On Resilience Challenges in Opportunistic Networks

Maria Mehrparvar
Abstract

On Resilience Challenges in Opportunistic Networks

Maria Mehrparvar

In opportunistic networks, due to node mobility and sporadic connectivity, disconnection and network partitioning are prevalent. Nonetheless, the network resilience against such sporadic connectivity can be provided through adapting store-carry-and-forward-based routing protocols which exploit users' mobility to flow the data in the network even in the absence of end-to-end connectivity. Opportunistic networks, however, are exposed to some other challenges such as jamming attacks or buffer limitations which limit the usage of node contacts or node behavior. The main objective of this thesis is to understand the impact of these challenges on the resilience of the network. The challenges are applied in different network topologies using different forwarding protocols.

Generally, we find that store-carry-and-forward routing, by exploiting diversity in space-time paths, provides a high degree of resilience in the network, which depends on the network topology. The network resilience is maintained as long as significant number of nodes or node contacts are not affected. In the case of jamming, the studied routing protocols behave similarly with the exception of spray and wait routing which for some messages results in delay improvement while intensifying the challenge. For limited buffer sizes, spray and wait again shows different behavior in the low-traffic network where the average delay of delivered messages improves much more significantly compared to the other studied routing protocols, though with increasing the buffer size many more messages get delivered.
To My Loved Ones...
Acknowledgements

I would like to express my special gratitude to my supervisor, Christian Rohner, for his guidance, encouragement and great support throughout the course of this thesis. I would also like to thank Lars-Åke Nordén and Prof. Per Gunningberg whose teaching skills aroused my interest in the field of mobile communications and encouraged me to do a master’s thesis in such an interesting subject. Finally, I would like to express my thanks to Fredrik Bjurefors for his valuable comments and suggestions.
Contents

1 Introduction .................................................. 1
   1.1 Opportunistic Networks .................................. 1
   1.2 Routing in Mobile Opportunistic Networks .......... 2
      1.2.1 How Opportunistic Routings Differ from Traditional Ad-hoc Routings? .......... 3
      1.2.2 Routing Protocols .................................. 4
         1.2.2.1 Epidemic Routing Protocol ................. 4
         1.2.2.2 Two-hop Routing Protocol ............... 4
         1.2.2.3 Spray and Wait Routing Protocol ....... 4
   1.3 Mobility Models ........................................ 5
      1.3.1 Random Waypoint .................................. 5
      1.3.2 Shortest Path Map-Based Movement ............ 6
   1.4 Resilience in Opportunistic Networks ............... 7

2 Thesis objectives and Contributions ..................... 9

3 Jamming ..................................................... 11
   3.1 Problem Description .................................... 11
   3.2 Related Works ......................................... 13
   3.3 Experiments ............................................ 14
   3.4 Evaluation Methodology ................................ 15
   3.5 Trace-based Performance analysis .................... 15
      3.5.1 Trace Inflation Process ......................... 16
         3.5.1.1 How Trace Inflation Algorithm Works? .. 16
         3.5.1.2 What is the Purpose of Trace Inflation Process? ... 17
      3.5.2 Filtering towards Forwarding Contacts ........ 17
      3.5.3 Building Forwarding Contact Graph and Computing the Minimum Delay Path .... 18
   3.6 Metrics ................................................ 18
   3.7 Results ................................................. 19
   3.8 Implication on Design and Selection of Routing Protocols ....................... 23

4 Buffer constraint ........................................... 25
   4.1 Problem Description .................................... 25
   4.2 Related Works ......................................... 25
   4.3 Experiments ............................................ 27
   4.4 Evaluation Methodology ................................ 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5 Metrics</td>
<td>27</td>
</tr>
<tr>
<td>4.6 Results</td>
<td>28</td>
</tr>
<tr>
<td>4.7 Implication on Design of Routing Protocols</td>
<td>31</td>
</tr>
<tr>
<td>5 Conclusion</td>
<td>33</td>
</tr>
<tr>
<td>6 Future Work</td>
<td>35</td>
</tr>
<tr>
<td>Bibliography</td>
<td>37</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Opportunistic Networks

Nowadays, personal mobile devices such as latest generation mobile phones, Personal Digital Assistants (PDAs) and laptops are an ubiquitous part of people's daily lives. Short range wireless communication capabilities, for example Bluetooth [2] and WiFi [15], have been integrated into these mobile devices. Moreover, thanks to a huge number of mobile applications, e.g. location based services (LBSs), networked games and mobile social network applications (SNAs) user interaction and information sharing has been provided in many innovative ways. These applications would not work without the availability of the Internet connectivity. However, despite all the mentioned capabilities, the connectivity of these mobile devices with the Internet is still an issue which should be addressed. The connection of the mobile devices to the Internet could be through wireless access points connected to a wired network, which is what has been applied for example in WiFi wireless LANs [1] and cellular networks [12]. However, an infrastructure based connectivity is not always preferable because, for example, it is expensive to accommodate all the devices with sufficient bandwidth in cellular network or to deploy sufficient number of access points to cover all the devices due to the inherent limitations of hotspots' range in WiFi networks. Therefore, a self organized network which does not require any infrastructure and which can scale well as the number of nodes in the network increases is required. Thanks to the integration of short range wireless communication technology into mobile devices, another type of network, called opportunistic network, has emerged which is a more suitable alternative to deal with the mentioned issues. Opportunistic networks are considered as a type of delay-tolerant networks, constructed by human-carried mobile devices, which can spontaneously communicate with each other by leveraging users' mobility. In opportunistic networks, due to the mobility of the nodes, disconnections, network partitions, as well as highly variable delays are the norm and the underlying topology of the network is highly dynamic. Moreover, the mobility of nodes is not predictable. In this type of network, it is not usually feasible to provide contemporaneous end-to-end path between users to interact with each other. This implies that a message destination is not reachable at the time when it is generated. Nonetheless, intermittent connectivity or lack of end-to-end paths can be overcome by taking advantage of users' mobility. User mobility results in new disconnections and connections among
nodes. Therefore, a message could be carried by a mobile node with no connection to any other node until a new connection comes up and in this way the message may eventually reach its destination.

However, sporadic connectivity is not the only challenge in opportunistic networks. There are some other challenges which can affect the usage of node contacts or node behavior. Two different challenges, studied in this work, are jamming and limited buffer capacities, which are described in detail in Section 3.1 and 4.1 respectively. The challenges can limit the contribution of the nodes in data forwarding which, in turn, can affect the resilience of the network. Before starting to explain resilience and how resilience is provided in opportunistic networks, let us explain in more detail how opportunistic routing works and how it differs from traditional ad-hoc routing.

## 1.2 Routing in Mobile Opportunistic Networks

As mentioned in the previous section, in opportunistic networks the existence of contemporaneous end-to-end paths for the network nodes is not assumed [3]. In these type of networks, in contrast to the Internet, disconnections are the norm and are not the exception. In Sensor Network with Delay Tolerance (SeNDT), sensors are mostly turned off to preserve power, and therefore they construct a loosely connected DTN network [36]. In wildlife tracking networks, where connectivity of the networks depends on animal movements, animals may move far away from each other and hereby they may cause disconnection [18]. In many other networks similar disconnections may occur due to, e.g. node failure, node mobility, node sparseness, signal attenuation and energy saving effort. Hence, for applications which do not require contemporary end-to-end communication in such networks, asynchronous communication could be applied. Since the connectivity of the network in not constantly maintained, a routing protocol is needed to route messages throughout the time slots during which a link on a path to the destination exists. Therefore, routing is carried out according to store-carry-and-forward strategy. This implies that when a message is received by a node which does not have a connection to any other node, it should be buffered in the current node until the next link in the end-to-end path comes up. In figure 1.1 different snapshots of a network, which show node connectivity conditions at four different times, are illustrated. Assume node $A$ generates a message destined to node $G$ at time $T_1$ and there is no direct path from node $A$ to $G$ at any time. However, the message from node $A$ can be forwarded to node $G$ by node $B$ at $T_4$, if intermediate nodes carry it.
1.2.1 How Opportunistic Routings Differ from Traditional Ad-hoc Routings?

A basic and extreme approach for message delivery, in these types of networks, is direct delivery [36]. In direct delivery, a message is never replicated and the source of the message passively waits for the final destination to come in its communication range. It means that the probability that a message be transferred when an encountered node is not final destination is 0. This method uses few resources. However, since the probability for the sender to meet the destination could be very low or even zero, and even if the source and the destination meet each other the quality of the link could be very low, it often results in a low delivery ratio.

Another potential approach is multi-hop routing [6]. This method, which is applied in traditional mobile ad-hoc networks, allows nodes to compensate for short transmission range of wireless communications through taking advantage of neighboring nodes as relays. It exploits multiple cooperative relays until a message is received by its final destination and hereby makes communication between nodes possible, even if they never come within direct coverage range of each other. However, the main issue of multi-hop routing is that it does not exploit the broadcasting nature of wireless communication. Instead, it applies unicast data communication and the next hop for each message is chosen at the sender side. Hence, if a message is not received by
the pre-defined next hop, message delivery cannot be achieved. In fact, conventional ad-hoc routing cannot use the opportunities arose from the unselected relay nodes which are closer to the destination than the relay node selected by the source.

However, in contrast to traditional ad-hoc routing, opportunistic routing tries to take advantage of path diversity [39], which means that it exploits multiple neighboring nodes as relay nodes whose links can be considered as independent communication links. In an extreme approach, called flooding, a node broadcasts a message to any node in its transmission range, which allows the message be received by the closest node to its destination. This routing protocol applies transfer probability 1 for all encountered nodes and replicates the message every time it meets another node. This method has a high delivery ratio at the expense of high resource consumption as well as network congestion [3] caused by too many redundant message replicas generated and disseminated in the network. There are many other proposed routing protocols that are between these two extreme approaches, i.e., direct delivery and flooding. Since there is a trade-off between delivery ratio and delivery delay in opportunistic networks, it is important to decide to which nodes a message should be forwarded, and how many copies should be generated per message.

1.2.2 Routing Protocols

In this thesis, three different controlled flooding-based routing protocols are applied. These protocols which do not assume any knowledge about network topology, provide different levels of path diversity and redundancy in the network. All these protocols share the assumption that a node can only forward a message to the nodes that do not have a copy of it.

1.2.2.1 Epidemic Routing Protocol

Under epidemic routing [35], when two nodes come into transmission range of each other, they exchange copies of messages, which they do not have in common. One of the goals of epidemic routing is to deliver messages to their destination with high probability. Epidemic routing exploits all possible space-time paths to deliver a message from its source to its destination. However, since it generates and disseminates too many message replicas, it introduces maximum diversity in the network at the cost of high redundancy which impose high buffer overhead on nodes.

1.2.2.2 Two-hop Routing Protocol

The redundancy introduced by epidemic routing can be reduced by limiting the number of hops a message is allowed to take from its source to its destination to two. Under two-hop routing [13], the source node of a message transmits copies of the message to all encountered nodes. These relay nodes, however, are only allowed to transfer the message copy to the destination node. In other words, the relay nodes are not allowed to transfer the message to other relay nodes. Consequently, this method generates less number of redundant message copies than epidemic routing.

1.2.2.3 Spray and Wait Routing Protocol

Spray and wait routing is a restricted two-hop forwarding scheme in which the total number of copies per each message which is allowed to be disseminated in the network
is pre-defined. Under spray and wait routing protocol [32], a node generates a limited number of copies $N$ to be transmitted for every message originating at the node. The node then forwards the copies to the first $N$ distinct encountered nodes. Each of these relay nodes, availing a message copy, are only allowed to directly transmit the message to its final destination. In this way, spray and wait routing in comparison with two other mentioned methods introduces the minimum level of diversity and redundancy in the network.

1.3 Mobility Models

In opportunistic networks, node movements considerably increase the opportunity for communication between a sender and a receiver and consequently increase the chance for message delivery. These movement capabilities are implemented through mobility patterns [19]. Therefore, the mobility model of the nodes is of major importance to design high performance routing protocols as well as to derive sensible performance results.

Since it is difficult to have access to real mobility patterns, synthetic mobility models could be applied instead. These models can simulate the behavior of real mobile nodes to some extent. In fact, a mobility model is a set of rules and algorithms that defines the node movement patterns [19]. Random Waypoint (RWP) and Shortest Path Map Based Movement (SPMBM) are two different mobility models which are applied in this thesis.

1.3.1 Random Waypoint

Random waypoint is a movement model which imposes no restrictions on node mobilities. In this model, for each mobile node the next destination could be any random location on the network area and the route selection algorithm is so that each node moves along a direct line from the starting location to the next location at a constant speed [8], and therefore this model creates zigzag paths within the network area. As an example, the movement trace of a node is shown in Figure 1.2 where the node moves from one waypoint $P_i$ to the next waypoint $P_{i+1}$. 
1.3.2 Shortest Path Map-Based Movement

In order to obtain a more realistic movement pattern of mobile nodes, movement models can take advantage of actual road maps. Map-based movement models limit the node movements to paths which are defined by map data belonging to real cities [19].

Under shortest path map-based movement model, a mobile node can select any random point on the map as its next destination. Then, Dijkstra’s shortest path algorithm [17] is applied to find the shortest path to that selected point. In this work, the map data of Helsinki downtown area is used.
1.4 Resilience in Opportunistic Networks

We define resilience as the capability of the network to undergo changes on node contacts or node behavior imposed by different challenges, and it still functions on an acceptable level which varies depending on the network characteristics. Opportunistic networks take advantage of spacial-temporal diversity, i.e., the availability of multiple space-time paths, to achieve resilience in the network. In other words, through broadcast transmission all the opportunities offered by wireless propagation can be leveraged by opportunistic routing protocols in order to deliver data.
Chapter 2

Thesis objectives and Contributions

Opportunistic networks are exposed to some challenges which can affect node behavior or usage of node contacts, which in turn affect the resilience of the networks and is not clear how resilient the networks will be when these challenges are enforced. The goal of the thesis is to understand and explain the effects of different challenges, i.e., jamming attacks and buffer constraints, on the performance of different opportunistic forwarding schemes. In this thesis, we not only develop different simulation models in which the calculations are event-driven, but also apply a new method for performance evaluation which is lied on contact traces.

In these type of networks, due to the absence of knowledge about dynamic topological reconfigurations of the network, arose from sporadic disconnection and reconnection of mobile nodes, it is an intricate task to design efficient forwarding techniques. Routing performance ameliorates if more information about the expected topology of the network can be disclosed [16]. The results of our evaluation can be used to design more efficient routing protocols or to perform more informed protocol selection for different networking environments with different characteristics.

Furthermore, Since it is high-priced and time-consuming to implement and deploy real opportunistic networks, the research community is really dependent on the accuracy of simulation results. During the course of the thesis we recognized the importance of a careful simulation methodology to obtain useful results, which is particular to opportunistic networks. Hence, it is also tried to point out the issues which simulations are confronted with, and should be addressed by the research community.
Chapter 3

Jamming

3.1 Problem Description

Since the wireless communication is conducted through a share medium, wireless networks are exposed to many threats which can prevent them from maintaining connectivity in a wireless environment. Jamming [30] is one of the threats that can be used to disrupt the communication by emitting radio signals in the same frequency as the networks, which in turn, decreases signal to noise ratio. Signal-to-noise ratio (SNR) is one of the key factors in determining packet delivery ratio (PDR) in a network. At the bit level, SNR should be high enough to provide an accurate bit error rate. To extract associated bit information of a signal with high probability, SNR should exceed a certain threshold value, called $\gamma_o$. Jammer signals, by attenuating SNR, decrease the communication range of the nodes. The communication range specifies the range in which a node can communicate with another node with adequate SNR. The communication range includes two components, namely hearing range and sending range. The hearing range of a receiver node defines the range within which the potential senders can deliver their message to the node so that SNR of the sender’s signal be greater than the minimum required SNR to accurately decode the signal data. Similarly, the sending range of a transmitter node defines the range which the potential receivers required to be within, to decode the transmitter’s message successfully. Considering the standard free-space configuration model, the power of the received signal at $d$ meters away from the transmitter is:

$$ P_R = \frac{P_T G}{4\pi d^2} $$

where $P_T$ is the transmission power and $G$ is the product of the sending and receiving antenna gain in the line-of-sight (LOS) between the receiver and the transmitter [24]. Given the same average ambient noise floor, $P_N$, across the entire space, in a non-jamming scenario, the hearing range and sending range of a node will be equal to a circle centered at the node with the radius [24]:

$$ r_c = \sqrt{\frac{P_T G}{4\pi \gamma_o P_N}} $$

Assume an stationary jammer which continually emits radio signals. The received jamming signal’s power attenuate with distance. Therefore, the effect of a jammer is...
restricted to a circle centered at the location of the jammer. The jammer range is represented as a circle for simplicity. In reality, however, it is not a perfect circle. On the boundary of the circle, the received jamming signals equal the present ambient noise level of the wireless environment. This circle is called Noise Level Boundary (NLB) of the jammer with radius $R_J$ [24]. NLB defines the jammed region and nodes which are located inside the region, are considered to be jammed. For these nodes, received jamming signals are larger than the ambient noise level.

At the network topology level, the consequent reduction of the communication ranges caused by jamming signals can result in the changes of the neighbor list of the nodes. Hence, nodes which are located outside the jammer’s NLB can also be affected by the jammer because they may lose some of their neighbors which they have before the jamming signals start to disrupt the network communication.

According to neighboring changes, caused by jamming signals, the nodes of the network could be categorized into three different groups [23, 24]:

- **Unaffected Node**: Though the hearing range of an unaffected node may slightly change, it experiences no change in its neighbor list. An unaffected node together with all its neighbors are located out of the Jammer’s NLB circle.
- **Boundary Node**: The hearing range of a boundary node is attenuated and its neighbor list is therefore reduced. However, it can still hear from its unaffected neighbors as well as some of other nodes within finite steps.
- **Jammed Node**: The hearing range of a jammed node has been severely reduced so that it has no boundary node or unaffected node within its hearing range. A jammed node is located within the jammer’s NLB circle.

Figure 3.1 illustrates the classification of different wireless nodes under a jamming scenario. The NLB, which is depicted by dashed red line, determines the jammed region. Nodes $\{n1, n2, n9\}$ are jammed nodes; nodes $\{n3, n5, n10\}$ are boundary nodes; nodes $\{n4, n6, n7, n8\}$ are unaffected nodes.

![Figure 3.1: Illustration of a jamming scenario](image)

However, for simplicity, it is assumed that both the hearing range and the sending range of the nodes which are located within the NLB of the jammer are zero, and therefore the link state of a pair of nodes $a$ and $b$ could be defined as:

$$I_{a,b} = I_{b,a} = \begin{cases} 
0 & ||Z_a - Z_J||_2 \leq R_J \text{ or } ||Z_b - Z_J||_2 \leq R_J \\
1 & ||Z_a - Z_J||_2 > R_J \text{ and } ||Z_b - Z_J||_2 > R_J 
\end{cases}$$
where \( Z_a \) and \( Z_j \) are the positions of node \( a \) and jammer respectively and \( \| \cdot \|_2 \) indicates the Euclidean distance between a node and the jammer.

Generally, the level of interference caused by a jammer depends on the relative transmission power of the jammer and wireless nodes, the distance between the jammer and the nodes as well the MAC protocol implemented by the network nodes [37]. Nodes which are closer to the jammer or are exposed to jammer with higher transmit power are affected more by the jammer. MAC protocol is applied to decide when nodes are allowed to access the shared medium. A MAC protocol usually detects a channel as idle if the signal strength value is lower than a threshold. The threshold could be either fixed or determined according to the measured signal strength values. The signal strength that has the minimum value among the most recent measured signal strength values when the channel is idle is chosen as the current threshold value. Consequently, if a stationary jammer continually transmits signals at a constant transmission power, the static nodes detect the channel as idle because they consider the energy emitted by the jammer as ambient noise.

Fortunately, mobility increases the probability of communication between nodes. The reason is that when nodes randomly moves around within a network, where jamming signals are disrupting the communication, they may get the chance to pass through an unjammed area and hence be able to communicate. However, the probability that the network get disconnected, even in the presence of a few number of jammers is very high [27]. In order to investigate the impact of jamming on the wireless communication, we have conducted experiments, which are explained in section 3.3.

### 3.2 Related Works

Wireless communication is vulnerable to different kind of denials of service attacks at all protocol layers. Resilience of wireless ad hoc networks is therefore necessary for both military applications and commercial applications. Jamming is one of the techniques that can be used to restrain the wireless communication, for example by preventing nodes from receiving data. In [28] it is shown that a wireless link can easily break even with very low energy consumption.

Guevara Noubir in [27] investigates the impact of both randomly and optimally spread out jammers over an area. The results for randomly located jammers show that the existence of even a few number of jammers increase the probability that the network get disconnected. For the experiments, 400 nodes are deployed within an area of 2000 \( \times \) 2000 m and it is assumed that the communication range of each jammer is 200 m. When the number of jammers exceeds 100, all the nodes get disconnected. Jammers can also be located in a way that the minimum number of jammers be require to prevent all communications. In his theorem the minimum number of required jammer to cover an area \( A \), given a jamming range \( JR \) is computed as:

\[
\frac{2A}{3\sqrt{3}JR^2}
\]

The theorem indicated that 39 jammer are enough to prevent all the communication.

In [37], the effectiveness of a jammer on the ability of wireless nodes in sending and receiving data is investigated. A constant jammer which continually emits a radio signal is placed near two wireless nodes which acts as a sender and a receiver. The
nodes are located so that the jammer has the same effect on both of them. While the jammer is reasonably close to the sender and a fixed threshold value is used by MAC protocol of the network, the jammer can completely prevent the sender from sending out the packets. If the adaptive threshold, which is chosen according to the surrounding signal strength, is applied the sender can still send approximately three-fourth of the packets, even when the jammer is very close to the sender. However, the packet delivery ratio (PDR) in both cases is low since most packets get corrupted by the jammer, especially when the jammer is located close to the sender. In the paper it is also shown that the delivery ratio could be used to distinguish between congested and jammed networks. However, it is not possible to conclude if low delivery ratio is because of jamming or the mobility of nodes.

### 3.3 Experiments

All the simulations are carried out in an discrete event-driven simulator, i.e., the Opportunistic Networking Environment (ONE) simulator [19] written in Java. The ONE simulator has explicitly been designed to evaluate opportunistic protocols. The simulations are run for different combinations of mobility models and routing protocols to have different distributions of nodes and packets. As mentioned before, the mobility modes used during the simulations are random waypoint and shortest path map based movement models. The applied routing protocols are epidemic, two-hop and spray and wait protocols. All the mentioned combinations are tested with the same network configuration parameters. Simulation runs are performed with 100 nodes which are distributed in a rectangular simulation world with dimensions $4500 \times 3400$ meters that are the length and width of the world, respectively. The transmission range of the nodes are set to 10 meters. These parameters can model the simulation environment as a sparse delay tolerant network. The simulation environment is also modeled so that the effects of the limited resources, i.e., buffer size and bandwidth, in the network are eliminated. Consequently, the allocated buffer capacities are large enough so that each node is able to store every received message; and the bandwidth is set to a high value to guarantee the exchange of all messages between encountered nodes for each contact. Each message is generated periodically at a randomly selected node destined to a single receiver. In the experiments, it is also assumed that collision can not affect the message delivery process.

In this work, it is assumed that a stationary jammer at the center of the simulation area continuously sends radio signals, and the jammer’s radius is set to different values, starting from 0 and incrementing with strictly increasing steps until it reaches the half of the width of the area, i.e., 1700 meters.

The simulator code is changed to provide the position of the involved nodes in the log files. These log files, which are generated by the simulator report classes, are actually files that log node encounters. The log files are hereafter referred to as contact traces. Then, the contact traces are used to assess the performance of different opportunistic routing schemes under the presence of the jammer based on a method described in Section 3.4.
3.4 Evaluation Methodology

The performance evaluation of the opportunistic forwarding schemes is implemented based on a modular method described in [25]. This method which is called trace-based performance analysis applies a Space-Time-Graph methodology.

Different processing steps of the evaluation process are shortly illustrated in Figure 3.2.

First, contacts which contain nodes located inside the jammer’s transmission range are removed from the original contact trace, generated by the simulator, because they are supposed to lose their communication ability completely. One alternative for the performance analysis is to feed the modified traces to the event-driven simulator and to directly derive the desired metrics. In this thesis, however, for evaluating the performance of the opportunistic network at the presence of a jammer, the ONE simulator is only used to generate the contact traces. Then, we implement different steps of the trace-based performance analysis. It should be mentioned that the actual implementation of the method varies for different routing strategies.

The modified traces, instead of being fed to the simulator, are used as input for our programs. The trace-based performance analysis is described in detail in section 3.5. In [25], it is mentioned that using this method, while the results outstandingly match the simulation results, the run times are considerably shorter than for the simulator. This consequently allows for more scalable experiments at the presence of larger traces and bigger number of messages. We use this method to eliminate the need for backtracking while computing the delay corresponding to the shortest path for each delivered message during the simulation runtime. The delays are computed over a reduced set of contact records, which constructs space-time paths from the source to the destination node.

3.5 Trace-based Performance analysis

The performance evaluation of the opportunistic forwarding schemes is implemented based on a modular method which applies a Space-Time-Graph methodology.
For each generated message it is desirable to find the shortest space-time path corresponding to the minimum delay of the message. Each contact record $C_k = (n1, n2, t_{s,k}, t_{e,k})$ in the trace file includes encountered nodes, contact start time and contact end time. The modified trace, which excludes the jammed nodes, is time-sorted according to the start time of the contacts. The procedure of finding the minimum-delay path out of the time-sorted trace is as follow:

### 3.5.1 Trace Inflation Process

First, the modified trace is artificially inflated.

#### 3.5.1.1 How Trace Inflation Algorithm Works?

The trace inflation algorithm [25] works in a way that each record is replicated as many times as the number of records in the contact trace with start time greater than the start time of the current trace, i.e., all subsequent contacts, and end time smaller than or equal to its end time.

<table>
<thead>
<tr>
<th>Algorithm 3.1 Trace inflation process [25]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: <strong>INPUT</strong> modified trace file $D$</td>
</tr>
<tr>
<td>2: <strong>OUTPUT</strong> inflated trace file $D_{inf}$</td>
</tr>
<tr>
<td>3: <strong>VARS</strong> $L$: list storing ongoing contact records</td>
</tr>
<tr>
<td>4:</td>
</tr>
<tr>
<td>5: <strong>INITIALIZATION</strong></td>
</tr>
<tr>
<td>6: <em>copy 1st contact record $C_1$ from $D$ to $D_{inf}$</em></td>
</tr>
<tr>
<td>7: <em>add $C_1$ to $L$</em></td>
</tr>
<tr>
<td>8:</td>
</tr>
<tr>
<td>9: <strong>while</strong> !eof ($D$) <strong>do</strong></td>
</tr>
<tr>
<td>10: <em>read $C_k$ from $D$;</em></td>
</tr>
<tr>
<td>11: <em>write $C_k$ in $D_{inf}$;</em></td>
</tr>
<tr>
<td>12: <strong>foreach</strong> contact $C_j$ in $L$</td>
</tr>
<tr>
<td>13: <strong>if</strong> $t_e(C_j) &lt; t_s(C_k)$</td>
</tr>
<tr>
<td>14: <em>remove $C_j$ from $L$</em></td>
</tr>
<tr>
<td>15: <strong>else</strong></td>
</tr>
<tr>
<td>16: <em>write $C_j$ in $D_{inf}$, $t_s(C_j) = t_s(C_K)$</em></td>
</tr>
<tr>
<td>17: <strong>end</strong></td>
</tr>
<tr>
<td>18: <strong>end</strong></td>
</tr>
<tr>
<td>19: <em>add $C_k$ to $L$</em></td>
</tr>
<tr>
<td>20: <strong>end while</strong></td>
</tr>
</tbody>
</table>

As described in the algorithm 3.1, while parsing a contact, the previous terminated contacts are eliminated from the list of ongoing contacts $L$, and the remaining contacts are replicated after their start time has been updated to the start time of the currently parsed contacts.

16
3.5.1.2 What is the Purpose of Trace Inflation Process?

In an opportunistic network, when a new connection appears at time $t$, some of the previously established connections are still available while the others are terminated. For a message with source $s$, destination $d$, generated at $t_0$, represented as $m = (s, d, t_0)$, the terminated connections, e.g., those with $t_0 < t_g$, cannot be used for the message delivery. Among the ongoing connections, it is desirable to find those which include a node on the shortest path to the destination. For example, in Figure 3.3, a message generated at node 6 at time 710 can be forwarded to node 3 through the path 6 − 5 − 1 − 3, which is available by the time-overlapping contacts $C_4$, $C_3$, and $C_0$. In order to find the path to the destination, the contact records should be backtracked continuously to compare the start time of currently parsed record with the end time of the preceding contacts. However, backtracking for finding the minimum-delay path for each message is computationally expensive. By applying trace inflation process the need for backtracking is eliminated.

![Figure 3.3: Original trace with 8 and inflated trace with 20 contact records [25].](image)

3.5.2 Filtering towards Forwarding Contacts

For each generated message, only contacts are desired that can result in forwarding of the message. These contacts are called forwarding contacts. Therefore, the irrelevant contacts should be discarded from the inflated list during a so called contact filtering step. For a message generated at time $t$ at node $s$, upon the appearance of the first contact involving $s$ with contact start time greater than $t$, all the previous contacts in the sequence of time-sorted contacts are filtered out. For the generated message, one node is chosen as a next hop on the path to the message's destination according to the applied routing strategy, and hence contact filtering step is based on the corresponding
routing protocol in the network environment. The procedure of contact filtering is so that contact records availing no node with a copy of the message are immediately filtered out. Considering the assumption that encountered nodes are only allowed to exchange messages that they do not have, contacts in which both nodes have a copy of a message are not considered as forwarding contacts for the message, and therefore are eliminated. This implies that only contacts including one node possessing a copy of the message, called 1-entry contacts, are retrieved in the contact trace.

The retrieved contact trace, which only includes 1-entry contacts, is then manipulated based on the corresponding routing strategy. If contact filtering procedure is conducted under the epidemic scheme, since nodes possessing a copy of the message can transmit it to nodes that do not, all 1-entry contacts are categorized as forwarding contacts. Under two-hop forwarding scheme, nodes other than the source node which possess a message copy are only allowed to forward it to the message's destination. Therefore, all 1-entry contacts including the source node as well as the first 1-entry contact including the destination node are considered as forwarding contacts. The reason why other 1-entry contacts involving the destination node are eliminated is that upon the first appearance of the destination node, the minimum delay path is found and hence contact filtering procedure is terminated. Under spray and wait routing, for each message, the source node generates a limited number of copies $N$ to be transmitted. therefore, only the first $N$ 1-entry contacts including the source node as well as the first 1-entry contact involving the destination node are retained.

3.5.3 Building Forwarding Contact Graph and Computing the Minimum Delay Path

The reduced set of contact records, which can be represented as a sparse space-time graph, constructs space-time paths from the source to the destination node. The computation of the shortest space-time path, corresponding to the minimum delay, is the last step of computing delay time for the message delivery. the delay value can then be used as a metric to assess the performance of the opportunistic routing strategies.

3.6 Metrics

Two common metrics considered to evaluate the performance of the routing protocols at the presence of a jammer are delay and delivery ratio: Since changes of the neighbor list of the nodes and hence node contacts, caused by jamming signals, result in delay changes, the delay of delivered messages in the network are used to measure the effectiveness of the jammer on the resilience of the network. The delays are compared with the delay values when no challenge is enforced. Furthermore, a jammer through affecting node contacts can prevent the receivers from receiving the packets within the simulation runtime, and therefore packet delivery ratio can also be used to measure the impact of the jammer's transmission range on the resilience of the network. In this work, since messages which are generated at the end of simulation run do not get a fair chance for delivery, only messages which reach their destination within the simulation runtime when no challenge, i.e., jammer, is introduced to the network, are considered while computing delivery ratio in the challenged network. In other words, the message delivery ratio in the challenged network is defined as the ratio of delivered messages to the total number of messages that get delivered when no challenge is enforced.
3.7 Results

Each simulation is run 10 times with different seed values. The illustrated results in Figures 3.4 and 3.5 are based on the average values of the results acquired in all simulation runs.

Figure 3.4 compares average message delivery delays for varying transmission range of the jammer and under different scenarios.

Under shortest path map based mobility, all the routing protocols behave considerably similarly. Up to the jammer radius of approximately 800 meters, the curves do not change significantly by increasing the jammer radius. Through considering delivery ratios of the messages, depicted in Figure 3.5, it could be observed that the overall trend of delivery ratio for the corresponding routing protocols and under the same range of radius stays at a high level, so that most messages are delivered to their destination within the limited simulation time. However, with further increase in the jammer radius, though the delivery ratio decreases drastically, the value of average delay starts to increase significantly and becomes substantially large, up to a factor of 5 in the case of epidemic routing. It could be concluded that the network remains resilient against jammer up to the transmission range of approximately 800 meters.

Under random waypoint mobility, it can be observed that the jammer easily affects the throughput of the opportunistic network when two-hop and spray and wait routing protocols are applied. The delivery ratio soon starts to degrade rapidly as compared to that of epidemic routing. Despite of the rapid degradation of the delivery rate, the curve of average delay does not experience significant changes. These observations are of course not due to a resilient behavior of these protocols. The reason is that the average delay is calculated only over messages that actually are received within the simulation time. This could be a fundamental issue of the experimentation methodologies that take only into consideration average delay of delivered messages as the evaluation metric.

For epidemic routing, however, the trend of average delay shows different behavior. While the delivery ratio decreases rapidly, the trend of average delay experiences significant increment up to the jammer radius of about 1000 meters and after that it starts to decrease considerably. As it mentioned before, this observation is because of the calculation of the average delays over delivered messages. By looking at the delay distribution of the delivered messages it is recognized that up the jammer radius of around 1000 meters many messages with high delays survive in the network. The reason is that, due to the nature of the epidemic algorithm, in comparison with two-hop and spray and wait, many more message replicas are disseminated and all possible contacts are used for message delivery. Thus, jammer cannot eliminate those messages with high initial delay. For many retrieved messages, it also takes more time to be delivered through other alternative paths exploited by the routing protocol. However, with further increase in jammer radius, those messages with high delay are also eliminated and only few messages are retrieved. Hence, the average delay decreases rapidly after a certain jammer radius.
Figure 3.4: Average Delay for random waypoint and shortest path map based mobility models with respect to jammer radius

Figure 3.5: Delivery ratio for random waypoint and shortest path map based mobility models with respect to jammer radius
To address the issue, it could be suggested that the average delay be computed only over messages that are delivered for all jammer radii. From Figures 3.6 and 3.7, it is observed that the average delay of messages for all the scenarios is either increasing or does not change. However, in this way, only messages may be considered that experience small delay or are not affected by the jammer. Consequently, it may result in average delay values which are considerably smaller than the average delay values when no challenge is enforced.

![Image](image1)

(a) Epidemic  
(b) Two-hop  
(c) Spray and wait

Figure 3.6: Average delay for random waypoint over messages that are delivered for all jammer radius

![Image](image2)

(a) Epidemic  
(b) Two-hop  
(c) Spray and wait

Figure 3.7: Average delay for Shortest path map based over messages that are delivered for all jammer radius

The impact of jamming signals on each individual message is also examined. Figure 3.8 illustrates the effect of the jammer for five randomly selected messages that get delivered for all jammer ranges. The results show that when epidemic and two-hop are applied, for each message the delay associated with the larger jammer’s transmission range is equal or greater than the delay associated with the smaller jammer’s transmission range.
Figure 3.8: Delay of five randomly selected messages under shortest path map based mobility

For spray and wait routing protocol, the results are slightly different. The results show that as the jammer’s transmission range increases, a few number of nodes experience smaller delays. In Figure 3.9, each line, differentiated with different color, represents the difference between the aggregation of delay values between two subsequent increasing jammer radii for messages that experience lower delay with increase in jammer radius under spray and wait routing.
3.8 Implication on Design and Selection of Routing Protocols

The substantial difference in the resilience of the network starts to appear after a certain jammer range, hereafter referred to as $R_{\text{effective}}$, which depends on the diversity offered by the topology. In other words, the studied routing protocols can perform well and therefore can be used in networks which are exposed to a jammer if the transmission range of the jammer does not exceed $R_{\text{effective}}$.

In the previous section we saw how jamming has negative effect on the delivery time of individual messages. Spray and wait, however, results in improvement of the delivery time of some messages. When this protocol is applied, each source node can only disseminate a limited number of message replicas. Hence, jamming by blocking some nodes may give the delivery chance to some other nodes which are located on the path resulting in a faster message delivery. Therefore, as the jammer’s transmission range increases, a few number of nodes experience smaller delays. This means that using first encountered contacts as relay nodes does not always result in a faster message delivery, which should be considered while designing routing protocols.
Chapter 4

Buffer constraint

4.1 Problem Description

Another major challenge in opportunistic networks stems from the small form of mobile devices which suffer from resource limitations such as limited buffer sizes so that nodes can only store a limited number of messages.

In these type of networks, as explained before, the underlying topology of the network is highly dynamic which makes it difficult to acquire global topology information. Therefore, in order to increase the probability for message delivery to occur, many replicas of the same message may be disseminated in the network. Moreover, nodes store messages in their buffer and may carry them for long periods of time until the appearance of new forwarding opportunities. This replication-based routing, together with the long-term message storage performed by many DTN routing protocols \cite{22, 33} impose high buffer overhead on nodes. Hence opportunistic nodes’ buffer are highly likely to be congested.

Since buffer limitations substantially affect the efficiency of forwarding strategies in opportunistic networks, in this thesis the performance of routing protocols under different buffer constraints is investigated.

4.2 Related Works

Designing efficient routing strategies in delay tolerant networks is a difficult issue due to two key challenges, i.e., the unpredictable mobility of nodes and the resource constraint. While there has been work \cite{10, 9, 35, 7} that put so much effort on design of efficient forwarding strategies that took into consideration the first challenge, little work has been done that focused on the second one.

Floyd and Fall \cite{11} discuss different kinds of congestion collapse on the Internet, which are applicable for opportunistic networks \cite{14}. Congestion collapse may occur because of retransmitting messages which have already been received by the destination node. Therefore, buffer timeouts are not substantial in opportunistic networks and a node should not occupy its buffer with a message for a long period of time. Some messages, though consuming bandwidth in the network, are dropped before being delivered to the destination. These undelivered messages are another contributing factor for congestion in opportunistic networks. In opportunistic networks, messages
can be considerably larger than packets in IP networks. While transmitting larger messages, thus causing longer transmission time, with higher probability encountered nodes go out of transmission range of each other and the link may break in the middle of the transmission. The problem could be overcome through partially transmitting messages, called message fragmentation [29]. However, message fragmentation may result in congestion collapse in the network if fragments of message do not get delivered to the destination. Due to the absence of some segments of a message, it is not reassembled and is discarded by its destination. Congestion collapse can also occur due to increased control data transmitted through congested paths. Due to the highly dynamic topology of opportunistic networks, pervasive amount of control data may be imposed to the network which can, in turn, cause congestion collapse in the network. Hence, there is a trade-off between keeping the information up-to-date and the cost of doing so [14]. Another form of congestion in opportunistic network happens because of long transmission time between the request and receipt of a message, which results in unwanted messages. The problem could be addressed by providing message buffers with timeout to discard unwanted messages. Since opportunistic forwarding schemes take advantage of nodes other than the source to further forward messages, each node can potentially be a source node or a relay node. This causes conflict of interest when a relay node generates a message for itself. The conflict of interest, which is illustrated in Figure 4.1, cause another form of congestion, called in-network congestion [14]. Nodes labeled S cannot transmit their message through nodes labeled B, because these nodes are congested with their own messages.

![Figure 4.1: In-network congestion in opportunistic network [14]](image)

The majority of researches for congestion control in DTNs are based on buffer management [5, 20, 21, 31]. The effect of buffer management strategy on the performance of the network should be considered while designing routing protocols. In routing protocols proposed in [19, 31] message replication strategies together with long-term message storage cause high storage overhead on the nodes. In [38] buffer-constrained epidemic routing strategies is analyzed and some buffer management strategies such as First-in-first-out (FIFO) or Last-in-first-out (LIFO) are evaluated. It is concluded that FIFO performs better than LIFO in the context of both average delay and delivery ratio. It is also observed that, in term of delivery ratio, giving priority to source messages while using FIFO policy, causes epidemic routing in a network where buffer sizes are so small, performs as well as in a network with unlimited buffer capacity. Hence, the authors conclude that deleting older message replicas can result in significant improvement in buffer size. However, it causes messages disseminate slower, and
therefore the average delay decreases. For example, in the extreme case where buffers get full so that they hold only their own messages, no relying happens. Consequently, the performance degrades to that of source-destination transmission scheme.

In [21], some buffer management policies such as FIFO, LIFO, and drop oldest (DO) are evaluated for epidemic routing. FIFO results in the highest delivery ratio while DO gives the smallest delay.

In [33], it is concluded that epidemic routing results in the minimum delivery delay when no buffer constraint is enforced. However, it performs poorly for limited buffer sizes.

4.3 Experiments

The simulations are performed using the ONE simulator. Like the jammer experiments, the simulation runs are performed with 100 nodes and the same combinations of mobility models and routing protocols are applied. Since the goal of the experiments is to investigate the impact of buffer constraints on the performance of the opportunistic routing protocols, for the simulations, it is not assumed that the buffer size is unlimited. Instead, the allocated buffer sizes are restricted to certain values. For the experiments, 500 and 1000 messages are generated respectively.

All messages are assumed to have the same size and are generated periodically from a random source node to a random destination node. We look at scenarios where the mobile nodes act as routers, applying First-In-First-Out (FIFO) buffer management scheme. When a new message arrives at a node with full buffer, the oldest messages are removed until enough free space for the newly arrived message is provided. For the sake of simplicity, each buffer size value is set to integer multiple of the corresponding message length value during each experiment. The buffer capacity range varies from 1% to 20% of the number of generated messages. Since all forwarding schemes are deployed so that a message copy is forwarded to an encountered node only if it does not have it, redundant deliveries for the same message do not occur.

4.4 Evaluation Methodology

Our evaluation methodology is as follow: For each scenario, the time required for almost all generated messages to reach their destination is computed under condition that no challenge is introduced, i.e., buffer capacities are supposed to be unlimited. This implies that we achieve approximately 100% delivery ratio. Then, buffer size restrictions are enforced and the simulations are run over the computed time span in the unchallenged scenario. In this manner, the impact of buffer limitations on the performance of the studied routing protocols is investigated.

4.5 Metrics

The performance metrics applied to assess the performance of the forwarding schemes are delay and delivery ratio. The delivery ratio refers to the ratio of the number of delivered messages to the total number of generated messages and the delay metric is defined as the average delay of all delivered messages during the overall simulation runtime.
4.6 Results

The results show that while epidemic routing results in minimum delivery delay and highest delivery ratio under no buffer constraint, it performs poorly when buffer sizes are limited. However, the goal of these experiments is not to compare the performance of the routing protocols with each other. In our Experiments, the simulation run-time varies to a great extent for different routing protocols. For example, this time for epidemic routing is approximately one-third of that of two-hop routing under random waypoint mobility. In fact, the goal is more biased towards individual investigation of the behavior of the routing protocols under limited buffer size. In other words, the routing protocols should be compared to themselves and not each other.

Figures 4.2 and 4.3 illustrate the delivery ratio and average delay of different scenarios for varying buffer sizes. On the x-axis, the buffer capacity is indicated as a percentage of the fixed traffic load of 500 messages, while the y-axis illustrates the delivery ratio corresponding to each buffer capacity level.

Under both random waypoint and shortest path map based movement models, routing efficiency, in the context of delivery rate, generally grows very fast as the buffer space increases until a certain threshold value. The reason is that with further increase in the buffer capacity less messages get dropped which results in higher delivery ratio. After that threshold value, the further increase of the buffer capacity does not improve the performance of the forwarding schemes because approximately 100% delivery is reached. For example, in the case of spray and wait and two-hop routing, when shortest path map based movement mobility is applied, the threshold value is achieved while buffer size is set to approximately 6% and 12% of the traffic load, respectively. This value for epidemic routing increases to about 70%. The results imply that these protocols are not resilient if the buffer capacities are smaller than certain values. From Figure 4.4, it could be observed that the trends of delivery ratios corresponding to 1000 generated messages are quite the same as those of 500 generated messages.

However, the trends of average delay of different scenarios do not conform to one another. While the delivery ratio of epidemic routing is increasing rapidly with the increase of buffer capacity, its average delay is fluctuating around the same level for the corresponding buffer sizes. The average delay of two-hop non-uniformly increases up to a certain buffer size, after which it becomes relatively smooth. The trend of spray and wait, on the contrary, experiences reduction with the further increase in buffer capacity before it becomes smooth.

The results for a 1000 message traffic load are quite the same as those of 500 messages while epidemic and two-hop are applied (see Figure 4.4). However, the trend of spray and wait surprisingly resemble that of two-hop for double amount of messages.

Under spray and wait routing, only a few replicas per message are disseminated in the network, because the source node forwards message replicas to the first $N$ encountered nodes which are only allowed to forward the replicas to the message destination. Therefore, the message replicas are not uniformly distributed in the network. Furthermore, for small buffer sizes, some of these replicas get dropped. However, it should be taken into consideration that overloading an individual node does not necessarily mean that there is congestion in the network [34, 26] and it could be due to non-uniform distribution of traffic. In the low-traffic network, not only the replicas are non-uniformly distributed, but also the number of distributed replicas per (destination) node is very small. This implies that the probability that the relay nodes meet the destinations becomes lower in comparison with higher-traffic networks in a limited time. It can be observed that the delivery ratios for 500 and 1000 messages for the smallest buffer size
are around 0.4 and 0.5, respectively (see Figures 4.3a and 4.4a). Moreover, it takes more time for the relay nodes to meet the destination. Therefore, the average delay of delivered messages for small buffer sizes is very high. With increasing the buffer size, the number of dropped replicas decreases, which in turn leads to more uniform distribution of the replicas and hence earlier delivery of messages. When the number of generated messages over a certain space/time span increases, i.e., 1000 messages are generated, better coverage of messages is achieved and more nodes get the chance to receive and relay a copy of any messages in the network. Hence, the probability that relay nodes meet the destination increases and the relays are more probable to meet the destination earlier. Therefore, the delay is reduced as compared to the situation where only 500 messages are generated even though more message delivery is performed. However, for small buffer sizes a lot of messages get dropped. With the increase of the buffer size, the network experiences less message dropping and delivery ratio increases. This implies that a lot of old messages that get dropped by the newly arrived ones, now get the chance to be delivered to their destination. Some of these message are those with high delays when no buffer constraint is introduced. Consequently, increasing buffer capacity increases the average delay. It should be reminded that buffer capacities are relative to the number of generated messages, and therefore generating more messages does not congest the nodes.

Under epidemic routing, message replicas are more uniformly distributed throughout the network, in comparison to the other routing protocols. Therefore, buffer size increment does not affect the delay performance of delivered messages as much as those of two-hop and spray and wait.

![Graphs showing delivery ratio and average delay for varying buffer capacities](image)

Figure 4.2: Average delay and delivery ratio for varying buffer capacities and fixed traffic load of 500 messages under random waypoint mobility
Figure 4.3: Average delay and delivery ratio for varying buffer capacities and fixed traffic load of 500 messages under shortest path map based mobility

Figure 4.4: Average delay and delivery ratio for varying buffer capacities and fixed traffic load of 1000 messages under shortest path map based mobility

The delay fluctuations in the plots are partly due to the fact that changing buffer capacity causes different subset of messages get either dropped or delivered for each buffer size. Therefore, in order to study the impact of buffer limitations on delay value of the delivered messages more closely, the average delay of messages that were delivered to their destination for all buffer capacities are also calculated (see Figures
The plots show that for all the protocols the average delay generally improves very fast as the buffer space increases until a certain value. The reason is that with further increase in the buffer capacity less message copies get dropped and thus more messages get the chance to be delivered within the limited simulation time. After a certain buffer size is reached the delay trend stops changing due to the fact that buffer size is large enough to avoid message drops because of buffer overflow.

### 4.7 Implication on Design of Routing Protocols

The results indicate that when a routing protocol that results in a more uniform distribution of messages is applied, delivery time of messages get less affected by buffer size. This could be considered as an important factor while designing efficient routing protocols.
Chapter 5

Conclusion

In order to assess the performance of the opportunistic network at the presence of a jammer, we use two different metrics, i.e., average delay and delivery ratio. We show that it is important to study delay and delivery ratio together to better understand the impact of jamming on the performance of the forwarding protocols, because delay distributions for low delivery ratios is skewed towards small delay values when most of the nodes or node contacts are affected. It is actually a fundamental issue of the experimentation methodology that take only into consideration average delay of delivered messages as the evaluation metric.

We find that in spite of sporadic partial-connectivity and node mobility in opportunistic networks, store-carry-and-forward routing by exploiting diversity in space-time paths, provides a high degree of resilience against jamming attack in the network. The impact of the jammer on an individual message can be significant when a contact opportunity is missed. For each message, the delay corresponding to the larger jammer transmission range is equal or greater than that of the smaller jammer transmission range, when epidemic and two-hop routing are applied. For spray and wait the result is slightly different. The jammer, by blocking some nodes, can give the delivery chance to some other nodes which are located on the path resulting in a faster message delivery. Consequently, as the jammer’s transmission range increases, a few number of nodes experience smaller delays.

However, the network resilience is maintained and it performs well if a significant amount of node contacts are not affected. From the experiments, it is observed that the substantial difference in the performance of the network starts to appear after a certain jammer range, which depends on the diversity offered by the topology. After that, a significant amount of the node contacts get affected. For example, in our experiments, this value for shortest path map based movement is around 800 meters. Up to this jammer range, the jammer hardly affect the throughput of the network and neither delivery ratios nor average delays experience considerable changes.

We also observe that routing efficiency, in the context of delivery rate, generally grows very fast as the buffer space increases until a certain threshold value. After that threshold value, the delivery ratio stabilizes and the further increase of the buffer capacity does not improve the performance of the forwarding schemes. In fact, after a certain buffer size the network performs as well as a network with unlimited buffer capacity.

The results show that the performance of a routing protocol depends on the number
of replicas of different messages disseminated in the network. For example, when the number of messages are doubled over the same space/time span and with the same ratio of buffer size to the number of generated messages, for both spray and wait and two-hop, the trend of delivery ratio shows improvement for the small buffer sizes. Moreover, when the number of distributed replicas per (destination) node is higher, the relay nodes are more probable to meet the destination earlier, resulting in lower delay.

The behavior is similar for the studied scenarios, with the exception of the spray and wait routing protocol in low-traffic network (500 messages) where the average delay of delivered messages improves much more significantly compared to the other studied routing protocols, though with increasing the buffer size many more messages with high delay get delivered.
Chapter 6

Future Work

When we enforced buffer constraints, one of the confronting issues in our experiments was that the average delay was computed over delivered messages, which made evaluation, in the context of average delay, difficult. It would result in better evaluation if we run the simulations for longer time, resulting in delivery of all generated messages when the challenges are enforced. In this manner, we can better understand how the studied challenges influence the delivery time of messages.

In this thesis, we evaluate the challenges separately from one another. It would be interesting to take into account both challenges together while evaluating the performance of the opportunistic network. Moreover, eliminating the unlimited bandwidth assumption would lead to more realistic results.
Bibliography


