A Practical Approach to Reliable Flooding in Mobile Ad hoc Networks

Robert Sombrutzki[†], Anatolij Zubow[*]

[†]Humboldt Universität zu Berlin, Unter den Linden 6, Berlin, Germany

[*]Department Telecommunication Systems, Technical University of Berlin, Einsteinufer 25, Berlin, Germany

Abstract

Flooding in Mobile Ad hoc Networks (MANET) is an important communication primitive. It serves as a building block for higher layer protocols like content distribution, route discovery in routing protocols as well as used by services like Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP).

The nodes in real MANETs are not uniformly distributed. There are always dense and sparse parts in the network. For the dense parts of the network the redundancy provided by naive flooding is to high leading the packet loss due to collisions, wasting radio resources and thus need to be reduced. On the other hand, even in stationary networks without node mobility wireless links are lossy due to external and internal interference, fading or weak signal. Thus the transmission of a packet can fail. Both characteristics need to be considered when designing a flooding protocol.

The proposed flooding scheme operates using purely local information about the network topology and is therefore in contrast to methods which rely on an overlay routing structures suitable for MANETs. It achieves a very high reliability while still being efficient as follows. First, we repeat the transmission of the flooding message at the network layer as long as we find strongly connected neighboring nodes which so far have not successfully received the flooding message. In each iteration the most promising neighboring node is selected according to a novel metric. Second, to achieve a high reliability we use unicasting at the link-layer for the transmission of flooding messages to the selected peer node. This allows us to compensate for dropped flooding messages due to lossy links or MAC collisions and allows us to adapt the level of redundancy in order to improve reachability while keeping the message overhead low. As long as the selected peer does not successfully acknowledge the packet reception or a passive acknowledgment was overheard the MAC transmission is repeated. Third, to achieve an efficient solution we piggyback flooding messages with the address of nodes we expect that they will receive the flooding message which is feasible due to the used link-layer unicasting. The proposed peer selection metric is of low complexity and thus can be computed on a per packet basis.

The proposed flooding scheme can be implemented on top of existing IEEE 802.11 or 802.15.4 PHY/MAC stacks without any modifications.

Results from extensive network simulation show that the proposed scheme is able to achieve a reachability of close to one even in very challenging networks where all other known methods fail. Moreover, our proposed scheme is able to achieve a high reachability in a very efficient way with low delay, e.g. in challenging networks the best known solutions requires up to four times more MAC transmissions to achieve the same level of reachability.

Key words: flooding, mobile ad hoc networks, wireless mesh networks, reliability, multicasting

1. Introduction

Mobile ad hoc networks (MANETs) have received much attention in recent years in industry as well as academia [1, 2, 3]. A MANET is a multi-hop wireless mesh network without any fixed infrastructure, in which nodes can be mobile. MANETs are increasingly important because ad hoc wireless communication is rapidly becoming ubiquitous. Potential applications range from specific applications like disaster response applications to vehicular communication.

Flooding in MANETs is an important communication primitive due to the absence of any fixed communication infrastructure. It serves as a building block for higher protocols like content distribution, route discovery in routing protocols like DSR [4] and AODV [5] as well as services like Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) which are used for lookup the MAC and IP address respectively.

Flooding is a mechanism by which a message originated at a node should be transmitted possibly via multi-hop to any other node in the network. This is a fundamental difference to broadcasting where the message is is intended to just the nodes in the direct wireless communication range of the broadcasting node. In general the flooding tries to cover all nodes in the network or a subset of nodes in a geographical area.

The simplest form of flooding is the naive flooding. Here a node which receives a flooding message for the first time rebroadcasts it only once. This simple scheme is remarkably re-

Email addresses: sombrutz@informatik.hu-berlin.de (Robert Sombrutzki[†]), zubow@tkn.tu-berlin.de (Anatolij Zubow[*])

liable, i.e. most of the network nodes are covered, as long as the MANET is highly meshed, i.e. between two pairs of nodes there are multiple non-overlapping paths in the network. However, in a dense network, i.e. the nodes have plenty of neighbors, the level of redundancy offered by the naive flooding is too high, i.e. redundant transmissions to nodes which already received the flooding message, thus wasting the scarce spectrum. In contrast, in a sparse lossy network where the nodes have only a few weak neighbors, the naive flooding scheme performs worse in terms of reachability because the level of redundancy is not sufficient high.

To summarize, the goal is to have a reliable and efficient flooding scheme which is able to adapt its level of redundancy to the different sparse and dense parts of the network.

Contributions: The contributions in this paper are as follows.

First, we present a general framework for flooding which can be used to implement various flooding schemes known from the literature.

Second, we propose a flooding scheme which achieves a very high reliability while still being efficient. Our approach achieves this as follows. First, we repeat the transmission of the flooding message at the network layer as long as we find strongly connected neighboring nodes which so far have not successfully received the flooding message. In each iteration the most promising neighboring node is selected according to a novel metric. Second, to achieve a high reliability we use unicasting at the link-layer for the transmission of flooding messages to the selected peer node. This allows us to compensate for dropped flooding messages due to lossy links or MAC collisions and allows us to adapt the level of redundancy in order to improve reachability while keeping the message overhead low. As long as the selected peer does not successfully acknowledge the packet reception or a passive acknowledgment was overheard the MAC transmission is repeated. Third, to achieve an efficient solution we piggyback flooding messages with nodes we expect that they receive the flooding message which is feasible due to the used link-layer unicasting. The proposed peer selection metric is of low complexity and thus can be computed on a per packet basis. Finally, our proposed flooding scheme can be implemented on top of existing IEEE 802.11 or 802.15.4 PHY/MAC stacks without any modifications.

Third, we present results from an indepth evaluation by means of network simulations where we compare our approach with other state-of-the-art flooding schemes. Our results show that the proposed flooding scheme based on reunicasting flooding messages achieves a reachability of close to one where other known approaches fail. Moreover, our method has the lowest message overhead.

Outline: The remainder of the paper is structured as follows. In Section 2 we summarize the most important works from the literature aiming to optimize the flooding operation. Section 3 characterizes real world wireless networks using the example of Humboldt Wireless Lab research testbed [6]. In Section 4 performance metrics are introduced allowing us to compare different flooding schemes with each other. The problem statement is given in Section 5. Thereafter, in Section 6 we present a general framework for flooding. Based on this framework we propose a reliable and efficient flooding scheme in Section 7. Section 8 discusses the proposed approach and compares it against other similar methods known from literature. In Section 9 we evaluate and compare our approach with state-of-the-art approaches from literature by means of network simulations. Finally, Section 10 concludes the paper and gives a short outlook.

2. Related Work

In the following we summarize the most important works from the literature which aim to optimize the flooding operation. Flooding schemes can be categorized in approaches either aiming to reduce or to increase the level of redundancy provided by the naive flooding approach.

Reducing the redundancy: The broadcast storm problem is known to be a serious problem of flooding [7]. It was shown that flooding is vulnerable to packet collisions due to contention even in networks with moderate density[8]. In moderate to dense networks flooding causes lots of redundant (duplicate) messages wasting network capacity and thus increasing network contention and packet collisions. This is because every node receives the message from all its neighbors in wireless communication range and only a few messages are lost due to collisions. Thus there is a need for flooding protocols which do not cause the broadcast storm problem. The basic approach is to reduce the number of redundant broadcast packets. However, this can reduce the reachability, i.e. not all nodes will receive the flooding message. Thus there is a tradeoff between redundancy and reachability.

In the literature a large amount of approaches to reduce redundant messages were proposed. The first class proposes the use of routing overlay networks whereas the second class uses algorithms to selectively drop messages. Routing overlay networks like multicast trees[9] or backbone networks[10] allow an efficient broadcast of the flooding message, i.e. the message is rebroadcasted only by a subset of nodes in the network. The main drawback of such approaches is that because of the frequently changes in the underlying routing structure due to mobility the overlay routing structure need to be updated very frequently resulting in high maintenance costs or reduced reliability thus making it unsuitable for MANETs. The second class of approaches is based on the idea to use only local information for the decision whether a message need to be rebroadcasted or dropped. In probabilistic flooding [11] approaches the message is rebroadcasted with a certain probability which can be fixed or can depend on the local network topology. In counter-based flooding the message is only rebroadcasted if the number of overheard flooding messages is smaller than a given threshold. With multi-point relaying (MPR [12]) the redundancy is reduced by restricting the rebroadcasting of a flooding message to nodes being selected as MPR nodes. Moreover, Lipman et al. [13] proposed a localized minimum spanning tree based flooding.

The challenge faced by all approaches is not to create the problem of poorly connected nodes where the flooding message can fail due to insufficient redundancy, i.e. the message is rebroadcasted by too few neighbors.

Increasing the redundancy: Flooding has also been shown to be susceptible in sparse networks where nodes have only a small number of neighbors which are often connected by links with high packet losses due to weak signal and external interference. Sometimes there exists only a single path connecting two parts of the network. Here flooding would fail to reach the poorly connected nodes. Hence, the objective is to increase redundancy in order to make sure that also poorly connected nodes will receive the flooded message. Possible strategies to achieve this are: i) rebroadcasting the flooding message multiple times, ii) repetition of the whole flooding, i.e. the ultimate source of the flooding repeats the flooding multiple times, iii) using other link-layer mechanisms than broadcasting, i.e. unicasting, multicasting [14, 15, 16] or anycasting which gives a direct feedback on the success of the packet transmission. The challenge faced by approaches of the third category are to find a feasible neighbor abstraction as well as the neighbor selection algorithm. Both aspects will be discussed in Section 8 in detail.

3. Properties of Real World Networks

The Humboldt Wireless Lab (HWL) is a stationary wireless mesh network (WMN) at the campus of the Humboldt University, Germany [6]. It consists of about 100 mesh nodes based on IEEE 802.11a/b/g which are deployed indoors as well as outdoors. For the experiment we selected a subset of 40 nodes. Fig. 1 shows two important characteristics of HWL namely the distribution of the link qualities, measured as Packet Delivery Rate (PDR), as well as node degree, i.e. number of neighbors. The following neighbor abstraction was use. Every pair of nodes having a link with a PDR of at least 50% are neighbors.

The following observations can be made. First, links with intermediate PDR are common. This is due to external (WiFi and non-WiFi devices) and internal (e.g. collisions due to hidden node) interference [17]. Even at the most robust modulation coding scheme, here 1 Mbps in 802.11b, the majority of links is lossy. Second, the network is heterogeneous with respect to the node degree, i.e. there are dense parts in the network where nodes have lots of neighbors and sparse parts where nodes have only a few number of neighbors.

Despite the fact that the HWL is a stationary network this is a challenging environment for a flooding protocol. Note, that in MANETs the situation is more severe due to the increased channel variation because of mobility of the nodes.

The challenge faced by a flooding protocol is to adapt its level of redundancy to the different sparse and dense parts of the network.

4. Performance Metrics

To be able to compare the different flooding approaches with each other the following performance metrics are used:

1.) **Reliability** which is the percentage of network nodes receiving the flooding message.

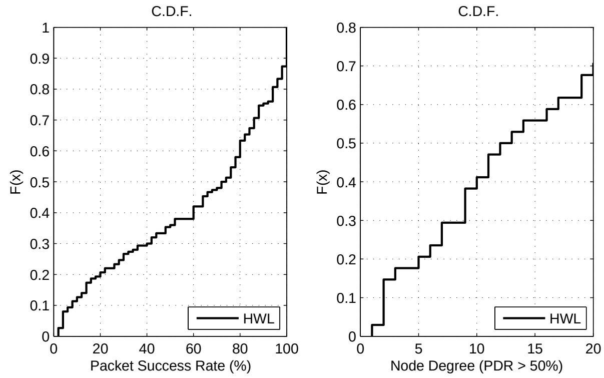


Figure 1: Link quality & node degree measured in HWL testbed (802.11b, 1 Mbps, frame size of 100 Bytes, RF channel 6).

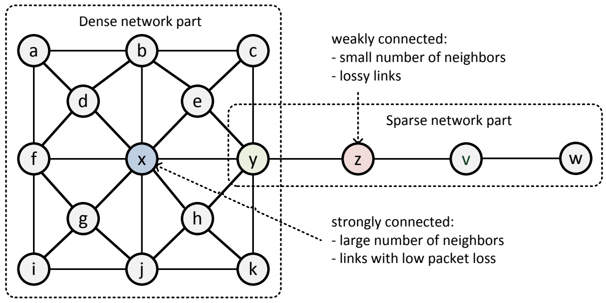


Figure 2: Illustration of a network having dense and sparse parts.

2.) **Efficiency** which is measured as the total number of flooding frame transmissions in the network divided by the number of nodes which successfully received the flooding message.

3.) **Latency** measured as the duration from the point in time the flooding operation was started to the point in time the flooding message was received by the last node. Nodes which do not receive the message are omitted.

Obviously there is a tradeoff between reliability and efficiency. The higher the reliability the lower the efficiency, i.e. in general it requires more effort in terms of frame transmissions to cover the hard to be reach nodes in the network. Since the latency is only calculated from the nodes which receive the flooding message, again we have a tradeoff between reliability and latency. The latency is small as long as only the easily accessible nodes are reached.

The required reliability, latency and efficiency are application depend. If we target to use flooding for the route discovery in routing protocols we have to distinguish between reactive and proactive routing protocols. For the former one a very high reliability is very important because a single flooding is used for route discovery and any failed route discovery creates a high latency on the application layer. Moreover, even if a route was discovered it is likely that it is only suboptimal in terms of the routing metric decreasing the performance of the corresponding network flow. With proactive protocols the situation is different. Here the route discovery is performed regularly so that a single failed flooding is not a problem. However, the flooding must be efficient because otherwise network capacity is wasted due to the periodic floodings initiated by every node in the network. Finally, a very reliable flooding is required when using higher layer services like Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) or when using flooding for content distribution, e.g. distribution of a binary router image.

5. Problem Statement

The objective of this paper is to improve the flooding operation in MANETs in terms of reliability, efficiency and latency where overlay-based approaches fail due to mobility. Since there is a tradeoff between these three metrics a framework for flooding is proposed allowing to shift the optimization in one of these three directions.

In particular we aim to achieve a reliable flooding scheme. Here we focus on networks with inhomogeneous node densities where a flooding scheme needs to adapt the provided redundancy depending on whether it operates in sparse or dense parts of the network. This cannot be achieved by approaches like gossiping, probabilistic flooding as well as MPR approaches because they just tackle the inefficiency by reducing the amount of redundancy and thus are unable to provide sufficient redundancy in the sparse parts of the network to improve the reliability.

Moreover, the objective is on a practical flooding scheme which can be implemented on top of existing physical and MAC layer protocols like IEEE 802.11 or 802.15.4 without any modifications.

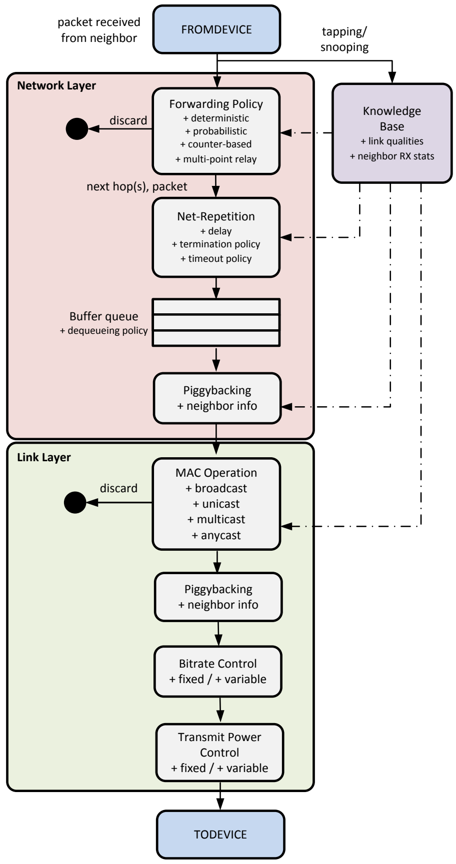


Figure 3: General flooding framework.

6. General Flooding Framework

A plenty of approaches were proposed in the literature to optimize the flooding operation. In this section we propose a general framework for flooding which can be used to implement the variety of approaches. The proposed framework consists of three components (Fig. 3): i) network layer, ii) link layer and iii) knowledge base. Each component can be configured independently.

6.1. Network Layer

The network layer for flooding consists of four main blocks: i) forwarding decision, ii) repetitive transmission, iii) a buffer queue and iv) a piggybacking component (Fig. 3).

The forwarding decision can be based on different policies like deterministic, probabilistic, counter-based or multi-point relaying (MPR [12]). The naive flooding is an example for deterministic forwarding. Note, that some approaches like MPR restrict the forwarding of the flooding message to a set of nodes (e.g. the MPR set in [12]).

The repetitive transmission block is responsible for repetitive sending a flooding message on the network layer which can be either zero (corresponds to naive flooding) or a higher number. For repetitions larger than zero a timeout counter is set to schedule the repetitive transmission. Note, that using the information from the knowledge base (see Sec. 6.3) a scheduled transmission can always be canceled. This depends on the used flooding decision, e.g. in the MPR approach a scheduled transmission is canceled if we already know that all of our neighboring MPRs were able to receive the flooding message.

The buffer queue is used to handover the flooding packets to the link layer. Different dequeueing strategies can be applied here.

Finally, to avoid redundant packet transmissions information from the knowledge base about which node already received the flooding message need to be propagated in the local neighborhood. This is the objective of the piggybacking block which attaches such information to a flooding packet. So any neighboring node can learn about successful reception of the flooding message by overhearing the flooding messages and reading the piggybacking information.

Note, that at any step the forwarding of a received flooding message can be canceled based on information from the knowledge base.

6.2. Link Layer

The link layer for flooding consists of four main blocks: i) MAC operation, ii) piggybacking component, iii) bitrate control and iv) transmit power control (Fig. 3).

Four different options are available for the MAC operation in order to transmit the flooding message: i) broadcasting, ii) unicasting, iii) multicasting and iv) anycasting.

Most flooding approaches use broadcasting. Some propose to use multicasting in order to make sure that the flooding reaches all neighbors [14, 15, 16]. Here a packet is transmitted to more than one receiver. On successful reception every receiver acknowledge the transmission by sending an ACK packet which can be send using a slotted acknowledgment scheme [18, 19]. The transmission is repeated until the flooding message is acknowledged by all multicast peers or the maximum number of retries was reached. However, we believe that also link layer operations like unicasting or anycasting can be used. In unicasting the node has to select a neighboring node as peer node for transmission. The transmission is repeated until the flooding message is correctly received by this peer or the maximum number of retries was reached. In anycasting the node selects a set of neighboring nodes for transmission similar to multicasting with the difference that it sufficient when at least one candidate node was able to successfully receive the packet.

Note, that approaches which rely on unicasting, multicasting or anycasting need to provide an algorithm for the selection of the peer node(s).

The piggybacking component attaches information about the set of nodes which are expected to receive the flooding message. When using unicasting as MAC operation one might add the link layer destination of the packet. Note, that this is a speculative approach because also a unicast transmission can fail.

The last two components are bitrate (modulation & coding scheme) and transmit power control. In dense parts of the network with strong links it might be favorable to use a higher bitrate or lower transmit power.

Within the link layer an enqueued flooding message can be canceled based on information from the knowledge base. Thus it is possible than an ongoing unicast transmission is canceled before being acknowledged or reaching the maximum number of retries.

6.3. Knowledge Base

The objective of the knowledge base is to hold information about the local neighborhood of a node. First, it contains information about link qualities to and between neighboring nodes. Second, it keeps statistics about which flooding message was received by which neighbor based on overhearing flooding messages. The former is obtained using link probing with a packet size which corresponds to that of the flooding message. The latter is determined using the algorithm given in Listing 1. From an overheard flooding message we can get the unique flooding ID (ultimate source of the flooding message and a sequence number) which is used to lookup the corresponding knowledge base. We can add both the ultimate source of the flooding as well as the source address of the last hop to the knowledge base.

7. Proposed Flooding Solution

In this section we propose our flooding scheme which is based on the general framework for flooding given in the previous section. Our approach is based on three components. First, we repeat the transmission of the flooding message at the network layer as long as we find strongly connected neighboring nodes which so far have not successfully received the flooding message. In each iteration the most promising neighboring node is selected according to a novel metric. Second, to achieve a high reliability we use unicasting at the link-layer for the transmission of flooding messages to the selected peer node. Third, to achieve an efficient solution we piggyback flooding messages with the address of nodes we expect that they receive the flooding message which is feasible due to the used link-layer unicasting.

Algorithm 1 Knowledge base is updated on overhearing a flooding packet p.

procedure UPDATEKNOWLEDGEBASE(p)
  $\mathrm{fl\_ID} \leftarrow p^{\mathrm{fl\_ID}}$ ▷ get the flooding ID from the packet.
  $V^{\mathrm{fl\_ID}} \leftarrow \mathrm{getKB}(\mathrm{fl\_ID})$ ▷ get knowledge base for flooding with ID flId
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{\mathrm{flooding\_src}}$ ▷ add ultimate source of the flooding
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{\mathrm{src\_addr}}$ ▷ layer-2 source of this packet already received the flooding message
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{V^*}$ ▷ add the piggybacked information
end procedure

7.1. Network Layer

Neighbor abstraction. The following neighbor abstraction model is used. The one-hop neighbors of node x are computed as follows (Listing 2). First, any node having a link to x with a PDR of greater than zero is a potential one-hop neighbor (line 3). Second, we remove from this set those nodes which can be reached via multi-hop at lower cost, i.e. the shortest path using multiplicative PDR as path metric (Alg. 3) has two or more hops. Note, that the shortest path is calculated using the subgraph representing the two-hop neighborhood of x only.

Example: With the illustrative example given in Fig. 4 the value of $\mathrm{strong\_nb}(x)$ is calculated. Here the edges represent the PDR of a link. For simplification here all links are used to be bi-directional. For each neighbor node of x the algorithm calculates in the first step the shortest path using only nodes from the set N^*. As path metric the multiplicative PDR is used, i.e. the PDR of a path is the product of the link PDRs. In our example this calculated value is depicted in the upper right corner of each neighboring node. In the second step all neighboring nodes having a path metric of more than the link PDR towards x are removed from the set of one-hop neighborhood.

Forwarding decision. The forwarding decision on the network layer is deterministic. The basic idea is to repeat the transmission of the flooding message at the network layer as long as we find strongly connected neighboring nodes which so far have not successfully received the flooding message (see $\mathrm{strong\_nb}(x)$.

The detailed algorithm looks as follows. At first we calculate the set of strongly connected one-hop neighbors using our neighbor abstraction model:

$$C = \{c \mid c \in \text{strong\_nb}(x) \land c \notin V_x\} \tag{1}$$

where V_x represents the nodes who already received the flooding message which are calculated using the information from the knowledge base.
Thereafter, we keep from C only those neighboring nodes covering a non empty set of nodes not covered by any other neighboring node including x:

$$C^{'} = \{c \mid c \in C \land (\text{nb}(c) \backslash (\text{nb}(\text{nb}(x) \backslash \{c\}) \cup \text{nb}(x))) \neq \emptyset\} \tag{2}$$

here $\text{nb}(x)$ represents any neighbor of x (Listing 4).
Finally, we keep $C^{'}$ if it is not empty otherwise we take C:

$$C^{''} = \begin{cases} C, & \text{if } C^{'} = \emptyset \\ C^{'}, & \text{otherwise} \end{cases} \tag{3}$$

The transmission of the flooding message at the network layer is repeated as long as $C^{''}$ is not empty and the maximum number of net layer transmissions (R_{NET}) is not reached.

The very first transmission is scheduled immediately. The subsequent transmissions are performed using a uniform random backoff in some interval I_{BO}, e.g. [0, 25 ms], after the completion of the link layer operation of the previous transmission (using TX feedback packets).

Piggybacking. At the networking layer the piggybacking information attached to a flooding packet contains just the information about the nodes in the local neighborhood which we know that they already received the flooding message.

7.2. Link Layer

In contrast to other approaches which are using broadcasting at the link layer to forward a flooding message we are exploiting the benefits of unicasting. The basic idea is not to rebroadcast but to reunicast a flooding message towards a carefully selected neighboring peer node. By having a explicit link-layer acknowledgment we are able to deal with the problem of poorly connected nodes (weak signal or interference) where the flooding message can fail due to insufficient redundancy. Furthermore, in contrast to broadcasting we have an efficient way to deal with collisions due to the exponential backoff scheme used for unicasting which is an important mechanism in saturated networks.

MAC operation. Our approach is to use unicasting for the transmission of flooding message. Therefore, we formalize the objective of selecting a unicast peer for the transmission of a flooding message in the following way:

Instance: Node x which received the flooding message.

Objective: Find a unicast peer node c from $C^{''}$ which ether covers the maximum number of nodes not covered by any other neighboring node including node x normalized by the size of the common neighborhood of c and x, $c \in C^{'}$. If $C^{''} = C$ select a random unicast peer from C.

This optimization problem can be formulated as follows:

$$c = \arg\max_{c} \left\{ m_c^x \middle| c \in C^{''} \right\} \tag{4}$$

where the set $C^{''}$ is calculated as in eq. 3 and subject to the metric m which is calculated as:

$$m_c^x \leftarrow \frac{|\text{nb}(c) \backslash (\text{nb}(\text{nb}(x) \backslash \{c\}) \cup \text{nb}(x))|}{|(\text{nb}(\text{nb}(c)) \cup \text{nb}(c)) \cap \text{nb}(x)|} \tag{5}$$

Complexity: The optimal solution for this peer selection has a quadratic complexity in the number of two-hop neighbors M, i.e. $\mathcal{O}(M^2)$.

Example: Our metric can be best explained using the example given in Fig. 2. Here we assume that none of the nodes received the flooding packet. Let us assume that node z has to estimate the candidate with the highest metric. In the example z has two neighbors y and v. The calculated metrics would be $m_y^z = \frac{|\{c,e,x,h,k\}|}{|\{y,v\}|} = 2.5$ and $m_v^z = \frac{|\{w\}|}{|\{y,v\}|} = 0.5$ respectively. Hence, node z would choose node y as unicasting peer.

Piggybacking. The piggybacking information attached to a flooding packet contains additional information about the set of local neighbors which are expected to receive the flooding message:

$$V_x^* = \begin{cases} C^{'}, & \text{if } C^{'} \neq \emptyset \\ c, & \text{otherwise} \end{cases}$$

Note, we add just the next hop unicast peer, c, to the piggybacking list, if $C^{'}$ is empty.

Algorithm 2 Select strongly connected one-hop neighbors.

procedure STRONG_NB(x)
    $N^* \leftarrow \text{nb}(\text{nb}(x)) \cup \text{nb}(x)$ ▷ two-hop nbs incl. x
    $C \leftarrow \text{nb}(x)$ ▷ candidate set
    for all $c \in \text{nb}(x)$ **do**   ▷ ..
        if $\text{PDR}(x, c) < \text{shortest\_path}(x, c, N^*)$ **then**   ▷ shortest path from x to c with PDR as multiplicative path metric in subgraph $\forall(c1, c2) \in E : c1, c2 \in N^*$
            $C \leftarrow C \backslash \{c\}$ ▷ remove c from candidate set
        end if
    end for
return C
end procedure

7.3. Knowledge Base

We piggyback flooding messages with information about nodes we know that they already received the flooding message (p^{V^*}). Moreover, we can also add the layer-2 destination address of a flooding packet ($p^{\text{dst\_addr}}$) to the knowledge base

Algorithm 3 Link metric from x to y as seen from z where V is set of nodes which already received the packet.

procedure LINK_METRIC(x,y,z,V)
  if $(x == z)$ and $(y \in V)$ **then**
return 1.0 ▷ if x equals z or y has already received
  end if
return $\mathrm{PDR}(x, y)$ ▷ Use PDR as metric.
end procedure

Algorithm 4 All direct neighbors of x with sufficient good link quality. N

procedure NB(x)
  $N^* \leftarrow (n \mid n \in N \wedge (x, n) \in E \wedge \mathrm{PDR}(x, n) > 0)$
return N^*
end procedure

if we immediately (after T_{SIFS}) receive an corresponding acknowledgment packet afterwards. Thus the *updateKnowledgebase()* function for the knowledge base need to be extended. Here we process not only the flooding unicast packets but also the layer-2 acknowledgment packets.

Moreover, the knowledge base is an active component in our solution. Every time the set of nodes which already received the flooding message (V_x) changes, the corresponding flooding message scheduled for transmission is discarded, the number of net layer transmissions is decremented by one and a TX feedback packet (status abort) is created which is afterwards consumed by the networking layer resulting in a repetition of the flooding message by recalculating C''.

Algorithm 5 Knowledge base is updated on overhearing a flooding packet p.

procedure UPDATEKNOWLEDGEBASE(p)
  $\mathrm{fl\_ID} \leftarrow p^{\mathrm{fl\_ID}}$ ▷ get the flooding ID from the packet.
  $V^{\mathrm{fl\_ID}} \leftarrow \mathrm{getKB}(\mathrm{fl\_ID})$ ▷ get knowledge base for flooding with ID flId
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{\mathrm{flooding\_src}}$ ▷ add ultimate source of the flooding
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{\mathrm{src\_addr}}$ ▷ source of this packet already received the flooding message
  if $\mathrm{isUnicastData}(p)$ & $\mathrm{rxCorrespondingAck}()$ **then**
    $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{\mathrm{dst\_addr}}$ ▷ dst of flooding packet can be added if we overhear the corresponding ack packet, i.e. dst address if ack equals $p^{\mathrm{src\_addr}}$ and gap between p and ack equals T_{SIFS}.
  end if
  $V^{\mathrm{fl\_ID}} \leftarrow V^{\mathrm{fl\_ID}} \cup p^{V^*}$ ▷ add piggy-backed information about nodes which received the flooding message
end procedure

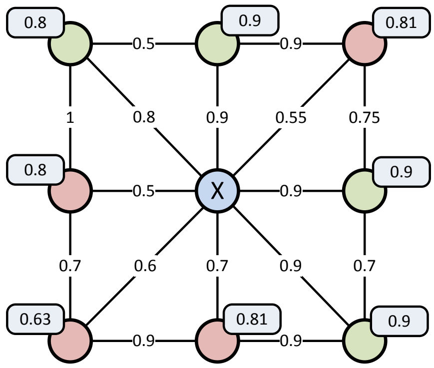


Figure 4: Example network where the vertices represent the PDR of the link between the two nodes.

7.4. Known Limitations

The proposed flooding scheme has limitations. First, only a fixed bitrate on the physical layer is used, i.e. the most robust modulation and coding. Second, we keep the transmit power fixed to the maximum power.

8. Discussion

In this section we discuss our proposed approach and compare it against other similar methods from literature.

8.1. Trading Reachability against Efficiency

As mentioned in section 4 there is a tradeoff between reachability and efficiency. In general to cover all nodes in the network, i.e. including those hard to reach, you have to pay a lot in terms of number of frame transmissions. Therefore, our proposed method provides two configurable parameters R_{NET} and R_{MAC} which allows us to limit the maximum number of repetitive transmissions on the network and the MAC layer respectively. For applications which require a very high reachability (e.g. content distribution or ARP and DHCP) both values have to be set to a large value, e.g. 3 and 6. A higher efficiency at the cost of reachability can be achieved by using smaller values, e.g. 1 and 2.

8.2. Neighbor Abstraction

There is a need for a metric which allows us to decide whether a node is a neighbor of another node or not. Most approaches propose to use metrics like ETX/ETT and check whether the estimated value is above some threshold. However, the selection of the threshold is arbitrarily. Other approaches propose to use the geographical distance [20] which is however not a good idea in highly shadowed and/or faded environments. In contrast, in our approach we have a clear neighbor abstraction. A node is a neighbor of another node if the shortest path between both nodes using multiplicative PDR as path metric has a length of one.

8.3. *Comparison to MPR*

In the MPR approach [21] a forwarding node decides on the set of next hop forwarder, i.e. the so-called MPR set. The flooding message itself is simply rebroadcasted. Hence there is no link layer protection for packet loss and thus the flooding message can fail. Afterwards, the flooding message is only allowed to be rebroadcasted by the nodes from the MPR set. In contrast, in our approach there is no pre-selection of forwarding nodes. Every node has the same chance to forward the flooding message. However, we make sure that important nodes in our neighborhood, i.e. those from C' having the highest metric (eq. 5), will receive the flooding message first using reliable link layer unicasting.

9. Performance Evaluation

The performance of the proposed flooding scheme is analyzed in this section by means of simulations. First, we describe our methodology. Second, we present the flooding schemes under study. Third, a performance evaluation of different flooding schemes regarding performance metrics like reachability, efficiency and latency (Sec. 4) is provided.

9.1. *Methodology*

The proposed solution was evaluated by mean of network simulations. We have implemented different flooding schemes using the Click router framework [22] and evaluated them in the NS-2 network simulator [23]. The flooding operation started 100 s after the node placement to make sure that PDR value of any link in the link table stabilized. A random node was selected as flooding source and a single packet with a size of 100 Bytes at application layer (132 Bytes at MAC layer) was transmitted. At the end of the flooding we calculated the share of nodes which receive the flooding message (reachability), the duration of the flooding as well as the number of MAC transmissions. The experiment was repeated for 20 other random flooding sources. Finally, the experiment was repeated for 25 different node placements.

The wireless path loss model was chosen so that a communication range of up to 65 m was possible without any packet loss whereas at 80 m the packet loss was 90%. Moreover, a block fading model was used, i.e. the fading was constant for the duration of a single frame.The most important remaining parameters are given in Table 1.

Parameter	Value
PHY/MAC layer	IEEE 802.11b
Bitrate (MCS)	1 Mbps (fixed)
Communication range	65 m (PDR=1), 80 m (PDR=0.1)
Shadow fading σ	2 dB
No. of nodes	100, 200
Packet size (application)	100 Bytes
Node placement	Random & multi box
No. of seeds	20×25
TX power	24 dBm

Table 1: Simulation Parameters

9.2. *Flooding Schemes under Study*

The proposed flooding scheme will be compared with the naive flooding used as baseline as well as state-of-the-art flooding schemes suitable for MANETs. Thus only approaches which rely on local information about the topology are selected. Note, that due to mobility approaches relying on overlay routing structures are inappropriate, i.e. the overlay structure needs to be updated very frequently resulting in high maintenance costs or reduced reliability. Hence the following flooding schemes are evaluated:

1.) **Naive flooding** which represents the base line. Every received flooding message is rebroadcasted exactly once.

2.) **Flooding with repetitive rebroadcasting (rep. RBC)** where every received flooding message is rebroadcasted multiple times. The number of repetitions r was varied from 0 to 3.

3.) **Probabilistic flooding (prop. RBC)**[8] where a node rebroadcasts a flooding message only with a given probability: a) 95% and b) 85%. The number of repetitions r was varied from 1 to 4. Note, that there is just a single Bernoulli trial which decides whether the flooding message is discarded or rebroadcasted r times.

4.) **Multi-point relaying (MPR)** where a flooding message is rebroadcasted only by nodes in the MPR set as calculated by the previous hop [12]. We extended the approach by allowing the flooding message to be rebroadcasted multiple times, i.e. the parameter r is the number of repetitions.

5.) **Flooding with repetitive reflooding (rep. RFL)** where the source of the flooding repeats the whole flooding multiple times [24], i.e. the parameter r is the number of repetitions where $r = 0$ corresponds to the naive flooding.

6.) **Proposed approach** where the maximum number of retries on the MAC layer and NET layer are configurable parameters: $R_{\text{MAC}} = 0, 2, 4, 6$ and $R_{\text{NET}} = 0 - 3$. The backoff interval I_{BO} was set to [0, 25 ms].

9.3. *Simulation Results*

In this section we present results from the evaluation of the performance of the proposed and other selected flooding schemes. First, in Sec. 9.3.1, we study the performance in a random network where even a simple flooding scheme is already able to achieve a high reachability. Here we are primary interested in comparing the efficiencies, i.e. number of required MAC transmissions per reached node, of the different flooding schemes. Second, in Sec. 9.3.2, we focus on scenarios which are challenging for naive flooding. Here several densely network parts are connected by very sparse parts of the network (i.e. bridges), making the naive flooding scheme performance

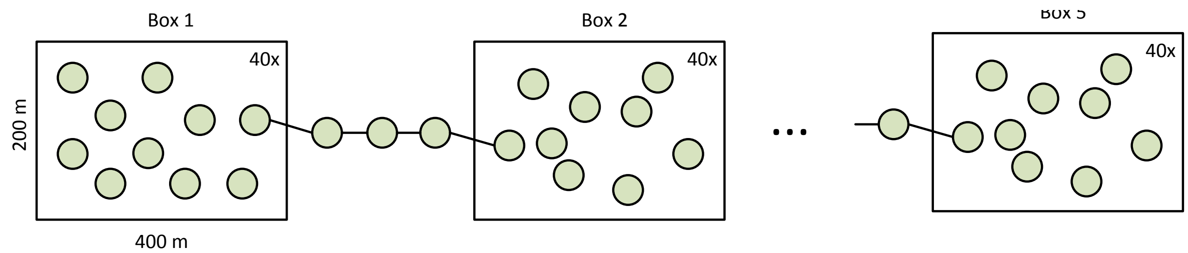


Figure 5: Placement simulating dense and sparse parts of the network.

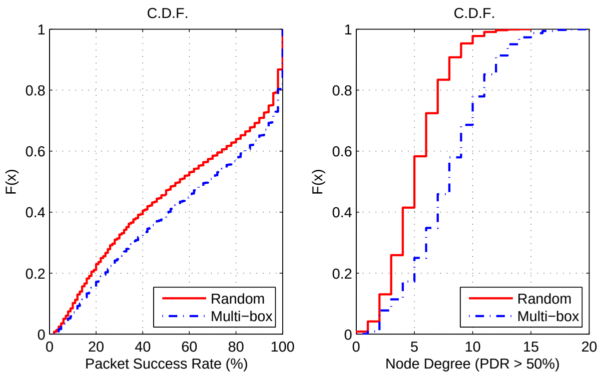


Figure 6: Distribution of link qualities (PDR) and node degrees for the two placements.

worse in terms of reachability because insufficient level of redundancy.

9.3.1. Random Networks

Experiment. We consider a network where 100 nodes were randomly placed as follows. We made sure that every placed node had at least 1 neighbor with a PDR of at least 0.9. Moreover, the maximum number of neighbors was restricted to 15.

Results. Fig. 7a shows the boxplot for the reachability metric where the diamond represents the mean value. As expected the naive flooding performs worse, i.e. median of 94% and mean of 86%. The reachability can be improved by using flooding with repetitive rebroadcasting (rep. RBC). Here we can see that we can almost reach every node in the network besides some outliers. However, even with four repetitive rebroadcasts there is a run where only 1% of the nodes, i.e. only the ultimate source of the flooding, were reached. When using probabilistic flooding (prop. RBC) we see that the reachability is decreased when using a smaller value for the forwarding probability. But in all cases the reachability is lower compared to repetitive rebroadcasting. This is clear indication that self-interference, i.e. collisions of the flooding packets, is not the cause for the low reachability but rather the existence of weak or faded links. This statement is reinforced by the fact that the reachability is significantly increased when using repetitive rebroadcasting, i.e. with three repetitions 99% and 97% respectively. It is also possible to achieve a high reachability when using flooding with repetitive reflooding (rep. RFL). The classical MPR approach ($r = 0$) performs worst, i.e. on average only 47% of the nodes were covered. When using repetitive rebroadcasting ($r > 0$) the reachability can only be slightly improved. Even with three repetitions on average only 87% of the nodes were covered. Our proposed flooding scheme achieves the highest reachability in the configuration $R_{\text{MAC}} = 6$, $R_{\text{NET}} = 3$. Here there were only four outliers out of 500 runs were the smallest had a value of 91%.

The downside of having a high reachability is a low efficiency (Fig. 7b). To achieve a reachability of close to one the best approach, i.e. our proposed scheme with $R_{\text{MAC}} = 2$, $R_{\text{NET}} = 1$, requires 2.3 times the number of MAC transmissions compared to naive flooding. Thus the additional 130% of MAC transmissions are required in order to reach the uncovered 14% of the nodes in naive flooding. Moreover, some approaches are able to achieve the same level of reachability at a much lower cost. When targeting a reachability of close to one the only feasible approaches are our proposed scheme with $R_{\text{MAC}} = 2$, $R_{\text{NET}} = 1$, rep. RBC with $r = 3$ and rep. RFL with $r = 4$. The efficiencies of the three approaches, however, differ greatly. Our proposed scheme requires less than half the number of MAC transmissions (50% and 47%) to achieve the same level of reachability. The MPR approach is the most efficient one requiring only one third of MAC transmissions per reached node compared to naive flooding.

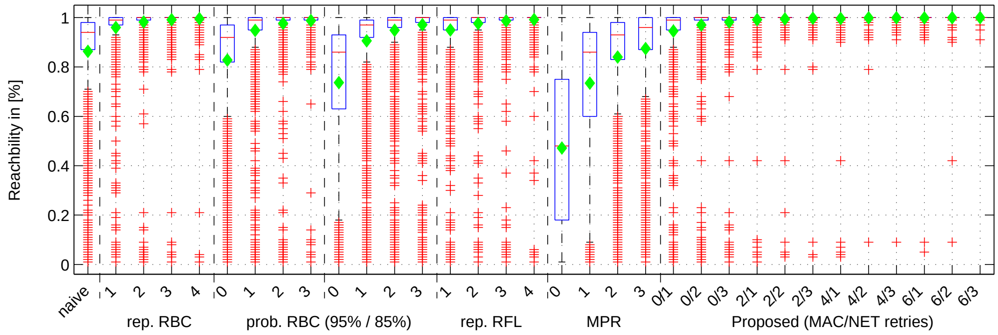
Regarding the delay we see that approaches having a high reachability have also an increased delay. Again, from the three approaches having similar high reachability, i.e. our proposed scheme with $R_{\text{MAC}} = 2$, $R_{\text{NET}} = 1$, rep. RBC with $r = 3$ and rep. RFL with $r = 4$, our approach has the lowest delay which is on average smaller by 10% and 7% respectively. Most importantly in our scheme the outliers are much smaller.

Summary. Our approach is the best when reachability is the top goal. It achieves the same level of reachability at a much lower cost and also lowest delay. The classical MPR approach performs worst in terms of reachability.

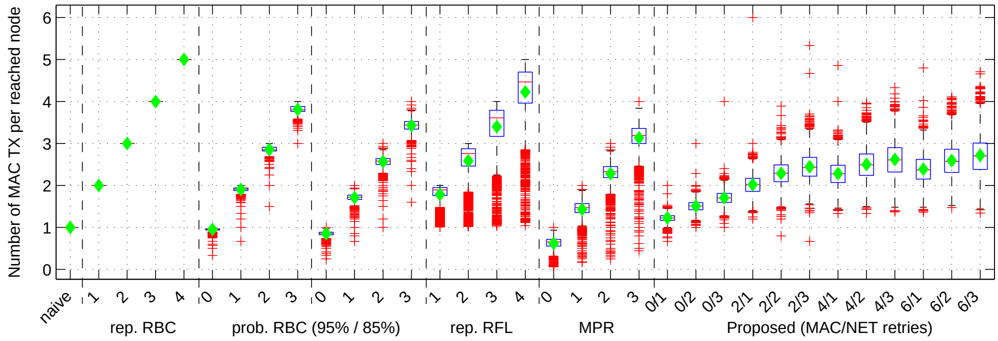
9.3.2. Loosely Connected Networks

Experiment. We consider a network where the nodes where placed according to the scheme give in Fig. 5. In total 200 nodes were distributed evenly on 5 bounding boxes, i.e. 40 nodes were placed randomly in each box. Neighboring boxes were connected with a string of three nodes. The objective was to simulate networks with dense parts which are loosely connected, e.g. a wireless network spanning multiple buildings or floors. The resulting distribution of link qualities (PDR) and node degrees is given in Fig. 6. We see that the values are quite similar to the random network in the previous section.

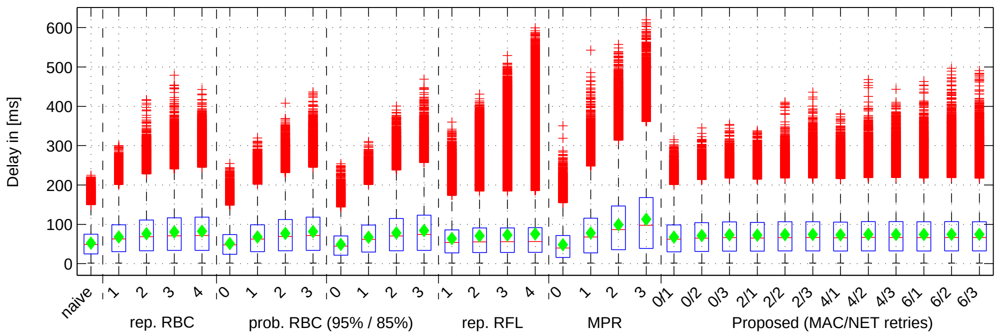
Results. Fig. 8a shows the boxplot for the reachability of



(a) Reachability.



(b) Efficiency.

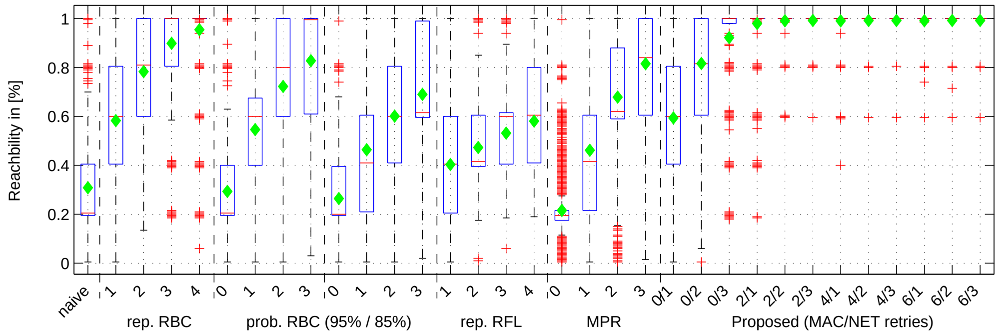


(c) Delay.

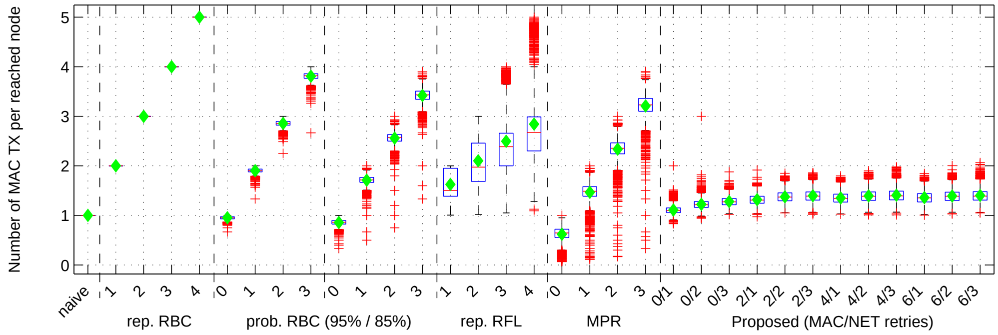
Figure 7: Performance in random networks.

the different approaches. Here we can clearly see that the naive flooding fails to achieve a reasonable reachability, i.e. in the median only 20% of all nodes were reached. This corresponds to just the nodes in the box where the flooding was initiated, i.e. the naive flooding was unable to overcome just a single bridge connecting two boxes. Only in some rare cases if was successful. With repetitive rebroadcasting (rep. RBC) the reachability can be improved to some degree. With four repetitions a mean value of 95% was achieved, but lots of outliers remain. With probabilistic flooding (prop. RBC) the reachability is very low, 29% and 26 respectively. Moreover, reducing the forwarding probability further decreases the reachability. This scheme reduces the redundancy in situations where the already provided redundancy is too low, i.e. the node at the bridges. Even with four repetitions the reachability remains low; i.e. 83% and 69% respectively. Again, the results leads us to the conclusion that weak links and not packet collisions are the cause for the low reachability. The situation is also severe when using repetitive reflooding (rep. RFL). Even with $r = 4$ on average only 58% of the nodes were reached. Here we clearly see the disadvantage of this scheme - any progress in terms of traversed bridges is discarded when the flooding is repeated. Again, the classical MPR approach performs worst, i.e. only 20% average reachability. Unfortunately the increase in the number of repetitions does not lead to a high reachability, i.e. mean value of just 81% for $r = 3$. The proposed flooding scheme is able to reach nearly all nodes (99.2% on average) when using configuration $R_{\mathrm{MAC}} = 4$, $R_{\mathrm{NET}} = 2$ or higher.

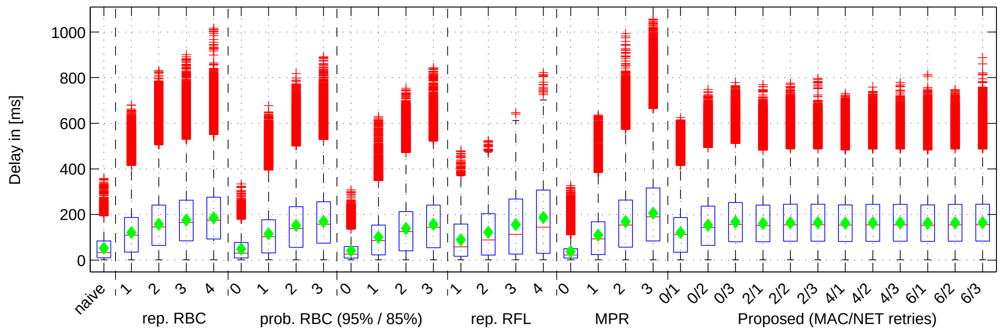
Next, we take a look at the efficiency (Fig. 8b). The highest achieved mean reachability among all methods excluding our



(a) Reachability.



(b) Efficiency.



(c) Delay.

Figure 8: Performance in loosely connected networks.

proposed scheme is just 95% which is achieved by repetitive rebroadcasting with $r = 4$. However, this scheme requires 3.8 times more MAC transmissions to achieve the same level of reachability compared to our method $R_{\text{MAC}} = 2$, $R_{\text{NET}} = 1$. This clearly indicates the advantage of the proposed scheme. Finally, we see that with increasing values of R_{MAC} and R_{NET} the efficiency does not increases but converges to some value. So for networks with unknown topology we can recommend to set both parameters on a high value.

Regarding the delay we again compare repetitive rebroadcasting with $r = 4$ with our method $R_{\text{MAC}} = 2$, $R_{\text{NET}} = 1$. With our approach the mean delay is 13% lower. Furthermore, the delay of the max outliers is much lower.

Summary. Our approach is the only method which is able to achieve a reachability close to 1. All other approaches achieve a reachability of less than 95%. Our approach can covers 95% of the nodes requiring 74% less MAC transmissions and having the lowest delay compared to the best known flooding scheme. Again, the classical MPR approach performs worst.

10. Conclusions & Future Work

Flooding is an important communication primitive used in MANETs as well as wireless stationary mesh networks. It serves as a building block for content distribution and higher protocols like routing and services like ARP and DHCP. Therefore, it must be reliable, i.e. the flooding message should be successfully received by all nodes in the network, efficient, i.e. the number of MAC transmissions should be low, and have a low delay.

In this paper we proposed a novel flooding scheme which exploits the possibilities provided by the link layer in order to improve the flooding operation. By means of network simulations we showed that the proposed scheme is able to achieve a reachability of close to one even in very challenging networks where all other known methods fail. Moreover, our proposed scheme is able to achieve a high reachability in a very efficient way, e.g. in challenging networks the best known solutions requires up to four times more MAC transmissions to achieve the same level of reachability. Finally, the proposed flooding scheme has a low delay.

The proposed flooding scheme can be implemented on top of existing standards like IEEE 802.11 or 802.15.4 without any modifications to the MAC layer.

As future work as a further way to improve the efficiency we consider to extend our flooding scheme with a variable bitrate (modulation & coding scheme) and transmit power control.

References

[1] G. Gaertner, V. Cahill, Understanding link quality in 802.11 mobile ad hoc networks, Internet Computing, IEEE 8 (1) (2004) 55–60.

[2] J. P. Macker, M. S. Corson, Mobile ad hoc networking and the ietf, ACM SIGMOBILE Mobile Computing and Communications Review 2 (1) (1998) 9–14.

[3] M. Bansal, R. Rajput, G. Gupta, Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations (1998).

[4] D. B. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks, in: Mobile Computing, Vol. 353, 1996, pp. 153–181.

[5] C. E. Perkins, E. M. Royer, Ad-hoc On-Demand distance vector routing, in: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, WMCSA '99, IEEE Computer Society, Washington, DC, USA, 1999.
URL http://portal.acm.org/citation.cfm?id=837511

[6] M. Scheidgen, A. Zubow, R. Sombrutzki, HWL - A high performance wireless sensor research network, in: Networked Sensing Systems (INSS), 2012 Ninth International Conference on, IEEE, 2012, pp. 1–4. doi:10.1109/inss.2012.6240552.
URL http://dx.doi.org/10.1109/inss.2012.6240552

[7] S. Y. Ni, Y. C. Tseng, Y. S. Chen, J. P. Sheu, The broadcast storm problem in a mobile ad hoc network, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom '99, ACM, New York, NY, USA, 1999, pp. 151–162. doi:10.1145/313451.313525.
URL http://dx.doi.org/10.1145/313451.313525

[8] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, J.-P. Sheu, The broadcast storm problem in a mobile ad hoc network, Wireless networks 8 (2-3) (2002) 153–167.

[9] H. Lim, 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, ACM, 2000, pp. 61–68.

[10] S. Butenko, X. Cheng, D.-Z. Du, P. M. Pardalos, On the construction of virtual backbone for ad hoc wireless networks, Cooperative Control: Models, Applications and Algorithms 1 (2003) 43–54.

[11] Y. Sasson, D. Cavin, A. Schiper, Probabilistic broadcast for flooding in wireless mobile ad hoc networks, in: Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, Vol. 2, IEEE, 2003, pp. 1124–1130.

[12] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, Optimized Link State Routing Protocol (OLSR), network Working Group Network Working Group (2003).
URL http://hal.inria.fr/inria-00471712

[13] J. Lipman, P. Boustead, J. Chicharo, J. Judge, Optimized flooding algorithms for ad hoc networks, in: Proceedings of the 2nd Workshop on the Internet, Telecommunications and Signal Processing (WITSP'03), Citeseer, 2003.

[14] J. Chen, M. Huang, Beam: broadcast engagement ack mechanism to support reliable broadcast transmission in ieee 802.11 wireless ad hoc networks, in: Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, Vol. 4, IEEE, 2004, pp. 2838–2842.

[15] S.-T. Sheu, Y. Tsai, J. Chen, A highly reliable broadcast scheme for ieee 802.11 multi-hop ad hoc networks, in: Communications, 2002. ICC 2002. IEEE International Conference on, Vol. 1, IEEE, 2002, pp. 610–615.

[16] K. Tang, M. Gerla, Mac layer broadcast support in 802.11 wireless networks, in: MILCOM 2000. 21st Century Military Communications Conference Proceedings, Vol. 1, IEEE, 2000, pp. 544–548.

[17] D. Aguayo, J. Bicket, S. Biswas, G. Judd, R. Morris, Link-level measurements from an 802.11b mesh network, SIGCOMM Comput. Commun. Rev. 34 (4) (2004) 121–132. doi:10.1145/1030194.1015482.
URL http://dx.doi.org/10.1145/1030194.1015482

[18] A. Zubow, M. Kurth, J. P. Redlich, An Opportunistic Cross-Layer Protocol for Multi-Channel Wireless Networks, in: Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, IEEE, 2007, pp. 1–5. doi:10.1109/PIMRC.2007.4394509.
URL http://dx.doi.org/10.1109/PIMRC.2007.4394509

[19] A. Zubow, M. Kurth, J. P. Redlich, Opportunistic Protocols in Multi-rate Environments, in: Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on, IEEE, 2008, pp. 743–751. doi:10.1109/SENSORCOMM.2008.24.
URL http://dx.doi.org/10.1109/SENSORCOMM.2008.24

[20] W. Lou, J. Wu, A reliable broadcast algorithm with selected acknowledgements in mobile ad hoc networks, in: Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE, Vol. 6, IEEE, 2003, pp. 3536–3541.

[21] A. Qayyum, L. Viennot, A. Laouiti, Multipoint relaying for flooding broadcast messages in mobile wireless networks, in: System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, IEEE, 2002, pp. 3866–3875.

[22] E. Kohler, R. Morris, B. Chen, J. Jannotti, F. M. Kaashoek, The click modular router, ACM Trans. Comput. Syst. 18 (3) (2000) 263–297.

[23] Ns2 - network simulator, http://www.isi.edu/nsnam/ns/ (2009).

[24] B. Blywis, Gossip routing based reliable route discovery in wireless multi-hop networks, Ph.D. thesis, Freie Universitaet Berlin (2012).