Telematics
Computer Systems

Freie Universität Berlin

A Survey of Flooding, Gossip Routing, and Related Schemes for Wireless Multi-Hop Networks

Bastian Blywis Mesut Günes Felix Juraschek Oliver Hahm
Nicolai Schmittberger

Computer Systems and Telematics
Institute of Computer Science
Freie Universität Berlin, Germany
{blywis, guenes, jurasch, ohahm, schmittb}@inf.fu-berlin.de

Technical Report
TR-NO: TR-B-11-06

October 10, 2011

Contents

List of Figures

List of Tables

Abstract

Flooding is an essential and critical service in computer networks that is used by many routing protocols to send packets from a source to all nodes in the network. As the packets are forwarded once by each receiving node, many copies of the same packet traverse the network which leads to high redundancy and unnecessary usage of the sparse capacity of the transmission medium. Gossip routing is a well-known approach to improve the flooding in wireless multi-hop networks. Each node has a forwarding probability $\mathtt{p}$ that is either statically per-configured or determined by information that is available at runtime, e.g, the node degree. When a packet is received, the node selects a random number $\mathtt{r}$. If the number $\mathtt{r}$ is below $\mathtt{p}$, the packet is forwarded and otherwise, in the most simple gossip routing protocol, dropped. With this approach the redundancy can be reduced while at the same time the reachability is preserved if the value of the parameter $\mathtt{p}$ (and others) is chosen with consideration of the network topology.

This technical report gives an overview of the relevant publications in the research domain of gossip routing and gives an insight in the improvements that can be achieved. We discuss the simulation setups and results of gossip routing protocols as well as further improved flooding schemes. The three most important metrics in this application domain are elaborated: reachability, redundancy, and management overhead. The published studies used simulation environments for their research and thus the assumptions, models, and parameters of the simulations are discussed and the feasibility of an application for real world wireless networks are highlighted. Wireless mesh networks based on IEEE 802.11 are the focus of this survey but publications about other network types and technologies are also included. As percolation theory, epidemiological models, and delay tolerant networks are often referred as foundation, inspiration, or application of gossip routing in wireless networks, a brief introduction to each research domain is included and the applicability of the particular models for the gossip routing is discussed.

CHAPTER 1

Motivation and Introduction

1.1 Introduction

Gossip routing, sometimes also referred to as *gossiping* or *probabilistic flooding*, is an approach to improve the performance of flooding. Flooding, also referred to as *blind flooding* [1], is an important service[1] in computer networks and is applied when a source node has to send some data to all nodes or a particular node in the network. This is usually achieved by broadcasting the data packets. Each node that receives the packet forwards it as broadcast if it has not been forwarded previously. In this way the packet traverses the whole network and reaches a subset of the nodes. Flooding in wireless networks benefits from the broadcast property of the transmission medium. This property enables routers to transmit only one packet that is received by all neighbors, instead of one packet per dedicated link, as it is the case in wired networks. *Mobile ad-hoc networks* (MANETs) [2], *wireless mesh networks* (WMNs) [3], and *wireless sensor networks* (WSNs) [4] are specific multi-hop wireless networks that require sophisticated flooding schemes.

Before we will discuss the benefits, deficiencies, and improvements of flooding in more detail in Section 1.2, it is necessary to introduce and clarify some important terms in the next section that are relevant in the context of this technical report.

1.1.1 Terminology

Several of the terms that are used in this report and in the related literature, e.g., *broadcasts* are ambiguous and have different meanings in the research and application domains of telecommunications. For the understanding of this technical report it is important to specify their significance in the context of flooding and gossip routing.

Entities of the Network

A network is made up of several entities and the terms node, station, and router are used synonymously in this report. They describe entities that join or create a network and enable data communication. *Node* is the abstract term that originates from graph theory but is also used in the domain of WSNs. Nodes are the vertices of a graph that are connected with each other by edges, respectively links in the context of computer networks. In IEEE documents, nodes are often referred to as *stations* and usually identify devices that can communicate on the ISO/OSI layer 2 with each other. In contrast, *routers* are devices that communicate on ISO/OSI layer 3 and connect sub-networks to enable multi-hop communication. As flooding can take place on layer 3, layer 2, or the so called underlay routing layer 2.5 we will not differentiate between the terms in the following. Most of the discussed improved flooding schemes can be applied on any of these layers.

Broadcast and Flooding

The term *broadcast* can be used in the following contexts. On the *network layer*, a broadcast is a communication principle where a source node sends a packet to all nodes in a sub-network. The most

[1] Flooding is also a protocol, even though a very simple one.

common example is an IPv4 datagram broadcast usually to the last address in the particular address interval of the sub-network [5], e.g., `192.168.2.255` for the `192.168.2.0/24` network. The group of broadcast receivers is dependent on the subnet mask that defines a logical sub-network as part of a larger address space. Upon packet reception, the network layer protocol implementation evaluates the destination address in the packet header. If the destination address and the broadcast address configured for the node match, the packet is identified as a broadcast. Due to misconfiguration of the subnet mask it can occur that a broadcast sent by node A is identified by node B as an unicast to some other node C; unicasts can be accidentally evaluated as broadcasts vice versa.

Data link layer (DLL) broadcasts refer to the transmission of packets, called frames in this context, to all stations that are (normally) connected in the same network segment. In Ethernet respectively IEEE 802.3, the address `FF:FF:FF:FF:FF:FF` is reserved for broadcast frames. Higher layer broadcast packets usually use DLL broadcast frames if the network technology supports broadcasting. Thus network layer broadcasts are often received by all stations on the same segment[2]. When radio transceivers are used instead of wired network interface cards, an important property changes. Not all stations on the same network can communicate on the DLL with each other due to the limited radio communication range. For example, the maximum range of IEEE 802.11 transceivers can be limited to only a few meters in indoor scenarios while the network spans the whole building. In this application context the term network segment is unfortunately not well defined. Although radio technologies like IEEE 802.11 have a broadcast address, broadcasts of one station are limited to its physical layer (PHY) broadcast domain (sometimes also called a *collision domain*) and are not received by all nodes in the network. Further on, there is no strict difference between broadcast and unicast frames as the medium is shared by all stations and both types of frames are received by all stations that are in range. With the help of special devices like wireless repeaters, the range can be extended on the DLL and network layer packets can be forwarded over multiple intermediate stations by using routers. When a node receives a frame in the latter case, the payload, which is a network layer packet, is placed in a new frame and is sent to the next station. All nodes in MANETs, WMNs, and WSNs are usually routers and can provide this service. In contrast, wireless repeaters are more common in infrastructure based IEEE 802.11 networks.

The term flooding is used synonymously with *network-wide broadcasting*. All nodes that are part of the network are potential destinations of a particular packet. In the following, the term *flooding* shall be understood as forwarding of network layer packets over multiple hops using DLL layer broadcasts on a broadcast transmission medium. Broadcast as well as unicast network layer packets can be flooded. The only difference is whether a single or all nodes are addressed.

Copies and Duplicates

When a flooded packet is received by a node, it is broadcasted to all of its neighbors. As each neighbor will also broadcast the received packet this leads to many copies of the same packet that traverse the network at the same time. When multiple copies are received by the same node, all but the first copy are considered to be duplicates. The reception of many duplicates increases the redundancy and represents an unnecessary use of the sparse network resources (time, energy, etc). In most cases, duplicates are detected based on sequence numbers that are contained in each packet's header but also alternative approaches like the application of so-called *bloom filters* [6] are possible[3]. In general, some kind of duplicate detection is an integral component of most protocols for wireless networks as otherwise loops cannot be detected. Therefore protocols like the *spanning tree protocol* (STP) [7] and its many variants are normally not required[4].

1.2 Applications and Deficiencies of Flooding

Routing protocols often apply flooding to disseminate topology information or to sent route requests and replies over the network. The destination is either a particular node or all nodes shall receive the information to update their routing information base. *Link state routing* protocols as a representative of the class of proactive protocols periodically flood neighborhood information of any node. For example, the *Open Shortest Path First* (OSPF) protocol [8] applies flooding based on multicast addressing and *Optimized Link State Routing* (OLSR) [9] is an example from the wireless domain. In contrast, reactive

[2] Proxies can extend the range of layer 2 and layer 3 broadcasts.

[3] It has to be considered, that the application of bloom filters can lead to false positives.

[4] *Wireless distribution systems* (WDS) with wireless repeaters usually run STP as loops can span the wireless and wired network when multiple gateways are available.

protocols run an ad-hoc route discovery procedure when a packet has to be sent to a destination and no routing information is available[5]. In many reactive protocols a route discovery message is sent to all neighbors as broadcast. If they cannot provide the required routing information, the packet is forwarded to their neighbors and subsequently flooded over the whole network. Depending on the protocol, if some node can eventually answer with a route reply, the particular packet is either sent as unicast or flooded again in the opposite direction[6]. An IETF Internet-Draft [10] from 2001 tried to formally specify the route discovery procedure that is used in most of the well know MANET routing protocols, e.g., the *Dynamic Source Routing* (DSR) protocol [11] or the *Ad hoc On-demand Distance Vector* (AODV) routing protocol [12] but was never published as RFC.

There are several other application scenarios of flooding besides the route discovery. Signaling is an important service in networks that monitor particular devices or use sensors to detect events in the real world. Examples include the monitoring of servers, fire detection (an application of WSNs), or intrusion detection. In these applications delay and reliability are the most important metrics. Service and resource advertisement/discovery protocols can also make use of flooding. Advertisements/requests are sent either periodically or on demand to all nodes in a particular distance or over the whole network. In this scenario the packets can either be broadcasts, multicasts, or anycasts. In general every application layer protocol that relies on network layer broadcasts in multi-hop networks requires some form of flooding, respectively a network-wide broadcast. Wireless networks are the most relevant example in the context of this survey. While there are dozens of proposed ad hoc routing protocols [13], little focus has been on the network layer broadcast of application layer data. In most cases the data packets are handled like route request, i.e., they are forwarded from node to node and looping packets are detected based on a sequence number. It is often assumed that flooding as a service "just works".

Although flooding is a very simple to implement service, it has some deficiencies. As all nodes re-broadcast the first copy of a received packet, nodes in the same physical broadcast domain will receive the same packet multiple times (duplicates). Therefore redundant data is unnecessarily sent over the medium. Especially in wireless networks, broadcast transmission may only be available with low data rates that are supported by all stations, for example the `BSSBasicRateSet` rates defined in the IEEE 802.11 [14] standard. An overview of the data rates for IEEE 802.11a/b/g is available in Table 1.1. In the case of the infrastructure mode with a *basic service set* (BSS) each station that wants to associate with the access point has to support the rates in the `BSSBasicRateSet` advertised by the access point. In contrast, the *independent basic service set* (IBSS) used in the ad-hoc mode has no central entity. Therefore all nodes will usually fall back to a data rate of 1 Mbps on 2.4 GHz and 6 Mbps on 5 GHz for broadcast and multicasts as the "most common denominator" for all stations. This applies to data broadcasts and also management packets that are broadcasted. Broadcast packets can therefore take significant time on the medium due to the low data rate, which curbs high-speed unicast data transmissions and decreases the overall performance of the network. The broadcasts also increase the contention and the overall noise level[7] as well as the delay and most probably reduce the *packet delivery ratio* (PDR). Due to these issues and the generally unreliable wireless medium, several packets might be lost and have to be retransmitted. In the worst case the retransmission has to be executed not by the previous hop but by the source of the packet that can be several hops away. When we assume that a route request packet was lost by some router, the result could be a sub-optimal or failed route discovery. Acknowledgement-based loss detection cannot be applied for flooded packets because the neighbors are often not known[8] and thus it cannot be guaranteed that all nodes in the neighborhood receive the packets. Further on, the hidden station problem in wireless networks can normally be solved by the *multiple access with collision avoidance* (MACA) protocol. For broadcast transmissions the signaling with *request to send* (RTS) and *clear to send* (CTS) packets cannot be used: there is no single CTS receiver to reply but a group of nodes and the CTS receiver does not know if all neighbors received the RTS. An additional related issue is the *ACK implosion problem*[9]. In a reliable one-to-many communication every destination would have to answer with an ACK packet to signal the successful reception of the corresponding packet. This may lead

[5] The required routing information is usually the next hop towards the destination.

[6] While flooding is generally undirected, the term opposite shall only highlight that the original source of the request is now the destination of the reply. Yet flooding is also not completely direction-less as the copies of the packet will (mostly) only increase the distance from the source due to the duplicate detection.

[7] The interference range is larger than the communication range. Therefore a station cab detect the medium as free by applying a *clear channel assessment* (CCA) but the transmitted packet might not be successfully received due to an decreased signal-to-noise ratio.

[8] For example to reduce the overhead that would be introduced by a HELLO protocol or the neighbor might not be known reliably because the network is mobile.

[9] While the ACK implosion problem is usually discussed as a problem in multicast protocols with feedback [15], the same general problem applies in this context.

to problems on the receiving side because of the potentially large number of ACKs that are transmitted: each acknowledgement is a single packet sent with a data rate from the `BSSBasicRateSet` taking up resources[10]. The optimization of flooding as a core networking service is therefore an important task for the optimal operation of computer networks. Without a sophisticated approach a high fraction of the resources is wasted and the overall performance of the network will be sub-optimal.

Many reactive routing protocols cache routing information and intermediate nodes answer route requests with a route reply in place of the destination[11] to reduce the overhead and delay of flooding. The analytical study by Westphal et al. [16] showed that the probability of such a *route hit* is fairly low (23%) in the considered scenario. Caching can therefore not fully resolve the problem to optimize flooding in wireless networks. In addition, in most protocols routing table or cache entries have a particular lifetime that is usually configured with a specific default value. When this default value is too high or the network topology is very dynamic, outdated information could be communicated if an intermediate node answers the request. The result would be a successful route discovery but an unusable route and eventually a new route request has to be run. If this process repeats multiple times, communication can be hindered in a serious way. The optimization of timeout parameters is another often overlooked [12] critical issue for the performance of wireless multi-hop networks.

1.3 Optimal and Approximated Solutions - An Algorithmic View

Algorithmically, the problem to minimize the number of broadcasted packets has been most notably researched in the domain of graph theory. Regardless what improved scheme s is applied, it can be assumed that it will perform[13] better than *simple flooding* but worse than using a *minimum connected dominating set* (MCDS).

$$\text{performance(flooding)} \leq \text{performance(s)} \leq \text{performance(MCDS)} \tag{1.1}$$

The MCDS is a minimal subset of nodes that connects all other nodes, i.e.:

- The MCDS is a subgraph.
- Nodes in the MCDS are (directly) connected with each other; they are called *dominators*.
- Every non-MCDS node is connected by an edge with a MCDS node; they are called *dominatees*.
- The network partitions when any MCDS node is removed. The cardinality of MCDS is minimal.
- Multiple MCDS can exist for a graph.
- The *connected domination number* is the minimum number of nodes in a connected dominating set [17].

Related problems are the *minimum dominating set* problem where the particular nodes do not have to be connected and the *traveling tourist problem* [18] where a minimal tour shall be found so that each landmark is visited (the node of the landmark is traversed or any neighbored node). The MCDS is also a Steiner tree where all nodes are terminal [19]. Steiner trees are often constructed as multicast trees where the terminals are the multicasts receivers and the tree is rooted at the multicast source. Although a very similar approach, the *minimum spanning tree* (MST) problem does not directly take the broadcast property of wireless communication into account. Thus using the unmodified MST protocol, more packet will be transmitted (as unicast) compared to the MCDS.

The simple definition of the MCDS does not consider directed or weighted edges and is based on a simple graph model. It has to be extended to match the properties of a wireless network to get a MCDS that can actually be used for communication. For example, a MCDS that includes links with very low quality satisfies the constrains but will not be practical in real world applications as retransmissions will negate the improved flooding. The introduction of weighted and directed edges does not make the problem to minimize the *connected dominating set* (CDS) easier to solve.

The MCDS has to be determined in a centralized way with global information, i.e., the graph respectively the network topology has to be known. The problem to determine the MCDS is NP-complete [20]

[10] Most notably, the time on the medium is referred but also the resources of the receiver

[11] A flag in the reply often marks if the destination or any other node generated the packet.

[12] The RFCs for the MANET routing protocols only specify static values.

[13] Performance is left as an abstract set of metrics that are discussed in the next section in the context of gossip routing.

802.11	Frequency	Data Rate [Mbps]	Mandatory Rate	PHY	Modulation and Spreading
original	315-353 THz	1	×	IR	16-PPM
	315-353 THz	2	×	IR	4-PPM
	2.4 GHz	1	×	FHSS	2GFSK
	2.4 GHz	2	×	FHSS	4GFSK
	2.4 GHz	1	×	DSSS	DBPSK + 11-Chip Barker Code
	2.4 GHz	2	×	DSSS	DQPSK + 11-Chip Barker Code
a	5 GHz	6	×	OFDM	BPSK
		9		OFDM	BPSK
		12	×	OFDM	QPSK
		18		OFDM	QPSK
		24	×	OFDM	16-QAM
		36		OFDM	16-QAM
		48		OFDM	64-QAM
		54		OFDM	64-QAM
b	2.4 GHz	1 & 2	×	HR/DSSS	see 802.11 original DSSS
		5.5	×	HR/DSSS	DQPSK + 8-Chip CCK
		11	×	HR/DSSS	DQPSK + 8-Chip CCK
		5.5		HR/DSSS	PBCC (BCC + BPSK)•
		11		HR/DSSS	PBCC (BCC + QPSK)•
g	2.4 GHz	1, 2, 5.5, 11	×	ERP-DSSS/CCK	see 802.11 b
		6, 12, 24	×	ERP-OFDM	OFDM
		9, 18, 36, 48, 54		ERP-OFDM	OFDM
		22, 33		ERP-PBCC	PBCC (BCC + 8-PSK)•
		6, 9, 12, 18, 24, 36, 48, 54		DSSS-OFDM	DSSS-OFDM•

Table 1.1: Overview of the IEEE 802.11 data rates and physical layers. The • symbol marks optional modes. Please not that the OFDM PHY can also provide half- and quarter-clocked operation in some regulatory areas.

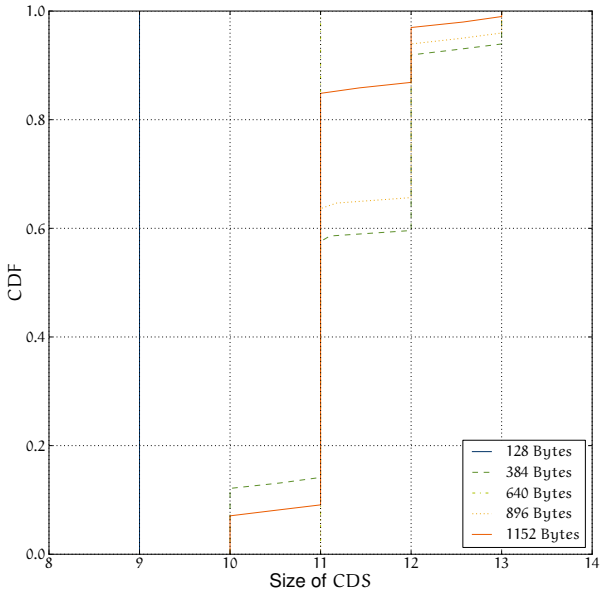


Figure 1.1: MCDS approximation for the DES-Testbed. The Berman algorithm was run 100 times on the network graphs, that were generated by probing with different sized HELLO packets. Because the second phase of the algorithm connects pieces of black nodes randomly, the CDS can differ in size.

but there are several approximation algorithms. The algorithm that has been presented by Guha and Khuller and was modified by Berman [21] provides an approximation ratio of $\ln(\Delta) + 3$ where Δ is the maximum node degree of the graph. The algorithm is shown in Algorithm 1. In the first phase, nodes are colored black to reduce the number of pieces where a piece is either a white node or a CDS of black nodes. Then in the second phase, the black CDS are connected. The algorithm is only applicable for a connected, unweighted, and undirected graph. As an example, we run the Berman algorithm on the network topology graph of the DES-Testbed; the results are shown in Figure 1.1. The MCDS has a size of 9, i.e., the 9 nodes in the CDS have to forward all flooded packets to reach all nodes in the network. Thus there is a lower limit of 10 transmissions as the source does not have to be included in the MCDS. When the packet size is larger, some links are not available anymore and thus the MCDS size increases. Of course, the CDS will not be usable in real world applications for flooding because of the simple graph model.

If the graph is weighted[14], an approximation ratio of $(c_n + 1)\ln(n)$ can be achieved, where $c_n \ln(k)$ refers to the approximation factor of the corresponding Steiner tree problem with k terminals. The algorithm shown in Algorithm 2 starts to create a *set cover* based on a greedy algorithm [22] and then connects the selected nodes by a weighted Steiner tree to obtain a CDS. The ratio of the node weight and the number of elements that are added to the set cover are the metric to select nodes in the first phase. A more detailed description of the metric is not provided by the authors.

An alternative algorithm called S-MIS [23] by Li et al. starts with a *maximal independent set* (MIS) and then creates a Steiner tree to connect the selected nodes. The MIS has the following properties:

- The nodes in the MIS are not adjacent, i.e., no edge connects any two nodes.
- The dependent set is maximized, i.e., no more nodes can be added to the MIS.

The algorithm achieves an approximation ratio of $4.8 + \ln(5)$ in unit-disc graphs. Each MIS is also a *dominating set* (DS).

When the graph contains unidirectional edges like the links in wireless networks, we require a *strongly connected dominating set* (SCDS) [24] as backbone for the flooding. In a strongly connected set, each router can reach any other router over a finite number of hops. Due to this property, a single[15] CDS can be used to flood packets from any source while in the *weakly connected* case, a dedicated CDS might be required for any source in the worst case. Du et al. propose two approximation algorithms called

[14] Guha and Khuller consider a node weighted graph but it can be transformed into an edge weighted graph.

[15] Remark: This statement is only true when each leaf node is connected by a bidirectional edge with any SCDS node. Du et al. in fact consider only bidirectionality for the CDS nodes.

Algorithm 1 MCDS approximation with the Berman algorithm

Require: unweighted graph G, all nodes colored white
  while white nodes in G **do**
    select the white node n that will decrease the number of pieces the most
    color n black
    color all neighbors of n gray that are white
  end while
  while more than one black component in G **do**
    connect two black components by coloring gray nodes black
  end while

Algorithm 2 MCDS approximation for a node weighted graph

Require: weighted graph G
  each node in G and its corresponding neighbors are a set s in the universe U
  empty set cover $C \subseteq U$
  while the universe U is not covered **do**
    Add s to C where s has the best ratio of the weight and number of added elements to C
  end while
  for all $n \in C$ **do**
    set weight of n to zero
  end for
  Connect all $n \in C$ by a node weighted Steiner tree using an approximation algorithm

Connected Dominating Set using Breadth First Search tree (CDS-BFS) and *Connected Dominating Set using Minimum Nodes Steiner tree* (CDS-MNS) for strongly connected, directed disk graphs. CDS-BFS starts to find a dominating set by the greedy algorithm shown in Algorithm 3 that gives nodes with large transmission ranges a high priority. Subsequently, a breath first search is applied to create two trees that connect all nodes in the DS. Both the forward tree and backwards tree are rooted at the node that has the largest transmission range. The union of all nodes in both trees is a SCDS. The algorithm achieves an approximation factor of $O(1)$ if there is a maximum and minimum transmission range for all nodes, i.e., the transmission ranges are bounded. CDS-MNS achieves a factor in the same complexity class but absolutely produces a smaller SCDS.

We conclude from our brief overview of the optimization problem and the proposed approximation algorithms, that there are several potential solutions. Nevertheless, the properties of the network respectively the graph determine how optimal an approximated solution can be. The following properties have to be considered:

- Directed or undirected graph
- Weighted or unweighted graph
- Centralized or decentralized algorithm

Du et al. differentiate the class of decentralized algorithms further into distributed and localized algorithms. In the former class, the decisions are decentralized, while in the latter class they also require only a constant number of rounds. Especially the weights of the edges or nodes warrant a more detailed discussion. We will refer again to the issues discussed in this section, in our review of the gossip routing protocol simulations in Chapter 5.

1.4 Gossip Routing

As we have introduced, flooding is an important service in many routing protocols especially for wireless multi-hop networks. Its optimization has been in the focus of research especially since the advent of MANETs and WSNs. The most simple and common approach to limit the number of flooded packets is to use a *time-to-live* (TTL) or *hop-limit* (HL) field in the packet header. Each router that receives the packet decreases the value until it reaches zero and the packet is eventually dropped. This ensures that looping packets are removed from the network but routers may receive and forward the same packet multiple times as duplicate detection has to be provided in addition. The initial value of the TTL/HL

Algorithm 3 Greedy dominating set approximation for directed graphs

Require: directed disk graph $G = (V, E)$
  empty dominating set S
  while edges left in V **do**
    add node n with largest transmission range to S
    add each neighbor m of n to S that can be reached from n: $(n, m) \in V$
    remove all (n, m) from V
  end while

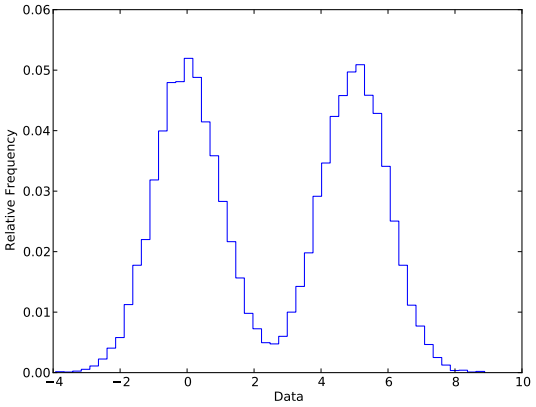


Figure 1.2: Histogram of a bimodal distribution created by two normal distributions with $\mu_1 = 0$, $\mu_2 = 5$, and $\sigma = 1$ based on 10.000 samples each.

also has to be considered and configured adequately. If it is too high, packets will loop unnecessarily and if it is too low, not all nodes in the network have a chance to receive the packet requiring to resend it with a higher value. An unique *sequence number* or packet *id* enables to accurately detect and drop looping packets which significantly reduces the redundancy. Nevertheless, routers may still receive several duplicates due to the broadcast property of the medium and therefore time and bandwidth for faster unicast data flows is still wasted. Sometimes both approaches are used together, for example to enable duplicate detection based on the sequence number and to limit the distance a packet may travel from the source.

Gossip routing is an approach to minimize the redundancy of flooding while still retaining full reachability. In contrast to flooding, where packets are always forwarded as long as the TTL/HL does not reach zero, the approach is probabilistic. Each node forwards packets with a given probability p or drops them with probability $1 - p$. This simple gossip routing variant where p has a fixed/static value is sometimes referred to as *pure gossip* [25], (a) *simple probabilistic scheme* [26,27], *blind gossiping*, or *fixed probability gossip*. Alternatively, the forwarding probability can be dependent on other information, e.g., the node degree, the number of received duplicates, or global topological information. More advanced gossip routing variants can introduce multiple chances to forward packets: when the packet is not forwarded at first, it can be sent nevertheless when a particular condition applies, e.g., few duplicates are received from the node's neighbors. As an added benefit, the probabilistic approach of gossip routing is little interfered by topology changes and thus especially suited for mobile networks [26].

Gossip routing is also considered to belong to the class of *rumor mongering* protocols [28, 29] that have an upper limit for the number of sent packets, i.e., the forwarding of a specific packet terminates after finite time. In this class of protocols, reliability can be traded off with the number of packets that are sent. So called *anti-entropy* protocols [28] are the opposite as they sent an unlimited number of messages[16] but ensure high reachability, reliability, and/or a consensus even in scenarios with high failure rates.

Percolation theory [30, 31] is often referred to as the foundation or inspiration of gossip routing in computer networks. Several of the findings from percolation theory are assumed to hold also in (common)

[16] For example, the database replication protocol in [28] sends packets periodically independent of the state and thus does not terminate. Of course, when a routing protocol applies gossip routing to periodically spread topology information, this behavior also resembles the anti-entropy approach.

wireless networks. A particular theorem says and its proof shows that there is a particular forwarding probability p_c. For $p \geq p_c$ all/most nodes will receive the packets that are sent by a source and for $p < p_c$ only a limited subset will receive them. The network as a system can be characterized as *bimodal* and there are only two specific outcomes. An example for a bimodal distribution is depicted in Figure 1.2 that is created by two normal distributions. At $p = p_c$ the system radically changes its behavior. It was shown in [32, 33] that the so-called *"phase-transition-phenomenon"* could be observed in simulations of random and regular graphs. We discuss percolation theory and its applicability in the domain of wireless multi-hop networks in Section 2.1.

There are several overall goals a good gossip routing protocol should achieve besides the redundancy reduction [34]. The forwarding decision should be based only on local information to reduce the overhead. The gossip algorithm should perform $\leq O(d_i \times \text{poly}(\log(n)))$ computations at each node per time unit where d_i is the degree of node i and n is the number of nodes in the network, i.e., it is bounded by the node degree[17]. The memory consumption should be low and in $O(\text{poly}(\log(n)) + |F_i|)$ where $|F_i|$ is the space required by node i. Synchronization between nodes should not be required, i.e., the forwarding decision is made independently by each node at any particular time.

Further on, gossip protocols show *scalability*, *adaptability*, and *graceful degradation* [29]. The number of nodes in the particular network does not influence the overall performance of the protocol (scalability), i.e., it performs equally well in all topologies. Adaptability is ensured as nodes can be added or removed at random times without requiring a restart of the protocol. Depending on the particular gossip protocol, a particular number of failures (failing nodes or links) will not lead to a rapid drop in performance or render the protocol totally dysfunctional. As there is no hard upper limit of failures that can be sustained, (some) gossip protocols may show graceful degradation and not a sudden drop in performance.

1.4.1 Optimization Problems

In general, gossip routing protocols are often developed and specified with a particular topology in mind. This topology is modeled as a graph $G(E, V)$, where E is a set of edges that are (virtual) links in real networks and V is a set of nodes. Graph models can be differentiated in two major classes: regular and random. While all nodes[18] in the former class have uniform properties, e.g., uniform node degree, the node properties in the latter class are (more) diverse. Random graphs [35] are closer to the topologies of real multi-hop network deployments and are therefore primarily used for the evaluation of gossip routing. They are created by a random process. For example, n nodes are *independent and identically distributed* (iid) in a square, rectangular, or disk area and all pairs of nodes are connected with an edge if their euclidean distance d is below a particular threshold distance d_{max} that represents the radio range:

$$e_{a,b} \in E \Leftrightarrow d(v_a, v_b) \leq d_{max} \wedge v_a, v_b \in V \tag{1.2}$$

Random geometric graphs and *unit disc graphs*[19] are representatives of random graphs. In these two simple models, the edges are also often undirected and unweighted, respectively, the weight is equal for all edges. In contrast, *random euclidean graphs* [36] always have weighted edges, where the weight is determined by the euclidean distance of all two node pairs. *Random proximity graphs* are a special case where each node is connected with its k nearest neighbors.

Besides the optimization and specification of gossip routing protocols, the graph model can also be used for simulations and to define particular performance metrics. The already introduced reachability and redundancy as well as the number of transmitted packets are common metrics. Considering graph G, the reachability metric R that shall be maximized, can be defined as a function as follows:

$$\underset{s \in V}{\text{maximize}} \; R(s); \qquad R(s) = \frac{N_\rho^s}{\|V\|} \tag{1.3}$$

$$R(s) \rightarrow [0, 1] \tag{1.4}$$

where $N_\rho^s \subseteq V$ is the number of nodes that received the packet from source node s and $\|V\|$ represents the cardinality of the node set. The optimization of the reachability is most important because further, more specific problems depend on it. All nodes shall receive the packets sent by the source to improve the reliability and overall performance, e.g., of a route discovery.

[17] The $\log(n)$ is not further discussed by the author but most probably originates from the assumed network model.

[18] We assume an infinite regular graph. In finite regular graphs that are, e.g., neither a torus nor a hypercube, border nodes often differ from non-border nodes in particular properties.

[19] When d_{max} is half as large in a unit disc graph compared to a random geometric graph, the models are mostly equivalent.

The next optimization problem is particularly important for routing protocols that apply gossiping or flooding.

$$W(u_0, u_k) \quad : \quad u_0 \rightarrow u_1 \rightarrow \ldots \rightarrow u_k \tag{1.5}$$

$$\underset{u_0, u_k \in V}{\text{maximize}} \; D(u_0, u_k); \qquad D(u_0, u_k) \quad = \quad \|W_{u_0, u_k}\|, \; \forall u_0, u_k \in V, \; u_0 \neq u_k \tag{1.6}$$

$$D(u_0, u_k) \quad \rightarrow \quad [0, \|V\| - 2] \tag{1.7}$$

W is a walk, i.e., a path or route from node u_0 to u_k over $k-1 \in \mathbb{N}$ intermediate nodes and W_{u_0,u_k} is a set of walks from u_0 to u_k . Therefore, not only shall all nodes be reached, but the number of (disjoint) paths shall be maximized so that the routing protocol can select the best route based on a particular routing/path metric. The cardinality of the set of walks is called *diversity* D in this survey. For node disjoint paths[20] the number is bounded by $\|V\| - 2$ because every node but the source and destination can only appear once on each path; the diversity can also be 0 if the graph is not (strongly) connected. For a real application in route discovery it should be considered that a packet has to reach its destination but another packet also has to travel back in the opposite direction (either as a broadcast or a unicast) so that communication is possible in both directions[21]. As this procedure is highly protocol specific, we leave the formulation of the diversity optimization problem for specific routing protocols open.

The redundancy optimization problem C is defined as follows:

$$\underset{u_0, u_i \in V}{\text{minimize}} \; C(u_0, u_i); \qquad C(u_0, u_i) \quad = \quad \|RX_{u_i}(s_{u_0,\, seq})\|, \; \forall u_i \in V, \; 0 < i < k \tag{1.8}$$

$$C(u_0, u_i) \quad \rightarrow \quad [1, d(u_i)] \tag{1.9}$$

where u_i is an intermediate node that is $k - i$ hops away from u_k, the destination[22]. RX is a set of copies of the packet with sequence number seq that was sent by the source u_0 and were received by u_i. C is (upper) bounded by the node degree $d(u)$, i.e., there are at most $d(u) - 1$ duplicates of a received packet. As you might notice, the redundancy shall not be minimized for the destination node. This relaxed constraint is important to achieve the aspired high diversity.

As last, the optimization problem for the delay shall be defined as follows:

$$\underset{u_0, u_k \in V}{\text{minimize}} \; T(u_0, u_k); \qquad T(u_0, u_k) \quad = \quad t_{u_k} - t_{u_0}, \; t_{u_k} > t_{u_0} \tag{1.10}$$

$$T(u_0, u_k) \quad \rightarrow \quad (0, \infty] \tag{1.11}$$

where t_{u_k} represents the time of arrival of the first copy of a packet at u_k that was sent by u_0 at t_{u_0}. For a real world application in routing protocols, the delay in the opposite direction has also to be considered, as the *round trip time* (RTT) is relevant for the whole route discovery and especially the configuration of particular timeout values at higher layers.

Unfortunately, several of these optimization problems respectively the corresponding metrics are orthogonal. The interdependency of the metrics is depicted in Figure 1.3. Not all of them can be optimal at the same time. As we discuss in Chapter 4 there are specific gossip routing schemes that focus on particular subsets of these metrics.

1.5 Focus and Constraints of this Survey

In this survey we elaborate a selection of gossip routing protocols/variants that have been proposed in the last years for application in wireless multi-hop networks. Further on, gossiping is discussed as an approach that is applied in other protocols besides for routing. We also discuss related fields of research where improvements for flooding have been proposed. As we will see, the fundamental ideas of all these protocols are very similar, if not equal: ensure that a (broadcast) packet arrives at a destination and/or minimize the number of packets that are sent.

[20] Routing protocols with a hop count metric and duplicate detection based on sequence numbers will most often create only node disjoint paths in the route discovery phase. The number of link/edge disjoint paths can be determined as an application of the maximum flow problem.

[21] While there are source-sink oriented protocols especially in WSNs that only require unidirectional communication, bidirectionality should nevertheless be provided on a link level so that the reception of frames can be acknowledged.

[22] The redundancy optimization problem is here defined for a directed gossiping, i.e., there is a specific destination. The problem is also relevant for the undirected case with a slightly modified formula.

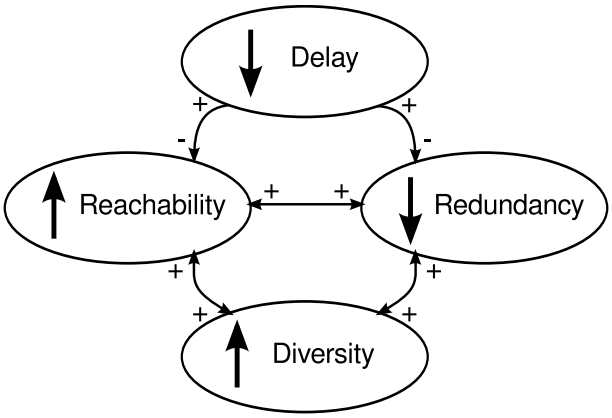


Figure 1.3: Metrics for the evaluation of the gossip routing protocols. Two of them shall be minimized and the other two maximized as represented by the arrows left of the names, e.g., up arrows represent an aspired maximization. The arrows between the metrics represent how a particular metric affects the other, for example: a high delay can effect a reduction of the redundancy.

We focus on the differences and similarities of the gossip routing and the related approaches. The applicability to real world problems is critically discussed and the simulation scenarios are reviewed based on this benchmark[23]. This includes the *a priori* selection of particular parameters or the dynamic and maybe collaborative computation of specific values that are required for the algorithm. In this context, we will highlight issues when information is required that is either not available for the particular entity or when it has to be determined in a way that introduces an additional high cost, i.e., it requires significant network resources. The *management overhead* of protocols is a prime example.

The survey is foremost focused on gossip routing in wireless mesh networks that use IEEE 802.11 based network interface cards which is our central domain of research [37,38]. Although most of the discussed approaches are applicable for many types of networks, the IEEE 802.11 standard and the network model introduce several constraints that have to be considered for real world use and for an optimization of a protocol. The criteria are as follows:

- Mobility is limited or not existent as the core mesh backbone is stationary; only the clients of the mesh network can be mobile. This differentiates the considered network model from MANETs where all nodes are mobile[24].
- The nodes can be deployed in an indoor environment which reduces the radio range and might effect asymmetric and unidirectional links. Even outdoor nodes exhibit effects like attenuation, multi-path propagation, and scattering. The so-called *free space* model (see Section 5.3) cannot be assumed, which was also observed in [39] for the DES-Testbed.
- The *medium access control* (MAC) sublayer and physical layer (PHY) cannot be modified as they are standardized by the IEEE. Non-802.11 technologies, e.g., in WSNs apply a similar broadcast scheme with carrier sense and exponential binary back-off.
- Energy efficiency is not a primary concern as all WMN backbone routers are connected to a power socket; mobile nodes have sufficient battery capacity and are recharged daily. This is a clear difference to WSNs where nodes often have to operate for extended periods without recharging or will fail if the energy is depleted. Packet loss due to link failures, bit errors or interference are much more likely than failing modes.
- The nodes are not position-aware as GPS is not available due to the (potential) indoor deployment, high cost, or other reasons.

Despite the focus, we also discuss several protocols where, e.g., location information is required or the energy consumption shall be minimized. Overall, gossip routing is considered for networks that are

[23] We argue that improvements that are achieved and evaluated in non-realistic scenarios have limited significance for subsequent real world applications.

[24] We acknowledge that a particular subset of nodes in real world MANETs will remain stationary for longer times and that the degree of mobility will overall differ from node to node and time to time. Nevertheless, MANETs exhibit a significant higher rate of mobility than WSNs and WMNs.

available in the real world or can be deployed with available equipment. No changes to the hardware design are necessary and the required modifications to the software components, including the operating system, are technically feasible. The gossiping is often a component of another protocol that we will only briefly introduce or refer to the corresponding publications.

1.6 Structure

The remainder of this paper is structured as follows. A selection of network types and classes and corresponding models are discussed in Chapter 2. Subsequently in Chapter 3, research fields and protocols that are related to gossip routing are introduced and their differences elaborated. In Chapter 4, the gossip routing protocols that are the focus of this survey are discussed. We evaluate the scenarios of the simulation based studies in Chapter 5. Chapter 6 reviews the required information of the protocols, presents a classification, and highlights core schemes. The paper ends with a summary, outlook, and conclusion in Chapter 7.

CHAPTER 2

Network Types and Models

The common graph models were already briefly introduced in Section 1.4. In this chapter, we give an overview of other network types and models that are often referred to either as related or even as basis of the gossiping principle as depicted in Figure 2.1. The applicability of these types and models to the real world problems of gossip routing is discussed and differences are highlighted. In particular, percolation theory is introduced, delay tolerant networks are discussed, and epidemiological networks are elaborated.

2.1 Percolation

First of all, we start with a brief overview of percolation theory. Subsequently, three percolation models are introduced that are commonly referenced in literature. We then discuss the application of these models for real world networks.

2.1.1 Introduction to Percolation Theory

Percolation theory is a research field in the domain of spatial random processes [31] that is applied in electro engineering [40], physics [41, 42], biology [43], and many other fields. In the considered systems the randomness is a property of the geometry of the particular system. Common examples are the spreading of diseases in a population that is distributed over a specific area (see also Section 2.2) or the forming of wet areas (pools of water) when rain falls. The term "percolation" comes from another very descriptive example. Consider a layer of some porous material, e.g., styrofoam or pumice stone. How likely is it that some fluid can percolate through the layer when there are cavities distributed by some random process? General problem statements in this research domain are:

- How likely is it that a disease spreads to the whole population?
- What is the largest pool of water that will be formed?
- Is there a path of length l on the porous material?

A system is said to percolate at a specific probability p_c (critical point) when a phase transition can be observed. In the example with the porous material, where the probability p determines if there is a cavity at each position, for $p \geq p_c$ (supercritical) there will be a path from the top to the bottom and otherwise there is none (subcritical). Another simple example is the melting/freezing point of water at $p_c = 0°C$. The percolation probability $\Theta(p)$ is shown as function of the (forwarding) probability p in Figure 2.2. In the subcritical phase there is a very limited chance that the system percolates while in the supercritical phase the probability is nearly 100%. The system is classified as bimodal as there are only two outcomes. Depending on the particular system/network model, the phase transition can show different shapes [44] and can happen either rapidly or take a (very) limited time[1]. Often times the system is infinite [45] as this makes the mathematical analysis much more simple, e.g., border effects can be ignored. Further on, the system can be either discrete or continuous [46]. Discrete systems are easier to formulate and to analyze but lose properties of the problem domain when the problem is in continuous space. While

[1] The phase transition may happen during a particular interval $[p_{c_{low}}, p_{c_{max}}]$ but when this interval gets too large we cannot call it a phase transition anymore. In percolation theoretical problems the transition is usually a rapid process.

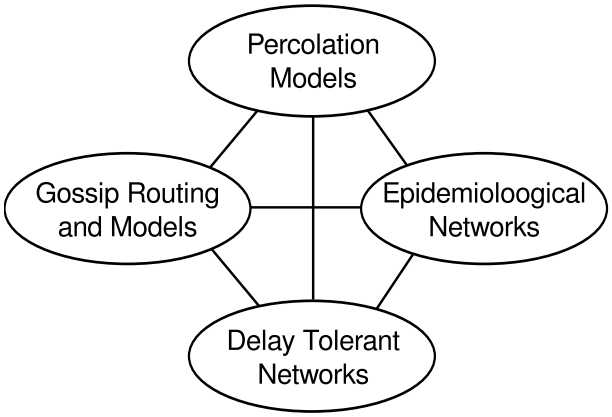


Figure 2.1: Network types and models that are related to gossip routing

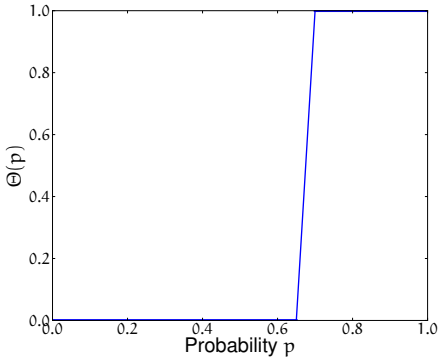


Figure 2.2: Percolation probability as function of the probability p. $p_c = 0.65$ is the critical value when the system changes its behavior, e.g., an infinite cluster forms or, in the context of wireless networks, most of the routers receive the packets.

classical percolation models are static, they can also be dynamic and move according to some stochastic process [47].

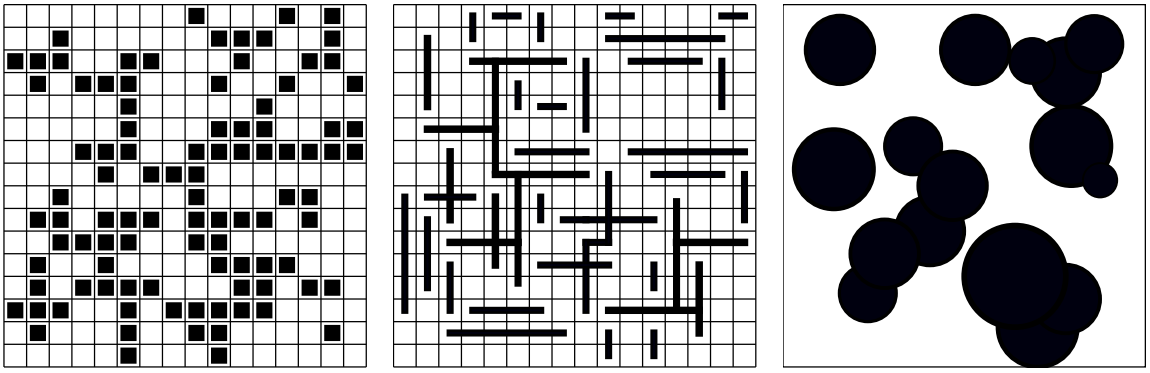
The problems and mathematical models of percolation theory are related to the research domain of *random graphs* [35]. These graphs are created using some random graph model, e.g., *uniform random graph*, *binomial random graph*, or *random graph process*. For example in the Erdõs–Rényi random graph model, edges are inserted independent from each other with probability p. A common problem for this model is to determine $p \geq p_c$ so that all n vertices are connected with each other with high chance.

2.1.2 Percolation Models

In the *site percolation* model the squares (sites) in a square lattice are either occupied with probability p or empty with probability $1 - p$. The outcome whether a square is occupied or empty is totally independent of the state of its neighbor squares. All occupied squares next to each other are connected and form a cluster. An example is shown in Figure 2.3a. With increasing value of p more squares are occupied and larger clusters are formed. When a square in between four other occupied squares becomes occupied, all of the five squares are connected; there is no individual chance. The site percolation model is a good representative of the porous material in the above example.

The *bond percolation* model considers the sides of the squares in a square lattice. With probability p a side is open and with probability $1 - p$ it is closed. An example is shown in Figure 2.3b. Neighboring squares with open sides form cluster. In contrast to the *site percolation* model, a square can be connected with all or only a subset of its neighbors.

The third model [31,47] uses a Poisson point process where points are distributed over a d dimensional area. Around each point a disc is constructed with a random radius. The radii are independent and identically-distributed. Overlapping discs form a connected cluster. An example is depicted in Figure 2.3c.



(a) Site Percolation. Horizontally or vertically neighbored occupied squares are connected with each other.

(b) Bond Percolation. The edges connect neighbored squares which are considered open at this side.

(c) Boolean Percolation with independent and identically-distributed radii.

Figure 2.3: Percolation Models

Lattice Type	Node Degree	Site Percolation	Bond Percolation
Honeycomb	6	0.6962	0.65271
Square	4	0.592746	0.5
Triangular	3	0.5	0.34729
Diamond	4	0.43	0.388
Simple Cubic	6	0.3116	0.2488
Body-centered Cubic		0.246	0.1803
Face-centered Cubic		0.198	0.119
Hypercubic (4d)		0.197	0.1601
Hypercubic (5d)		0.141	0.1182
Hypercubic (6d)		0.107	0.0942
Hypercubic (7d)		0.089	0.0787

Table 2.1: Critical values for the size and bond percolation models. Based on: [49].

While the positions of the points and the radii are often continuous, a discrete variant of the model can also be defined. In this case the points are distributed on a lattice and the radii are randomly selected from a discrete distribution.

The square (2-dimensional) lattice in the examples can be replaced with many other finite or infinite structures:

- Lattices with higher dimensions
- (Honey-) Combs
- Hypercubes

The critical value p_c is dependent on the lattice type and the percolation model. A selection of values is shown in Table 2.1. We have to note that only for some of these combinations, analytical results are available while for the others, the particular p_c is based on empirical studies, i.e., simulations. Overall it is known that networks of higher dimensions have lower critical values and that p_c for the site percolation model is, in all but one known case, at least as high as for the corresponding bond problem[2].

Besides these traditional percolation models, percolation has also been studied in other random graphs. Callaway et al. [50] remark that several studies showed that real world networks, e.g., links on websites [51] or the topology of the Internet [52] show no Poisson distribution of the node degree but often power-law or exponential distributions. They learned from numerical simulations of percolation that power-law graphs are resistant against single node failures, i.e., the graphs are well connected. Yet this only applies to the removal/failure of random nodes. When a particular fraction of nodes with high node degree is

[2]See [48] for a description of the special network model where the order of the critical values are reversed.

removed, the largest component in the graph will be destroyed. The graph models that are actually used in simulations of mobile networks will be discussed in Chapter 5.

2.1.3 Applicability for Wireless Networks and Differences

Although very often referenced and applied for gossip routing, (traditional) percolation models deviate in some aspects from wireless networks. Wireless networks are most often described as random graphs by the models that where introduced in Section 1.4.1. It might be tempting to simply align the nodes of the random graph on top of a square lattice model as described in the previous section but there are some important differences to consider.

1. The site and bond percolation models use d-dimensional graphs whereas wireless networks have varying node degree. As we elaborated, in the site model each occupied site is always connected with each occupied neighbor site. In the domain of wireless networks it would mean that there either is a link to all nodes within some specific communication range or there is no link at all. In the bond model the probability for each link is individual and independent from the others. This fits the "random nature" of wireless networks much better. Nevertheless, when the considered model is d-dimensional, there can only be $0 \ldots d$ links. Therefore there is an upper limit and the dimensionality has to be selected appropriately for specific network models.

2. Wireless networks are finite. Percolation theory most often considers infinite graphs although the theorems also hold for finite graphs. Nevertheless, border effects can only be ignored in infinite or very large graphs. This has obvious implications for the application of percolation theory in the domain of wireless networks.

3. The edges in the discussed percolation models are not lossy. In wireless networks there is a probability that packets are lost on the medium, e.g., due to interferences or collisions. Therefore even when there is a particular probability p_c for that the packets should reach most/all nodes, the required probability p will most probably have to satisfy $p >> p_c$ due to packet losses.

4. In the percolation models, multiple edges of the same node do not interfere with each other; they are considered independent. In wireless networks a node cannot send packets to two or more neighbors at the same time as unicast due to the shared medium and the common case with one transceiver. This difference is resolved if we assume that nodes have dedicated network interface cards and orthogonal channels for each link or if communication takes place as broadcast. The former is better modeled by the the *bond percolation* model and the latter by the *site percolation* model.

5. Although the previous difference can be resolved, percolation theory does not consider that edges interfere. In wireless networks the transceivers have a communication and (a larger) interference range. Therefore two nodes in a wireless network might interfere with each other even if there is no link between them.

6. In the site and bond percolation models, the edges are open with probability p. The probability that edge e_1 from node n is open/closed is independent from the probability that e_2 from the same node is open. In gossip routing the probability to forward packets is in the focus. A packet is either transmitted to all or none of its neighbors.

7. The edges in the models are bidirectional and symmetric. This assumption does not hold for wireless networks (see also discussion in Section 5.3).

8. The links in wireless networks have a particular quality. This quality can be described with a metric, e.g., *packet delivery ratio* (PDR). The PDR is dependent on the data rate, channel frequency, mechanisms like RTS/CTS, or packet size[3] and usually changes over time due to multiple external factors. In the discussed models there either is an edge or not based on an a priori random process.

9. As the properties of a wireless network are time-variant, the critical probability p_c required to reach all nodes in the network will change. For the gossip routing an upper bound for p_c is required, i.e., the minimum forwarding probability for that all nodes are reached at every time from every source.

[3] The frame length as it is normally called in this context.

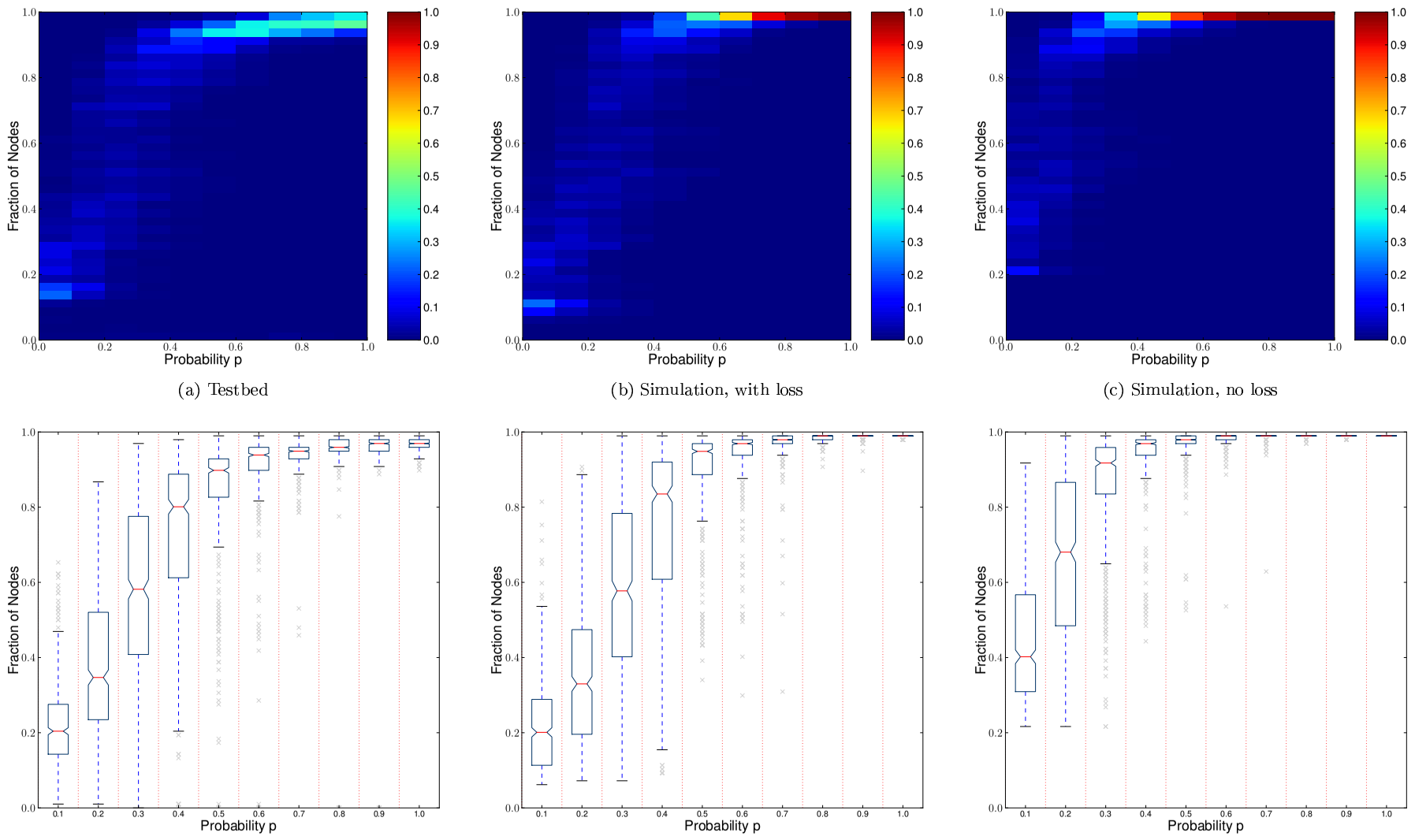
10. The value of p_c is also dependent on the source node's position in the wireless network. While some value p_c might satisfy to reach all nodes from source A, this configuration might not enable to reach all nodes from source B because $p_{c_B} > p_{c_A}$. This particular issue is not in the focus of percolation theory as the nodes are often anonymous.

11. Continuous percolation models fit the non-discrete deployment and radio ranges of nodes in wireless networks much better than the discrete models.

12. The boolean percolation model is the closest to the random graph model. The Poisson point process is applied for the random deployment of the nodes while the random radii represent the random link ranges. Nevertheless, several of the issues we discuss for the simulation scenarios in Chapter 5 also apply for this percolation model, especially the loss-free free space propagation like links, if the model is not extended appropriately.

Some of the listed problems can be solved when lattices of higher degree are used to model particular properties of wireless networks. In this case the random process that populates the sites has to be defined in a sophisticated way. There are of course further percolation models that might be better applicable. For example, (Gaussian) *random fields* have also been used to study percolation [42, 53]. Finding a percolation model (and parametrization) that fits a common wireless network model is a non trivial task. To highlight the effect of a too high abstraction, we ran a gossip routing experiment in the DES-Testbed and then the same experiment in a graph based simulation (with and without lossy links). As depicted in Figure 2.4, the loss-free simulation shows a higher reachability than the one with lossy links. Although the topology and the source were the same, the results from the testbed are worse than the simulation with lossy links: the variance is higher and the median is lower. In all three scenarios we observe a phase transition but p_c is different for each. Most notably, it is the lowest in the loss-free simulation that is the closest to the percolation models.

Despite these issues, percolation theory can be applied to research gossip routing in wireless networks. Percolation theory should at least give a lower bound of the probability p_c that is required to reach all nodes in the network from all source nodes.



(a) Testbed (b) Simulation, with loss (c) Simulation, no loss

(d) Testbed (e) Simulation, with loss (f) Simulation, no loss

Figure 2.4: Fraction of nodes that receive the packets with gossip0 from the source. The pseudo-color plot show the fraction of execution where a particular fraction of nodes was reached and the box plots show the median with 95% confidence interval.

2.2 Epidemiological Models

The spread of diseases is often researched based on two well known models [54]. In the *Susceptible-Infected-Recovered* (SIR) model by Kermack and McKendrick [55], the individuals are either not infected (susceptible), infected, or have recovered from the infection and can not be infected anymore. In contrast, in the *Susceptible-Infected-Susceptible* (SIS) model [56], recovered individuals do not develop immunity and can be infected again. The most important parameters of the model are the recovery rate γ and the infection rate β. In both models, the state of the population N at time t is thus described by

$$N(t) = S(t) + I(t) + R(t) \tag{2.1}$$

where $R(t)$ is zero in the SIS model. It is also assumed that each individual has the same chance of infection and recovery; thus the mean infective period is $\frac{1}{\gamma}$. Both models can be extended to include death and birth rates for the individuals. New states for exposed (infected but not infectious) or carriers (infectious but not sick) can be included.

Fundamental problems in the domain of epidemiological research are

- How many individuals will contract a disease or recover from it per time unit?
- Will the number of infected increase or decrease in $t + 1$?
- How many initial infected individuals are required so that the whole population will be infected (pandemic)?
- How many people have to be immune, either by contracting the disease and recovering or by vaccination, to prevent a pandemic?
- How do non-constant populations due to birth, death, or migration effect the spreading?
- Is there a (stable) equilibrium of infected and disease-free individuals?

The findings and models of this research domain are applicable to some degree for flooding in computer networks: the routers are individuals and the disease is a particular information. The infection rate can describe a probability that a transmission fails or that a neighbor is not randomly selected to receive the information. Deaths can represent the failing of routers or the deletion of the information, e.g., due to a cache replacement algorithm. Births can represent newly deployed or restarted routers. The models are especially applicable for delay tolerant networks and data dissemination and replication protocols (see Section 3.1) where information is (slowly) spread and the nodes store data for some specific time ("they are infected") that is periodically forwarded or advertised. Flooding as a component of a routing protocol requires quasi instantaneous forwarding to all nodes and immediate feedback for up-to-date information about the reachability of other nodes. The properties of the wireless medium are also not well represented, although, weighted epidemiological networks have been proposed to model individual infection probabilities [54].

2.3 Delay Tolerant Networks

Delay tolerant networks (DTN) [57] exhibit a high mobility of the nodes, significant variation in the number and qualities of links and/or links over very large distances with high delays. The network provides no continuous or instantaneous connectivity but over time a communication between any pair of nodes is assumed to be possible. Therefore nodes often store received packets for some time until a route to (or next hop towards) the destination is available. Fall describes the following core challenges for DTNs in [57]:

- Path and link characteristics
  - Latency is high
  - Data rate is low
  - Frequent disconnections
  - Long queuing times
- Network architectures

  - Interoperability
  - Security
- End system characteristics
  - Limited longevity
  - Low duty cycle operation
  - Limited resources

Especially due to the long delays in DTNs, TCP and normal routing is hardly applicable and novel approaches are required for *delay and disruption-tolerant interoperable networking* [58]. Examples for DTNs are interstellar communication, connection of remote sites by satellites or couriers, city buses that act as a backbone network, or WSNs with long, asynchronous sleep schedules of the nodes.

Models of delay tolerant networks can be used to research epidemics, information spreading via gossiping in social networks, or *opportunistic networking* [59, 60] where network partitioning is assumed for some periods. Jain et al. model a DTN as a directed multi-graph [61] as multiple links may exists between pairs of nodes and to represent the time-dependency as links may exists only for a particular time and with different capacities. Routing is difficult in these networks as the traditional metric based approach cannot be applied. Both reactive and proactive protocols will fail if the source and destination are not in the same connected subgraph. Reliability is defined as the primary goal and redundancy is therefore tolerated and even proposed. Routing algorithms with *zero knowledge*, *partial knowledge*, and *complete knowledge* are discussed. The algorithms in the first group will make random decisions without any knowledge about the topology, e.g., the forwarding of packets to random neighbors so that a random walk is achieved (similar to *hot potato routing*). For algorithms in the second group some information is available like weights for the edges in the network graph. The particular values are provided by *"knowledge oracles"* for queue lengths, statistics about the contacts, or traffic demands; oracles replace the metrics that are used in traditional routing protocols. All of these oracles try to predict current and future states based on knowledge from the past. Routing with complete knowledge is realized by linear programming based on the oracles' predictions in a centralized way. The oracles and routing algorithm classes form a framework that allows a novel approach to networking.

How the oracles can learn the required information for their predictions and how accurate they are will be the most important factor for the performance of DTNs. If the information can be gathered at all and used in a (distributed) algorithm is up for discussion. In the simulation scenarios that are presented in [61], the movement patterns of the mobile nodes are known and they repeat periodically.

Like the discussed epidemiological models, DTNs consider networks with properties that differ significantly from the networks that are used for gossip routing. In these traditional wireless multi-hop networks, instantaneous route discovery and subsequent high data rate communication over an extended time[4] as well as access to other networks via gateways are the prime objectives.

2.4 Conclusion

As we have discussed, the introduced network types and models enable the research of problems that are related to flooding and gossip routing. Nevertheless, there are significant differences in the fundamental research topics and the models are not directly applicable to wireless multi-hop networks. Some important modifications and parameter settings are required which are non-trivial to realize.

[4] Remark: High data rate and extended time compared to the DTNs and not wired networks.

CHAPTER 3

Related Fields of Research

There are several research fields that are related to or overlapping with gossip routing and the optimization of flooding, e.g., *data distribution*, *reliable broadcast*, or *sleep scheduling* as depicted in Figure 3.1. This section gives a brief overview and elaborates the relevant differences and similarities for a selection of protocols. In contrast to the gossip routing protocols discussed in Chapter 4, probabilistic route discovery is not the focus. Nevertheless, many of the applied approaches and schemes are similar or even equal to the ones applied for gossip routing. Many published gossip routing protocols are inspired by other fields of research and the particular publications often reference them as related work.

The publications addressed in this chapter are grouped based on their focus. Some publications could arguably be placed in more than one group yet are only listed once, classified based on their prime application scenario and focus.

3.1 Data Dissemination and Replication

The focus of the class of *data dissemination* protocols is to spread some data over a network of nodes. While routing or topology information is also data, the primary content is often application layer data.

3.1.1 Epidemic Database Replication

Anti-entropy and *rumor mongering* are two schemes for the update of distributed databases [28] inspired by epidemic processes. With the *anti-entropy* approach, random pairs of databases compare their contents periodically and resolve all differences. Databases periodically distribute updates (called "rumors") to random destinations using *rumor mongering*. The spreading of rumors ends, when the spreading entity encounters a particular number k of destinations that have already registered the rumor (*counter based* variant). The number of spreading databases exponentially decreases over time. The parameter k is most important for the performance of the protocol: if k is too small, the rumor spreads to a limited number of other databases which results in inconsistencies and if k is too large, too many unnecessary rumors are sent. In another variation, called *blind* variant of rumor mongering, the database may stop to spread a rumor with probability 1/k at any time.

While both approaches are close to the gossip routing protocols, they assume that every database can create an end-to-end connection to any other database over multiple hops. Although it is not explicitly stated in [28], the authors assume a wired network.

3.1.2 Epidemic Routing

Gossip routing is related to *epidemic routing* [62] where messages are stored on (mobile) nodes and are probabilistically forwarded to neighbors: they are "infected". A *store-carry-forward* paradigm is applied that models the spreading of diseases in a population as we introduced in Section 2.2. The scheme is suitable for opportunistic networking [60] where delay is not the prime priority. Vahdat et al. applied an anti-entropy approach in their protocols for application in WSNs in [62] and showed that packet delivery with high reliability is possible when delays of up to several hours in the considered scenarios are tolerable. In gossip routing protocols, the packages are immediately forwarded or in some cases only stored for a very limited time. If there are no other neighbors to forward the packet to but the one that sent the

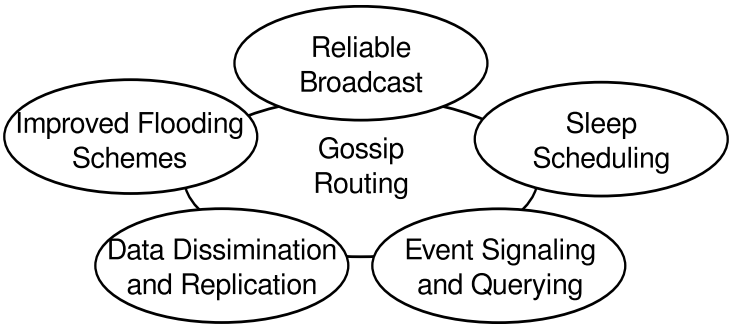


Figure 3.1: Gossip Routing and related fields of research

packet to the current node, the packet will be lost. Overall, the epidemic routing scheme is better suited for data distribution than route discovery.

3.1.3 Route Driven Gossip

Route driven gossip (RDG) [63] is an approach for probabilistic reliable multicast based on the *Dynamic Source Routing* (DSR) protocol. All nodes manage two data structures: a list of multicast members with (at least) one known route (called *active view*) and a list of members without any known route (called *passive view*). The two disjunct lists are required as each node has only a partial view of the network. Additionally, a data buffer stores all received packets that shall either be forwarded or provided on-demand by a pull-request. The authors argue that because of the assumed unreliable, infrastructure-less wireless network and costly route updates, only probabilistic reliability can be achieved.

Multicast packets, negative acknowledgements, and membership information are distributed by a gossip scheme. All nodes periodically send messages that contain information about the new packets in their buffer to a random subset of members in the active view set. The messages can also include piggy-backed pull-requests for missing packets that are determined based on the packet-id. Packets that are new in the buffer are sent only a limited number of times and are then stored until they are finally removed. Thus in the RDG protocol, the term *gossip* refers to the random distribution of messages in the network. There is no parameter p that determines the forwarding probability or other parameters that are common to gossip routing protocols.

The variant *Topology-aware RDG* (TA-RDG) adds a weighting function to improve the efficiency. The members from the active view that are to receive the periodically sent messages are not selected at random but the selection is weighted based on their distance: members that are close by get a higher chance. The weight is provided by the routing protocol and can also be some other metrics besides the hop distance. Simulations showed that the network load could be significantly decreased compared to RDG.

3.1.4 Anonymous Gossip

Chandra et al. propose *Anonymous Gossip* (AG), to improve the reliability of multicasting in mobile networks [64]. AG is implemented in multicast AODV[1]. The protocol has two phases: (i) multicast of a (data) packet and (ii) recovery of lost packets based on AG. The second phase is periodically repeated and run in the background. All nodes sent information about the received packet(-s) in gossip messages to random neighbors in the multicast tree. The gossip messages can either be randomly accepted by the receiver that are members of the multicast group[2] or forwarded and thus can travel multiple hops. Accepted messages are replied with a unicast packet and evaluated to enable the detection of lost packets that are then recovered. The random selection of neighbors is weighted by their distance and thus locality of the gossiping is achieved. To reduce the hop count that gossip messages have to take through the multicast tree, unicast can be used once the addresses of other multicast group members have been learned, e.g., from the replies or overheard packets. The parameter p_{anon} determines the probability

[1] The RFC for AODV already contains some support for multicasts but the specification is not complete and was never updated by any subsequent RFCs. More information is available in [65]. The spiritual successor, the *Dynamic MANET On-demand* (DYMO) routing protocol, seems to have dropped multicasts entirely from the Internet-Drafts.

[2] Note that the multicast tree consists of multicast group members and multicast routers. The latter will only forward packets and are not interested in the content.

that a node creates a gossip message in the current round but there is no clear information about the probability to accept or forward the packets in the publication.

AG is closer to the gossip routing protocols than RDG, as there is some (limited) probabilistic forwarding of packets. Nevertheless, the multicast tree based forwarding is an important difference.

3.1.5 DLA-based Multicast Routing Algorithm

Torkestani et al. propose multiple algorithms to approximate a *minimum weight Steiner connected dominating set* (WSCDS) for multicast routing in MANETs [66]. Three centralized learning automata-based heuristics are introduced and one of them was implemented as distributed algorithm called *DLA-based Multicast Routing Algorithm* (DLAMRA) where DLA stands for *Distributed Learning Automata*. A learning automate randomly selects actions from a set of available actions. The environment gives some response that acts as reinforcement signal[3]. This way, the probability vector that determines the probability distribution to select the next random action is updated. When the process is repeated, an optimal solution can be found after several rounds. Distributed learning automata are interconnected in a network and activate and effect each other via the environment. To solve the WSCDS problem, each vertex in the graph is represented by an automata. DLAMRA creates a Steiner tree from the source to the multicast receivers and considers the relative speed of the nodes as weight to keep the tree stable as long as possible. The neighbors of a node represent the action set and therefore the selection of an action represents the selection of the neighbor as dominator. The algorithm in DLAMRA was evaluated on unit-disk graphs and compared with other algorithms. The authors claim that it outperformed the others but there are some open questions. For example, an average CDS size of 5 nodes was found in networks of 100 nodes and 10 terminals with 200 units radio range that are distributed over an area of 1000×1000 units. This value seems fairly low and the difference to the other algorithms remains significant for larger terminal sizes.

3.1.6 Trickle

The *Trickle* algorithm [67] uses a gossiping approach to distribute code updates in a wireless sensor network. Each node broadcasts a *code summary* consisting of metadata to its neighbors. Based on these summaries, the nodes can detect whether they have outdated versions of their software and should contact the sending node to receive an update. A *polite gossip* approach is applied to reduce the number of broadcasts. If a node has received several packets with the same metadata in some specific time interval, it will refrain from broadcasting itself. As broadcasts are randomly uniformly distributed, the energy consumption is shared by all nodes in the network - a prime objective in sensor networks. The applied scheme is very similar to epidemic routing and the discussed epidemic database replication approaches.

3.1.7 SPAWN

Nandan et al. propose the *Swarming Protocol for vehicular Ad-hoc Networks* (SPAWN) that uses a gossip approach for the propagation of content availability information [68]. SPAWN creates a peer-to-peer overlay network on top of a unicast routing protocol and IEEE 802.11 as host-to-network technology. As the nodes in vehicular networks have only very short term connections with stationary and sparsely deployed gateways, it is not possible to fully download large files. Thus the nodes periodically broadcast gossip messages containing a content id, a bitfield of the available chunks, a timestamp, and a list of nodes that have processed and forwarded the message. Two gossip modes are proposed. In the *probabilistic SPAWN* mode, nodes that are interested in a particular file will forward received gossip messages with a high probability and nodes that are currently not downloading the file will forward the messages with a lower probability. In the *rate-limited SPAWN* mode, each node stores gossip messages in one of its two types of caches: (i) Gossip messages for files that the node is currently not downloading are stored in the *non-interested cache* and (ii) gossip messages for files that are currently downloaded are stored in the *interested cache*. Non-interested cache entries are gossiped at a lower rate than entries in the interested cache. For both caches, the selection of forwarded entries can either be based on the timestamp (recent entries have higher priority) or the packet can be randomly selected. Missing chunks of a file are downloaded in a peer-to-peer manner from nodes that are close by.

[3] The signal can be positive or negative.

3.2 Reliable Broadcast

Reliable broadcast protocols consider the reliable delivery of broadcast packets as the primary objective and therefore accept a higher redundancy.

3.2.1 Reliable Broadcast in LANs

In the general domain of distributed systems, the reliability of broadcasts is an important issue. For extended LANs where multiple segments are connected by switches (or bridges), several reliable broadcast protocols have been proposed, e.g., [69, 70] to ensure reliability as well as ordering. A *sequencer* has the task to receive broadcast messages as unicast and to deliver them to all nodes in the network via broadcast. As a sequence number is attached by the *sequencer* to the packet, losses can be detected and packets reordered.

The networks in this scenario have significant higher data rates and much lower bit error rates than the wireless networks considered in this study. Most importantly, wireless networks can not provide direct communication between any pair of nodes. The sequencer approach is only viable when all entities are in the same physical broadcast domain.

3.2.2 Reliable Broadcast for ZigBee

Reliable broadcast has also been researched for applications in IEEE 802.15.4/ZigBee networks [71]. The hierarchical address space and tree structure of the standard are exploited to achieve reliability and minimize redundancy. Each node selects a subset of 1-hop neighbors (*forward nodes*) that have the task to forward broadcast packets to all 2-hop neighbors. All other 1-hop neighbors are called non-forward nodes. Lost packets can be detected as the transmitting node should receive the forwarded packets from the forward nodes (all links are bidirectional). In the case of a detected packet loss, the particular packet can be retransmitted multiple times until the sender overhears enough broadcasts from its neighbors when they forward or a specific limit of retransmissions is reached.

The required hierarchical structure for this approach is not available for gossip routing in WMNs and MANETs without routing and address assignment protocols that are available to configure the logical network topology beforehand.

3.2.3 Double-Covered Broadcast

Lou and Wu propose a reliable *Double-Covered Broadcast* (DCB) scheme for media with high transmission error rates by applying so called double coverage [72, 73] which is actually a similar idea as the MPR approach of OLSR (see Section 3.5.2). Their *Forwarding Node Set Selection Process - Enhanced Double Coverage* (FNSSP-EDC) algorithm selects so called *forward nodes* (comparable to MPRs) for each node from its 1-hop neighbors that cover the node's 2-hop neighbor set. All other 1-hop neighbors are *non-forward nodes*. They are covered by at least two *forward nodes* and thus are likely to receive forwarded packets: there are (at least) three chances. The links between each node and its *forward nodes* are assumed to be bidirectional. When a packet is sent by node A and then forwarded by its *forward nodes*, node A overhears the procedure (passive acknowledgement). If it detects that any *forward node* did not forward the packet, it retransmits the packet multiple times until it knows that the packet was successfully received by all selected neighbors. *Forward nodes* will not forward packets that are received multiple times, thus active acknowledgements are required when passive acknowledgements fail or are not available. In contrast to the MPRs, DCB calculates the *forward nodes* on a per packet-basis. Each sender attaches an addresses list of its *forward nodes* to the packet. This enables to optimize the *forward node* selection as only candidates can be considered that probably have not yet received the packet.

While this scheme has a high reliability, the overhead is also high but not as high as with flooding in error-free cases as only a subset of the 1-hop neighbors forwards the packets. In real world scenarios, DCB might get problems with distinct asymmetric and unidirectional links. The problem of asymmetric[4] links shall be resolved by establishing a feedback path over one intermediate node to inform the neighbor.

The idea of the DCB looks promising but requires specific information about the local topology. Unfortunately, only a simulation based study is presented in the publication that used a simple radio model (*two-ray ground reflection*, see also Section 5.3) where the discussed link problems do not arise;

[4] We assume that the authors actually refer to unidirectional links or links with very exposed asymmetry. Figure 4 in their publication is a clear indicator for this assumption.

the network was also modeled as a unit disc graph with an 900×900 m^2 area and 250 m transmission range. The algorithm is not probabilistic as it always tries to determine the best forward nodes set. This can require significant resources if the FNSSP-EDC algorithm has to be run often. Although the OLSR protocol runs a similar algorithm only when the 2-hop neighborhood changes, this approach has shown to cost lots of resources [74]. This problem was a primary reason why the B.A.T.M.A.N. protocol [75] was designed[5].

3.3 Signaling and Querying

Signaling and querying are the most important tasks in distributed sensor networks that monitor real world phenomena. Latency, respectively the delay, and reliability are the primary concerns for this group of protocols.

3.3.1 Gradient Broadcast

GRAdient Broadcast (GRAB) [76, 77] is a protocol to transmit a packet from a cluster of wireless sensor nodes that have detected an event (stimulus) to some sink node. Not all sources will report the same detected event as the redundant information would spent too much energy. The *Center of Stimulus* (CoS) algorithm determines a single source to generate a report based on the signal strength, i.e., the strength with that the event was detected.

Each node maintains a cost field that represents its distance to the sink: the value is high if the distance is large and low if the node is close to the sink. The cost value represents how much energy is required to deliver packets via each node towards the sink. Nodes compare their own costs with the cost of the sender/forwarder from which they received a packet from, to decide if they shall forward the packet. Therefore, the global direction of the packet forwarding is determined by the cost gradient and the packet travels only towards the sink.

The cost gradient is setup by the source that broadcasts *advertisements packets* (ADV) that contain a cost field. The cost is initially set to 0 and each receiving node will compare the current value c_{cur} plus the cost to send a packet to this neighbor c_{neigh} with the last known cost value c_{prev} that is initially set to ∞. The ADV is forwarded for $c_{cur} + c_{neigh} < c_{prev}$ and dropped otherwise. c_{prev} is always updated with the lowest value and will therefore decrease monotonously. To be able to react to topology changes, specific measures have to be taken.

Source nodes attach a credit value to each packet that represents a specific resource that can be spent by forwarding the packet in the network. The credit is based on the cost of the source node to reach the sink plus an additional extra budget α. The parameter α determines how much the routes, that copies of a packet take through the network, may deviate from the direct, i.e., "cheapest" path. Nodes near the source may consume larger amounts of the credit to increase the initial number of copies that are created on the first few hops.

GRAB requires prior gradient setup by all sink nodes and is usable only for unicast flooding; communication between any nodes in the network is only possible when all nodes act as sink and sent ADVs. In this case, the ADV mechanism is similar to the route discovery approach applied in the B.A.T.M.A.N. protocol [75]. The authors discuss the impact of the credit α on the energy consumption and the ratio of successful delivered packets but they leave open how this value should be determined by the source. In summary, GRAB trades reliability for redundancy and fits well for WSN applications but not for gossip routing in WMNs or MANETs. The fundamental idea to restrict the forwarding to a particular region has also been applied in a gossip routing protocol (see Section 4.1). *Directed diffusion* [78] is a similar protocol from the WSNs domain.

3.3.2 Rumor Routing

Rumor routing [79] is an approach to avoid flooding in wireless sensor networks. Special packets called *agents* are probabilistically created by nodes that have detected an event. The agents are forwarded (randomly or away from the source in a straight line) by the nodes for a specific number of hops and carry a list of all events that they have encountered. Therefore, all nodes on the path and all other nodes that overhear the packet are informed of the events. Queries for events are forwarded in the same manner. When the path of a query packet intersects with the path of a matching agent packet, the query

[5] B.A.T.M.A.N. never got past the Internet-Draft stage but is used in several community networks.

can be routed directly to the event's source. Simulations showed that it is very likely that query and agent paths will intersect (in the considered network model).

Rumor routing is only applicable for unicast transmissions and in typical sensor network scenarios with events, sensors, and data sinks. The authors assume a uniform deployment of the nodes and symmetric radio ranges[6]. The approach has a very low redundancy but can have a high delay when the forwarding of queries and agents is not optimized. A gradient like approach could be used to ensure that the packets will always increase the distance from the source but dead ends have to be resolved in non-uniform deployments.

3.3.3 Service Gossip Protocol

Lee et al. propose a differential *service gossip protocol* for service discovery in MANETs [80]. Each node has tree-based service registry with generic services near the root and more specific ones towards the leafs. Services are periodically advertised via multicast and cached by all receivers. Service discoveries are answered by all nodes that have a corresponding entry in their registry. If the query did contain any keywords, the reply is appropriately refined. Replies are sent after a random waiting time to prevent storms of redundant replies. Nodes overhear replies to extend their list of known service providers and will only send replies with new information, respectively the not yet advertised service providers, to decrease the network load.

In this protocol the term gossip refers to the random and incremental spreading of information in the network; no probabilistic scheme is involved.

3.3.4 Broadcast Gossip Algorithm

Aysal et al. apply a gossip approach in WSNs without any central entity, where nodes shall reach an agreement on a particular value that represents an event [81–83]. Nodes wake up periodically and broadcast the particular value to their neighbors. All awake nodes update their value, i.e., calculate the (weighted) average while the sleeping nodes are unaffected. The authors show that a consensus of the value is reached in the whole network after some time, that is in the neighborhood of the average value which was measured by the nodes near the event. A strongly connected (network) graph with reliable, directional links and equal transmission radii is assumed. The algorithm is evaluated in numerical simulations based on a network model that uses random graphs and uniform radio ranges with no packet losses.

Dimakis et al. use a similar approach with (greedy) geographic routing, where nodes randomly select a destination in the network to receive the value [84]. The value is either accepted with a particular probability p and an updated value is calculated and stored. If the value is rejected, it is sent to another random node.

The gossip schemes that are applied for consensus protocols have a different focus than gossip routing. The algorithms usually take a longer time to terminate, i.e., the time until a consensus is reached can be much longer due to the sleep schedule than gossip-based route discovery. Additionally, the values are propagated in every round and not just once after they have been received. One of the most important parameters is the "mixing" parameter γ and/or the formula that is used to update the values. Depending on the application, desired speed of convergence, etc. it can be a simple average or a more complex variant that includes weighting.

3.4 Sleep Scheduling

Sleep schedule schemes can apply a random variable to determine the sleep/awake status. This approach requires no central entity or a distributed algorithm that calculates an (optimal) sleep schedule for the topology and thus management overhead can be avoided.

3.4.1 Gossip-based Sleep Protocol

Hou et al. propose the *gossip-based sleep protocol* (GSP) for wireless sensor networks [85] where each node randomly sleeps with probability p for a period. The protocol balances the number of sleeping and awake nodes so that the network remains connected and the network-wide energy consumption is reduced. The authors present a synchronous version (GSP1) and an asynchronous variant (GSP2) that removes

[6] We assume the authors actually refer to bidirectional links.

the synchronization overhead. Synchronization refers in this context to synchronous clocks on the nodes that enable all nodes to switch from sleep to awake mode (or vice versa) at the same time. In GSP2, the duration d of the sleep/awake period is randomly selected. A distributed algorithm to determine optimal values for p and the bound of d is not provided but the authors showed that the energy consumption could be minimized for some configurations.

GSP and similar protocols are applicable in well-connected networks with source-sink scenarios where the sink always stays awake[7]. With the random sleeping of nodes we can expect that a constant number of them is active per square unit/volume. Only when the nodes are deployed uniformly, low settings of p will result in a still (strongly) connected network. In the experiments presented by Hou et al., a fraction of < 0.05 is disconnected for $p = 0.25$ in a 10×10 grid topology.

The idea to temporarily disable some nodes with a particular probability and still retain reachability is very close to the idea of percolation theory (see Section 2.1). The awake nodes can be considered as the air bubbles in a porous material that is discussed as a percolation example. When there are enough nodes/bubbles a path exists through the network/porous material.

Sabitha and Sebastian apply the approach to AODV. In GOS-AODV [86] nodes will be awake with probability p and forward packets and sleep with probability $1 - p$.

3.5 Improved Flooding Schemes

This section contains protocols that focus on a general reduction of the flooding overhead like gossip routing protocols but they do not apply a probabilistic scheme.

3.5.1 Pruned Flooding

Lim and Kim propose two schemes to create broadcast trees [1] based on the assumption that a *minimum spanning tree* (MST) will result in the lowest number of forwarded packets. All nodes are either (i) part of the MST and forward packets, (ii) they are leafs and do not forward packets, (iii) or they are the source, i.e., the root of the MST that generates packets.

In the *self-pruning* scheme, each node i requires to know its neighbors which is achieved by attaching the list of the neighbor addresses N_i to each forwarded packet. This allows the receiver j to determine how many of its neighbors N_j have not yet received the packet. The packet is only forwarded when the condition $N_j - N_i \neq \emptyset$ applies.

Two-hop neighborhood information is required in the *dominant pruning* scheme where each sender determines a set of forwarders. The addresses of the forwarders are attached to each packet and thus the receiver will either drop or forward it. The scheme is called "dominant" as the sender makes the decision compared to the receiver in the "self-pruning" scheme. To calculate a minimum set of forwarders, the *greedy set cover* algorithm is proposed [22].

Lim and Kim ran numerical simulations[8] and compared the number of forwarded packets and the number of packet arrivals[9] of both proposed schemes, (blind) flooding, and the Berman algorithm (see Section 1.3). Simulations with $10, 30$, and 100 nodes deployed in a unit-square and different transmission ranges ($[0.05 \ldots 1.3]$ units) showed that *dominant pruning* was much closer to the optimal solution (approximated with the Berman algorithm) as the *self pruning* scheme. There is no information about the reachability. If the results hold in the real world is questionable as the network model assumed bidirectional and error-free links.

3.5.2 Multipoint Relays

Multipoint Relays (MPRs) [87] are used in the *Optimized Link State Routing* (OLSR) protocol [9]. All nodes select minimal subsets of their neighbors as MPR sets so that they can reach all of their two-hop neighbors via the MPR set. Each node may specify via a willingness value from 0 (`WILL_NEVER`) to 7 (`WILL_ALLWAYS`) if it wants to act as an MPR, e.g., based on their remaining energy. An abbreviated version of the MPR computation algorithm is shown in Algorithm 4. As shown, the willingness has a higher priority for the MPR selection compared to the node degree.

[7] This is a common assumption in WSNs as the sink is often a gateway node that also has unlimited power supply.

[8] The authors do not give specific information about the simulations but we assume that they run numerical simulations on undirected and unweighted graphs.

[9] The number of packets that are received by the nodes including duplicates. Therefore this metric is equivalent to the redundancy as discussed in Section 1.4.

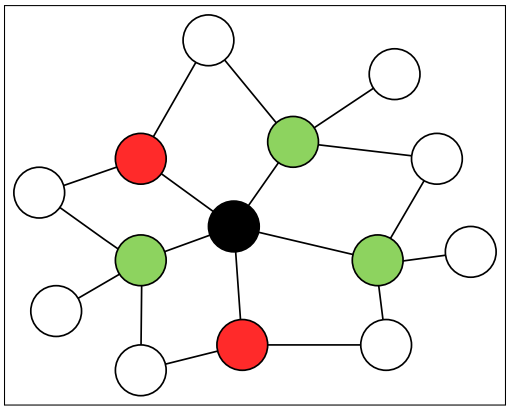


Figure 3.2: MPR Selection: The black node selects the green 1-hop neighbors as MPRs while the red nodes will not forward TC messages. All 2-hop neighbors (white) will receive the TCs send by the black node (if the network is reliable).

Algorithm 4 MPR Computation (abbreviated)

Require: List of 1-hop neighbors N, 2-hop neighbors N2, and their willingness
  add all $n \in N$ with willingness==`WILL_ALWAYS` to MPR set
  add all $n \in N$ to MPR set if they are the only way to reach a $n2 \in N2$
  while not all $n2 \in N2$ can be reached via the MPR nodes **do**
    for each $n \in N$ **do**
      r_n = number of nodes $n2 \in N2$ that are reachable via n and are not yet covered
    end for
    add $n \in N$ with highest willingness to MPR where $r_n > 0$
  end while

The MPRs are determined individually for each interface and subsequently the union of all sets is taken as the final MPR set. The selection of an optimal MPR set is a NP-complete problem and thus often more nodes than necessary are included by the (greedy) algorithm. While this leads to suboptimal performance due to higher redundancy, limited redundancy is in fact advocated for OLSR to ensure reachability. OLSR uses the MPRs to flood *topology control* (TC) messages that contain link state information to all nodes in the network. An example for the MPR selection is shown in Figure 3.2. The core mechanism of OLSR remains the same in the second version which is currently only available as an Internet-Draft.

While the goal of the MPRs is very close to the motivation of gossip routing, it uses no probabilistic elements. A very similar approach is discussed in [88] called *Ad Hoc Broadcasting Approach* that lacks the willingness parameter. MPRs and the *dominant pruning* scheme (see Section 3.5.1) are functionally equal.

3.5.3 Tree-Based Optimization

Jüttner and Magi propose a tree-based broadcasting scheme [89]. A spanning tree is determined in a distributed, asynchronous way where the nodes that are part of the tree are responsible to forward broadcast packets. It is assumed that the tree is stable and the topology does not change continuously. The *TreeCast* algorithm extends the tree once new links are detected and repairs the tree automatically when links are lost. Different trees can be detected based on an id and when two have to be merged because of a new link, one set of nodes will have to update the tree id. Vice versa when a tree breaks, both parts will get new ids.

This way TreeCast creates a tree that is subsequently used to forward broadcast packets but the tree will not be a minimum spanning tree in most scenarios. The algorithm does not consider different link qualities or unidirectional links. While the tree provides a cycle free structure with a reduced redundancy compared to flooding, lost packets can easily effect that the packets will never reach some parts of the network. The redundancy reduction that can be achieved depends on the order in that the nodes begin to run the algorithm. When nodes are started in a different order or specific packets are lost, different trees will be the result. The tree is not optimized when nodes join or leave but this way it stays stable

for a longer time which can be a benefit for some applications.

3.5.4 Mechanisms to Reduce Redundancy, Contention, and Collision

Tseng et al. propose *counter-based*, *distance-based*, *location-based*, and *cluster-based* schemes besides a *probabilistic scheme* to avoid broadcast storms [90, 91]. The central idea of the authors is to consider which additional coverage can be achieved by forwarding a packet. Their network model is based on unit-disc graphs where all nodes have the same radio range and all links are bidirectional.

In the *counter-based* scheme, each node counts the number of received copies c for each packet. Upon reception of the first copy, a random timer is started. The packet is forwarded after the timeout if the counter is still below a particular threshold C. This scheme is simple to implement as it requires no additional information. The approach is based on the idea that only a limited additional coverage can be achieved when many neighbors have already transmitted the packet. C is a static pre-configured value that is not dynamically adapted based on the node degree.

The *distance-based* scheme requires that nodes know the distances to each other. When a packet is received for the first time by node B from node A, the distance $\|AB\|$ determines what happens with the packet. If $\|AB\|$ is lower than the threshold d, the packet is dropped and otherwise a random timer is started. The packet is forwarded after timeout if no duplicate was received from any node C where $\|BC\| < d$. It is assumed that only a limited additional coverage can be achieved when a nearby neighbor already forwarded the packet. The authors propose RSSI as a measure of distance but depending on the radio technology and frequency, RSSI values can only provide a rough approximation of the distance (see also Section 5.4).

When more detailed position information is available, e.g., via GPS the *location-based* scheme can be applied. Upon reception of a packet, the node calculates the additional coverage cov that can be achieved by forwarding it. $cov \in [0, 1]$ is defined as a fraction of the coverage that can be achieved by the node (maximum: πr^2). If cov is below the threshold $cov_{min} \in [0, 0.61]$ the packet is dropped, otherwise the the packet is stored, a random timer is started, and the packet then forwarded after its timeout. For any duplicate that is received in the meantime, cov is updated and the (stored) packet is dropped as soon as cov falls below cov_{min}. The authors note that at most 61% additional coverage can be achieved in unit-disc graphs, i.e., when the two nodes are just within transmission range ($\|AB\| = r$). On average, when two nodes are randomly deployed within radio range, the expected additional coverage is about 41%. When multiple copies of packets are received from different neighbors, the additional coverage approaches zero rapidly.

The *cluster-based* scheme requires some clustering algorithm where all cluster heads can cover all nodes in their clusters. The cluster heads are a dominating set for the network. Only specific gateway nodes and the cluster heads will handle received packets by applying one of the above forwarding schemes. The clustering algorithm may introduce a significant management overhead which can negate the reduction of redundant broadcasts. This is especially true in mobile networks or in networks with unstable links. A full routing protocol based on a cluster-based scheme was also proposed as an Internet Draft [92].

To improve the performance, Tseng et al. subsequently proposed three further schemes [93, 94]: the *adaptive counter-based*, *adaptive location-based*, and *neighbor-coverage* scheme. As the first two names imply, a faster adaptation for dynamic topologies of MANETs is aspired.

The threshold C of the modified *counter-based* scheme is determined by the node degree d_n. C increases from $d_n = 0$ to n_1 and then decreases until n_2, where n_1 and n_2 ($1 \leq n_1 \leq n_2$) are constants. Therefore a high node degree and also a low node degree will result in a low threshold, while a medium node degree results in a high threshold. The cov_{min} threshold in the modified *location-based* scheme is adapted in a similar manner. Low node degrees lead to a high cov_{min} threshold and vice versa.

As last, the *neighbor-coverage* scheme uses the same approach as discussed in Section 3.2.3 and Section 3.5.2 where each node has 2-hop neighborhood information. Each packet is stored for a random time before it is forwarded. Node x maintains a set T that is initialized with $N_x - N_{x,h} - \{h\}$, where N_x is the neighbor set of x and $N_{x,h}$ is the neighbor set of node h from which the first copy of the packet was received. The packet is updated when a copy is received from node k by $T = T - N_x - N_{x,k} - \{k\}$ and is immediately dropped as soon as $T = \emptyset$.

As both schemes depend on a neighborhood discovery mechanism that introduces some overhead, the authors propose a dynamically adjusted HELLO interval that is determined by the neighborhood variation of each node.

3.5.5 Scalable Broadcast Algorithm and Ad Hoc Broadcast Protocol

Peng and Lu propose the *Scalable Broadcast Algorithm* (SBA) [95]. Each node runs a HELLO protocol for neighbor discovery. The list of neighbors is attached to each packet which enables the receiver to determine how many of its neighbors have not yet received the packet. The packet is forwarded after a random waiting time t if there are still neighbors that (presumably) have not received the packet. The timeout is determined depending on the node's degree d and the maximum degree of its neighbors $max(d_n)$ using the following formula:

$$t = \text{random}\left(0, \Delta \times \frac{1 + max(d_n)}{1 + d}\right) \tag{3.1}$$

where Δ is a constant value. Nodes get a higher preference based on their node degree compared to their neighbors. Thus the nodes that will achieve the largest additional coverage should forward the packet first. Simulations with mobile networks showed up to 60% reduction in the number of duplicates while at the same time the delivery ratio was on par with flooding. Omni-directional antennas, uniform transmission ranges, and bi-directional links were assumed.

Peng and Lu also propose the *Ad Hoc Broadcast Protocol* (AHBP) [96]. Like in SBA, each node has 2-hop neighborhood information gathered with a HELLO protocol. Each packet contains the addresses of a subset of neighbors called *Broadcast Relay Gateways* (BRG) that are equivalent to the *Forwarding Node Set* of FNSSP-EDC (see Section 3.2.3) and that shall forward the packet. In addition, a list of BRGs is piggybacked and extended with the addresses of the BRGs that have forwarded the packet to enable a duplicate detection. Non-BRG nodes will never forward packets and BRG nodes calculate a new BRG set based on the path and their 2-hop neighborhood information.

As a result, the greedy algorithm constructs a connected dominating set of the network that is not minimal. Link asymmetry and unidirectionality are not considered but could be handled by the HELLO protocol. The simulation of AHBP used a combination of the free-space and two-ray ground reflection model where such problems do not arise (see Section 5.3). The authors claim that the broadcast cost[10] can be reduced by $60 - 80\%$ compared to flooding in scenarios with mobile networks when AHBP is applied.

3.5.6 Internal Nodes Based Broadcasting

Stojmenovic et al. propose *internal nodes based broadcasting* [97–99], where *internal nodes* are nodes from a dominating set. Based on the works of Wu and Li [100], they propose modifications to create a connected dominating set where nodes with high degree get higher priority. The position of the nodes plays an important role as it is used to determine if a node is an *intermediate node*, i.e., it connects two of its neighbors u and w when $\text{distance}(u, w) > R$. The authors assume a unit-disk graph with radio range R. A pruning scheme that considers the number of covered neighbors is used to further reduce the number of packets. Further on, a retransmission scheme with negative acknowledgements is introduced. Simulations were run to compare the number of broadcasts of the proposed algorithm with MPRs (see Section 3.5.2), two clustering algorithms, and the *location-based scheme* with different thresholds that is described in Section 3.5.4. *Internal nodes based broadcasting* showed the best ratio between the reachability and the number of saved broadcasts. The authors leave an evaluation for networks with unidirectional links, different transmission ranges, hidden nodes, etc as future work.

3.5.7 Distributed Gradient Optimization

Neglia et al. [101–103] used an analytical framework by Nedic et al. [104] to research optimal epidemic-style forwarding in delay tolerant networks. They focus on a network where the number of nodes[11] and the mobility pattern is not known a priori. In their approach each node tries to minimize a convex objective function and periodically exchanges information with other nodes that eventually leads to a consensus algorithm style optimization.

The optimization problem is defined as follows:

$$\begin{aligned} &\underset{x \in \mathbb{R}^n}{\text{minimize}} \quad F(x); \qquad F(X) := \textstyle\sum_{i=1}^{m} f_i(x) \end{aligned} \tag{3.2}$$

[10] We assume this metric refers to the number of broadcast packets.
[11] Neglia et al. actually refer to agents.

$f_i : \mathbb{R}^n \rightarrow \mathbb{R}$ is a local convex function. In each time slot k, information is exchanged between nodes that is used to update current estimate $\hat{x}^i(k)$ at node i by:

$$\hat{x}^i(k+1) = \sum_{j=1}^{m} a_j^i(k)\hat{x}^j(k) - \zeta d_i(k) \tag{3.3}$$

$a^i(k)$ is a stochastic vector, i.e., $\sum_{j=1}^{m} a_j^i = 1$ that provides non-negative weights for each of the m neighbors of a node. The authors set the entries in the vector to $1/m$ if an estimate has been received from node j in slot k and 0 otherwise, i.e., all neighbors have equal weights. The second half of the formula describes a sub-gradient $d_i(k)$ of f_i at point $\hat{x}^i(k)$. Its purpose is to minimize f_i with a step size of ζ.

The algorithm converges to an optimal solution [104] under the following assumptions:

- All nodes can communicate with each other (directly or over multiple hops) infinitely often (in infinite time).
- The time between two communications between any pair of nodes is upper bounded by some positive integer.
- A value L to satisfy $\|\nabla f_i\| \leq L$ exists where $d_i(k) = \nabla f_i(x)|_{x=\hat{x}^i(k)}$

Neglia et al. extend the algorithm with different forwarding strategies like k-hop and *probabilistic* schemes. In the former, messages are only forwarded for at most k-hops and the latter is a gossip routing approach where packets are only forwarded with probability p. The probabilistic scheme is studied in numerical simulation where p is the consensus value that converges to a homogeneous value for all nodes after a particular number of iterations k. In the presented example, 10^5 iterations are required to get $p \approx 0.3241$ in a network with 100 nodes. The results from the simulation are compared with approximated results from the local cost function $f_i(p)$ that has been specified for this scenario. As last the influence of the parameter ζ on the convergence time is discussed. For some configurations the convergence time can be reduced to $< 10^2$ iterations but for others, the algorithm did not converge after 10^7 iterations and the simulation was aborted. When the algorithm converged, the same optimal solution was found in all cases.

The detailed description and formulation of the optimization problem based on the analytical framework is very sophisticated. The network model does not match real world networks and the focus differs significantly from gossip routing. The objective is similar to the protocol discussed in Section 3.3.4. Nevertheless, the approach could be applied to iteratively determine optimal parameters for gossip routing protocols. The protocol could be started with some default values that are than optimized.

3.6 Studies

Some authors conducted simulation based studies of multiple protocols that where introduced in this chapter.

3.6.1 Comparison of Broadcasting Techniques

Williams and Camp conducted a study [105] of five broadcasting techniques: *counter-based* scheme (Section 3.5.4), *location-based* scheme (Section 3.5.4), SBA (Section 3.5.5), and AHBP (Section 3.5.5). The authors compared the performance of the protocols with *simple flooding* and an optimal solution based on a *minimum connected dominating set* (MCDS) that is calculated with a brute force method[12]. The study consisted of four scenarios

- static nodes
- network congestion[13]
- mobile nodes
- mobile nodes and congested network

[12] The MCDS could not be determined for networks with more than 70 nodes

[13] Congestion was achieved by increasing the packet rate.

The IEEE 802.11 MAC protocol was used in scenarios with congestion and a *Null MAC*[14] otherwise. In both cases the radio range was set to 100 m, the mobility model was random waypoint, and all nodes were deployed in a 350m^2 area.

SBA and AHBP showed results that were closer to the size of the MCDS than simple flooding when the network size was sufficiently large. The counter-based and location-based scheme, as well as SBA showed problems in congested networks as the *Random Assessment Delay* (RAD)[15] timeout of 0.01 s was too low and not enough packets could be received in this time. The authors conclude that more research about the adaptation of the RAD is required.

3.6.2 Gossip versus Deterministic Flooding

Lin et al. published a study of *rumor mongering* (see Section 3.1.1) versus deterministic flooding on Harary graphs that are superimposed on the network [29]. Harary graphs consist of n nodes and are t-node as well as t-link connected. Thus the removal of $t-1$ nodes/links will not partition the network. The main focus of the authors is on fault tolerant broadcasting in abstract networks, i.e., computer networks, processors, etc. The general graph/network model that is used in the study, does not support a physical layer broadcast. In the considered rumor mongering scenario, each node that receives the same packet less than for the F-th time will forward it to B randomly chosen neighbors as unicast. First of all, The authors analyze deterministic flooding on the superimposed Harary graph. Their failure model considers equal and independent failure probabilities for all nodes in the network that may have two states: functional or failed. Link failures are not considered and all failures happen before the start of the protocol, i.e., a subset of nodes is removed from the graph before any broadcasts are sent. The fragility of the graph and the number of t-cutsets (set of t nodes whose failure will disconnect the graph) are discussed in detail. Second of all, a simulation is run to compare the performance of both approaches in Ethernet networks. The rumor mongering protocol showed a higher number of redundant packets as well as a longer time to spread the packet to all nodes in the network than the proposed Harary graph based flooding.

While the study introduces several interesting lemmas and theorems, the focus is on wired networks without a shared medium. The failure model does not consider the properties of wireless communication and thus the proofs and simulation results cannot be transfered to wireless networks. Especially the overhead that is required to construct the Harary graph is not considered for the performance.

[14] The *Null MAC* quasi realizes a graph based simulation without any effects of congestion, media access, etc.
[15] RAD is used as a general term to describe the timeout parameter/interval that is part of the studied protocols.

CHAPTER 4

Gossip Routing Protocols

In this chapter, we introduce and discuss a selection of different gossip routing protocols and studies that have been published in the domain of multi-hop wireless networks. The protocols apply a probabilistic approach to forward packets that represent route requests or other information, e.g., the link states. Each gossip routing protocol consist of a function that maps specific input parameters to a forwarding probability:

$$g(\ldots) = p \tag{4.1}$$
$$g(\ldots) \rightarrow [0,1] \tag{4.2}$$

We call g the *gossip function* in the following. Further schemes can be applied in addition to improve the performance compared to the simple gossip routing variant that uses only a pre-configured and thus static forwarding probability p. The gossip function of the simple gossip routing variant has no parameters. As will be mentioned in the following subsections, most of the gossip routing protocols are actually a component of a complete routing protocol (mostly AODV). In some cases the gossip function is implicitly specified by p and thus the function g omitted.

We try to provide the parameters of the experiment setups in a uniform way but not all parameters are available for each protocol. Some parameters are very specific for the particular algorithm while others are not mentioned in the publications. When no unit is denoted, the particular parameter is unit-less or the unit is not known, e.g., both the area and the radio range can be unit-less.

Acronyms for the gossip protocols are specified by us if they have not been specified by the authors. They are used as a reference in the tables in Chapter 6 and within this chapter.

4.1 Regional Gossip Routing

Li et al. propose an optimization of gossip routing by restricting the forwarding to a specific region [106, 107]: *Regional Gossip Routing* (RGR). They assume that all nodes are equipped with some localization device, e.g., GPS or alternatively some distributed localization service is available that provides an approximation of the particular positions. The transmission range is uniform in the considered network model and all nodes are distributed in a two-dimensional area. The forwarding of packets shall be restricted to an ellipse where the source and destination nodes are in the ellipse's focii. An example is shown in Figure 4.1. The position of the source node s and destination node d is piggybacked in each packet. Therefore every node $n \neq s \wedge n \neq d$ can determine if it is inside the ellipse if the following condition applies:

$$||sn|| + ||sd|| \leq l \times ||ds|| \tag{4.3}$$

where l is the ellipse factor and $||xy||$ is the euclidean distance between nodes x and y. Nodes outside of the ellipse drop all packets from s and d while nodes inside the ellipse forward the packets with probability p. Nodes on the first k-hops from the source will always forward but there is no information about the specific value k that should be used. The gossip function is thus:

$$g(k) = \begin{cases} 1, & \text{if } ||sc|| \leq k \\ p, & \text{else} \end{cases} \tag{4.4}$$

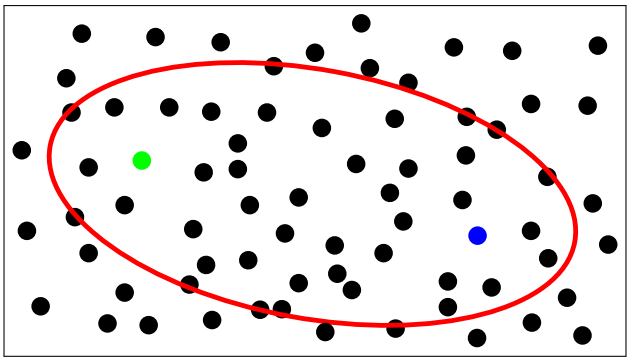


Figure 4.1: Regional gossip routing example. The forwarding of packages is restricted to an ellipsoid region with the source and destination nodes (green and blue) in its focii.

Parameter	Values
Nodes n	$1000, 1500, 2000$
Area	15×15
Ellipse factor l	$1.2, 1.4, 1.6, 1.8, 2, \infty$
Radio range r	$1, 1.5, 2, 2.5, 3$
Probability p	$p \in (0 \ldots 1]$, in 0.1 steps and $p \in (0.02 \ldots 0.30]$, in 0.02 steps
Source-destination-pairs	100, randomly selected
Packets per pair	1000

Table 4.1: Regional gossip routing experiment parameters

Where c is the position of the current node.

Simulations were run based on unit disc graphs and mobile nodes. A summary of the experiment parameters is shown in Table 4.1. No information is provided about the mobility model or the initial k-hop flooding. The authors observed that in some cases the number of packages could be reduced by up to 95% compared to flooding. Unfortunately, the presented data does not include confidence intervals or other measures of the variance. A comparison with geographic routing algorithms [108] that also try to improve the routing by location information and are applicable in the same scenarios would be interesting. How the protocol will perform when imprecise position information is available or the deployment is not uniform was not discussed.

4.2 Density Aware and Border Node Retransmission Based Probabilistic Flooding with Neighbor Elimination

Cartigny et al. study four improved flooding algorithms [26, 27] that are compared with a *simple probabilistic* scheme, i.e., gossip routing with static probability p.

Density Aware Probabilistic Flooding (DAPF) determines the forwarding probability p based on the node degree n:

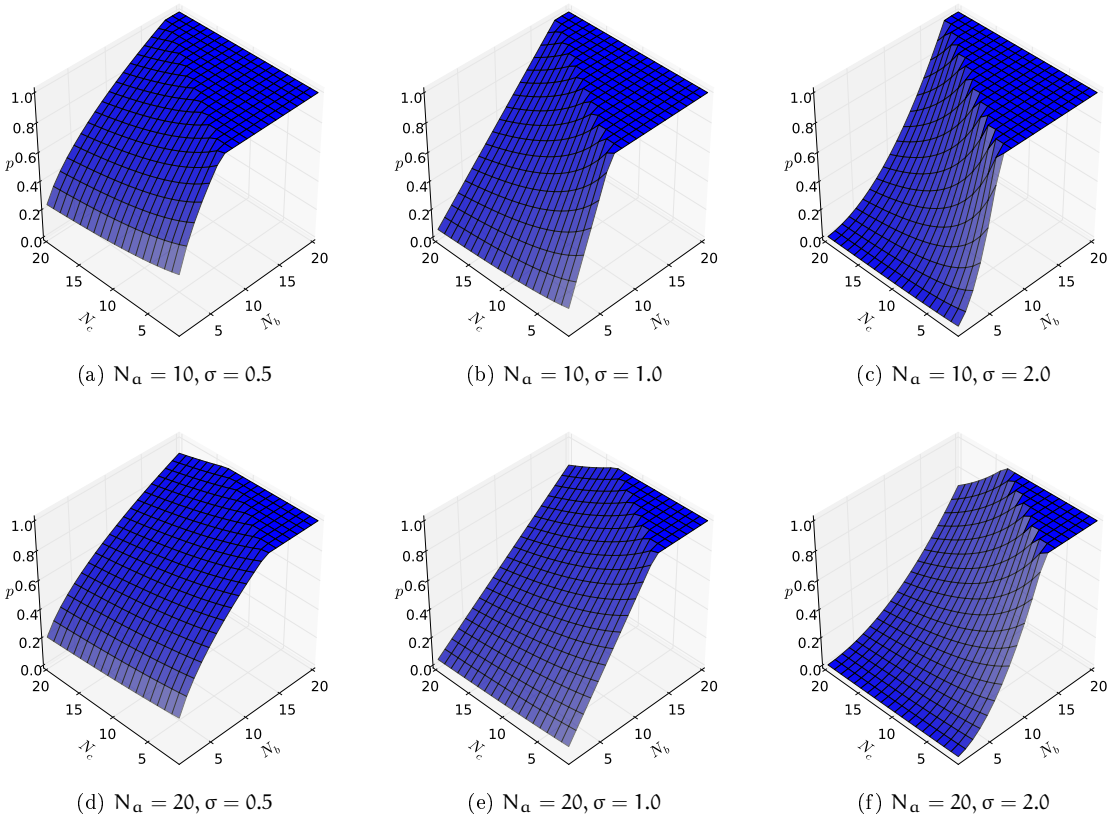
$$p = \frac{k}{n} \tag{4.5}$$

where $k \geq 1$ is a parameter to improve the reachability.

The *Border Retransmission Based Probabilistic Flooding* (BRBPF) scheme privileges nodes to forward packets that have a larger distance from the sender. As no positioning system is assumed, the receiver estimates the distance based on the number of common neighbors of both nodes:

$$\mu = \frac{N_b}{N_a + N_c} \tag{4.6}$$

N_b is the number of neighbors that are unique for the receiver, N_a is the number of neighbors unique for the sender, and N_c denotes the common neighbors. The forwarding probability is then calculated as



(a) $N_a = 10, \sigma = 0.5$ (b) $N_a = 10, \sigma = 1.0$ (c) $N_a = 10, \sigma = 2.0$

(d) $N_a = 20, \sigma = 0.5$ (e) $N_a = 20, \sigma = 1.0$ (f) $N_a = 20, \sigma = 2.0$

Figure 4.2: Examples for the gossip function of *Border Retransmission Based Probabilistic Flooding* where the sender has N_a unique neighbors, the receiver has N_b unique neighbors, both share N_c common neighbors, and the convexity coefficient σ.

follows:

$$p = \frac{A - \alpha}{M^{\sigma}} \mu^{\sigma} + \alpha \tag{4.7}$$

where A and α are used to bound the probability, σ is the convexity coefficient of the graph, and M is a constant representing the largest possible value for μ. The authors set $M = 0.601$ based on the numerical results in [109] (see also Section 3.5.4), $A = 1.0$, and $\alpha = 0.0$ in their experiments. The shape of the probability function is shown in Figure 4.2. The ratio between N_a and N_b has a strong influence on the steepness of the graph. If N_a (sender) has a high number of unique neighbors, the resulting probability p for N_b (receiver) will be very low.

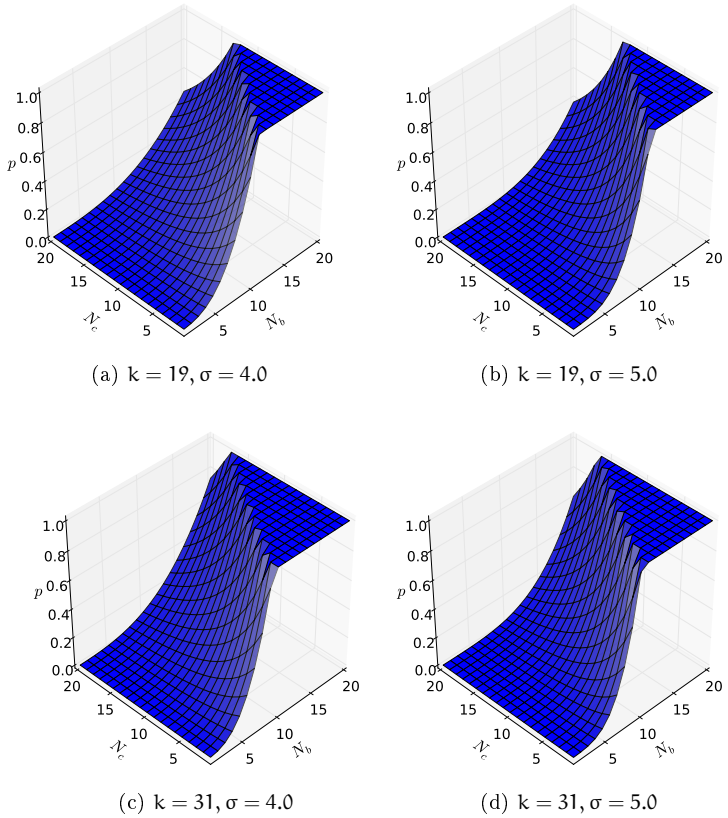
Density Aware and Border Node Retransmission Based Probabilistic Flooding (DABNRBPF) combines the ideas of the former two algorithms.

$$p = \frac{\frac{k}{n} - \alpha}{M^{\sigma}} \mu^{\sigma} + \alpha \tag{4.8}$$

A is replaced by the ratio of Equation 4.5. The probability function is shown in Figure 4.3 for the minimal and maximal values of σ and k that showed good results in their simulations. Both parameters have to be carefully tuned to the properties of the network, otherwise p may often have values close to 0.0 and 1.0.

Density Aware and Border Node Retransmission Based Probabilistic Flooding with Neighbor Elimination (DABNRBPFNE) is an extension of the former algorithm and is based on [95] (see also Section 3.5.5). It introduces a second chance to forward packets. When the packet is not forwarded because the random number is below the value calculated with Equation 4.8, the packet is stored. During the waiting time T, the node records which neighbors have forwarded the packet or which nodes are covered by the broadcasts of others. If any neighbors are not covered until the timeout, the packet is forwarded. The value of T is calculated as follows:

$$T = T_{min} + T_{max} \times x \tag{4.9}$$



(a) $k = 19, \sigma = 4.0$ (b) $k = 19, \sigma = 5.0$

(c) $k = 31, \sigma = 4.0$ (d) $k = 31, \sigma = 5.0$

Figure 4.3: Examples for the gossip function of *Density Aware and Border Node Retransmission Based Probabilistic Flooding* where the sender has $N_a = 20$ unique neighbors, the receiver has N_b unique neighbors, both share N_c common neighbors, and the convexity coefficient σ.

Parameter	Values
Simulation environment	ns-2
Nodes	25, 50, 75, 100, 125, 150, 175, 200
Area	2000×670 m^2
Average node degree	4, 7, 11, 15, 18, 22, 26, 30
Radio range	250 m
Mobility model	static network
Packets	500

Table 4.2: Experiment parameters of Cartigny et al.

T_{min} and T_{max} bound the waiting time and $x \in [0, 1]$ is randomly selected.

The algorithms were studied in simulations. The experiment parameters are listed in Table 4.2 but some are missing like the number and position of the sources and no radio model is mentioned. *Density Aware and Border Node Retransmission Based Probabilistic Flooding with Neighbor Elimination* showed the best performance regarding the reachability and reduction of unnecessary broadcasts. The results also show that the algorithm is capable to result in shorter paths as the nodes on the border of the transmission range have a higher probability to forward packets but the authors also mention that this might lead to problems in mobile networks. Unfortunately, the study does not provide confidence intervals or other measures for the variance and significance of the data.

4.3 Parametric Probabilistic Sensor Network Routing

Barret et al. propose several probabilistic *Parametric Probabilistic Sensor Network Routing Protocols* (PPSNRP) [25]. The first variant, called *Destination Attractor* (PPSNRP-DA), determines the

forwarding probability at the i-th node based on the distances between source S and destination D and the previous node n_{i-1} using the following function:

$$p_i = \begin{cases} (1+k)p_{i-1} & \text{moved closer to the destination} \\ (1-k)p_{i-1} & \text{moved further from the destination} \\ p_i & \text{same distance} \end{cases} \tag{4.10}$$

where k is some constant value to increase or decrease the probability and p_{i-1} is piggybacked in each packet by the previous node. The probability is adapted on each hop according to the direction the packet has taken: p_i increases when the packet approaches the destination and vice versa. This way, p_i simulates an attracting force. After specifying a recursive version, the final formula is specified by the authors as:

$$p_i = e^{k(\|SD\| - \|n_i D\|))} \tag{4.11}$$

where $\|xy\|$ is the hop distance between node x and y.

The second variant *Directed Transmission* (PPSNRP-DT) additionally considers the number of hops the packet has traveled from the source to the current node. All nodes that are on or close to the direct (and thus shortest) path get a higher forwarding probability. The general idea is to consider where the packet should be after i steps in the ideal case: If it is on the direct path, it should be i hops away from the source and $\|SD\| - i$ hops away from the destination.

$$p_i = e^{k(\|SD\| - \|n_i D\| - i))} \tag{4.12}$$

Due to their optimization based on topology information, *Destination Attractor* and *Directed Transmission* are suitable only for unicast transmission when such information is already available. The authors propose a light-weight distance estimation procedure that learns and spreads information based on received data packets.

Both introduced protocols are evaluated and compared to the performance of *flooding*, *pure gossip*[1], and three other protocols. The *Wanderer* protocol realizes a random walk on the network were packets are always forwarded to a random neighbor. Using *Shortest Path*, packets are forwarded only on the direct path from source to destination. The variant *Short Path* additionally considers that the topology information may be outdated or imprecise and thus the next hop is selected randomly from a group of neighbors that are closer to the destination. *Shortest Path Counting* is inspired by [110]. Each node n selects the next hop n_{i+1} based on the number of shortest paths (from source to destination) that the possible candidates are on:

$$p(n_i, n_{i+1}) = \begin{cases} \frac{x_{i+1}}{\sum x_j} & \text{if} \quad \|Dn_i\| \leq \|Sn_i\| \quad (n_i \text{ is closer to D}) \\ \frac{1/y_{i+1}}{\sum 1/y_i} & \text{if} \quad \|Dn_i\| > \|Sn_i\| \quad (n_i \text{ is closer to S}) \end{cases} \tag{4.13}$$

x is the number of shortest paths between D and the current node n_i, y is the number of shortest paths between S and n_i and the sum is calculated over all neighbors of n_i.

The simulations were run with 5000 uniformly distributed nodes in a unit-disc graph. The destination was positioned in the center while the source was selected randomly for each configuration. The effects of mobility and thus inaccurate information were modeled by random noise. Each value was distorted by a particular noise level, i.e., the value v was replaced by a uniform random number from $[v - v \times \text{noise}, v + v \times \text{noise}]$. An overview of the experiment parameters is shown in Table 4.3. The authors evaluated the results based on the fraction of delivered packets, the delay (called lag in the publication), and the number of packet transmissions. Directed transmission and destination attractors showed the best results.

4.4 Dynamic Probabilistic Broadcasting and Leveled Probabilistic Routing

Zhang and Agrawal [111] propose a probabilistic broadcasting scheme that uses a counter approach to reduce redundancy. Each duplicate is forwarded depending on the probability p that is adapted dynamically based on the number of received duplicates. Each duplicate reduces p by the constant d when more than N_c copies have been received. If no duplicates are received for time t and the packet counter has a value less than N_c, the probability is increased by the constant d_1. To limit the adaption,

[1] Pure gossip refers to gossip routing with the forwarding probability p as the only parameter.

Parameter	Values
Simulation environment	?
Nodes	5000
Area	?
Average node degree	≈ 6.7
Radio range	? (uniform)
Packets per pair	1000
Attractor factor k	0.001, 0.01, 0.022, 0.046, 0.1, 0.22, 0.46, 1.0, 10.0, 100.0
Gossip probability p	0.20, 0.25, 0.30, 0.35, 0.40, 0.425, 0.45, 0.475, 0.50, 0.55, 0.60, 0.70 0.80, 0.90
Maximum number of duplicate forwardings	0, 3, 10, 30, 100, 300, ∞
Noise levels [%]	0, 3, 10, 30, 100, 300

Table 4.3: Experiment parameters by Barret et al. The maximum number of *duplicate forwardings* refers to how many times duplicates of a packet are forwarded.

Algorithm 5 Dynamic Probabilistic Broadcasting

Require: received broadcast packet with a unique identifier id
  if id in $list_{rcvd}$ **then**
    if $count_{id} > N_c$ **then**
      $p = max(p - d, p_l)$
    end if
    $count_{id} = count_{id} + 1$
  else
    $count_{id} = 1$
    $list_{rcvd} \leftarrow id$
  end if
  forward packet with probability p
Require: Every time interval t
  for id in $list_{rcvd}$ **do**
    if no packet with id has been received within t **then**
      if $count_{id} < N_c$ **then**
        $p = min(p + d_1, p_u)$
      end if
      remove id from $list_{rcvd}$
    end if
  end for

p is bounded by an upper (p_u) and lower (p_l) value. The *Dynamic Probabilistic Broadcasting* (DPB) algorithm[2] is shown in Algorithm 5. The algorithm shall adapt the nodes' forwarding based on their node degrees and enable that an equilibrium is reached. The publication does not explicitly specify if the probability p is specific for each packet or if p is a shared value for different sources; we assume it is shared. The initial value of p is determined by the average node degree n_f (calculated as for the gossip variant in Section 4.11) as follows:

$$p = \begin{cases} 1, & \frac{6}{n_f} \geq 1 \\ \frac{6}{n_f}, & 0 < \frac{6}{n_f} < 1 \\ 0, & \frac{6}{n_f} \leq 0 \end{cases} \tag{4.14}$$

The constant 6 in the formula was chosen based on [94]. It is not further discussed if/how it should be adapted for particular network topologies, e.g., random networks.

Zhang and Agrawal measured the performance of their variant in a simulation environment. The discussed probabilistic broadcasting scheme was implemented as substitute of the flooding in the AODV

[2]The variable names and some statements have been modified to match the general format used in this technical report.

Parameter	Values
Simulation environment	GloMoSim
Nodes	$20, 40, 60, 80, 100$
Area	1000×1000
Average node degree	?
Radio range	250m
Packet rate	10/s, CBR
Simulation time	90s
Repetitions	10

Table 4.4: Experiment parameters by Zhang and Agrawal for DP-AODV. No information is provided about the number of connections or pairs of nodes that tried to establish routes.

protocol, called DP-AODV that stands for *AODV + dynamic probability*. For the evaluation, the results were compared with the original AODV and another variant called FP-AODV which used a fixed probability p. Unfortunately, the authors do not specify the used values of the parameters d, d_1, t, N_c, p_l, and p_u for DP-AODV and p for FP-AODV. In addition, it is left unclear how many nodes did actually sent data respectively how many route discoveries were run. Although the nodes are described as mobile, no mobility model is specified. The same applies for the radio model where only a radio range and data rate is provided. Therefore it can be assumed that the simulation was run on a unit-disc or similar graph. The know parameters are listed in Table 4.4.

The results of the study showed that FP-AODV outperformed the other two versions regarding redundancy, reachability, number of collisions[3], delay, and throughput. As there is no information whether the graphs show average or median, no confidence intervals are given, and the experiments were repeated only 10 times, some doubts about the improvements of FP-AODV over the other protocols remains. As the first N_c copies of a packet are forwarded with probability p and all further duplicates with a lower value, it can be expected that the redundancy is reduced compared to just forwarding all packets with probability p. In contrast, most other gossip routing variants in this chapter forward only one copy and should further reduce the redundancy. Therefore, based on the information, we would have suspected that AODV will forward less route requests than DP-AODV. The high number of collisions in AODV might be the reason.

In another publication [112], a second gossip routing variant is proposed. The *Leveled Probabilistic Routing* (LPR) algorithm calculates a connected but not minimal dominating set of nodes to forward the packets. The algorithm differentiates four groups of nodes[4]. The assignment to the groups is based on the average node degree (see Equation 5.1). The probability p_i for each node to have i neighbors in the considered network model is given by:

$$p_i = \binom{N-1}{i} (1-\alpha)^{N-1-i} \alpha^i \tag{4.15}$$

where N is the total number of nodes and α the area that each node can cover with its transmission[5]. Four different (forwarding) probabilities are specified for each of the four groups. Nodes that have no neighbor with a higher node degree than themselves belong to the first group and get probability p_1. Nodes that have no neighbor with lower node degree than themselves belong to the last group and get probability p_4. The second group is made up of nodes that have more neighbors with a higher node degree than neighbors with a lower node degree and get probability p_2. All remaining nodes are in the third group and get p_3. Thus the higher the node degree, the higher the forwarding probability ($p_1 > p_2 > p_3 > p_4$).

Simulations with LPR in AODV showed an 20% higher goodput compared to the original AODV. Three different sets of probabilities were used: LPRP-1, LPRP-2, LPRP-3. The parameters are listed in Table 4.5. Unfortunately, again no confidence intervals are given and a minimal speed of 0 sec was permitted for the used random waypoint model (see Section 5.1 regarding this remark).

[3] This metric actually lets suspect that some MAC protocol was used that is not specified in the article.

[4] An approach similar to *Enhance Adjusted Probabilistic* (EAP) as discussed in Section 4.11.

[5] Please note that the authors first of all discuss the probability p_i that a node belongs to a particular group and then assign forwarding probabilities for each group. p_i should not be confused with p_1, p_2, etc.

Parameter	Values
Simulation environment	GloMoSim
Nodes	100
Area	2000×2000
Average node degree	?
Radio range	377 m
MAC	IEEE 802.11
Packet rate	10/s, CBR
Packet size	512 byte
Simulation time	90 s
Repetitions	10
Probabilities	LPRP-1: $p_1 = 1.00, p_2 = 0.90, p_3 = 0.80, p_4 = 0.70$
	LPRP-2: $p_1 = 1.00, p_2 = 0.75, p_3 = 0.50, p_4 = 0.20$
	LPRP-3: $p_1 = 1.00, p_2 = 0.50, p_3 = 0.20, p_4 = 0.00$
Mobility model	Random waypoint with $0 - 25$ m/s

Table 4.5: Experiment parameters by Zhang and Agrawal for LPR.

4.5 Gossip-Based Ad Hoc Routing

Haas et al. studied four different gossip routing variants in regular and random networks [32, 33]. A summary of the experiment scenarios is shown in Table 4.6 and Table 4.7.

gossip1 [32, 33] is a slight variation based on simple gossiping. The parameter k specifies that for the first k hops the probability p is replaced by 1.0. This shall ensure that the gossiping does not terminate early on. Haas et al. evaluated the protocol in different topologies with a perfect MAC layer, i.e., no packets are lost. The links are additionally quasi dedicated media between two nodes and thus no multiple access protocol is required[6]. Simulations showed that depending on the particular scenario a probability $p \in [0.65, 0.86]$ is usually sufficient for all nodes to receive the packages from the source but the value of p can be decreased further if the node degree is increased. The source node's position had a strong influence on the fraction where the gossiping terminated early: it is larger for border nodes and lower for central nodes. The authors showed that there is a bimodal effect which was particularly pronounced in a random network with average node degree 8. k was set to 1 and 4 in the experiments but the effect of different values was not in the focus. *gossip1* is the basis for the next three variants.

gossip2 adds a second probability p_2 that is used when a node has fewer than n neighbors. This shall optimize the gossiping in networks with random topologies where the node degree varies. For example, in a grid topology all border nodes have a lower node degree than the others. Haas et al. argue that the neighborhood information can usually acquired without any additional overhead from other protocols that are run in parallel, e.g., a HELLO protocol. The variant showed slight improvements over *gossip1* with higher reachability for $p < 0.8$ and up to 13% less packets were sent.

gossip3 is an extension of *gossip1*. When a node would normally drop a packet because the random number if below p, the packet is stored instead. If fewer than m duplicates are received in a specified time, the packet is forwarded; otherwise it is finally discarded. This shall ensure that packets have a higher chance to be forwarded in regions with low node degrees. The value of the parameter m is configured statically for all nodes in the network and not adapted during runtime. Haas et al. observed the best improvements for $m = 1$ and that only 2% of the packets were sent after the timeout. Unfortunately, the value of the timeout is not specified by the authors. Overall *gossip3* performed as the best of all variants regarding the reachability and redundancy was therefore used to improve AODV. In AODV+G the flooding was replaced with *gossip3*. Simulations showed that while the packet delivery fraction, route length, and delay did not change, the routing load decreased by up to 5%. A bimodal behavior could be observed due to the mobility and congestion because the chance of packet losses was increased.

gossip4 introduces a zone model where each node has a zone of radius k' hops. When a node receives a packet for a destination which is in its zone, the packet is delivered as unicast. Besides this modification *gossip4* is the same as *gossip1*. The overall idea is inspired by the *zone routing protocol* (ZRP) [113] but showed limited advantages in large networks yet it performed better in small ones. Haas et al. do not

[6] The setup by Haas et al. is the same as in some of the other publications that are discussed in the section where unit-disc graphs or similar models are used.

explicitly specify how the zone is setup and managed and the corresponding overhead is not considered in their evaluations. The unicast protocol is not specified but we assume that the implementation is very close to ZRP which uses a proactive routing protocol in this case, e.g., OLSR. How packet losses inside the zone affect the performance is not specifically discussed. *gossip4* basically decreases the fraction of nodes that will forward packets by gossip routing between the source and destination. If N is the total number of nodes in the network, $N-2$ are candidates to forward the packets by gossip routing. In *gossip4* the value is decreased by the number of nodes inside the zone: $N-2-\frac{\pi \times k'^2}{A}$ where A is the total area and we assume a uniform deployment. Due to the routing protocol used in the zone and the unicast, *gossip4* is only applicable for route discovery and not for a network-wide signaling or other applications where there are multiple destinations.

Variant	Parameters	Nodes	Area [m^2]	Degree	k	Type	p_c
gossip1		20×50	–	3	4	regular	0.86
gossip1		20×50	–	4	4	regular	0.72
gossip1		20×50	–	6	4	regular	0.65
gossip1		1000	7500×3000	8	4	random	0.75*
gossip1		1200	7500×3000	10	4	random	0.65
gossip1		1000×1000	–	4	1	regular	0.65
gossip2	$p_2 = 1.00$, $n = 6$	1000	7500×3000	8	4	random	0.60*
gossip3	$m = 1$	1000	7500×3000	8	4	random	0.65*
gossip4	4-hop zone	1000	7500×3000	8	4	random	> 0.65*
gossip4	8-hop zone	1000	7500×3000	8	4	random	> 0.65*
gossip4	3-hop zone	100	?	13	1	random	> 0.65*
gossip3 in AODV+G	$m = 1$	150	3300×600	?	1	random	0.65
gossip3 in AODV+G	$m = 1$	150	1650×1200	?	1	random	≈ 0.50

Table 4.6: Experiment scenarios by Haas et al.: For each particular configuration the critical probability p_c is specified where the transition effect happened. The node degree value is an average when the network type is "random". The values marked with the *-Symbol have not been explicitly stated by the authors but have been deduced from their writing and the graphs. A question marks symbolizes unknown values. The last two rows represent the simulations in mobile networks with AODV+G; additional information is available in Table 4.7

.

Parameter	Values
Simulation environment	ns-2
Nodes	150
Area	1650×1200 , 3300×500
Average node degree	?
Radio range	250 m
MAC	IEEE 802.11
Packet rate	2/s
Packet size	512 byte
Simulation time	600s, start at 300s
Connections	30
Mobility model	Random waypoint with $1 - 20$ m/s

Table 4.7: Experiment parameters by Haas et al. for AODV+G

4.6 Gossip Routing in Wireless Mesh Networks

We studied multiple gossip routing protocol [37–39] in experiments in the DES-Testbed [39].

The most simple gossip routing variant was named *gossip0* based on the enumeration of Haas et al. and is an implementation of the simple gossip scheme where only the parameter p determines the forwarding.

gossip5 as a modification based on *gossip3*. Nodes forward stored packets after timeout when they did not receive a copy from all of its neighbors. Thus in contrast to *gossip3*, there is no fixed parameter m and the node degree of each node is considered. Higher reachability than with *gossip3* can be expected but also a larger number of sent packets. *gossip5* tends towards the ideas of the reliable broadcast protocols.

gossip10 is a modification of *gossip5*. In some situations it might be that a node receives a packet and forwards it immediately. In this case it is normally assumed that any neighbor has received it but it can also be lost due to interference. If the packet is lost on the first few hops or even when it is transmitted by the source, the gossiping terminates as no copies of the packet a left in the network. To resolve this issue, the number of received duplicates is counted for each forwarded packet and packets that are not forwarded but stored (as in *gossip5* and *gossip3*). When a copy is not received from all neighbors until a particular timeout, the packet is forwarded. Thus the node may actually sent the packet twice. High redundancy is expected from this variant but also high reachability.

The experiment parameters of the testbed based study are summarized shown in Table 4.8. Our focus was to research the reachability and redundancy that can be achieved in real world networks and if the gossip protocols, that have been previously only studied in simulations, showed some hidden issues. In the experiment scenarios, gossip routing was run as individual protocol and not as part of a routing protocol. *gossip1* to *gossip3* are the protocols specified in Section 4.5, *gossip6* is based on AGAR specified in Section 4.7, *gossip7* is based on PCBR specified in Section 4.9, *gossip8* is based on P-AODV specified in Section 4.10, and *gossip9* is based on DPR specified in Section 4.11. A bimodal effect and phase transition effect could be observed but these phenomenons depended on the position of the source node. We learned that 100% reachability was never achieved and that the average reachability was even lower. Especially the adaptive variants that relied on the node degree had problems as nodes that connected different building did rarely forward packets because of their low node degree. In [39], multiple sources sent packets at the same time and a dramatic decrease in the reachability could be observed even in best-case scenarios without any other data flows. Overall the results show that flooding and gossip routing can be a limiting factor for the performance of routing protocols.

4.7 Adaptive Gossip-based Ad Hoc Routing

The gossip routing protocol by Shi and Shen is called *Adaptive Gossip-based Ad Hoc Routing* (AGAR) [114] and is based on *gossip3*. The forwarding of stored packets after the timeout happened is slightly modified. While the packets in *gossip3* are always forwarded when fewer than m duplicates have been received, the following formula is used to determine whether the packet shall be sent:

$$\text{random}(0,1) \leq \frac{p}{d+1} \tag{4.16}$$

Parameter	Values
Number of Nodes	59, 105
Average node degree	8
Topology	random, static nodes
MAC	IEEE 802.11
Variants	gossip$\{0-3, 5-9\}$
Sources	$1, 10, 30, 50, 70, 90$
Packets per configuration	$100, 10000$
Packet rate	$1/s$
Probability p_2	1.0
Neighbor limit n	3
Duplicate limit m	1
Timeout	200 ms, 2 s
Flooding for k hops	1
T_{max}	100 ms
p_{min}, p_{max}	0.4, 0.9
n_f	4

Table 4.8: Parameters of the experiments in the DES-Testbed. Some parameters are only valid for particular variants. General parameters are in the upper section, individual ones are in the lower section.

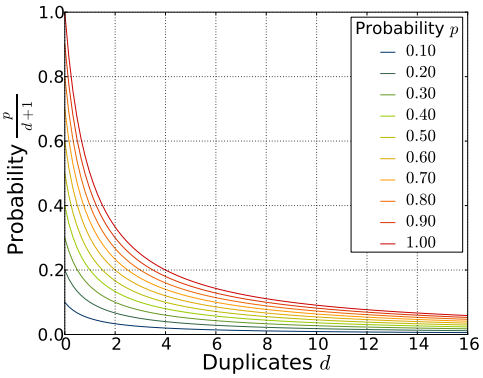


Figure 4.4: Gossip function of AGAR for the second chance to forward a packet. p is the pre-configured forwarding probability probability of the first chance.

where d is the number of received duplicates. The authors argue that this adaptive modification reduces flooding in networks with low node degree and that the second chance to forward packets is smoothly decreased. The forwarding probability is depicted as function of the received duplicates in Figure 4.4. As shown, the probability that a packet is forwarded after timeout is significantly reduced even when only 1 packet was received.

The experiment parameters are show in Table 4.9. Simulations with showed improvements over *gossip3* as AGAR reduced the routing load and end-to-end delay while the throughput is increased compared to AODV+G. The data differs only for some of the configurations and as no confidence intervals are given, a significant difference cannot be deduced. As the number or repetitions is low, the differences have a good chance to be caused by the small empirical data set.

4.8 Adjusted Probabilistic Flooding

Bani-Yassein et al. published a study [115, 116] that compared *flooding*, *fixed probabilistic flooding*, and *adjusted probabilistic flooding* (APF) in AODV. The algorithm of the latter protocol is shown in Algorithm 6. When the node degree is lower than the average degree ("typical of its surrounding environment" [115]) forwarding probability p_1 is used and otherwise p_2 where $p_1 > p_2$. Simulations were run with the parameters listed in Table 4.10. *Adjusted probabilistic flooding* saved the most broadcasts and had a reachability as good as flooding. Unfortunately, the graphs do not include any confidence intervals

Parameter	Values
Simulation environment	ns-2
Nodes	75
Area	2200×400 m^2
Average node degree	?
Radio range	250 m
MAC	IEEE 802.11
Packet rate	2/s
Packet size	512 byte
Simulation time	275 s
Connections	15
Repetitions	6
Mobility model	Random waypoint with $0-10$ m/s and pause time $0-250$ s

Table 4.9: Experiment parameters by Shi and Shen for AGAR

Algorithm 6 Adjusted Probabilistic Flooding

Require: received broadcast packet
Require: Average node degree $\overline{n}$, node degree n
  if $n < \overline{n}$ **then**
    $p = p_1$
  else
    $p = p_2$
  end if
  forward packet with probability p

and the description of the experiment scenarios is incomplete. For example, the number of sources or connections is missing and there is no is no information about the packet rate. The value of $\overline{n}$ is calculated in [116] with formula the formula shown in Equation 5.1 where $R = 0.8$. A reason for this value is not provided. Especially as the radio range is specified as 250 m and the area with 600×600 m^2, it does not fit.

4.9 Probabilistic Counter-based Route Discovery

Mohammed et al. propose two gossip routing variants [117–120]. In the *Efficient Counter-Based Scheme* (ECS) the received packets are always stored and the number of subsequently received duplicates is counted. Packets are forwarded after a *random assessment delay* (RAD) timer has expired and if not

Parameter	Values
Simulation environment	ns-2
Nodes	$25-100$
Area	600×600 m^2
Average node degree	?
Radio range	250 m
MAC	IEEE 802.11
Packet rate	?
Packet size	? byte
Simulation time	900 s
Connections	?
Repetitions	25
Mobility model	Random waypoint with $0-20$ m/s and pause time $0-40$ s

Table 4.10: Experiment parameters by Bani-Yassein et al. Note regarding the repetitions: The authors write that 25 mobility patterns were simulated.

Algorithm 7 ECS/PCBR-AODV

Require: received broadcast packet with identifier $\mathtt{id}$
  if $\mathtt{id}$ not in $\mathtt{list}_{\mathtt{rcvd}}$ **then**
    $\mathtt{count}_{\mathtt{id}} = 1$
    $\mathtt{list}_{\mathtt{rcvd}} \leftarrow \mathtt{id}$
    set RAD and wait for RAD to expire
    if $\mathtt{count}_{\mathtt{id}} \leq m$ **then**
      forward packet with probability p.
    else
      remove $\mathtt{id}$ from $\mathtt{list}_{\mathtt{rcvd}}$
      drop the corresponding packet
    end if
  else
    if $\mathtt{count}_{\mathtt{id}} \leq m$ **then**
      $\mathtt{count}_{\mathtt{id}} = \mathtt{count}_{\mathtt{id}} + 1$
      wait for RAD to expire
    else
      remove $\mathtt{id}$ from $\mathtt{list}_{\mathtt{rcvd}}$
      drop the corresponding packet
    end if
  end if

Parameter	Values
Simulation environment	ns-2
Nodes	$20 - 150$
Area	600×600
Average node degree	?
Radio range	100
MAC	IEEE 802.11
Packet rate	10/s
Packet size	512 byte
Simulation time	900s
Connections	10
Repetitions	30
Mobility model	Random waypoint $0 - 20$ m/s with steady state initialization
Duplicate limit m	4
T_{max}	0.01 s

Table 4.11: Experiment parameters by Mohammed et al. for ECS and ACBS

enough duplicates ($d \leq m$) were received. The RAD timer value is randomly selected from the interval $(0, T_{max}]$. The algorithm is shown as pseudo code in Algorithm 7. The approach is the same as in *gossip3* but that packets are always stored first and the initial k-hop flooding is missing. ECS was studied in simulation with the parameters in Table 4.11. Compared with *counter-based* and *fixed-probability* schemes[7] and flooding, ECS showed best results for reachability, number of packets, and latency.

The *Adjusted Counter-Based Broadcast Scheme* (ACBS) is an variant of ECS. Instead of dropping a packet when m copies are received, the packet is forwarded with probability $p_2 < p$ after the RAD timeout. The authors used (0.5, 0.25) and (0.65, 0.325) as parameters for (p, p_2) in simulations where the lower settings showed better performance. The parameters are the same as in Table 4.11 and the performance of ACBS was compared to ECS and the other three protocols from the previous study. ACBS show slightly better results than ECS.

ECS was integrated into AODV and called *Probabilistic Counter-based Route discovery* (PCBR) AODV and studied in simulations. The parameters are similar but not the same as in the previous studies; they are shown in Table 4.12. The performance of PCBR-AODV was compared with CB-AODV

[7] The authors do not provide specific information about these two schemes and their parameters in [117]. We assume that the parameters of all protocols were configured uniform.

Parameter	Values
Simulation environment	ns-2
Nodes	$20 - 200$
Area	1000×1000
Average node degree	?
Radio range	100
MAC	IEEE 802.11
Packet rate	4/s
Packet size	512 byte
Simulation time	900s
Connections	$1 - 35$
Repetitions	30
Mobility model	Random waypoint $0 - 5$ m/s
Duplicate limit m	3
T_{max}	0.01 s

Table 4.12: Experiment parameters by Mohammed et al. for PCBR-AODV

Algorithm 8 P-AODV

Require: received broadcast packet for the first time
Require: number of neighbors $n > 0$
  $p_{max} = 0.9$
  $p_{min} = 0.4$
  $p = \max(p_{max}(\frac{p_{max}^{n-1} - p_{max}^{n}}{1 - p_{max}}), p_{min})$
  if $random(0, 1) < p$ **then**
    forward packet
  end if

(*counter-based*), FP-AODV (*gossip-based*), and normal AODV. The routing overhead, collision rate, and throughput were improved by all variants compared to normal AODV. PCBR-AODV showed the best improvements but the end-to-end delay was increased. Unfortunately, the particular publication [120] provides still no detailed information about the parameters of CB-AODV, FP-AODV, and AODV.

4.10 P-AODV

Hanashi et al. propose P-AODV [121]. When a broadcast packet (AODV route request) is received for the first time by a node, the probability p to forward the packet is calculated based on the number of neighbors n. p has a high value when there are few neighbors and has a low value when the node degree is high but the value is bounded by p_{max} and p_{min}. A simplified representation of the original algorithm is shown in Algorithm 8. The approach is similar to *gossip2* by Haas et al. where a different but static probability p_2 is used when the node degree is low. The probability is shown as a function of the node degree in Figure 4.5 for a example values of of values p_{min} and p_{max}.

P-AODV was studied in simulation with the parameters in Table 4.13. The performance of the protocol is compared with AODV, AODV with fixed probability (FP-AODV), and adjusted probabilistic flooding (AD-AODV) (see Section 4.8 for the specification of FP-AODV and AD-AODV). While P-AODV showed the best results regarding throughput, latency, number of collisions, reachability, and number of broadcast packets, the authors give no information about the specific configuration of the other protocols and the graphs are lacking confidence intervals.

4.11 Adjusted Probabilistic, Enhance Adjusted Probabilistic and Dynamic Probabilistic Route Discovery

Jamal-Deen Abdulai continued the work by Mohammed et al. and is actually a co-author of some of the referenced publications. The *Adjusted Probabilistic* (AP) and *Enhance Adjusted Probabilistic* (EAP)

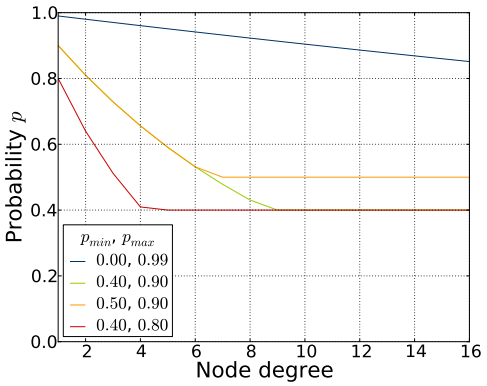


Figure 4.5: Examples for the gossip function of P-AODV. p_{min} and p_{max} are pre-configured parameters.

Parameter	Values
Simulation environment	GloMoSim
Nodes	80, 100
Area	600×600, 1000×1000
Average node degree	?
Radio range	250
MAC	IEEE 802.11
Packet rate	10/s
Packet size	512 byte
Simulation time	900 s
Connections	$10 - 40$
Repetitions	?
Mobility model	random waypoint $10 - 25$ m/s
p_{min}, p_{max}	0.4, 0.9

Table 4.13: Experiment parameters by Hanashi et al. for P-AODV

route discovery schemes are proposed in [122]. Both are of these are modifications to replace the flooding in AODV. AP is also called a *Two-P Scheme* as two groups are differentiated. Given the average node degree $\overline{n}$, when a node has degree $n \leq \overline{n}$ it forwards packets with probability p_1 and else uses p_2, where $p_1 < p_2$. In contrast, EAP is called a *Four-P Scheme* which, obviously, differentiates four groups. The authors created several random networks and determined the average node degrees. $\overline{\overline{n}}$ is the average of the average node degrees[8], while $\overline{n_{min}}$ and $\overline{n_{max}}$ are the minimum and maximum average node degrees respectively that were encountered. Based on the particular node degree, each node is in one of the four regions and uses a specific probability $p_1 > p_2 > p_3 > p_4$ to forward packets. The authors set $p = 0.7$ and calculated the four probabilities by

$$p_i = \frac{1}{i} p \tag{4.17}$$

For both schemes, AP and EAP, it is left unclear how the nodes get the required information about the total number of nodes in the network and the necessary values $\overline{n}$, $\overline{\overline{n}}$, $\overline{n_{min}}$, and $\overline{n_{max}}$. The algorithms are shown in Algorithm 10 and Algorithm 11. The authors also consider a *Three-P Scheme* in [123].

AP and EAP are evaluated in simulations and compared with AODV, FP-AODV, and gossip AODV (G-AODV) in [122][9]. The parameters are shown in Table 4.14; they do not differ much from the configuration in last sections. Like in Section 4.4, the authors state that the minimum speed in the random waypoint model was 0 m/s which could be a problem. The pause time for the model is not specified and it is unclear how many connections where established respectively how many nodes emitted route

[8] The authors use $\overline{n}$ as symbol and call it the average node degree. From their writing it has to be assumed, that they actually mean the average node degree of the average node degree of each of the random networks created with the same parameters.

[9] The authors do not explain the difference between G-AODV and FP-AODV and provide not helpful information where further information is available.

Algorithm 9 Dynamic Probabilistic Route Discovery (DPR). In this algorithm the variables n and n_c do not represent sets but the number of elements in the particular sets.

Require: received broadcast packet for the first time
  if $n \leq \overline{n}$ **then**
    $p = 1$
  else
    $p = 1 - e^{-\frac{n-n_c}{n}}$
  end if
  if $random(0,1) < p$ **then**
    forward packet
  end if

Algorithm 10 Adjusted Probabilistic Route Discovery (AP)

Require: received broadcast packet
Require: average node degree $\overline{n}$
  determine node degree n
  if $n \leq \overline{n}$ **then**
    $p = p_1$
  else
    $p = p_2$
  end if
  if $random(0,1) < p$ **then**
    forward packet
  end if

requests. EAP showed the best results with AP in second place regarding the routing overhead, number of collisions, network connectivity (reachability), and end-to-end delay but the graph provide no confidence intervals. Interestingly, the data shows that the reachability was very low ($< 50\%$) for small networks, reached a maximum for $100 - 150$ nodes, and then decreased monotonously due to collisions. The end-to-end delay shows an inverse behavior.

The *Two-P Scheme* (AP) and the *Three-P Scheme* where evaluated in [123] with the same simulation parameters and compared with AODV and FP-AODV. The *Three-P Scheme* showed the best results with the *Two-P Scheme* in second place. These results are not surprising, as more groups mean a more fine granular optimization of the forwarding probability to the network topology. This time the graphs include 95% confidence intervals that show that at least for some configurations and metrics the data differ significantly but for, e.g., the throughput there is only limited difference for the four protocols.

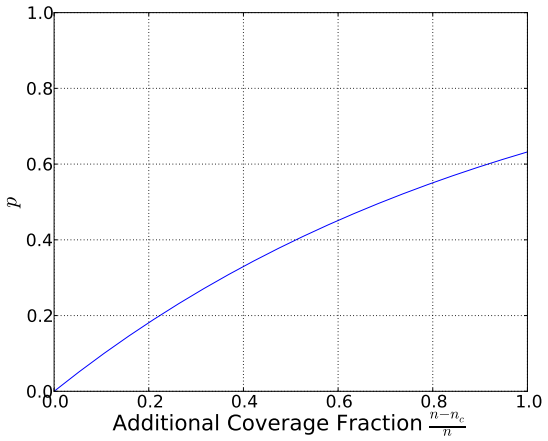
The last proposed AODV variant is *Dynamic Probabilistic Route Discovery* (DPR) [124]. When the node degree n is lower than or equal to $\overline{n}$, the algorithm results to flooding. The value $\overline{n}$ represents the average node degree in the network. When the node degree n is higher than $\overline{n}$, the additional coverage

Parameter	Values
Simulation environment	ns-2
Nodes	$25 - 300$
Area	1000×1000
Average node degree	?
Radio range	250 m
MAC	IEEE 802.11
Packet rate	4/s
Packet size	512 byte
Simulation time	900 s, started at 20 s
Connections	?
Repetitions	30
Mobility model	random waypoint $0 - 20$ m/s

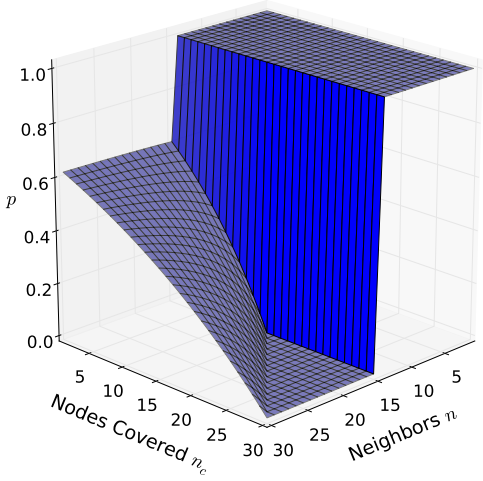
Table 4.14: Experiment parameters by Abdulai et al. for AP and EAP

Algorithm 11 Enhance Adjusted Probabilistic Route Discovery (EAP)

Require: received broadcast packet
Require: average node degree $\overline{\overline{n}}$, min. node degree $\overline{n_{min}}$, and max. node degree $\overline{n_{max}}$
  determine node degree n
  if $n \leq \overline{n_{min}}$ **then**
    $p = p_1$
  else if $\overline{n_{min}} < n \leq \overline{\overline{n}}$ **then**
    $p = p_2$
  else if $\overline{\overline{n}} < n \leq \overline{n_{max}}$ **then**
    $p = p_3$
  else
    $p = p_4$
  end if
  if $random(0,1) < p$ **then**
    forward packet
  end if



(a) DPR forwarding probability as a function of the additional coverage fraction $0.0 \leq \frac{n-n_c}{n} \leq 1.0$ for $n > \overline{n}$



(b) DPR forwarding probability as a function of the node degree n and the number of covered nodes n_c with $\overline{n} = 14$

Figure 4.6: DPR gossip function

that can be achieved by forwarding the packet determines the value of p. Each node includes a list of its neighbors in each forwarded (broadcast) packet. Upon reception of the packet, the nodes determines the set of their neighbors that (probably) have not yet received this packet based on the information. n_c is the set of neighbors that should have received the packet (covered nodes) and n is the set of neighbors of the receiver. If the set $n - n_c$ is empty, the node will not forward the packet; otherwise the larger the set, the higher the forwarding probability.

$$p = \begin{cases} 1 & , n \leq \overline{n} \\ 1 - e^{-\frac{n-n_c}{n}} & , n > \overline{n} \end{cases} \tag{4.18}$$

The approach is simple as it requires only 1-hop neighborhood information to apply self-pruning and is methodologically related to the location-based schemes discussed in Section 3.5.4. The algorithm is shown in Algorithm 9 and Figure 4.6 shows the forwarding probability function. If the number of neighbors is above $\overline{n}$, the forwarding probability p is bounded by 0 and 0.632.

DPR-AODV was evaluated in simulation and compared with self-pruning AODV (SP-AODV) based on [1], FP-AODV, and AODV. The simulation parameters are listed in Table 4.15. DPR-AODV performed best but was not directly compared with the X-*P Schemes*. There are several figures in the

Parameter	Values
Simulation environment	ns-2
Nodes	$25 - 225$
Area	1000×1000
Average node degree	?
Radio range	250 m*
MAC	IEEE 802.11*
Packet rate	4/s*
Packet size	512 byte*
Simulation time	900 s*
Connections	10
Repetitions	?
Mobility model	random waypoint $0 - 20$ m/s

Table 4.15: Experiment parameters by Abdulai et al. for DPR. The values that are marked with the * symbol are not explicitly stated in the DPR chapter in [124]. It is stated that the parameters are similar to the ones in the previous chapters.

Parameter	Values
Simulation environment	ns-2
Nodes	$25 - 225$
Area	1000×1000
Average node degree	?
Radio range	250 m*
MAC	IEEE 802.11*
Packet rate	4/s*
Packet size	512 byte*
Simulation time	900 s, started at 20 s
Connections	$1 - 35$
Repetitions	30
Mobility model	random waypoint $0 - 5$ m/s

Table 4.16: Experiment parameters by Abdulai et al. for DPR_2

appendix of [124] that include the AP variant and DPR where the former often showed the best results. The figures seem to be unreferenced in the main text and are thus not discussed.

Abdulai et al. did also introduce DPR in [125], yet the probability is calculated slightly different:

$$p = \begin{cases} \frac{n - n_c}{\overline{n}} & , n \leq \overline{n} \\ \frac{n - n_c}{n} & , n > \overline{n} \end{cases} \tag{4.19}$$

This formula does not result to flooding even when the node degree is very low and thus the achievable reachability should be lower than in the previous variant. Why DPR has been specified differently is unknown. We refer to it as DPR_2 in the following.

DPR_2 was evaluated in simulations and compared with AODV and FP-AODV[10] The parameters are shown in Table 4.16.

There are several open question after reviewing the publications by Abdulai et al. First of all, it is often unclear which parameter settings were used for the protocols in each of the simulation scenarios. For example, for the fixed probability variant FP-AODV there is no statement of the value. It might be that the authors used the same settings as in the referred publications. Second of all, as the experiment parameters differed from case to case, we have to be careful when comparing the results; especially as the experiment parameters are not always completely available or different terms are (supposable) used for the same protocols. As last, in some cases the authors used the end-to-end delay as metric while the route-discovery delay was used in others. Both could refer to the same data (time until a route reply arrives after a request was sent) but end-to-end, for example, could also include data packets.

[10]The authors actually call this version FPR-AODV that stands for *Fixed Probabilistic Route Discovery* (FPR) but from their writing it can be assumed to be the same as FP-AODV.

4.12 Discussion of the Studies on Gossip Routing

Getting a complete understanding of the experiments that were run by other research groups is a non-trivial task. We tried our best to extract the most important information from the discussed publication but some data is speculative: either the writing is confusing or different scenarios, terms, etc were used. Overall we can nevertheless state that there is a predominant simulation scenario. n nodes are randomly and uniformly deployed in a square or sometimes rectangle area (often 1000×1000 m^2). The radio model uses IEEE 802.11 for MAC, an uniform transmission range of 250 m, and the free-space model until some specific distance and then optionally the two-ray-ground model beyond this point. The physical layer was configured at 2 Mbps but no information is provided if this data rate applies to both unicast and broadcast frames. Rate adaptation algorithms were not used in the simulations or not named. The packet size of 512 byte seems to be standard and the packet rate varies between 4 and 10 packets per second. Mobility is simulated with random waypoint model where the nodes often move with up 25 m/s.

Surprisingly, we did not find any other testbed-based, i.e., real world based studies besides our own. ns-2 is the most used simulation environment and thus we assume that the most settings that are not explicitly stated are the default parameters of ns-2 or the available models.

We have learned that the discussed gossip routing protocols often apply the same approaches and ideas and that several protocols are just minor variations. Especially for the X-*P Schemes* in the Section 4.11 it is obvious that a more fine-granular optimization of the probabilistic forwarding will result in a higher performance. It should have become obvious, that gossip routing is not that far away from the ideas that were discussed in Chapter 3.

In the next chapter we will take a specific look at the assumptions of the discussed studies. We will also highlight which information is not readily available for the algorithms and has to be gathered in some way that introduces additional overhead in the protocols.

CHAPTER 5

Simulations and their Significance for Real World Networks

All studies, except our own testbed-based study, presented simulation based results. Therefore the specific scenarios and their effect on the results and significance for real world networks should be discussed as multi-hop networking differs in significant ways in the reality [126] from what is often assumed in theory [127]. We focus our discussion on the most common simulation scenario that was highlighted in Section 4.12.

5.1 Mobility Model

Most of the simulations tried to model a MANET where the mobility was based on the random waypoint model [128] that gained popularity during the advent of the research of MANETs. Each node randomly selects a destination in the considered simulation area and a particular velocity $v \in [0, v_{max}]$. The model has to be used very carefully as there are two major issues. First of all, the nodes tend to accumulate in the middle of the area after some time although they are initially uniformly distributed [129]. This is caused by the fact that when a node randomly choses its next destination, there is a higher probability that the direct way leads through the center than along the border. Second of all, as shown by Yoon et al. [130] the average speed decreases over the simulation time. When a node chooses a far away destination and a low speed, it might never reach the destination in simulation time or take a very long time until the next destination and speed are chosen. Over time all nodes might even get stationary, as zero is a valid speed in the original random waypoint model [131]. The average speed decrease problem is resolved, when the speed is limited to $v \in (0, v_{max}]$. Additionally, experiments should consider that the average speed of the mobile network converges only after some time and a *steady state* is reached. For example, Haas et al. started their AODV+G experiment after 300 seconds (see Section 4.5). Often there is no information in the publication about these issues and whether they have been considered.

5.2 Node Degree

The average node degree in a particular network can be approximated with the area of the network A, number of nodes N, transmission range R and the following formula:

$$\overline{n} = (N - 1)\frac{\pi R^2}{A} \tag{5.1}$$

In fact, several of the authors of the discussed protocols did refer to this formula. Unfortunately there are several problems that are based on fundamental assumptions about the network topology:

- The transmission ranges are not uniform in the real world
- Bidirectionality cannot be assumed
- The total number of nodes in the network is not known

- The node deployment is not uniform
- The area is not known

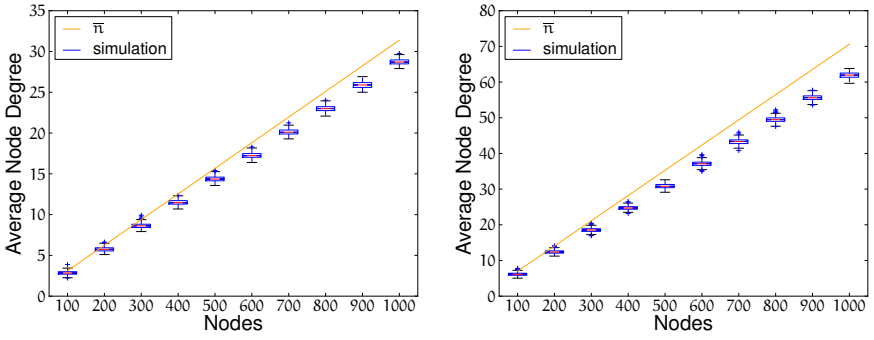
The total number of nodes has to be determined in some way. For example, it is available in proactive protocols like OLSR but not in the AODV routing protocol. Therefore more overhead is induced. The area is even more critical as it would either require localization based on GPS or some distributed localization algorithm. In both cases, network-wide communication is required. Even when the area can be determined based on the most distant nodes, this will only provide a rough approximation in some cases, as GPS will fail in indoor scenarios or in densely built residential area with high buildings. Real networks are also usually deployed over different floors and not just a two-dimensional space. Thus, the formula should be changed to compensate for this fact:

$$\overline{n} = (N-1)\frac{\frac{4}{3}\pi R^3}{A \times h} \tag{5.2}$$

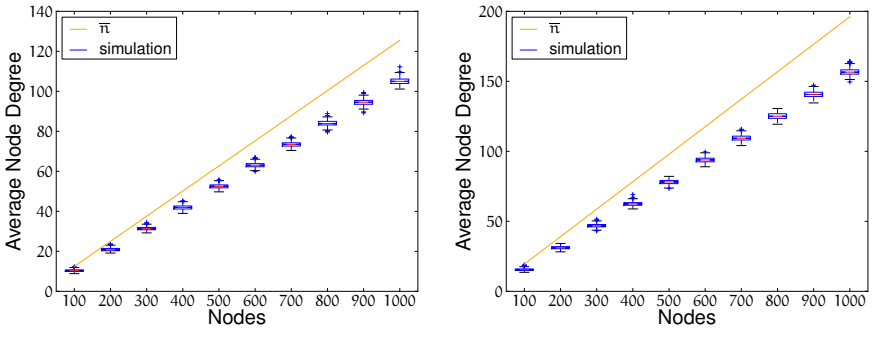
where h is the height or the volume where the nodes are deployed.

Nevertheless, the assumption that a network is uniformly deployed over a plane or a volume is (pretty) naive. As Milic and Malek [132–134] have shown in their empirical study of wireless mesh networks, the topology does not match the commonly used models. They argue that real world networks have a large number of bridges, i.e., nodes that connect subgraphs and are thus vital for the connectivity of the network. It can be expected that deployments of wireless sensor networks will also differ from the common network models. To some degree the mobility model might have counterbalanced the deviating node degree approximation. As discussed in Section 5.1, the nodes have a higher probability to be in the center of the area than to be at the border. The opposite might also be true: as the nodes accumulate in the middle, the formula will provide a value that is too low.

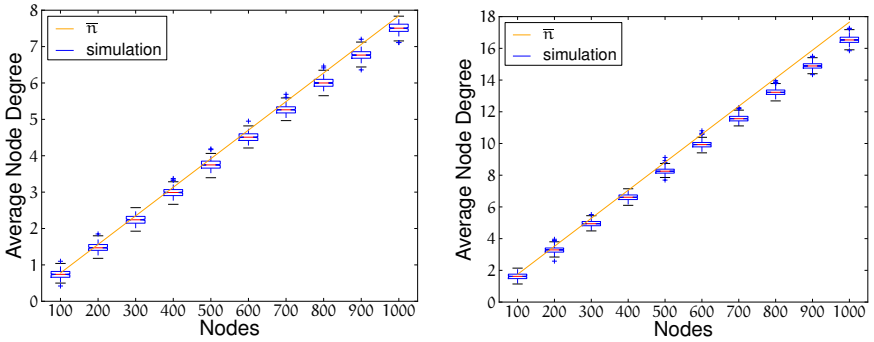
The approximation based on the formula differs even when we assume that all information is available and that the network model applies. Figure 5.1 shows the results from numerical simulations and the approximated average node degree. As we observe, the smaller the area and the larger the radio range the more both values differ. The explanation for these results is quite simple. The formula assumes disc-like radio propagation and that all of these discs cover a particular area. It is assumed that all nodes are uniformly distributed and that each disc covers more or less the same number of nodes. This assumption does not hold as the discs can protrude over the borders of the area, i.e., if a node has less distance to any border than the radio range. All of these particular discs contribute less to the average node degree.



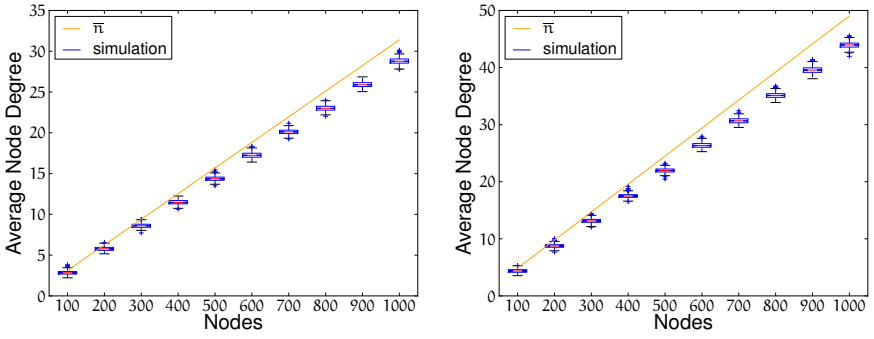
(a) radio range = 100 m, area = 10^6 m^2 (b) radio range = 150 m, area = 10^6 m^2



(c) radio range = 200 m, area = 10^6 m^2 (d) radio range = 250 m, area = 10^6 m^2



(e) radio range = 100 m, area = 40^6 m^2 (f) radio range = 150 m, area = 40^6 m^2



(g) radio range = 200 m, area = 40^6 m^2 (h) radio range = 250 m, area = 40^6 m^2

Figure 5.1: Comparison of the approximated and empirical average node degree. The average node degree is shown as a function of the number of nodes. Each box-and-whisker plot represents the average node degree from empirical data of 301 random graphs and the orange line shows the average node degree as calculated with Equation 5.1. The numerical simulation was run with the denoted radio ranges and areas.

5.3 Radio Ranges and Link Qualities

The *free-space* model and *two-ray-ground* models were used in most of the studies or a combination of them. Often the former model is used to model the communication between nodes up to a particular distance d_c from the sender and the latter model is used beyond this point. It is a common approach to use the lower value from both models.

The *free-space* model [135] is also called *free-space propagation* model and is defined as follows:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2} \tag{5.3}$$

where P_i is the transmission power of the transmitter t or the receive power at receiver r. G_i is the antenna gain, λ is the wavelength, and d is the distance between the two nodes. Sometimes an additional path loss coefficient L is included in the formula.

The *two-ray-ground* model that considers multi-path propagation (line of sight and reflection on the ground) is defined as follows:

$$P_r(d) = \frac{P_t G_t G_r {h_t}^2 {h_r}^2}{d^4} \tag{5.4}$$

where h_i is the height of the antenna.

Figure 5.2 shows an example with two different transmission power levels and two antenna heights. Depending on the configuration, we can see that d_c is at around $25.26\ m$ in one case and $101.03\ m$ in the other. The dashed horizontal line represents the minimum receive power/sensitivity for one of our transceivers in the DES-Testbed at $-89\ dBm$.

The *shadowing* model is a more advanced model and considers random processes that interfere with the communication. It is defined as follows:

$$\left[\frac{P_r(d_0)}{P_r(d)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) + X_{dB} \tag{5.5}$$

where X_{dB} is a normally distributed random variable with $\mu = 0$ and shadowing deviation σ_{dB} that depends on the environment and has to be empirically determined. β is the path loss that also depends on the environment, e.g., outdoor or indoor, free-space or obstructed. Overall, the model introduces some random effects and problems but it still has to be configured for a specific scenario. This could be the reason why it was not used for the discussed studies. Even for outdoor scenarios it is hard to provide good parameters as there can be line of sight or multi-path propagation links with or without obstacles that attenuate the signal, e.g., trees, walls, or groups of people.

All of these models are only able to describe some characteristics of wireless networks. Most importantly, asymmetric and unidirectional links do not exist. In the first two models the distance determines if a communication is possible. Although there is a random variable in the shadowing model, it will only effect that communication between two particular nodes (within communication range) is (only) impossible for a particular time respectively for a single packet. The random variable cannot model persistent unidirectional and asymmetric links that are common in wireless multi-hop networks as we have seen [39].

The interference range is also only modeled in an abstract way. If two nodes n_a and n_b have a distance d and $P_r(d)$ is below the reception sensitivity, i.e., the signal cannot be detected anymore, then both nodes are within interference range. When they have an even larger distance, it might happen that they are actually out of their carrier sense range. For example, in ns-2 different values can be configured for the carrier sensing threshold `CSThresh_` and the receiver signal threshold `RXThresh_` . If n_a and n_b are within interference range, both nodes could sent at the same time when they wait for the same number of slots or both nodes could sent at the same time, when they are out of carrier sensing range. In both cases there are two simultaneous transmissions that interfere. Of course this can happen multiple times when there are many nodes in an area. It is a common approach in simulations to consider only the strongest interfering signal to determine if a transmission succeeds: easier to compute but unrealistic. The cumulative interference should be considered to get a more realistic model where the signal to noise ratio is more reliable [136]. In this extended model more communications will fail due to the increased noise level. There are very limited information in the discussed publications about the radio and channel models and we have to assume that they are only realized in a very abstract way[1]. When the authors

[1] We acknowledge that there is a page limit for conference papers and journal articles and the information could have been omitted intentionally. Nevertheless, this information is critical for the assessment of the simulation.

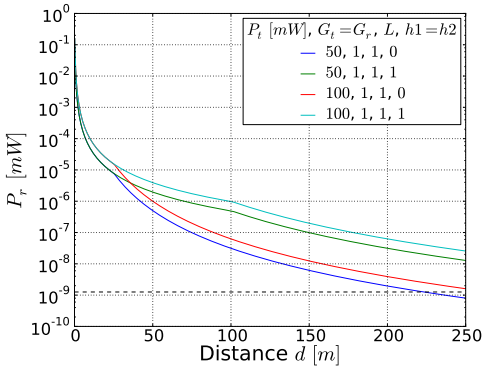


Figure 5.2: Receive power based on the free-space and two-ray-ground models

state that they limited the radio range to, e.g., 250 m we can calculate the reception sensitivity when P_t is provided but we do not known anything about the carrier sensing range or what interference model was used. Most notably, there are no gossip routing studies where the reachability decreased significantly due to interference. Some authors reported that the reachability decreased due to collisions, e.g., in Section 4.11 but they did not specify what they considered as a collision: simultaneous transmissions of nodes within transmission range due to chance or (also) failed transmissions due to decreased signal to noise ratios.

Chin et al. discuss in [137] that transient links are common in real world networks. These long range but low quality links have serious effects on all routing protocols that rely on a hop count metric. This applies to the protocols (AODV in most cases) that were used in the discussed studies. The shorter route is preferred once it is found and kept for a significant time in the routing table/cache. Only when sufficiently many packets are lost, the particular next hop entry in the routing table of a router is deleted; yet this does not fully solve the problem. Due to the transient link property, the link might disappear and reappear after some time starting the whole process again. A blacklist, e.g., like in the DSR protocol [11] can optimize the routing but is not applicable in mobile networks with a continuously changing topology. Hop-count is a suboptimal metric for wireless networks and Chin et al. propose a signal based route selection similar to what was discussed by Dube et al. in 1997 [138]. Therefore under real world conditions we have to expect that the results from the simulation will not hold.

One specific information is missing in most publications that can have a significant influence on the performance of the routing: the number of data link layer retransmissions. We have to assume that the authors used common values like $7 - 9$ retransmissions for the IEEE 802.11 MAC but this can be configured as desired. Combined with the abstract modeling of the wireless medium, the retransmissions will, without a doubt, make the network seem even more reliable. While this is also the case in real world networks, rate adaption schemes are often applied that configure a particular data rate based on the link quality. There are also implementations for simulation environments [139, 140] but most discussed publications state a fixed data rate of 2 Mbps[2]. We are unsure if this data rate applies to unicast, broadcasts, or both. In real world IEEE 802.11 networks, broadcast frames are always send with lower data rates than unicast frames as we introduced in Section 1.2. If the broadcasts are also sent with 2 Mbps in the simulations (instead of 1 Mbps), then the extended time that these frames take on the medium is not accurately modeled. Therefore we notice that there are further differences that may have a potential influence on the results.

Based on the discussed issues, we have to assume that routing protocols will probably have to run a larger number of route discoveries in real world networks and thus more packets than expected are flooded over the network. How and if the improved flooding schemes perform and scale under these conditions is (still) up for research. We have to add that there are several more advanced models. Alternatively, ray-tracing [141] can be used to get a very realistic simulation of the radio propagation in outdoor and indoor scenarios. Although these alternatives are very sophisticated, they often require too much computational resources to be viable for larger studies. In the end we have to come to the conclusion that there is (probably) little experience with flooding and gossip routing in real world like scenarios. The published results might not hold in networks that do not comply with the assumptions that the simulation models are based on.

[2]We have to remark, that different data rates will of course only make sense, when the properties of different physical layers/modulation schemes are appropriately modeled.

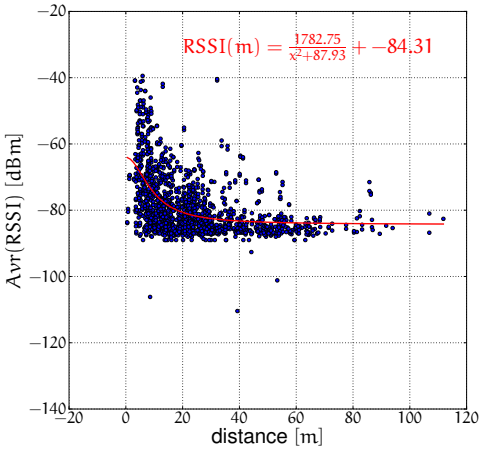


Figure 5.3: RSSI as function of the distance measured in the DES-Testbed with HELLO packets. The red line represents the fitted function shown in the upper region. The receiver has a documented receive sensitivity of -89 dBm. As the IEEE standard only requires that a particular ratio of the frames have to be successfully received at the receive limit, frames with lower RSSI may be received nevertheless.

5.4 Distances

The distance is required for some of the discussed schemes. When GPS is not available like in common indoor scenarios, the authors often propose *received signal strength indicator* (RSSI) values as a measure of distance. While the formulas from the previous section enable to calculate the distance based on the receive power P_r and the transmit power P_t, some facts have to be considered. First of all, RSSI was never meant to be used for such an application of IEEE 802.11 network cards. The original task was to detect when the RSSI value drops below a particular threshold so that a station can establish a link with another access point to achieve a soft hand over. The granularity and reliability of the RSSI values are driver and hardware dependent and distance measurements can exhibit significant errors [142,143].

Due to non free-space propagation and the experienced attenuation, there are already errors in outdoor scenarios. As we have measured in the DES-Testbed which is mostly deployed indoors, distance measurements in buildings are even more non-deterministic. Figure 5.3 shows the measured RSSI values for all links as a function of the distance. As depicted, there is a large interval of matching distances especially for low RSSI values. The authors of the discussed publications assumed that the distance measurements are mostly accurate but if the proposed algorithms are applicable and show the same improvements in comparison to flooding when the positions contain an error is not elaborated.

5.5 Scenario

The overall scenario, where a specific number of nodes are deployed over a rectangular area, is also an important point for discussion. Even when we consider the common scenario with about 1000×1000 m^2 and a radio range of $R = 250$ m as real world like, there is a problem with this configuration. When we run a simple numerical simulation and deploy two nodes randomly in a square area where the position is selected from a uniform distribution, we can evaluate the probability that these two nodes are already in radio range. The results from 1.000.000 repetitions are shown in Figure 5.4. As we can see, the probability that two randomly deployed nodes can communicate is relatively high: about 15%. When more nodes are added, the graph rapidly grows dense which results in a small network diameter and a low number of hops for the average shortest paths. Figure 5.5 shows that while the diameter can be larger than 10 hops in the considered scenarios[3], the average distance is much shorter. For the common scenario there are only 3 hops on average between the nodes. When we consider the fact that the nodes accumulate in the middle of the area when the random waypoint model is used (see Section 5.1), the true average shortest path is even lower during the experiment. We simulated only two-dimensional deployments as they were used for the simulation based gossip routing studies in Chapter 4. For three-dimensional deployments lower node degrees, higher diameters, and a larger average shortest path can be expected. Unfortunately,

[3]Please note that because only the largest component is evaluated for non-connected graphs, the diameter can be quite large as the graph will often form a chain-like topology.

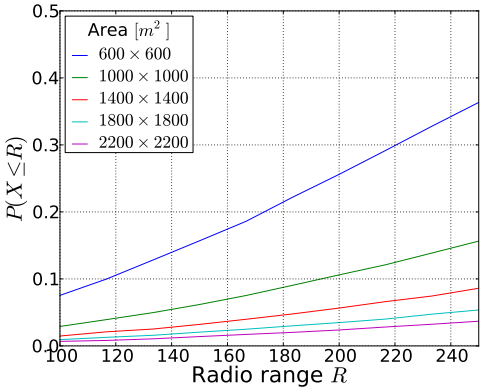
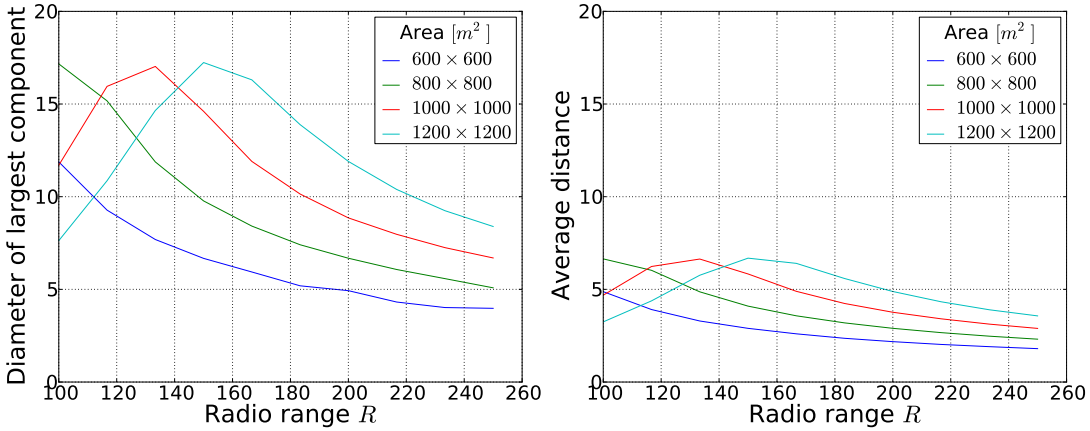


Figure 5.4: Probability that two nodes are within radio range R. The nodes are 1.000.000 times randomly deployed in a square area.



(a) Average diameter

(b) Average shortest path

Figure 5.5: Diameter and average shortest path in random graphs. 100 nodes are randomly deployed. If the graph is not connected, the largest component is evaluated. 1000 random graphs are evaluated for each configuration.

accurate simulation of radio propagation between different floors is even more complex due to the antenna characteristics.

As discussed in Section 2.1.2 and Section 5.2, random graphs have node degrees and topologies that will often differ from real networks. The studies in Chapter 4 and the proposed protocols in Chapter 3 are focused on mobile networks (MANETs in general) in a restricted space. If the scenarios are representative for the movement patterns of humans with communication devices is questionable but it might fit for some other entities. Nevertheless, for "normal" mobile networks deviating patterns with time variant differences and particular spatial distributions of nodes there is little experience with gossip routing.

The packet size, if stated, was fixed at 512 bytes and the packet rate was at $2-10$ packets per second. From the publications we are not sure in all cases, if the rates actually refer to the generation of application layer data. In our testbed-based experiments, they refer only to the rate of the flooded broadcasts but we assume that in the AODV based simulations, the application layer data is meant. While a *constant bit rate* (CBR) application layer data rate of $1-5$ kbyte is not entirely unrealistic, it is fairly low for many common application scenarios. In real world networks we expect, that the rate will be much higher and show bursts instead of CBRs. While our assumption is up for discussion, we nevertheless can assume that the simulated networks were not fully congested and that even local congestions were rare. There are only few packets per time unit, which means that the chance of collisions is low and few noise is contributed from the transmissions. Only a few authors explicitly considered the influence of congestion [32, 33, 105]. Congestions, i.e., full queues of the routers will inevitably have a negative effect on the delivery ratios as well as the noise level in the network. Based on our preliminary results [39] we expect that few broadcasts already have such an effect.

5.6 Recapitulation

As we have discussed, the simulation scenarios and the models differ in many ways from the properties of real networks. Simulations cannot be as complex and cannot model everything but we have to remark that the chances for these simulation based results to hold in a testbed are quite small. It is up to research if the proposed schemes can actually be realized at all and if the proposed solutions will actually show significant different results. Maybe there is little difference between the approaches. If flooding is able to provide a reliable data dissemination to begin with is an important question.

CHAPTER 6

Review and Classification

As discussed in Chapter 4, many gossip routing protocols apply the same techniques and require the same information. In this chapter we derive common properties for the review and classification of the protocols. After a brief description, the results are shown in Table 6.1, Table 6.3, and Table 6.4. Our review and classification is based on the publications of Kouvatsos et al. [88] and Williams et al. [105] but also includes a more fine-granular consideration of the available and required information, the assumptions, and interdependencies.

6.1 Properties

The following sections describe properties of the the gossip routing protocols. They are also metrics for the review.

6.1.1 Required Information

Required information is gathered and updated during runtime by the nodes either by a HELLO protocol or network-wide dissemination. Some of the following information can be pre-configured for all nodes but as soon as the network topology changes, updates are required to achieve a better performance. The results are listed in Table 6.1.

Average Node Degree

The average node degree $\overline{n}$ is an important value in some protocols as it has a direct effect on the forwarding probability. When the node's degree is below $\overline{n}$, the packet can be handled differently as when the node is in an area of high density respectively high node degree.

Neighbors

The number of neighbors in 1 or $2-\mathsf{hop}$ distance can serve different purposes. Either the node degree is required to adapt the forwarding probability or the information is applied to calculate the additional coverage that can be achieved (see Section 3.5.4). Further on, the flooding can be reduced when a subset of the 1-hop neighbors is selected to forward packets (see Section 3.5.2).

We notice that there are two fundamental different approaches that consider the number of neighbors. Either a high node degree shall result in a lower forwarding probability (like in DAPF or P-AODV) as there are many other potential forwarders or a high node degree shall result in a high forwarding probability as many nodes will receive the packet (like in the protocols that consider the additional coverage). In the adaptive counter-based scheme that was discussed in Section 3.5.4, the forwarding probability is the highest for a particular degree and lower for deviating values.

Area

The area refers to the spatial deployment of the nodes. As we discussed in Chapter 5, it is commonly a rectangular space where the nodes are initially deployed and then may move as specified by a mobility model. The deployment area property does also fit into Section 6.1.3 as it can remain static during

runtime. For mobile networks it is nevertheless important to get an update because the probability of all nodes to be near the center or near the border is not equal (see Section 5.1). The area is most often required to determine the average node degree in the network as specified in Equation 5.1.

Number of Nodes

Together with the area the number of nodes is required to calculate the average node degree based on the (uniform) radio ranges of the nodes. It can be learned when all nodes periodically flood packets over the network, e.g., to disseminate routing information like in the OLSR or B.A.T.M.A.N. routing protocols. The approach therefore induces additional costs due to an increased number of packets. Ironically, to advertise the presence of all routers to get an accurate estimate of the total number of nodes, this information should not be gossiped but flooded. None of the protocols that require the number of nodes did consider if the particular algorithm scales when only an estimate is available.

Distances

The distance between the sender and receiver can be used as metric to determine if the packet shall be forwarded. When the distance is large we can expect that a large additional coverage can be achieved by forwarding. A uniform deployment or at least a topology with an average node degree that has a low standard deviation is assumed in this case. Tseng et al. refer to this approach as *distance-based* schemes (see Section 3.5.4). Distances are measured either based on the locations or by other (inaccurate) means like RSSI values. None of the protocols that require the distances did consider if the particular algorithm shows a graceful degradation when only an estimate is available.

Locations

Relative or absolute locations can be used to optimize the flooding: either by a directed flooding towards the source or to derive the distance between two nodes (see previous section). Directed flooding is of course only applicable for unicast as it has a specific destination. Position information are usually provided by GPS. Protocols that combined improved flooding schemes with localization algorithms were not found.

Coverage

The additional coverage that can be achieved was already introduced in Chapter 3 and applied by some protocols in Chapter 4. It is a meta information that is either derived from the neighborhood discovery or the distances/positions between sender and receiver. In the latter case a uniform deployment has to be assumed whereas in the former case the network can have any distribution. Tseng et al. refer to this approach as *location-based* scheme (see Section 3.5.4).

Duplicates

Counter-based schemes (see Section 3.5.4) count the number of received duplicates for each packet. In most cases the duplicate count is compared to a specific pre-configured threshold or to the node degree to determine if a forwarding is required and/or to adapt the forwarding probability. *Counter-based* conditions can be problematic as each gossip routing protocol tries to minimize the number of forwarded packets. When one copy is expected to be received from each neighbor, the protocol resorts to flooding. In contrast, when a threshold is used, it has to be selected with a specific network model respectively an average node degree in mind. Too low values cannot ensure high reachability while too high values will again result in flooding. Nevertheless, this approach will not introduce additional costs and can therefore be integrated in any gossip routing protocol. Only in WSNs where energy is sparse, the reception of duplicates will be problematic as receiving requires significant energy due to the amplification of the signal.

Protocol	Average Node Degree	Neighbors	Area	Number of Nodes	Distances	Location	Coverage	Hops	Duplicates
RGR						•			
DAPF		1-hop							
BRBPF		2-hop					•		
DABNRBPF		2-hop					•		
DABNRBPFNE		2-hop					•		•
PPSNRP-DA					•	•			
PPSNRP-DT					•	•		•	
DPB									•
LPR		2-hop		•					
gossip0									
gossip1								•	
gossip2		1-hop						•	
gossip3								•	•
gossip4		k-hop						•	
gossip5		1-hop						•	•
gossip10		1-hop						•	•
AGAR								•	•
APF	•	1-hop	•	•					
ECS									•
ACBS									•
P-AODV		1-hop							
AP, EAP, Three-P	•	1-hop	•	•					
DRP, DRP_2	•	2-hop	•	•			•		

Table 6.1: Gossip protocol review – required information. Required information is marked by the • symbol. The protocol names/acronyms refer to Chapter 4. PPSNRP-DA and PPSNRP-DT can technically use location or distance information, e.g., number of hops.

Protocol	Unicast	Broadcast
RGR	•	
DAPF	•	•
BRBPF	•	•
DABNRBPF	•	•
DABNRBPFNE	•	•
PPSNRP-DA	•	
PPSNRP-DT	•	
DPB	•	•
LPR	•	•
gossip0	•	•
gossip1	•	•
gossip2	•	•
gossip3	•	•
gossip4	•	
gossip5	•	•
gossip10	•	•
AGAR	•	•
APF	•	•
ECS	•	•
ACBS	•	•
P-AODV	•	•
AP, EAP, Three-P	•	•
DRP, DRP_2	•	•

Table 6.2: Gossip protocol review – supported packet types. The • symbol marks the supported types of packets. The protocol names/acronyms refer to Chapter 4.

6.1.2 Supported Packet Types

Depending on the protocol and applied scheme, it is possible that not all types of packets can be transferred. Most of the proposed protocols shall be a replacement for flooding but the flooded packet can either be a broadcast or a unicast. A common example for the former case is a service discovery message that is sent to all nodes in the network[1]. Another fitting example is the dissemination of routing information by proactive routing protocols. In contrast, unicast packets are flooded by reactive routing protocols for their route discovery. The results of the review are available in Table 6.2.

6.1.3 Pre-configured Information

Pre-configured information refers to values that are statically configured. Particular information about the network topology has to be available a priori and/or particular assumptions have to hold at runtime so that the parametrization can be selected in an optimal way. The results are shown in Table 6.3

Forwarding Probability

The *forwarding probability* p is the best example for pre-configured information. As we have introduced in Section 2.1, depending on the node degree respectably the general network/percolation model, reception of all packets by most nodes from a specific destination can be assumed when $p \geq p_c$. It therefore has to be selected appropriately or an adaptive scheme has to be applied that considers particular network properties.

[1] We assume anycast addressing is not available like in IPv4 [144]

Probability Bounds

In some protocols the forwarding probability is bounded by a minimum and maximum value. This way it can be ensured that the packet will have a particular minimal chance to be forwarded while the upper bound will effect a reduction of the number of forwarded packets.

Initial Flooding

The *initial flooding* for k-hops that is applied to ensure that the gossiping does not terminate on the first hops has to be pre-configured; or at least none of the proposed protocols uses an adaptive variant. The value has to be either determined empirically or a specific network model has to be assumed, e.g., random uniform deployment with uniform radio ranges. Only this way, k can be optimized to reduce the flooding while ensuring a high reachability. The initial flooding approach does not consider the node degree of the source. Therefore when the degree is high, a large number of packets will be forwarded by the 1-hop neighbors which might result in collisions or increased noise levels. The same issue applies transitively for all $k-hop$ neighbors. In contrast, if the node degree of the source or around the source is low, no special schemes like retransmissions to ensure the reception are applied. It is a completely static approach.

Node Degree Classes

The probabilistic forwarding can be adapted based on the node degree. This is a more refined scheme as in addition to the node degree and the average node degree information that are required, multiple thresholds that assign nodes to particular classes have to be specified. The information base for the thresholds can be pre-configured but could also be based on an (adaptive) algorithm at run time. In the latter case, the node degree class approach would also belong into Table 6.1.

Timeouts

Timeouts are static in the discussed protocols or randomly selected from a static interval $[0, T_{max}]$. They are usually applied to wait for duplicate receptions after the first copy has been received. The timeouts on a per node basis can have a significant influence on the end-to-end delay between source and destination(-s). Surprisingly, none of the introduced protocols are based on the current network state.

Zone Radius and Ellipse Factor

Hybrid approaches can be applied where gossip routing is only used for, e.g., reactive route discovery when the packet is still afar from the destination. Once it enters a zone of k-hops around the destination unicast delivery based on proactive routing information can be used to route the packet.

As in one of the discussed protocols, an ellipse around the source and destination can be calculated to bound the forwarding of the packets to the area that is covered by the ellipse.

Both of these approaches imply that only unicast transmission is supported. For the ellipse approach, all nodes additionally require location information.

Duplicate Threshold

The number of received duplicates is an integral part of counter-based approaches (see Section 3.5.4). The general assumption is that the forwarding of the packet is not required when many neighbors have already forwarded it. A specific threshold $m \in [1, N-1]$ can be used to specify a condition that is often evaluated after a timeout happened.

Protocol	Forwarding Probability	Probability Bounds	Initial Flooding	Node Degree Classes	Timeouts	Zone Radius, Ellipse Factor	Duplicate Threshold
RGR	•		•			•	
DAPF							
BRBPF		•					
DABNRBPF		•					
DABNRBPFNE		•			•		
PPSNRP-DA							
PPSNRP-DT							
DPB		•			•		•
LPR	•		•				
gossip0	•		•				
gossip1	•		•				
gossip2	•		•				
gossip3	•		•		•		•
gossip4	•		•			•	
gossip5	•		•		•		
gossip10	•		•		•		
AGAR	•		•		•		•
APF	•						
ECS	•				•		•
ACBS	•				•		•
P-AODV		•					
AP	•						
EAP, Three-P	•			•			
DRP, DRP_2							

Table 6.3: Gossip protocol review – pre-configured information. Pre-configured information is marked by the • symbol. The protocol names/acronyms refer to Chapter 4. Timeouts may refer to a fixed or alternatively maximum value that is used to select a random timeout.

6.1.4 Assumptions

The discussed protocols have been specified for particular network models. Thus specific assumptions must hold so that an optimal performance can be expected. A universally applicable protocol would have no assumptions but that does not imply, that it performs optimal in any scenario. The assumptions of the protocols are listed in Table 6.4.

Deployment

Most protocols assume a random uniform deployment of all nodes in a specific area. Even when a mobility model is used, a steady state scenario is assumed where the properties of the network do not change. Some protocols consider variation of the node degrees and apply specific approaches in high or low density regions. Nevertheless, none of them addressed gossip routing in network topologies as discussed by Milic and Malek (see Section 5.2).

We consider that a protocol that requires a uniform deployment with a mostly homogeneous density will perform poorly if this assumption is not met. Therefore a graceful degradation of the performance cannot be expected. If this assessment holds can only be evaluated in further studies.

Radio Ranges

While most simulation based studies used uniform radio ranges, they are not necessary required to use some of the gossip routing protocols. Most notably, all protocols that require an approximation of the average node degree assume unit-disk graphs.

We assume that a protocol that requires a uniform radio range will perform poorly if this assumption is not met. Therefore a graceful degradation of the performance cannot be expected. Non-uniform radio ranges can result in unidirectional links and have an immediate effect on the neighbor discovery. The AODV RFC [12] specifies a very simple discovery procedure were nodes are accepted as neighbors as soon as a single HELLO packet is received from them. The HELLO packets contain no neighborhood information and thus offer no check for bidirectionality or 2-hop information. As very little information about the HELLO protocols is available for the simulation based studies, we will assume that gossip protocols that require 1-hop information are expecting bidirectional links if nothing else is explicitly stated. For protocols requiring 2-hop neighborhood information unidirectional links can be detected. We therefore assume that they are handled appropriately if there are no contradicting statements.

Link Symmetries

As a very simple graph model is often assumed, link asymmetries up to unidirectional links are not always considered. Asymmetric links were probably rare, if existent at all, in the simulation studies as discussed in Chapter 5.

We will consider a gossip protocol susceptible for lossy, asymmetric links when significant differences can be expected in the performance. Of course, this has to be proofed in further studies and represents at this time only our assessment after review of the particular publications.

6.2 Classification

In the following we will discuss possible ways to classify the discussed protocols. Williams et al. [105] distinguish *probability*, *area*, and *neighbor knowledge* based methods with different subgroups as shown in Figure 6.1. The rightmost level of items can be considered as example schemes but also as general groups in some cases. In contrast, Kouvatsos et al. [88] differentiate deterministic and probabilistic schemes as shown in Figure 6.2. Both teams of authors seem to base their classification on the publication by Tseng et al. [109].

Our classification, as shown in Figure 6.3, focuses only on this group. We differentiate between *static* and *adaptive* gossip routing protocols. The former group is configured based on assumptions about a particular network model and the protocols will not adapt when these assumptions do not hold. This is a feature of the latter group where particular properties about the network may be assumed but processes adapt the protocol based on gathered information, e.g., the node degree. Counter, location, distance, etc based schemes can occur in each group. We do not consider a protocol as adaptive when an adapted behavior is due to some static configuration. For example, gossip2 uses two different forwarding

Protocol	Uniform Deployment	Uniform Radio Ranges	Symmetric Links
RGR	•		
DAPF			
BRBPF		•	•
DABNRBPF		•	•
DABNRBPFNE		•	•
PPSNRP-DA	•		
PPSNRP-DT	•		
DPB			
LPR		•	•
gossip0			
gossip1			
gossip2			
gossip3			
gossip4		?	?
gossip5		•	
gossip10		•	
AGAR			
APF	•		
ECS			
ACBS			
P-AODV		•	•
AP, EAP, Three-P	•		
DRP, DRP_2	•		

Table 6.4: Gossip protocol classification – critical assumptions. The assumptions are marked by the • symbol. We consider that a particular model is assumed, when significant performance degradation can be expected if the assumption does not hold. No detailed information is provided for the unicast protocol that is used in gossip4 and the assumptions are thus unknown. The protocol names/acronyms refer to Chapter 4.

probabilities based on a pre-configured node degree threshold. Table 6.5 shows the classification of the gossip routing protocols.

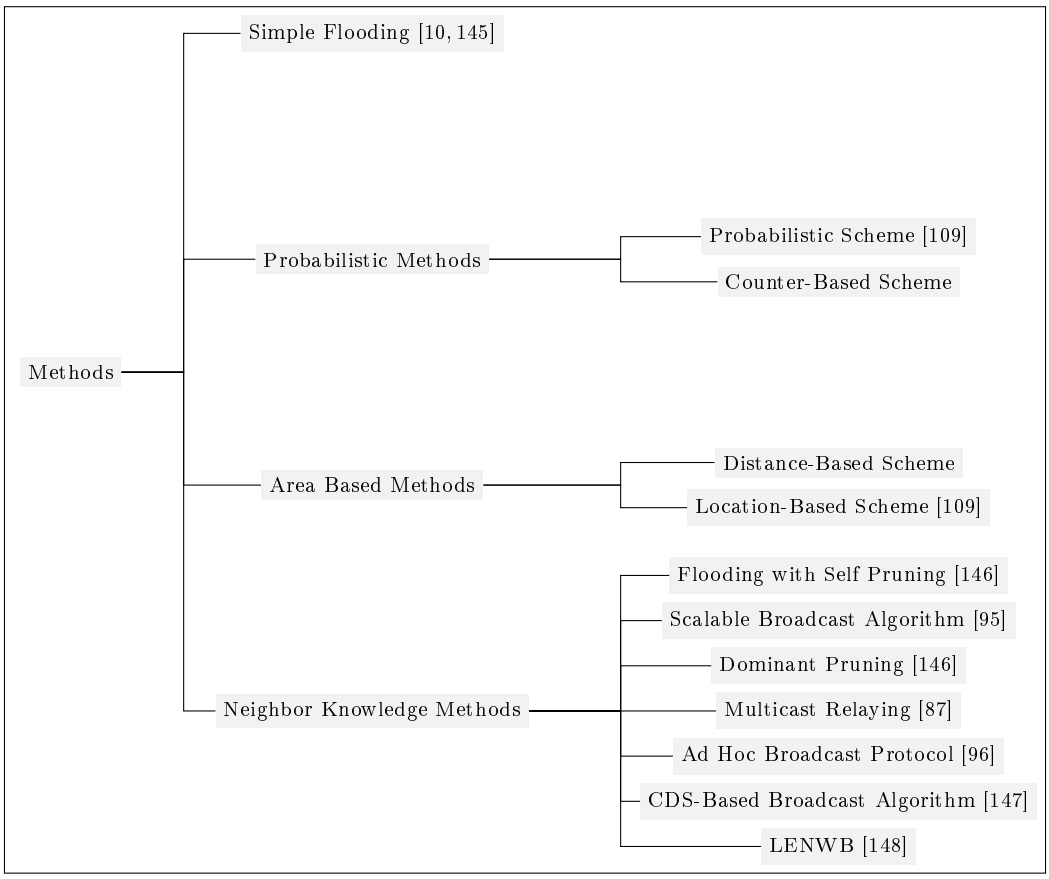


Figure 6.1: Classification by Williams et al. based on [105]. The references are the same as in the original publication.

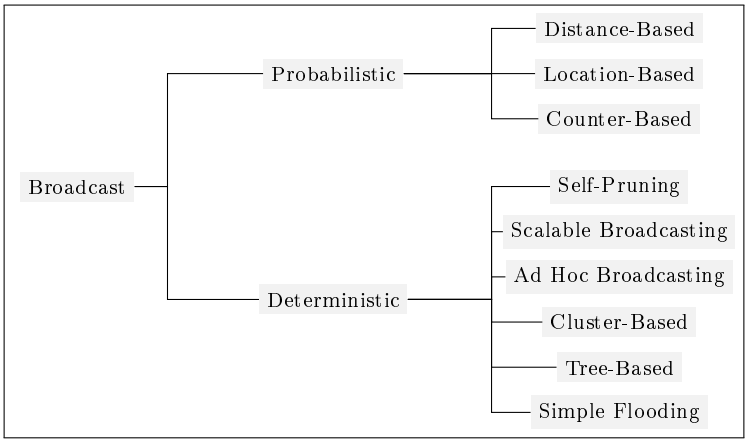


Figure 6.2: Classification by Kouvatsos et al. based on [88]

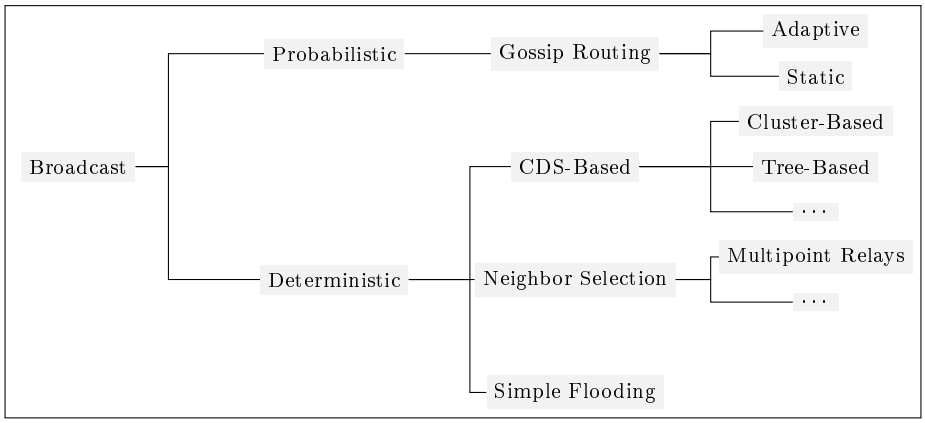


Figure 6.3: Classification of the improved flooding schemes

Protocol	Probabilistic	Static	Adaptive	Distance-Based	Location-Based	Counter-Based
RGR	•				•	
DAPF	•		•			
BRBPF	•		•		•	
DABNRBPF	•		•		•	
DABNRBPFNE	•		•		•	
PPSNRP-DA	•	•		•		
PPSNRP-DT	•	•		•		
DPB	•		•			•
LPR	•		•			
gossip0	•	•				
gossip1	•	•				
gossip2	•	•				
gossip3	•	•				•
gossip4	•	•				
gossip5	•		•			•
gossip10	•		•			•
AGAR	•		•			•
APF	•					
ECS	•	•				•
ACBS	•	•				•
P-AODV	•		•			
AP, EAP, Three-P	•		•			
DRP, DRP_2	•		•		•	

Table 6.5: Gossip protocol classification – critical assumptions. The assumptions are marked by the • symbol. We consider that a particular model is assumed, when significant performance degradation can be expected when the assumption does not hold. No detailed information is provided for the unicast protocol that is used in gossip4 and the assumptions are thus unknown. The protocol names/acronyms refer to Chapter 4.

CHAPTER 7

Conclusion

As we have discussed in this technical report, gossip routing and similar approaches have been proposed to improve flooding in wireless multi-hop networks. While the intentions can be different, e.g., the reduction of unnecessary broadcasts or provisioning of a reliable broadcast, the applied schemes are often equivalent. Often times, the assumed network models do not match reality and the research community therefore lacks sound studies. As we have elaborated, the commonly used simulation setups have significant issues regarding the mobility and radio models and the overall scenario does not fit todays wireless multi-hop networks. In some cases, the positive results might have been conditioned by the setup. We also discussed that very often critical information is missing in the publications which makes a review and assessment hardly possible. Based on the available information, it is not possible to specify the best approach or even to specify a rough order from best to worst.

Geometrically the fundamental optimization problems are easy to solve when global topology information and unlimited computational resources are available. Unfortunately, both are usually missing in wireless networks. Even if they would be available, changes in the topology would have to be detected, communicated, and the problem would have to be solved again. All of these tasks can not be solved in a perfect, real time way and will experience specific errors that will interfere with the process. For example, a centralized calculation of the MCDS requires precise information about the quality of each link. How this information is gathered is often ignored, e.g., it has to be communicated by flooding which (again) is not 100% reliable and introduces a significant overhead. We thus have to accept that approximations are the best we can get and optimal solutions are not possible.

Although flooding is a critical service, a complete understanding of the performance and limits is currently missing. Most notably, routing protocols will show a low performance when a reliable and also efficient network-wide dissemination of data is not possible. As there are also few studies of routing in real world networks, the influence of flooding based route discovery is an overlooked topic. Reachability and redundancy reduction seem to be orthogonal goals but it is our strong belief, that the reachability can only be increased when the number of (low data rate) broadcasts in IEEE 802.11 networks is reduced to the bare minimum.

Gossip routing was envisioned as one solution of the problem, yet as discussed, while it can be possible to configure a particular gossip routing protocol in an optimal way, it will only work when the assumptions hold and the required data for adaptive variants is available. While most of the protocols will work in large, uniformly deployed networks, we expect problems in smaller ones. Blind dropping of packets based on 1-hop and 2-hop information will more often result in limited reachability or flooding when the topology differs in significant ways.

7.1 Ongoing and Future Work

There are many research open problems. The discussed simulation based studies should be run again with more realistic settings. Even when these conditions were modeled appropriately, the results should be proved by repeated execution of the experiments. A sophisticated review and comparison of the testbed and simulation based results are required to improve the used models and to enable studies in networks that are larger and more diverse than current real world deployments.

The application of percolation theory for wireless multi-hop networks remains a promising combination of different research domains. Although the models have the issues as discussed in Chapter 5, percolation

theory was applied to analytically study the achievable bit rate and to prove the function of a distributed algorithm to connect a network. Franceschetti et al. [149] show that a maximum bit rate of $1/\sqrt{n}$ can be achieved when a particular scheduling and routing is used in a network that consists of so called highways. These highways are horizontal and vertical chains of nodes that form when nodes are distributed by a *Poisson point process* (PPP) in an area. For their analysis, the authors partition the space in boxes that are connected when two adjacent boxes contain at least one node. If the probability is high enough, i.e., the PPP has a sufficiently large exponent c (e^{-c^2}) then there is a large connected component and several paths from the left to the right side and from the top to the bottom of the area.

De Santis et al. [150] present two algorithms that connect all n nodes in a geometric random graph in $O(\log^2(n))$ or $0(\log^3(n))$ rounds where the resulting maximum node degree is in $O(\log^2(n))$ and $O(\log(n))$ respectively. This is achieved by successively increasing the radio ranges of the nodes, until the formed connected components are larger than a particular threshold C. Together with the parameter K that specifies the initial node degree, C determines if a large connected component arises and what node degree can be achieved.

We are currently focusing to bring percolation theoretic considerations, gossip routing, and restart problems together to improve our comparison of analytical, simulation, and testbed based studies. The focus is on the performance that can be achieved when one or several consecutive packets are sent over the network and packets are generated by different numbers of simultaneous sources.

Bibliography

[1] H. Lim and C. Kim, "Flooding in wireless ad hoc networks," *Computer Communications*, vol. 24, no. 3-4, pp. 353 – 363, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/B6TYP-4292M27-9/2/0f3b1055290e21b7bc136fa9f3a91a4d

[2] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501 (Informational), Jan. 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2501.txt

[3] I. F. Akyildiz and X. Wang, *Wireless Mesh Networks*. Wiley & Sons, March 2009.

[4] M. C. V. Ian Fuat Akyildiz, *Wireless Sensor Networks*. John Wiley & Sons Inc, August 2010.

[5] J. Mogul, "Broadcasting Internet Datagrams," RFC 919 (Standard), Oct. 1984. [Online]. Available: http://www.ietf.org/rfc/rfc919.txt

[6] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, July 1970.

[7] "Ieee standard for local and metropolitan area networks media access control (mac) bridges," 2004, iEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998).

[8] J. Moy, "OSPF Version 2," RFC 2328 (Standard), Apr. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2328.txt

[9] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[10] J. G. Jetcheva, Y.-C. Hu, D. A. Maltz, and D. B. Johnson, "A simple protocol for multicast and broadcast in mobile ad hoc networks," IETF Internet Draft, July 2001, version 01. [Online]. Available: http://tools.ietf.org/html/draft-ietf-manet-simple-mbcast-01

[11] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728 (Experimental), Feb. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4728.txt

[12] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Jul. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[13] "List of ad hoc routing protocols," last visited: May, 2001. [Online]. Available: http://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols

[14] IEEE Std 802.11-2007, "IEEE standard for information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks-specific requirements — Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," LAN/MAN Standards Committee, New York, NY, USA, pp. C1–1184, June 2007. [Online]. Available: http://dx.doi.org/10.1109/IEEESTD.2007.373646

[15] B. N. Levine and J. J. Garcia-Luna-Aceves, "A comparison of known classes of reliable multicast protocols," in *Proc. Conf. Int Network Protocols*, 1996, pp. 112–121.

[16] C. Westphal, C. Perkins, and R. Wakikawa, "Route hitting probability for a class of ad hoc routing protocols," in *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops (WiOPT)*, April 2008, pp. 475–480.

[17] F. Harary and B. Raghavachari, "The e-mail gossip number and the connected domination number," *Applied Mathematics Letters*, vol. 10, no. 4, pp. 15 – 17, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/B6TY9-3SNVJ50-4/2/f547755e49ae60de29535286c01c80c3

[18] Y. Alkhalifah and R. L. Wainwright, "A genetic algorithm applied to graph problems involving subsets of vertices," in *Proc. CEC2004 Evolutionary Computation Congress*, vol. 1, 2004, pp. 303–308.

[19] P. Klein and R. Ravi, "A nearly best-possible approximation algorithm for node-weighted steiner trees," *Journal of Algorithms*, vol. 19, no. 1, pp. 104 – 115, 1995. [Online]. Available: http://www.sciencedirect.com/science/article/B6WH3-45PTHKN-V/2/cb11bd27350c8c1991f6b0e439faccd0

[20] M. R. Garey and D. S. Johnson, *Computers and Intractability; A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1990.

[21] S. Guha and S. Khuller, "Approximation algorithms for connected dominating sets," *Algorithmica*, vol. 20, pp. 374–387, 1998, 10.1007/PL00009201. [Online]. Available: http://dx.doi.org/10.1007/PL00009201

[22] L. Lovász, "On the ratio of optimal integral and fractional covers," *Discrete Mathematics*, vol. 13, no. 4, pp. 383 – 390, 1975. [Online]. Available: http://www.sciencedirect.com/science/article/B6V00-45FCTD9-3D/2/cb12a4cb7c3a0445dedf5456df409cae

[23] Y. Li, M. T. Thai, F. Wang, C.-W. Yi, P.-J. Wan, and D.-Z. Du, "On greedy construction of connected dominating sets in wireless networks," *Wireless Communications and Mobile Computing*, vol. 5, no. 8, pp. 927–932, 2005. [Online]. Available: http://dx.doi.org/10.1002/wcm.356

[24] D.-Z. Du, M. Thai, Y. Li, D. Liu, and S. Zhu, "Strongly connected dominating sets in wireless sensor networks with unidirectional links," in *Frontiers of WWW Research and Development - APWeb 2006*, ser. Lecture Notes in Computer Science, X. Zhou, J. Li, H. Shen, M. Kitsuregawa, and Y. Zhang, Eds. Springer Berlin / Heidelberg, 2006, vol. 3841, pp. 13–24. [Online]. Available: http://dx.doi.org/10.1007/11610113_2

[25] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith, "Parametric probabilistic sensor network routing," in *WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. New York, NY, USA: ACM, 2003, pp. 122–131.

[26] J. Cartigny and D. Simplot, "Border node retransmission based probabilistic broadcast protocols in ad-hoc networks," in *HICSS '03: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9*. Washington, DC, USA: IEEE Computer Society, 2003, p. 303.

[27] ——, "Border node retransmission based probabilistic broadcast protocols in ad-hoc networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 189–204, January 2003.

[28] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, "Epidemic algorithms for replicated database maintenance," in *PODC '87: Proceedings of the sixth annual ACM Symposium on Principles of distributed computing*. New York, NY, USA: ACM, 1987, pp. 1–12.

[29] M. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: Low message overhead and high reliability for broadcasting on small networks," University of California, San Diego, La Jolla, CA, USA, Tech. Rep. CS1999-0637, 1999.

[30] G. Grimmett, *Percolation*, 1st ed. Springer-Verlag, April 1989.

[31] R. Meester and R. Roy, *Continuum percolation*. Cambridge: Cambridge Univ. Press, 1996, vol. Cambridge Tracts in Mathematics, no. 119.

[32] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing." in *Proceedings IEEE INFOCOM 2002, The 21st Annual Joint Conference of the IEEE Computer and Communications Societies*. New York, USA: IEEE, June 23-27 2002, iSBN 0-7803-7477-0. [Online]. Available: http://www.ieee-infocom.org/2002/papers/822.pdf

[33] ——, "Gossip-based ad hoc routing," *IEEE/ACM Trans. Netw.*, vol. 14, no. 3, pp. 479–491, 2006.

[34] D. Shah, "Network gossip algorithms," *Acoustics, Speech, and Signal Processing, IEEE International Conference on*, vol. 0, pp. 3673–3676, 2009.

[35] P. Erdös and A. Rényi, "On random graphs, i," *Publicationes Mathematicae (Debrecen)*, vol. 6, pp. 290–297, 1959. [Online]. Available: http://www.renyi.hu/~{}p_erdos/Erdos.html#1959-11

[36] M. Penrose, *Random Geometric Graphs*. Oxford University Press, USA, July 2003, vol. 9780198506263.

[37] B. Blywis, M. Günes, S. Hofmann, and F. Juraschek, "A Study of Adaptive Gossip Routing in Wireless Mesh Networks," in *Ad Hoc Networks*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari, M. Gerla, H. Kobayashi, S. Palazzo, S. Sahni, X. S. Shen, M. Stan, J. Xiaohua, A. Zomaya, G. Coulson, J. Zheng, D. Simplot-Ryl, and V. C. M. Leung, Eds., vol. 49. Springer Berlin Heidelberg, 2010, pp. 98–113. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-17994-5_7

[38] B. Blywis, M. Günes, F. Juraschek, and S. Hofmann, "Gossip routing in wireless mesh networks," in *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010)*, 2010.

[39] B. Blywis, M. Günes, F. Juraschek, and O. Hahm, "Challenges and limits of flooding and gossip routing based route discovery schemes," in *Local Computer Networks*, 2011, submitted for review.

[40] I. Webman, J. Jortner, and M. H. Cohen, "Critical exponents for percolation conductivity in resistor networks," *Phys. Rev. B*, vol. 16, no. 6, pp. 2593–2596, Sep 1977.

[41] J. Planès, S. Bord, and J. Fraysse, "Continuous percolation in organic conducting blends," *Physica Status Solidi (B), Basic Research*, vol. 230, pp. 289–293, 2002.

[42] E. T. Seppälä, A. M. Pulkkinen, and M. J. Alava, "Percolation in three-dimensional random field ising magnets," *Phys. Rev. B*, vol. 66, no. 14, p. 144403, Oct 2002.

[43] A. M. Reynolds, G. A. Sword, S. J. Simpson, and D. R. Reynolds, "Predator percolation, insect outbreaks, and phase polyphenism," *Current Biology*, vol. 19, no. 1, pp. 20–24, December 2008.

[44] M. Aizenman and D. Barsky, "Sharpness of the phase transition in percolation models," *Communications in Mathematical Physics*, vol. 108, pp. 489–526, 1987, 10.1007/BF01212322. [Online]. Available: http://dx.doi.org/10.1007/BF01212322

[45] R. van der Hofstad, *New Perspectives in Stochastic Geometry*. Oxford University Press, 2010, ch. Percolation and random graphs, pp. 173–247.

[46] A. Lesne, "The discrete versus continuous controversy in physics," *Mathematical Structures in Computer Science*, vol. 17, no. 02, pp. 185–223, 2007. [Online]. Available: http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=1003868&fulltextType=RA&fileId=S0960129507005944

[47] J. van den Berg, R. Meester, and D. G. White, "Dynamic boolean models," 1997.

[48] J. C. Wierman, "Pairs of graphs with site and bond percolation critical probabilities in opposite orders," *Discrete Applied Mathematics*, vol. 129, no. 2-3, pp. 545 – 548, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166218X03001835

[49] D. Stauffer and A. Aharony, *Introduction to Percolation Theory*, 2nd ed. Crc Pr Inc, July 1994.

[50] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Phys. Rev. Lett.*, vol. 85, no. 25, pp. 5468–5471, Dec 2000.

[51] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener, "Graph structure in the web," *Computer Networks*, vol. 33, no. 1-6, pp. 309 – 320, 2000. [Online]. Available: http://www.sciencedirect.com/science/article/B6VRG-40B2JGR-S/2/12aa9d9476c06da265c9686161c86908

[52] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," *SIGCOMM Comput. Commun. Rev.*, vol. 29, pp. 251–262, August 1999. [Online]. Available: http://doi.acm.org/10.1145/316194.316229

[53] H. Tomita and C. Murakami, *Research of Pattern Formation*. KTK Scientific Publishers, Tokyo, 1994, ch. Percolation pattern in continuous media and its topology, pp. 197–203.

[54] K. Eames and J. Read, "Networks in epidemiology," in *Bio-Inspired Computing and Communication*, ser. Lecture Notes in Computer Science, P. Liò, E. Yoneki, J. Crowcroft, and D. Verma, Eds. Springer Berlin / Heidelberg, 2008, vol. 5151, pp. 79–90. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-92191-2_8

[55] W. Kermack and A. McKendrick, "Contributions to the mathematical theory of epidemics—i," *Bulletin of Mathematical Biology*, vol. 53, pp. 33–55, 1991, 10.1007/BF02464423. [Online]. Available: http://dx.doi.org/10.1007/BF02464423

[56] V. Kotvalt, "Britton, n.f.: essential mathematical biology," *Photosynthetica*, vol. 41, pp. 356–356, 2003, 10.1023/B:PHOT.0000015523.14609.5a. [Online]. Available: http://dx.doi.org/10.1023/B:PHOT.0000015523.14609.5a

[57] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '03. New York, NY, USA: ACM, 2003, pp. 27–34. [Online]. Available: http://doi.acm.org/10.1145/863955.863960

[58] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838 (Informational), Apr. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4838.txt

[59] K. C. Lee and M. Gerla, "Opportunistic vehicular routing," in *Proc. European Wireless Conf. (EW)*, 2010, pp. 873–880.

[60] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134–141, November 2006. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2006.248176

[61] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 145–158, August 2004. [Online]. Available: http://doi.acm.org/10.1145/1030194.1015484

[62] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," Duke University, Tech. Rep. CS-2000-06, July 2000.

[63] J. Luo, P. T. Eugster, J.-P. Hubaux, P. Th, and E. J. pierre Hubaux, "Route driven gossip: Probabilistic reliable multicast in ad hoc networks," in *In Proc. of INFOCOM*, 2002, pp. 2229–2239.

[64] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous gossip: improving multicast reliability in mobile ad-hoc networks," in *Proc. 21st Int Distributed Computing Systems Conf.*, 2001, pp. 275–283.

[65] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, pp. 46–55, April 1999.

[66] J. Torkestani and M. Meybodi, "Weighted steiner connected dominating set and its application to multicast routing in wireless manets," *Wireless Personal Communications*, pp. 1–25, 2010, 10.1007/s11277-010-9936-4. [Online]. Available: http://dx.doi.org/10.1007/s11277-010-9936-4

[67] P. Levis, N. Patel, S. Shenker, and D. Culler, "Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks," in *In Proceedings of the First USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI*, 2004, pp. 15–28.

[68] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," in *WONS '05: Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 32–41.

[69] D. Venkatesulu and T. A. Gonsalves, "Efficient fault-tolerant reliable broadcast in an extended lan," *Local Computer Networks, Annual IEEE Conference on*, vol. 0, p. 149, 1997.

[70] M. F. Kaashoek, A. S. Tanenbaum, S. F. Hummel, and H. E. Bal, "An efficient reliable broadcast protocol," *Operating Systems Review*, vol. 23, pp. 5–19, 1989.

[71] P. Orlik, J. Zhang, B. Bhargava, G. Ding, G. Ding, Z. Sahinoglu, and Z. Sahinoglu, "Reliable broadcast in zigbee networks," in *In Proceedings of SECON*, 2005.

[72] W. Lou and J. Wu, "Double-covered broadcast (dcb): A simple reliable broadcast algorithm in manets," 2004.

[73] ——, "Toward broadcast reliability in mobile ad hoc networks with double coverage," *IEEE Transactions on Mobile Computing*, vol. 6, pp. 148–163, 2007.

[74] D. Johnson, N. Ntlatlapa, and C. Aichele, "Simple pragmatic approach to mesh routing using batman," in *2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries*, 2008. [Online]. Available: http://researchspace.csir.co.za/dspace/bitstream/10204/3035/1/Johnson3_2008.pdf

[75] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better approach to mobile ad-hoc networking (b.a.t.m.a.n.)," Internet-Draft, April 2008. [Online]. Available: http://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00

[76] F. Ye, S. Lu, and L. Zhang, "Gradient broadcast: A robust, long-lived large sensor network," University of California, Los Angeles, Tech. Rep., 2001. [Online]. Available: http://irl.cs.ucla.edu/papers/grab-tech-report.ps.

[77] F. Ye, G. Zhong, S. Lu, and L. Zhang, "Gradient broadcast: a robust data delivery protocol for large scale sensor networks," *Wirel. Netw.*, vol. 11, no. 3, pp. 285–298, 2005.

[78] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking (TON)*, vol. 11, no. 1, pp. 2–16, 2003.

[79] D. Braginsky and D. Estrin, "Rumor routing algorthim for sensor networks," in *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications.* New York, NY, USA: ACM, 2002, pp. 22–31.

[80] C. Lee, S. Helal, and W. Lee, "Gossip-based service discovery in mobile ad hoc networks," *IEICE TRANSACTIONS on Communications*, vol. E89-B, no. 9, pp. 2621–2624, September 2006.

[81] T. C. Aysal, M. E. Yildiz, and A. Scaglione, "Broadcast gossip algorithms," in *Proceedings of the Information Theory Workshop (ITW)*, May 2008, pp. 343–347.

[82] T. C. Aysal, M. E. Yildiz, A. D. Sarwate, and A. Scaglione, "Broadcast gossip algorithms: Design and analysis for consensus," in *Proceedings of the Conference on Decision and Control (CDC)*, December 2008, pp. 4843–4848.

[83] ——, "Broadcast gossip algorithms for consensus," *Trans. Sig. Proc.*, vol. 57, no. 7, pp. 2748–2761, 2009.

[84] A. G. Dimakis, A. D. Sarwate, and M. J. Wainwright, "Geographic gossip: efficient aggregation for sensor networks," in *IPSN '06: Proceedings of the 5th international conference on Information processing in sensor networks.* New York, NY, USA: ACM, 2006, pp. 69–76.

[85] X. Hou, D. Tipper, and S. Wu, "A gossip-based energy conservation protocol for wireless ad hoc and sensor networks," *J. Netw. Syst. Manage.*, vol. 14, no. 3, pp. 381–414, 2006.

[86] S. Sabitha and M. P. Sebastian, "Gos-aodv: a gossip-based sleep ad hoc on demand distance vector routing protocol," in *CSN '07: Proceedings of the Sixth IASTED International Conference on Communication Systems and Networks.* Anaheim, CA, USA: ACTA Press, 2007, pp. 13–18.

[87] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," in *HICSS '02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 9*. Washington, DC, USA: IEEE Computer Society, 2002, p. 298.

[88] D. Kouvatsos and I. haka Mkwawa, "Broadcasting methods in mobile ad hoc networks: An overview," in *Proceedings of the HetNet*, 2005.

[89] A. Jüttner and A. Magi, "Tree based broadcast in ad hoc networks," *Mob. Netw. Appl.*, vol. 10, no. 5, pp. 753–762, 2005.

[90] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM, 1999, pp. 151–162.

[91] ——, "The broadcast storm problem in a mobile ad hoc network," in *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM, 1999, pp. 151–162.

[92] M. Jiang, J. Li, and Y. Tay, "Cluster based routing protocol (cbrp)," IETF Internet Draft, August 1999, version 01. [Online]. Available: http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01

[93] Y.-C. Tseng, S.-Y. Ni, and E.-Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network," *Distributed Computing Systems, International Conference on*, vol. 0, p. 0481, 2001.

[94] ——, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network," *IEEE Transactions on Computers*, vol. 52, pp. 545–557, 2003.

[95] W. Peng and X.-C. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," in *MobiHoc '00: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. Piscataway, NJ, USA: IEEE Press, 2000, pp. 129–130.

[96] W. Peng and X. Lu, "Ahbp: An efficient broadcast protocol for mobile ad hoc networks," *J. Comput. Sci. Technol.*, vol. 16, no. 2, pp. 114–125, 2001.

[97] M. Seddigh, J. S. González, and I. Stojmenovic, "Rng and internal node based broadcasting algorithms for wireless one-to-one networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, pp. 37–44, April 2001. [Online]. Available: http://doi.acm.org/10.1145/584066.584069

[98] I. Stojmenovic, M. Seddigh, and J. Zunic, "Internal nodes based broadcasting in wireless networks," in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Volume 9 - Volume 9*. Washington, DC, USA: IEEE Computer Society, 2001, pp. 9005–. [Online]. Available: http://portal.acm.org/citation.cfm?id=820738.820821

[99] ——, "Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 13, pp. 14–25, 2002.

[100] J. Wu and H. Li, "A dominating-set-based routing scheme in ad hoc wireless networks," *Telecommunication Systems*, vol. 18, pp. 13–36, 2001, 10.1023/A:1016783217662. [Online]. Available: http://dx.doi.org/10.1023/A:1016783217662

[101] G. Neglia, G. Reina, and S. Alouf, "Distributed gradient optimization for epidemic routing: a preliminary evaluation," INRIA – Université Montpellier II - Sciences et Techniques du Languedoc, Tech. Rep. RR-7016, August 2009. [Online]. Available: http://hal.inria.fr/inria-00435184/fr/

[102] ——, "Distributed gradient optimization for epidemic routing: a preliminary evaluation," in *IFIP Wireless Days 2009*, December 2009.

[103] R. Masiero and G. Neglia, "Distributed sub-gradient method for delay tolerant networks," INRIA – Université Montpellier II - Sciences et Techniques du Languedoc, Tech. Rep. RR-7345, June 2010.

[104] A. Nedic and A. Ozdaglar, "Distributed subgradient methods for multi-agent optimization," *Automatic Control, IEEE Transactions on*, vol. 54, no. 1, pp. 48–61, Januar 2009.

[105] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM, 2002, pp. 194–205.

[106] X.-Y. Li, K. Moaveninejad, and O. Frieder, "Regional gossip routing for wireless ad hoc networks," in *Proc. 28th Annual IEEE Int. Conf. Local Computer Networks LCN '03*, 2003, pp. 274–275.

[107] ——, "Regional gossip routing for wireless ad hoc networks," *Mob. Netw. Appl.*, vol. 10, no. 1-2, pp. 61–77, 2005.

[108] F. Kuhn, R. Wattenhofer, and A. Zollinger, "An algorithmic approach to geographic routing in ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 1, pp. 51–62, 2008.

[109] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wirel. Netw.*, vol. 8, no. 2/3, pp. 153–167, 2002.

[110] S. D. Servetto and G. Barrenechea, "Constrained random walks on random graphs: routing algorithms for large scale wireless sensor networks," in *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*. New York, NY, USA: ACM, 2002, pp. 12–21.

[111] Q. Zhang and D. P. Agrawal, "Dynamic probabilistic broadcasting in manets," *J. Parallel Distrib. Comput.*, vol. 65, no. 2, pp. 220–233, 2005.

[112] ——, "Performance evaluation of leveled probabilistic broadcasting in manets and wireless sensor networks," *Transactions of the Society for Modeling and Simulation International (SCS)*, vol. 81, no. 8, pp. 533–546, 2005.

[113] Z. Haas, "A new routing protocol for the reconfigurable wireless networks," in *IEEE International Conference on Universal Personal Communications (ICUPC)*, 1997, pp. 562–566.

[114] Z. Shi and H. Shen, "Adaptive gossip-based routing algorithm," in *Proceedings, 23rd IEEE International Performance, Computing, and Communications Conference IPCCC*, 2004.

[115] M. B. Yassein, M. Ould-Khaoua, L. M. Mackenzie, and S. Papanastasiou, "Performance analysis of adjusted probabilistic broadcasting in mobile ad hoc networks," *International Journal of Wireless Information Networks*, vol. 13, no. 2, pp. 127–140, April 2006.

[116] M. B. Yassein, M. O. Khaoua, L. M. Mackenzie, S. Papanastasiou, and A. Jamal, "Improving route discovery in on-demand routing protocols using local topology information in manets," in *Proceedings of the ACM international workshop on Performance monitoring, measurement, and evaluation of heterogeneous wireless and wired networks*, ser. PM2HW2N '06. New York, NY, USA: ACM, 2006, pp. 95–99. [Online]. Available: http://doi.acm.org/10.1145/1163653.1163671

[117] A. Mohammed, M. Ould-Khaoua, and L. M. Mackenzie, "An efficient counter-based broadcast scheme for mobile ad hoc networks," in *Formal Methods and Stochastic Models for Performance Evaluation*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2007, vol. 4748/2007, pp. 275–283.

[118] A. Mohammed, M. Ould-Khaoua, L. M. Mackenzie, and J.-D. Abdulai, "Improving the performance of counter-based broadcast scheme for mobile ad hoc networks," in *Proceedings of the 2007 IEEE International Conference on Signal Processing and Communication (ICSPC 2007), 24-27 November 2007, Dubai, United Arab Emirates*. IEEE Computer Society Press, 2007, pp. 1403 – 1406.

[119] ——, "An adjusted counter-based broadcast scheme for mobile ad hoc networks," *Computer Modeling and Simulation, International Conference on*, vol. 0, pp. 441–446, 2008.

[120] A. Mohammed, M. Ould-Khaoua, L. M. Mackenzie, C. Perkins, and J.-D. Abdulai, "Probabilistic counter-based route discovery for mobile ad hoc networks," in *IWCMC '09: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing*. New York, NY, USA: ACM, 2009, pp. 1335–1339.

[121] A. Hanashi, A. Siddique, I. Awan, and M. Woodward, "Performance evaluation of dynamic probabilistic broadcasting for flooding in mobile ad hoc networks," *Simulation Modelling Practice and Theory*, vol. 17, no. 2, pp. 364–375, 2009.

[122] J.-D. Abdulai, M. Ould-Khaoua, and L. Mackenzie, "Improving probabilistic route discovery in mobile ad hoc networks," *Local Computer Networks, Annual IEEE Conference on*, vol. 0, pp. 739–746, 2007.

[123] J.-D. Abdulai, M. Ould-Khaoua, and L. M. Mackenzie, "Adjusted probabilistic route discovery in mobile ad hoc networks," *Computer and Electrical Engineering*, vol. 35, no. 1, pp. 168–182, 2009.

[124] J.-D. Abdulai, "Probabilistic route discovery for wireless mobile ad hoc networks (manets)," Ph.D. dissertation, University of Glasgow, 2009.

[125] J.-D. Abdulai, M. Ould-Khaoua, L. M. Mackenzie, and A. Mohammed, "Neighbour coverage: A dynamic probabilistic route discovery for mobile ad hoc networks," in *Proc. Int. Symp. Performance Evaluation of Computer and Telecommunication Systems SPECTS 2008*, 2008, pp. 165–172.

[126] M. Conti and S. Giordano, "Multihop ad hoc networking: The reality," *IEEE Communications Magazine*, vol. 45, no. 4, pp. 88–95, April 2007.

[127] ——, "Multihop ad hoc networking: The theory," *IEEE Communications Magazine*, vol. 45, no. 4, pp. 78–86, April 2007.

[128] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multihop Wireless Ad Hoc Network Routing Protocols," *Proceedings of the 4th Annual ACM/IEEE MobiCom'98*, pp. 85–97, 1998.

[129] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic properties of the random waypoint mobility model," *Wirel. Netw.*, vol. 10, no. 5, pp. 555–567, 2004.

[130] J. Yoon, M. Liu, and BrianNoble, "Random waypoint considered harmful," in *Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom 2003)*. San Francisco: IEEE, March 30 - April 3 2003, Mobility.

[131] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, T. Imielinski and H. Korth, Eds. Kluwer, 1996, vol. 353.

[132] B. Milic and M. Malek, "Analyzing large scale real-world wireless multihop network," *IEEE Communications Letters*, vol. 11, no. 7, pp. 580–582, 2007.

[133] ——, "Properties of wireless multihop networks in theory and practice," in *Guide to Wireless Ad Hoc Networks*, ser. Computer Communications and Networks. Springer London, 2009, pp. 1–26. [Online]. Available: http://dx.doi.org/10.1007/978-1-84800-328-6_1

[134] ——, "Npart - node placement algorithm for realistic topologies in wireless multihop network simulation," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, ser. Simutools '09. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, pp. 9:1–9:10. [Online]. Available: http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5669

[135] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[136] V. Mhatre, "Enhanced wireless mesh networking for ns-2 simulator," *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 69–72, July 2007. [Online]. Available: http://doi.acm.org/10.1145/1273445.1273455

[137] K.-W. Chin, J. Judge, A. Williams, and R. Kermode, "Implementation experience with manet routing protocols," *SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 5, pp. 49–59, 2002.

[138] R. Dube, C. D. Rais, K. yeh Wang, and S. K. Tripathi, "Signal stability based adaptive routing (ssa) for ad-hoc mobile networks," *IEEE Personal Communications*, vol. 4, pp. 36–45, 1997.

[139] M. Lacage, M. H. Manshaei, and T. Turletti, "Ieee 802.11 rate adaptation: a practical approach," in *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, ser. MSWiM '04. New York, NY, USA: ACM, 2004, pp. 126–134. [Online]. Available: http://doi.acm.org/10.1145/1023663.1023687

[140] S. H. Y. Wong, H. Yang, S. Lu, and V. Bharghavan, "Robust rate adaptation for 802.11 wireless networks," in *Proceedings of the 12th annual international conference on Mobile computing and networking*, ser. MobiCom '06. New York, NY, USA: ACM, 2006, pp. 146–157. [Online]. Available: http://doi.acm.org/10.1145/1161089.1161107

[141] S. Shrestha, S. Shrestha, A. Lee, J. Lee, D.-W. Seo, K. Lee, J. Lee, S. Chong, and N. H. Myung, "A group of people acts like a black body in a wireless mesh network," in *Proc. IEEE Global Telecommunications Conference GLOBECOM '07*, A. Lee, Ed., 2007, pp. 4834–4839.

[142] E. Elnahrawy, X. Li, and R. P. Martin, "The limits of localization using signal strength: a comparative study," 2004, pp. 406–414. [Online]. Available: http://dx.doi.org/10.1109/SAHCN.2004.1381942

[143] N. Patwari, A. O. H. III, J. Ash, R. L. Moses, S. Kyperountas, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, July 2005. [Online]. Available: http://dx.doi.org/10.1109/MSP.2005.1458287

[144] IANA, "Special-Use IPv4 Addresses," RFC 3330 (Informational), Sep. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3330.txt

[145] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for reliable multicast in multi-hop ad hoc networks," in *Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications*, ser. DIALM '99. New York, NY, USA: ACM, 1999, pp. 64–71. [Online]. Available: http://doi.acm.org/10.1145/313239.313291

[146] H. Lim and C. Kim, "Multicast tree construction and flooding in wireless ad hoc networks," in *Proceedings of the 3rd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, ser. MSWIM '00. New York, NY, USA: ACM, 2000, pp. 61–68. [Online]. Available: http://doi.acm.org/10.1145/346855.346865

[147] W. Peng and X.-C. Lu, "Efficient broadcast in mobile ad hoc networks using connected dominating sets," *Journal of Software*, vol. 12, no. 4, pp. 529–536, 2001.

[148] J. Sucec and I. Marsic, "An efficient distributed network-wide broadcast algorithm for mobile ad hoc networks," Rutgers University, Tech. Rep. 248, September 2000.

[149] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, 2007.

[150] E. De Santis, F. Grandoni, and A. Panconesi, "Fast low degree connectivity of ad-hoc networks via percolation," in *Proceedings of the 15th annual European conference on Algorithms*, ser. ESA'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 206–217. [Online]. Available: http://portal.acm.org/citation.cfm?id=1778580.1778602