundamental building blocks of hybrid routing protocols, proactive and reactive routing protocols, have changed and evolved since the majority of hybrid protocols were conducted. Many proactive or reactive protocols which were used in said research are now irrelevant or have been replaced by more recent versions.

It has been demonstrated that there are two categories for hybrid protocols in terms of architecture and scope. Architecturally, both monolithic and compositional protocols have their merits and downsides. Monolithic protocols have to find a way to incorporate future progress in the proactive and reactive routing protocols they are based on, while compositional protocols face the challenge of reducing overhead and prevent additional routing loops problems. Because of their increased complexity, compositional protocols may require a deeper understanding of hybrid routing before feasible solutions can be proposed. This understanding may, as has been mentioned, be gained through thorough and comparable testbed experiments, which could be conducted in the IoT-Lab. The IoT-Lab constitutes a testbed specifically constructed for IoT research. It features a number of nodes large enough to create significant results and gives researchers a high degree of control over their experiments.
With regard to scope, both approaches– area-centered and path-centered– may work for distinct sets of use cases. As the IoT evolves, time will tell which of these use cases is more common, and whether the clear distinction made in section 4.2 can be made at all.

It has been discussed that the research concerning hybrid protocols has been mostly supported by simulation results. However, in order to be able to draw resilient conclusions about the suitability of different hybrid protocols, practical experience has to be gathered, and comparable results have to be created. One way to achieve this may be through testbed experiments in which several promising hybrid routing protocols face the same challenges and are evaluated for their performance in dealing with them. Through this process, the correctness of the suggestions made in this paper can be disproved or verified. Additionally, pitfalls which were not considered during the modeling of earlier simulations may be uncovered– and can then be incorporated into future research and protocol design. Conducting simulations may help in the startup process of these efforts, but can not be a substitute for real-world experiences.

The field of hybrid routing protocols for the IoT is an open one, but with the help of testbed research, this promising paradigm can be elevated towards a meaningful addition to the IoT.

References

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

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

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

[4] C. Perkins, S. Ratliff, J. Dowdell, and L. Steenbrink, "Dynamic MANET On-demand (AODVv2) Routing," Internet-Draft – work in progress 06, IETF, December 2014.

[5] J. Yi and T. Clausen, "Collection Tree Protocol for Lightweight On-demand Ad hoc Distance- vector Routing - Next Generation (LOADng-CT)," Internet-Draft – work in progress 02, IETF, July 2014.

[6] ITU, *ITU-T G.9903: Narrow-band orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks: Amendment 1.* International Telecommunications Union, May 2013.

[7] 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.

[8] V. Ramasubramanian, Z. J. Haas, and E. G. Sirer, "SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '03, pp. 303–314, ACM, 2003.

[9] S. Roy and J. J. Garcia-Luna-Aceves, "Node-Centric Hybrid Routing for Ad Hoc Networks," in *Proceedings of the International Workshop on Mobility and Wireless Access*, MobiWac '02, (Washington, DC, USA), pp. 63–, IEEE Computer Society, 2002.

[10] M. Goyal, E. Baccelli, M. Philipp, A. Brandt, and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks," RFC 6997, IETF, August 2013.

[11] Z. Haas, M. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," draft, IETF, July 2002.

[12] L. Wang and S. Olariu, "A Two-Zone Hybrid Routing Protocol for Mobile Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, pp. 1105–1116, Dec. 2004.

[13] P. Samar, M. R. Pearlman, and Z. J. Haas, "Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 12, pp. 595–608, Aug. 2004.

[14] P. Sholander, A. Yankopolus, P. Coccoli, and S. Tabrizi, "Experimental comparison of hybrid and proactive MANET routing protocols," in *MILCOM 2002. Proceedings*, vol. 1, pp. 513–518 vol.1, Oct 2002.

[15] M. Joa-Ng and I.-T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 17, pp. 1415–1425, Aug 1999.

[16] T. Hamma, T. Katoh, B. Bista, and T. Takata, "An efficient zhls routing protocol for mobile ad hoc networks," in *Database and Expert Systems Applications, 2006. DEXA '06. 17th International Workshop on*, pp. 66–70, 2006.

[17] J. Whitbeck and V. Conan, "HYMAD: hybrid DTN-MANET routing for dense and highly dynamic wireless networks," *CoRR*, vol. abs/1006.3426, 2010.

[18] Z. Haas, M. Pearlman, and P. Samar, "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks," Internet-Draft – work in progress 02, IETF, July 2002.

[19] Z. Haas, M. Pearlman, and P. Samar, "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," Internet-Draft – work in progress 02, IETF, July 2002.

[20] Z. Haas, M. Pearlman, and P. Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," Internet-Draft – work in progress 02, IETF, July 2002.

[21] D. Kotz, C. Newport, and C. Elliott, "The mistaken axioms of wireless-network research," tech. rep., Dartmouth Computer Science, July 2003.

[22] G. Lim, K. Shin, S. Lee, H. Yoon, and J. S. Ma, "Link stability and route lifetime in ad-hoc wireless networks," in *Parallel Processing Workshops, 2002. Proceedings. International Conference on*, pp. 116–123, 2002.

[23] S. Roy and J. Garcia-Luna-Aceves, "Using minimal source trees for on-demand routing in ad hoc networks," in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, pp. 1172–1181 vol.2, 2001.

[24] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, pp. 153–181, 1996.

[25] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications*, SIGCOMM '94, 1994.

[26] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proceedings of the INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution*, INFOCOM '97, 1997.

[27] 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.

[28] C. Gomez, P. Salvatella, O. Alonso, and J. Paradells, "Adapting aodv for ieee 802.15.4 mesh sensor networks: theoretical discussion and performance evaluation in a real environment," in *World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium on a*, pp. 9 pp.–170, 2006.

[29] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott, "Experimental evaluation of wireless simulation assumptions," in *Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '04, pp. 78–82, 2004.

[30] D. Cavin, Y. Sasson, and A. Schiper, "On the accuracy of manet simulators," in *Proceedings of the Second ACM International Workshop on Principles of Mobile Computing*, POMC '02, pp. 38–43, 2002.

[31] A.-S. Tonneau, N. Mitton, and J. Vandaele, "A survey on (mobile) wireless sensor network experimentation testbeds," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, pp. 263–268, May 2014.