A Hybrid MANET-DTN Routing Scheme for Emergency Response Scenarios

Christian Raffelsberger, Hermann Hellwagner
Institute of Information Technology
Alpen-Adria-Universität Klagenfurt
Klagenfurt, Austria
{*christian.raffelsberger, hermann.hellwagner*}@*aau.at*

***Abstract*—Emergency response operations are a promising application area for mobile ad-hoc networks (MANETs). Most existing MANET routing protocols assume that an end-to-end path between source and destination can be established. However, this assumption may not hold in a hastily formed network established during an emergency response. This paper evaluates a store-and-forward mechanism for proactive routing protocols to mitigate the effects of network disruptions. The mechanism is integrated into two routing protocols. The modified protocols are evaluated in an emergency response scenario that includes a disaster area mobility model and a wireless obstacle model. The scenario represents a realistic first responder operation after an incident in a chemical facility. The evaluation results show that networks for disaster responses benefit from the modified routing protocols.**

***Keywords*-wireless networks; mobile ad-hoc networks; routing protocols; simulation;**

I. Introduction

In emergency response operations, first responders need to communicate and exchange data in order to establish and maintain situational awareness and a common operational picture. However, after man-made or natural disasters, fixed communication networks may not be available, either because they have been destroyed or are overloaded in the aftermath of the disaster. Hence, there is a need to establish ad-hoc communication networks until the fixed communication infrastructure becomes available. Mobile ad-hoc networks (MANETs) are a promising solution for setting up temporary communication networks in emergency situations.

Hastily formed ad-hoc networks for emergency response operations are diverse in terms of connectivity and networking equipment. Connectivity situations may range from well-connected networks, where almost all nodes are interconnected to sparse networks, where only a small fraction of nodes are connected at a certain time. Between these two extremes, the network may also be intermittently connected, providing several partitions of well-connected nodes. For instance, different search and rescue teams may be separated from each other but members of the same team are interconnected. Such connectivity characteristics impose some challenges on the communication network, especially on the routing protocol.

The majority of state-of-the-art routing protocols for mobile ad-hoc networks [1] assume that an end-to-end path between source and destination is available. Even though these protocols where designed for MANETs that are prone to link failures, they cannot deliver packets when no source-to-destination path exists. Routing algorithms for Delay or Disruption Tolerant Networking (DTN) [2] relax this assumption by allowing nodes to store messages until they can be forwarded to the destination (or an intermediate node). This mechanism is called store-and-forward (or store-carry-forward) and increases the robustness of routing in the presence of disruptions. DTN is mainly intended for sparse networks that rarely provide contact opportunities. Thus, DTN routing does not work efficiently in well-connected networks. For instance, many DTN routing schemes replicate packets in order to decrease the delivery delay and increase the delivery probability. However, replication imposes a high storage and bandwidth overhead which may decrease performance in well-connected networks.

In this work, we evaluate a hybrid MANET-DTN routing approach that uses local packet buffers to improve the performance of a MANET routing protocol. We describe how this approach can be integrated into the Optimized Link State Routing (OLSR) and the Better Approach To Mobile Ad-hoc Networking (BATMAN) protocols. Additionally, we evaluate the modified protocols in a realistic emergency response scenario. The simulation scenario uses a disaster area mobility model [3] and a wireless obstacle model [4] to represent realistic first responder movements on a hybrid indoor/outdoor disaster site. Simulation results show that an emergency response network benefits from the hybrid MANET-DTN routing approach.

The contributions of this paper are twofold. First, to the best of our knowledge, this is the first time that a hybrid MANET-DTN routing scheme has been evaluated in a realistic emergency response scenario. Second, this is the first integration of a DTN mechanism into OLSR that does not require to change the basic routing algorithm or any routing control message formats.

The rest of the paper is structured as follows: Section II briefly describes the MANET protocols that are extended. Section III summarizes other hybrid approaches. Our approach to integrate MANET and DTN routing is described in Section IV. Section V introduces the evaluation scenario and the simulation setup. The experiments and results are

978-1-6128-4937-9/13/$31.00

described in Section VI and Section VII. The last section concludes the paper and outlines possible future work.

II. MANET Routing Protocols

The Optimized Link State Routing (OLSR) protocol [5] is one of the best known and most widely-used MANET routing protocols. Since OLSR is a proactive link-state protocol, all nodes periodically exchange routing information and each node has a complete view of the network topology. The main difference to traditional link-state protocols is the concept of multipoint relays (MPRs). The 1-hop neighbors that are needed to reach all 2-hop neighbors form the MPR set of a node. Only the nodes in the MPR set need to forward routing control messages (e.g., link updates). Hence, the concept of MPRs reduces the processing and routing overhead compared to traditional link-state protocols.

The Better Approach to Mobile Ad-hoc Networking (BATMAN) [6] is another proactive protocol for MANETs. In order to reduce complexity, every node only maintains status information about its direct neighbors. All nodes regularly broadcast originator messages (OGMs) in the entire network and every node keeps track via which neighbor it received OGMs. If a node needs to send a packet to a certain destination, it uses the neighbor that forwarded most OGMs for that destination.

III. Related Work

Neither MANET nor DTN routing protocols are suited for networks that may get partitioned but also provide well-connected regions. MANET routing protocols are unable to provide inter-partition communication, whereas DTN routing protocols are not efficient in the well-connected regions. As a result, recent approaches try to combine these two routing paradigms.

Lakkakorpi et al. [7] propose an adaptation scheme that is applied at the sender and dynamically switches between IP-based routing using AODV and the DTN bundle protocol [8] for data delivery. The sender's decision is based on information that is locally available or can be determined by means of probing packets (e.g., message size, network density, path length, path delay). Evaluations show that the adaptive approach yields better performance than pure MANET or DTN routing if the network is not too dense.

DTS-OLSR [9] builds a DTN overlay network that supports the exchange of bundles on top of OLSR. Nodes use modified OLSR control messages to build and maintain a hierarchical overlay network which uses the bundle protocol for data delivery. Nodes that do not support the full DTN stack use the nearest DTN-capable node to transmit and receive bundles. Experiments in a testbed have shown that the overhead for building and maintaining the overlay decreases the performance in well-connected networks. However, in the presence of frequent disruptions DTS-OLSR outperforms pure OLSR.

Robust Replication Routing (R3) [10] is another hybrid approach. Instead of combining or mixing existing protocols, the authors propose a new routing metric that can cope with disconnections. The metric is based on the distribution of path delays. If a path has unpredictable, varying delays, R3 replicates the packet and uses multiple paths in order to minimize the overall expected delay (DTN-style routing). If the path delay is well-predictable, only the path providing the minimum delay is used (MANET-style routing). Evaluations of R3 in simulations and testbeds showed that R3 can achieve the performance of MANET routing protocols in well-connected networks and also compete with DTN protocols in sparse networks.

BATMAN Store-and-forward (SF-BATMAN) [11] is similar to our work as it combines the proactive routing protocol BATMAN with a store-and-forward mechanism in a backward-compatible way (i.e., no BATMAN operations or control messages have to be changed). However, the authors of [11] evaluate SF-BATMAN in a general DTN-scenario whereas this paper uses a realistic emergency response scenario. Additionally, this paper also evaluates a store-and-forward enabled version of OLSR.

IV. MANET-DTN Integration

Our approach centers around two decisions: when to store a packet instead of sending it instantly and when to send a stored packet. The first check is performed whenever a data packet is received. In traditional MANET routing, a data packet is dropped if the routing table does not contain an entry for the packet's destination. To integrate a store-and-forward mechanism, packets need to be buffered until a route is available. Additionally, it is important to check if an existing routing table entry may be invalid, as stale routes would cause packet losses. This check is needed as routing protocols need some time to detect and handle (e.g., purge) stale route entries. It is important to note that these modifications do not change the routing decisions of the underlying MANET routing protocol. Thus, packets are always send to the node that was selected by the MANET routing algorithm to be the best next hop for the packets' destination.

To handle possibly obsolete routes, our approach defines a $MaxLinkTimeout$ parameter and stores packets if the link was not active (i.e., a packet was received via the link) in the last $MaxLinkTimeout$ seconds. Since proactive routing protocols periodically exchange control information, such a link validity check can use information that is already provided by the routing protocol. For instance, BATMAN provides information about when the last router originator message (OGM) has been received. If the most recent OGM was received less than $MaxLinkTimeout$ seconds ago, the route is considered to be active. Similarly, OLSR nodes regularly exchange HELLO messages that can be used to detect obsolete routes. Basically, our hybrid MANET-DTN approach could also use a custom probing mechanism to determine which links are active. However, it is beneficial to rely on information that is already provided by the routing protocol, since no additional control overhead needs to be introduced to perform the link validity check.

The following pseudo code describes the decision logic for storing packets:

procedure RECEIVEDATAPACKET($packet$)
  $destAddr$ = **getNextHop**($packet$)
  if $destAddr == NULL$ **then**
    bufferPacket($packet$)
  else if hasValidLink($destAddr$**) ==** false **then**
    bufferPacket($packet$)
  else
    sendTo($destAddr, packet$)
  end if
end procedure

If the MANET routing algorithm does provide a path to the destination (i.e., `getNextHop()` returns `null` because there is no routing table entry for that destination) the packet is stored. If the next hop could be determined, it is checked if there is a valid link available. As described above, the link validity check method `hasValidLink()` is routing protocol specific and uses the $MaxLinkTimeout$ parameter to determine if a link is valid. Due to space constraints the pseudo code for the method is omitted.

The second modification in order to integrate a store-and-forward mechanism is the decision logic for sending buffered packets. In proactive routing protocols, such a decision can be made whenever a routing control packet has been received. There are three cases when a buffered packet can be sent. First, a new route has been found. Second, a stale route has become available again. Third, the next hop address of an existing route has been modified. Apart from deciding when to send packets, the order in which to send the packets needs to be defined. In this work all packet buffers are first in, first out (FIFO) queues and the oldest packets are discarded first if the buffer is full. Packets are removed from the queues after they have been forwarded. Thus, at any time only a single copy of a packet exists in the network.

The method that processes buffered packets has to perform another link validity check to decide whether packets can be sent or still have to be buffered:

procedure PROCESSBUFFEREDPACKETS
  for all packet in buffer **do**
    $destAddr$ = **getNextHop**($packet$)
    if hasValidLink($destAddr$) **then**
      sendTo($destAddr, packet$)
    end if
  end for
end procedure

V. Scenario Description and Simulation Setup

It is important to evaluate routing protocols under the specific settings of the target domain to get more accurate results. This section describes the emergency response scenario that is used to evaluate the hybrid MANET-DTN approach. Additionally, information about how the scenario is modeled in the simulation environment is given.

A. Scenario Description

The scenario has been adopted from [12] and models an emergency response operation after an explosion in a chemical plant. The scenario is depicted in Fig. 1. Several first responder teams search and rescue victims from two buildings that are affected by the explosion. The scenario consists of 25 nodes that move according to a specific disaster area mobility model [3]. The mobility model defines several disaster areas that are assigned to nodes. Additionally, obstacle areas that restrict the available paths between areas can be defined. Every node either moves within its designated area or acts as a transport node between two areas (using the shortest available path). Further information about the mobility model can be found in [3].

The scenario consists of two Incident Locations (IL 1/2) which represent buildings that contain victims. The victims are rescued by two search and rescue teams, each consisting of four first responders. All first responder nodes move independently of each other. Victims are first transported to the Patients Waiting For Treatment Area (PWFTA). Four additional nodes represent first responders that transport victims between the PWFTA and the two Casualty Clearing Stations (CCS 1/2), where they are picked up by four ambulances and are brought to the exit point. Besides the nodes that move between areas, there are four nodes located in the PWFTA, two nodes in each CCS and one node in the Technical Operational Command (TOC). These nodes do not leave their designated area but move randomly within the area.

One important aspect of the scenario is that some nodes also temporarily operate inside buildings. A wireless obstacle model [4] is used to model the effects of working indoors. To be more precise, if an obstacle is in the line of sight between two nodes, the signal is attenuated following the wireless obstacle model. In the scenario there are eight nodes (i.e., the nodes moving between the PWFTA and the two ILs) affected by wireless attenuation caused by obstacles. In particular, these nodes experience temporal disconnections from the rest of the network. As a result, the nodes form a separated network partition, although the network is well-connected most of the time [12].

Another important aspect of the scenario is the generated network traffic. Every first responder node regularly sends packets to the node that is located in the incident command center in front of the chemical plant (see TOC in Fig. 1). This traffic model has been chosen since status updates

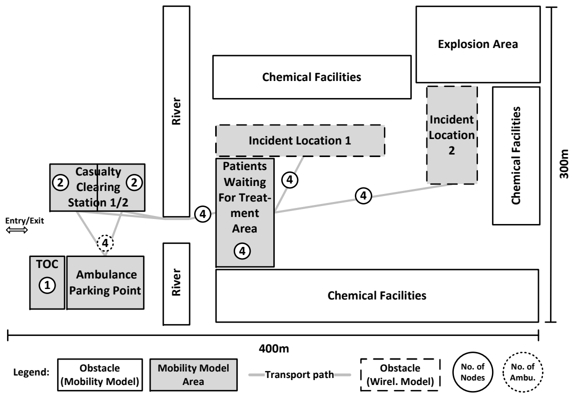

Figure 1. Map of the simulation scenario.

and other information about a first responder and his/her surroundings (e.g., photos taken by first responders, data from body sensors) are important to increase the situation awareness for the incident commander.

This scenario offers two distinct features, compared to other scenarios that have been used to evaluate hybrid MANET/DTN approaches [7][9][10][11]. First, it models a realistic disaster response by using a disaster area mobility model and considering obstacles that restrict wireless communication. Second, the resulting network is dense and well-connected and provides more communication opportunities between nodes (i.e., disruptions are on the order of seconds to minutes but not hours or days as in other scenarios).

B. Simulation Setup

The simulations are performed using the OMNet++ network simulator. The hybrid MANET-DTN approach is combined with existing implementations of BATMAN and OLSR that are part of the INETMANET framework for OMNet++. To simulate network load, all nodes send (after an initial waiting time of 60 s) UDP packets to the node that is located in the command center (i.e., the node located in the TOC). The simulation time of every experiment is 3000 seconds and every experiment is repeated 20 times. The most important simulation parameters are listed in Table I.

Table I
SIMULATION PARAMETERS

Wireless model	
MAC protocol	802.11 (g)
Propagation model	Free-space path loss ($\alpha = 2$)
Transmission range	100 m
Transmission rate	54 Mbps
Wireless obstacle model [4]	
Per-wall attenuation	18 dB
Indoor attenuation	0.5 dB/m
Mobility model [3]	
Node speed	1 to 2 m/s
Speed (vehicles)	5 to 12 m/s
On-Off traffic model	
On-time	3-7 s
Off-time	5-10 s
Packet rate	10 packets/s (during on-time)
Packet size	1024 byte
Sent packets per node (mean)	11897
OLSR routing parameters	
Metric	Expected transmission count
Hello interval	2 s
TC and MID interval	5 s
BATMAN routing parameters	
OGM interval	1 s
Route purge timeout	640 s
OGM window size	64

VI. EXPERIMENTS

We evaluate the effects of a store-and-forward mechanism on packet delivery ratio (PDR) and delay, two widely used routing protocol performance metrics. In a first series of experiments, several parameters for the link validity check, that is performed in the `hasValidLink()` method, are evaluated. This method determines if a link is still available and packets sent via this link are likely to be delivered. In OLSR and BATMAN, nodes regularly send control messages to announce themselves (i.e., OGMs in BATMAN and HELLO messages in OLSR). If such a message from a neighboring node has been received recently, the link to this neighbor is likely to be valid. To be more precise, `hasValidLink()` checks if the link has been updated in the last $MaxLinkTimeout$ seconds, where $MaxLinkTimeout$ is set to 1 s, 3 s and 5 s. If `hasValidLink()` returns false for the next hop of a packet, the packet is buffered. Otherwise, it is instantly sent. As a result, the $MaxLinkTimeout$ parameter influences the packet delivery ratio. If it is set too high, more packets are lost because of outdated link information. On the other hand, setting this parameter too low causes many data packets to be buffered unnecessarily, which increases the processing overhead or even causes packet losses if the buffer is full.

In a second set of experiments the buffer capacity is varied between 50 and 1000 packets. For the given traffic pattern, a buffer size of 1000 represents the unlimited buffer case, as no packets are dropped because of full buffers. Additionally, packet buffering is disabled (i.e., the buffer size is set to 0) to show routing performance without the store-and-forward mechanism. It is expected that larger buffer capacities increase the packet delivery ratio as more packets can be buffered in the case of route failures. However, the increase comes at the expense of a higher packet delay.

VII. RESULTS

The packet delivery ratio (PDR) is an important metric to evaluate the performance of routing protocols. The unmodified versions of OLSR and BATMAN achieve an average PDR of 83% and 80%, respectively. Figure 2 shows the average PDR (including the 95% confidence intervals) of OLSR and BATMAN for different buffer sizes and $MaxLinkTimeout$ values. In general, a higher buffer

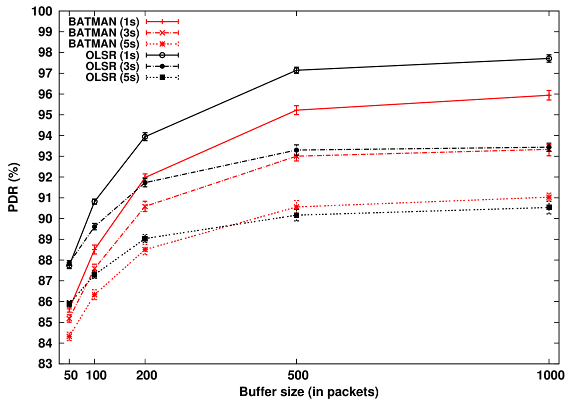

Figure 2. Packet delivery ratio for different buffer capacities and $MaxLinkTimeout$ values.

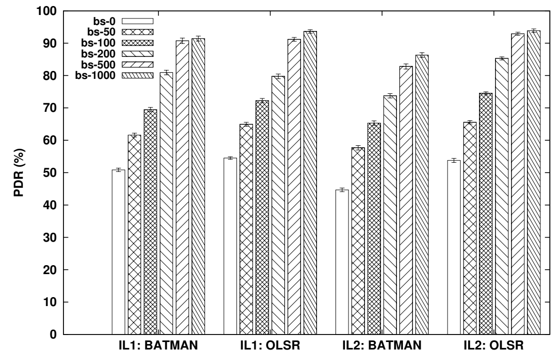

Figure 3. Average packet delivery ratio for varying buffer sizes (bs) and a $MaxLinkTimeout$ of 1 s, for the two group of nodes that move between the PWFTA and the Incident Locations IL1 and IL2.

capacity results in an increase of the PDR as longer disruptions can be covered by the store-and-forward mechanism. However, for a $MaxLinktimeout$ of 5 s and 3 s the PDR cannot be increased any further, since the buffers get never filled completely.

Figure 2 also shows how the $MaxLinkTimeout$ parameter influences the PDR. Reducing the allowed link timeout causes the store-and-forward mechanism to react earlier to link breaks. Thus, less packets are lost on stale routes but are only sent if a link update has been received recently. However, it is important to take the default route update interval of the routing protocol into account when adjusting the $MaxLinkTimeout$ parameter. If the $MaxLinkTimeout$ is set too strict (i.e., much smaller than the default update interval), the PDR would decline if the buffer capacity is not sufficient. This is due to the fact that more packets are buffered unnecessarily (i.e., packets could actually be sent instantly because there is a link to the next hop available) and cause packet drops if the buffer is full. Thus, the smallest $MaxLinkTimeout$ value that we evaluated is 1 s (i.e., the OGM update interval of BATMAN).

For $MaxLinkTimeout$ values of 3 s and 5 s and small buffer sizes (i.e., buffer capacity ≤ 200) OLSR achieves a higher average delivery ratio than BATMAN for the same parameter set. This is an indication that OLSR repairs routes more quickly than BATMAN and is able to send buffered packets via a repaired route before the buffer gets full and packets are dropped. For bigger buffer capacities (i.e., ≥ 500) the advantage disappears as a further increase of the PDR is limited by other factors (e.g., transmission errors, packets buffered at the end of the simulation, routing loops). For a $MaxLinkTimeout$ of 1 s OLSR outperforms BATMAN for all buffer capacities and achieves a PDR of nearly 98% for a buffer capacity of 1000, whereas BATMAN achieves a PDR of about 96%.

The network is diverse in terms of connectivity. Thus, it is interesting to investigate the packet delivery ratio of certain hosts. Basically, the nodes that move between the two Incident Locations IL1 and IL2 and the Patients Waiting For Treatment Area have the lowest connectivity. Thus, these hosts should benefit most from the hybrid MANET-DTN routing scheme. Figure 3 shows the PDR of the two first responder teams that enter the two Incident Locations. Every bar in the diagram shows the average PDR of the nodes that belong to the same team for a certain buffer capacity. Without the store-and-forward mechanism (denoted by bs-0) about the half of all packets do not reach the command center. The store-and-forward mechanism increases the PDR of OLSR to over 93% for both teams (for bs-1000). BATMAN achieves a slightly lower PDR of 86% for the team moving into IL1 and 91% for the team moving into IL2.

The packet delivery ratio of the nodes that are not prone to disruptions (i.e., the nodes in front of the facility) cannot be significantly improved by the store-and-forward mechanism. However, the PDR of these nodes is also not negatively affected by buffering packets. Hence, the overall network benefits from the hybrid MANET-DTN approach.

The end-to-end packet delays are short if the store-and-forward extension is disabled. All packets are delivered within 38 ms if only instantly available paths are used. If the store-and-forward extension is enabled, the average end-to-end delay increases as some packets are stored until a path gets available. The delay is mainly influenced by the buffer capacity as larger buffers may hold packets for a longer time. Apart from the buffer capacity, the connectivity settings and the link timeout also influence the delay of buffered packets. Table II contains the packet queuing times for varying buffer sizes and a $MaxLinkTimeout$ of 1 s. As the queuing times are asymmetrically distributed, the table contains the quartiles (denoted by Q1, Q2 and Q3) instead of the mean values. The queuing times show that network disruptions are rather short and the majority of stored packets can be sent within a few seconds. In the case of higher $MaxLinkTimeout$ values (i.e., 3 s and 5 s), the queuing times are higher for both protocols, while less packets get

Table II
QUARTILES OF THE QUEUING TIME T_Q FOR VARYING BUFFER SIZES AND A $MaxLinkTimeout$ OF 1 S.

Buffer	OLSR: T_Q (s)			BATMAN: T_Q (s)		
size	Q1	Q2	Q3	Q1	Q2	Q3
50	0.23	0.48	0.84	0.16	0.91	3.00
100	0.25	0.51	0.97	0.36	1.45	5.21
200	0.26	0.56	1.20	0.68	2.20	7.87
500	0.29	0.61	1.69	0.81	3.06	10.07
1000	0.29	0.63	1.81	0.81	3.17	10.64

queued. This is an indication that most packets are stored because of short-lived link disruptions (i.e., the link validity check method returns false) and not as a result of long term disruptions, caused by the mobility of nodes.

As the basic route calculation algorithms of BATMAN and OLSR are not changed, the hybrid MANET-DTN scheme does neither directly impact the hop count of a packet nor the overall routing control traffic. However, it is important to note that the store-and-forward mechanism has some implications on these two measures. Particularly, it decreases the relative routing overhead (i.e., the ratio between control traffic and data traffic) as more data packets can be delivered. Similarly, the average hop count is slightly increased as the store-and-forward mechanism mainly increases the PDR of the nodes that are farther away from the destination and utilize longer multi-hop paths.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we evaluated how a hybrid MANET-DTN approach, based on the integration of a store-and-forward mechanism into a proactive MANET routing protocol, performs in a disaster scenario. The simulation scenario included a realistic first responder mobility model and a wireless obstacle model that allowed us to model a realistic emergency response. The simulation results show that a store-and-forward mechanism is beneficial for the packet delivery ratio of both MANET routing protocols. Thus, it can be stated that a hybrid MANET-DTN routing scheme increases the robustness of the network as disruptions can be compensated. On the other hand, the increase comes at the expense of a higher packet delay. Although there are applications that cannot cope well with high and varying delays (e.g., multimedia streaming, real-time communication), we believe that networks for emergency responses benefit from this extension. Future work could include to identify the application and its type of traffic (e.g., by means of the port number) to decide which packets to buffer.

The hybrid MANET-DTN mechanism could also be adapted for reactive routing protocols. Actually, reactive protocols contain a similar store-and-forward mechanism as data packets are usually stored until the route finding process has finished. However, data packets are dropped if no route can be found. If a reactive routing protocol is used, it is more difficult to decide when to send buffered packets as there are no periodic routing updates that can be used as decision points. Instead, new routes have to be explicitly requested, which causes a higher routing overhead. Hence, finding a trade-off between discovering communication opportunities on time and saving network resources is another interesting topic for future work.

ACKNOWLEDGMENT

This research was funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 261817, the BRIDGE project and was partly performed in the Lakeside Labs research cluster at AAU.

REFERENCES

[1] E. Alotaibi and B. Mukherjee, “A survey on routing algorithms for wireless ad-hoc and mesh networks,” *Computer Networks*, vol. 56, no. 2, pp. 940–965, Feb. 2012.

[2] T. Spyropoulos, R. N. Rais, T. Turletti, K. Obraczka, and A. Vasilakos, “Routing for disruption tolerant networks: taxonomy and design,” *Wireless Networks*, vol. 16, no. 8, pp. 2349–2370, Nov. 2010.

[3] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, M. Frank, and P. Martini, “Modelling mobility in disaster area scenarios,” in *Proc. 10th ACM Symp. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM ’07)*. ACM, 2007, pp. 4–12.

[4] C. Sommer, D. Eckhoff, R. German, and F. Dressler, “A computationally inexpensive empirical model of IEEE 802.11p radio shadowing in urban environments,” in *Proc. 8th Int. Conf. Wireless On-Demand Network Systems and Services (WONS ’11)*. IEEE, 2011, pp. 84–90.

[5] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” IETF RFC 3626, 2003.

[6] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, “Better approach to mobile ad-hoc networking (B.A.T.M.A.N),” IETF draft-openmesh-b-a-t-m-a-n-00, 2008.

[7] J. Lakkakorpi, M. Pitkänen, and J. Ott, “Adaptive routing in mobile opportunistic networks,” in *Proc. 13th ACM Int. Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM ’10)*. ACM, 2010, pp. 101–109.

[8] K. Scott and S. Burleigh, “Bundle protocol specification,” IETF RFC 5050, 2007.

[9] R. Pant, A. Tunpan, P. Mekbungwan, R. Virochpoka, and K. Kanchanasut, “DTN overlay on OLSR network,” in *Proc. 6th Asian Internet Engineering Conference (AINTEC ’10)*. ACM, 2010, pp. 56–63.

[10] X. Tie, A. Venkataramani, and A. Balasubramanian, “R3: Robust replication routing in wireless networks with diverse connectivity characteristics,” in *Proc. 17th Ann. Int. Conf. Mobile Computing and Networking (MobiCom ’11)*. ACM, 2011, pp. 181–192.

[11] L. Delosieres and S. Nadjm-Tehrani, “Batman store-and-forward: The best of the two worlds,” in *Proc. IEEE Int. Conf. Pervasive Computing and Communications Workshops (PERCOM Workshops ’12)*. IEEE, 2012, pp. 721 –727.

[12] C. Raffelsberger and H. Hellwagner, “Evaluation of MANET routing protocols in a realistic emergency response scenario,” in *Proc. 10th Workshop Intelligent Solutions in Embedded Systems (WISES ’12)*. IEEE, 2012, pp. 88 –92.