Peggy Begerow; Sebastian Schellenberg; Jochen Seitz; Thomas Finke; Juergen Schroeder

Reliable multicast in heterogeneous mobile ad-hoc networks

Original published in:

Electronic communications of the EASST. - Berlin : Techn. Univ. - Bd. 56.2013, insges. 11 S.

ISSN (online): 1863-2122
DOI: 10.14279/tuj.eceasst.56.811.806
URL: http://dx.doi.org/10.14279/tuj.eceasst.56.811.806
[Visited: 2016-09-08]

Electronic Communications of the EASST
Volume 56 (2013)

Proceedings of the Combined workshop on Self-organizing, Adaptive, and Context-Sensitive Distributed Systems and Self-organized Communication in Disaster Scenarios (SACS/SoCoDiS 2013)

Reliable Multicast in Heterogeneous Mobile Ad-hoc Networks

Peggy Begerow, Sebastian Schellenberg, Jochen Seitz, Thomas Finke, and Juergen Schroeder

11 pages

Guest Editors: Michael Zapf, Florian Evers
Managing Editors: Tiziana Margaria, Julia Padberg, Gabriele Taentzer
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Reliable Multicast in Heterogeneous Mobile Ad-hoc Networks

Peggy Begerow[1], Sebastian Schellenberg[2], Jochen Seitz[3], Thomas Finke[4], and Juergen Schroeder[5]

[1] peggy.begerow@tu-ilmenau.de [2] sebastian.schellenberg@tu-ilmenau.de
[3] jochen.seitz@tu-ilmenau.de
www.tu-ilmenau.de/kn
Communication Networks Group
Ilmenau University of Technology, Germany

[4] thomas.finke@hs-heilbronn.de [5] juergen.schroeder@hs-heilbronn.de
Faculty of Electronics and Information Technology
Heilbronn University, Germany

Abstract: In disaster scenarios, communication infrastructure could be damaged or completely failed. Mobile Ad-hoc Networks (MANETs) can be used to substitute failed communication devices and thus to enable communication. As group communication is an important part in disaster scenarios, multicast will be used to address several nodes. In this paper, we propose our new reliable multicast protocol RMDA (Reliable Multicast over Delay Tolerant Mobile Ad hoc Networks). We introduce an efficient group management approach and a new method for reliable multicast delivery over Delay Tolerant Networks. We show, that our protocol is adaptive to different kinds of MANETs, e.g. with or without clusterheads, respectively. For those without, we use our name resolution over adaptive routing approach.

Keywords: multicast; MANET; name resolution; adaptive routing

1 Introduction

MANETs have been verified to be suitable for disaster scenarios. In these situations, different groups of first-aiders are involved in helping activities, e.g. fire-fighters, policemen, or paramedics. Often, messages need to be sent to an entire group, for example that all fire-fighters should extinguish a fire in a defined area. For enabling communication in disaster scenarios, Mobile Ad-hoc Networks (MANETs) can be used to substitute failed infrastructure. If there is a big area to cover, several separate MANETs could be built or they could merge and split frequently. If messages need to be exchanged between different networks having no stable connection, Delay Tolerant Networking (DTN) can be used. Messages like rescue request or warnings should reliably reach the destinations. Therefore, using DTNs is a appropriate way to ensure delivery even if there is no current network connection. Unmanned aerial vehicles (UAVs) like multicopters could be used as ferries to transport the messages in a delay tolerant way.

Traditional multicast approaches developed for infrastructure-based networks are not suitable for MANETs, because they do not perform well in a dynamically changing ad hoc network environment. Additionally, typical multicast trees usually require a global routing substructure

such as link state or distance vector. The frequent exchange of routing information, initiated by continuous topology changes, produces high management and processing overhead. Due to the special properties of mobile ad-hoc networks, e.g. dynamic topologies, limited energy resources, variable bandwidth, and limited physical security, it is important to develop protocols that consider these properties.

Multicast protocols of traditional networks fail in DTNs because they try to find a connected multicast graph between source and destination nodes before forwarding data packets. Routing protocols designed for DTN instead work with the store-carry-and-forward-principle where two nodes exchange messages with each other only when they have contact. It is difficult to manage the structural connectivity of a multicast constitution during the lifetime of a multicast session.

In this paper, we propose an approach for providing reliable multicast communication between different types of MANETs, which are unpredictably connected with each other.

The paper is organized as follows. In Section 2 we show related work to multicast, routing, and name resolution in MANETs. A brief description of our new designed framework is given in Section 3. The paper is finally concluded in Section 4.

2 Related Work

In this section, we present related work to our framework.

2.1 Multicast in MANETs

Since MANETs have become an important research topic, several multicast protocols for this kind of networks were proposed. S. Mäki et al. [MAH00] presented a group management protocol for ad-hoc networks. In this paper, a fully distributed and certificate-based system for group membership management is presented. It is intended to adapt to highly dynamic ad-hoc networks. The group members are denoted by their public signature keys and each group has a public signature key to represent the group. The fully distributed approach causes a lot of management traffic. Other focuses of group management are described by J. Liu et al. [LSSI05]. They consider the design of key attributes identifying the groups. However, the drawback is that it is too general because we need knowledge about the group membership.

However, there exists a series of multicast protocols for MANETs, such as MAODV (Multicast Ad-hoc On-Demand Distance Vector Protocol) [RP00] and ODMRP (On-demand Multicast Routing Protocol) [YLSG02]. MAODV builds multicast trees to reduce end-to-end latency while others like ODMRP builds mesh-topologies to ensure robustness, but have considerable control overhead due to frequent network flooding. A bi-directional tree is more efficient and avoids sending duplicate packets to receivers. The decrease of the refresh interval like in ODMRP influences the scalability.

All existing protocols have their own advantages and disadvantages. The advantages of overlay multicast are the robustness and the low overhead. Some protocols create overlay networks and use unicast routing to forward packets. Energy aware multicast protocols like the Lifetime-aware Multicast Tree (LMT) protocol [MP04] optimize either total energy consumption or system lifetime of the multicast tree.

In our framework, we will use an underlying multicast protocol in the network if available. Otherwise, we use our new approach only.

2.2 Delay Tolerant Networking

DTNs are networks, where no stable path between the source and the destination exists. Such situations can occur in disaster scenarios. For our design of a new multicast protocol, we use the possibilities of Delay Tolerant Networking, because there are scenarios where no end-to-end paths are available. Z. Narmawala et al. [NS09] advised a multi-copy routing protocol for multicast in DTNs called Multicast In Delay Tolerant Networks (MIDTONE) which forwards encoded packets. In this approach, several copies of a message are sent into the network. Therefore, the main disadvantage of this approach is the large overhead.

The Delay and Disruption Tolerant Multicasting Protocol (DTCAST) [AMZO09] combines on-demand routing segments of the ODMRP protocol with short-distance epidemic data spreading. In addition, it proposes two-class delivery guarantee for messages using explicit and implicit acknowledgments. DTCAST has a minor percentage of unsuccessful delivery for nodes, which is caused by data loop prevention.

The MembersOnly protocol [NK10] distributes the group membership list under consideration of malicious nodes. This protocol is primarily focused on role-based as well as geographic-based groups, because the group membership does not change.

However, none of the proposed protocols guarantees a reliable delivery of messages to every group member, because they do not know, which group members are registered if the MANETs are not connected.

2.3 Adaptive Routing

The performance of MANETs is strongly affected by the used routing protocol. Therefore, a number of routing protocols is available, which can be divided into two main groups, namely the reactive and the proactive routing protocols. The proactive protocol family computes the routes periodically or with every change in topology with the advantage that routes will be immediately available when required. The reactive routing protocols on the other hand search for routes when they are needed. Compared to proactive protocols, the nodes do not have full knowledge about the network. Reactive routing decreases the packet overhead for synchronization of the nodes but increases the delay for route finding.

In disaster scenarios, it is difficult to select the best routing protocol for a specific network constellation because of the changing topologies and network parameters.

Adaptive routing, which allows switching between different routing protocols depending on a given network context, is used to overcome this problem and to achieve best routing performance in changing scenarios.

Therefore, we designed a new approach [FSS+12][SBH+13]. This enables our system to perform well in different network scenarios.

2.4 Name Resolution in MANETs

The resolution of human readable names to local IP addresses is one of the most important tasks in IP-based networks. In reliable wired networks, this task is usually done by the well known Domain Name System (DNS) [Moc87]. As this system is centralized and hierarchical, it is not practical for frequently changing MANETs.

Several mechanisms were proposed to provide name resolution in ad-hoc networks. One way is using a still centralized but modified approach [AL09] by adding redundancy or intelligent service placement. However, such mechanisms can not prevent single point of failures definitely. Another way is using fully distributed systems but keeping the task in the Application Layer. Multicast DNS (mDNS) [CK11] and the Ad-hoc Name Service System (ANS) [JPK04] use multicast messages to request and reply the resolution of names. However, this causes high overhead during flooding of the multicast messages.

Instead of seeing name resolution as an Application Layer task, it is possible to integrate it in other layers, e.g. in routing mechanisms. Engelstad et al. [ETE03] proposed the idea of taking name requests and replies piggybacked with the route requests and replies of the reactive Ad hoc On-demand Distance Vector routing protocol (AODV) [PBD03]. However, this is limited to one routing protocol only. Therefore, we proposed a different approach [FSS+12] by combining an adaptive routing framework with name resolution extensions for all routing protocols. This allows the system to react to changes of the network scenario and provides optimal performance for route or name finding, respectively.

3 Concept

In this section, we present details on our new framework for reliable multicast over DTNs.

3.1 Example Scenario

Figure 1 shows an example of a multicast scenario with multiple different MANETs based on RMDA. A multicast group is a group of nodes being interested in the same information. In Figures 1, 4, 5, and 6, "'SOS"' and "'Helper"' are such groups. The group "'Helper"' could be a group of nodes providing help activities such as fire fighter or life guards. The "'SOS"' group could consists all nodes, where the user needs some help. The groups are established to enable aimed distribution of data to interested nodes for saving traffic. The group list contains all known groups and their attributes, while the member list contains all group members for one group.

3.2 Reliable Multicast over Delay Tolerant Mobile Ad hoc Network (RMDA)

In our approach, we propose a multicast protocol that enables multicast group management and reliable message transmission over heterogeneous MANETs. The RMDA protocol is designed to support group type activities in disaster scenarios with consideration of the characteristics of MANETs. Different groups with different members are identified with unique group addresses. As we consider rapidly changing network scenarios, we assume that nodes leave and join networks frequently. With every change, they probably get a new IP address. Therefore, we use the

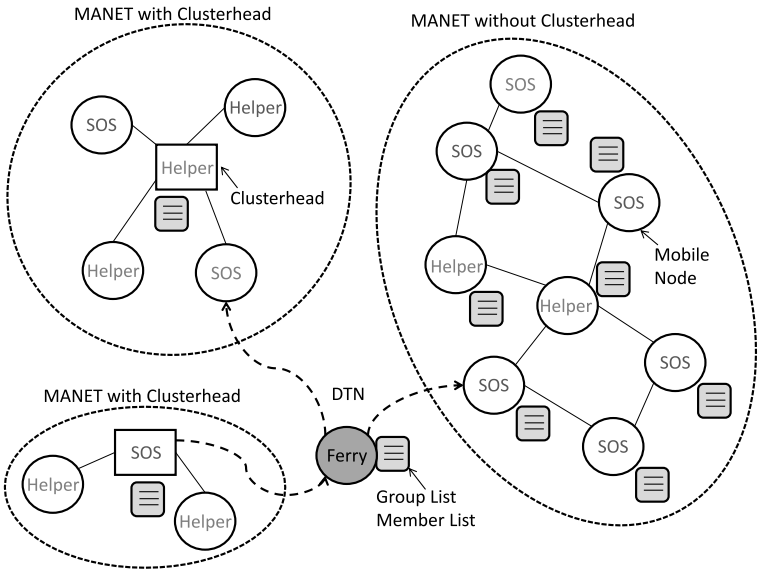

Figure 1: Multicast scenario with multiple MANETs based on RMDA

identities for group member management as they remain the same. In our protocol, full knowledge about the members is required either by the clusterhead only or by all nodes separately.

Our protocol presents a new method for the recognition of reliable delivery. Let t_M be the time, when a message is sent to the DTN. This message is reliably delivered if the amount of received acknowledgments falls into the tolerance interval. This interval is given by the number of members in the group member list at a certain time t_d and a defined variance being computed on demand (cf. Figure 2). If the reliability requirement for a message delivery is fulfilled, the message and the acknowledgments can be deleted. Therefore, the storage of the DTN nodes is free again and the message is not infinitely saved.

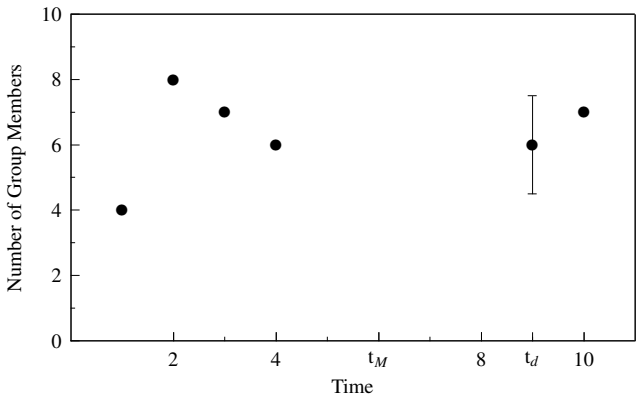

Figure 2: Example for the progress of the group member lists

A spatially separeted subnet sends only one ACK to the message sender. This ACK contains the quantity of the delivered messages. Our concept avoids ACK-implosion. An ACK-implosion while using reliable multicast protocols occurs if too many ACKs are transmitted back to the sender and therefore produce huge traffic.

The protocol is divided into different modules. The first one is the group management module which is responsible for creating and terminating groups as well as for controlling the joining and leaving of group members. The group management module calculates the average amount of members in each group.

The second part is the transmission module, which is responsible for a reliable transmission of multicast messages. The transmission module decides whether the message is reliably delivered based on the relationship between the average amount of members and the received acknowledgments. That means, if the number of acknowledgments is greater or equal than the average amount of members, the message is reliably delivered. In local MANETs, the transmission module uses underlying functionality like multicast or routing if available. The RMDA protocol describes an own layer. This RMDA layer is located above the addressing layer, above the DTN layer, or directly above the transport layer. The protocol uses the underlying layer functionalities. Figure 3 shows the ISO/OSI protocol architecture with reference to the protocol stack.

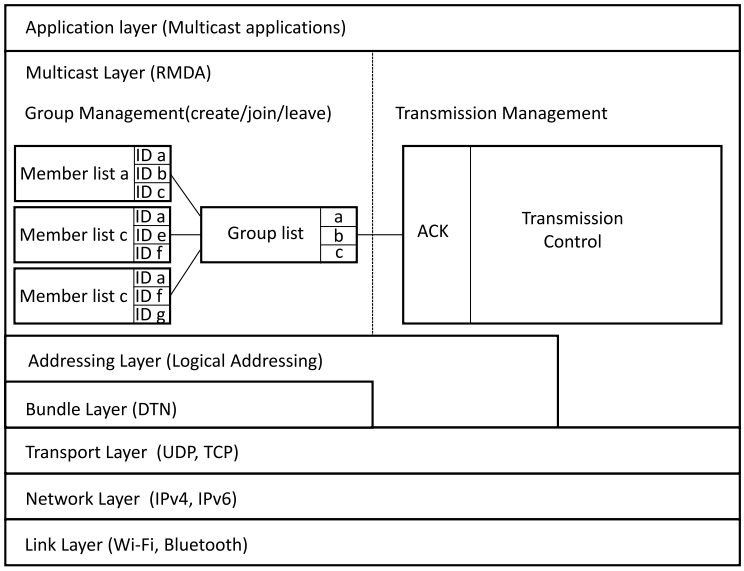

Figure 3: ISO/OSI layer structure with RMDA

3.3 Group Management

In disaster scenarios different types of MANETs can occur, for instance MANETs with or without clusterheads. Clustering algorithms are described by M. Agarwal et al. [AM09]. A clusterhead is a node that acts as a manager of a network cluster. The different network organizations require also a different group management. In MANETs with clusterheads, the clusterhead is re-

sponsible for group management. If a node wants to create a new group, it sends a *CreateGroup* messge to the clusterhead. The creator of such a new group is automatically a group member. Thereafter, the clusterhead floods a *NewGroup* message into the local network. In RMDA a node can join a group by sending a *JoinGroup* message to the clusterhead. A *LeaveGroup* message will be used for leaving a group. If a node doeas not send *Hello* messages for a defined time period, it is automatically deleted from the member list.

In MANETs without a clusterhead, every node participating in our system has a group list and a member list. A new group is created by registering the new group in the group list. For this purpose, the creator of a new group is automatically a group member. Changes or creation of new lists have to be distributed over the complete network, which generates a lot of traffic. Therefore, we assume that the group membership does not frequently change.

The protocol uses logical IDs for member management. Therefore, new nodes do not need to join a group if they come from another MANET and are already members of the group. If the MANET comes in contact with another MANET or a ferry is used, the member list and the group list will be exchanged in different ways. A node in a MANET without a clusterhead first receives, then compares, next updates, and finaly floods the list through the network. Also the ferry compares and updates its own lists. In MANETs with clusterhead, the ferry compares its list with that of the clusterhead only.

3.4 Multicast in Subnetworks with Clusterheads

A cluster is defined as an amount of nodes being in communication range. Every communication including that with other MANETs is processed via the clusterhead. All nodes have to know the IP address of the clusterhead. The clusterhead stores the group list and the member list and also sends periodical advertise-messages via broadcast into the network to be able to manage its network. Therefore, it can store messages for other nodes or distribute messages to specific nodes.

If a ferry, or a node, comes in radio range with a clusterhead-based network, it receives the advertise-message from the clusterhead. The ferry acts as a gateway between separated MANETs and sends the multicast message to the clusterhead. From this point on, the clusterhead is responsible for the delivery of the group messages, because it has the global view on the local network. The clusterhead stores the multicast message and sends an acknowledgment with the amount of group members to the sender. Additionally, it uses the underlying routing protocols for the transport of the multicast messages. It can use the logical IDs of the group members for the direct assignment of the IP addresses.

Figure 4 shows the exchange of messages between the ferry, the clusterhead, and the group members as described above. In step (1) the ferry sends the message to the clusterhead. Next, the message is delivered to the group members in step (2). Finally, the clusterhead sends a delivery acknowledgment to the ferry in step (3).

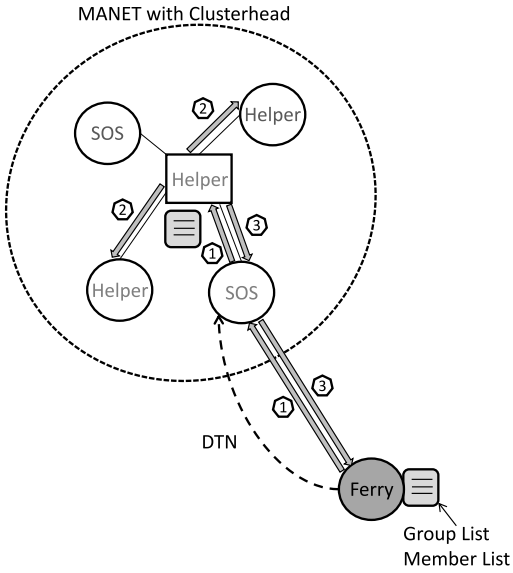

Figure 4: Message exchange if a ferry reaches a MANET with clusterhead

3.5 Multicast in Subnetworks without Clusterheads

As we consider MANETs in disaster scenarios with heterogeneous networks, we cannot ensure that every subnet has a clusterhead dealing with the management of multicast groups. If a ferry reaches such a network, it has to find the group members by its own. In our previous work [FSS+12], we presented an approach for mapping names to local IP addresses by using an adaptive routing framework. We also use this approach for finding group members to keep the additional traffic low.

In our naming scheme, we consider several name classes, e.g. a class 'identity' and a class 'service'. Every name class has its own properties, e.g. if a name is allowed to be multihomed on several IP addresses. For supporting multicast groups, we introduce the new class 'multicast_group' which allows to place a group name, e.g. *helper_group*, on different nodes.

If the ferry reaches an unknown network without a clusterhead, it tries to resolve the multicast group class name. For our proactive module based on OLSR, the ferry has global knowledge about the routes and names in the network, after the initial exchange of Hello and Name Advertisement (NADV) messages. It can immediately check its Host Address Mapping (HAM) table and the routing table to find group member nodes and to instantly send out the group messages.

In our reactive mode based on AODV, the ferry needs to send out a route request (RREQ) with an encapsulated name request (NREQ) containing the group name. If this request reaches the regarding node or another node with the requested knowledge, our mechanism creates a name reply (NREP) together with the remaining route reply (RREP) and sends it back via unicast to the ferry. After a defined timeout, the ferry stops waiting for replies and sends the message to the retrieved group members.

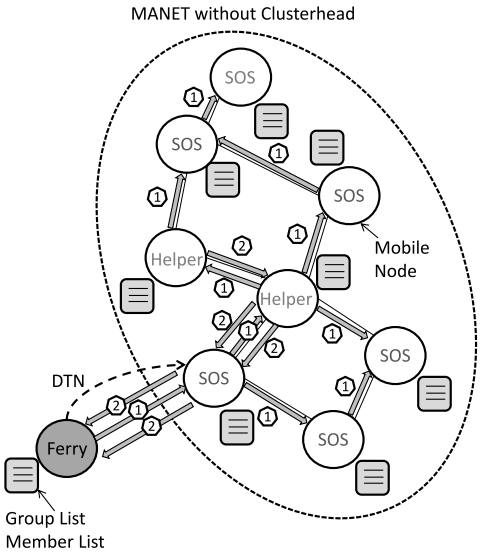

Figure 5: Discovery of group members if a ferry reaches a MANET without clusterhead

Figure 5 and 6 show the message exchange between the ferry and the nodes in a MANET without a clusterhead and with reactive routing enabled. Figure 5 shows the discovery of group members by using name resolution. The ferry sends out a RREQ/NREQ for the multicast group in step (1) and gets back a RREP/NREP by the remaining nodes in step (2). The message delivery is shown in Figure 6. In step (3), the ferry sends out the message to the found group members, which send back an acknowledgment in step (4).

4 Conclusion and Future Work

In this paper, we presented an approach for reliable multicast in MANETs over Delay Tolerant Networking. We described a robust and efficient group member management by using node identities as member names and by well-organized member list exchange. We designed our protocol for being adaptive to several kinds of MANETs, e.g. networks with clusterheads or without, respectively. For finding group members in networks without clusterheads, we use our previously published name resolution mechanism. Due to efficient acknowledgment handling, we minimize the caused traffic. Our approach enables reliability, as a message sender tries to deliver the message until the average amount of group members has received it.

As future work, we consider the automatic assignment of groups on the basis of attributes. Simulation results will be compared with existing approaches to proof the better performance of our mechanism. Finally, we will add some security aspects to our framework.

Acknowledgements: The authors would like to thank the administration and members of the International Graduate School on Mobile Communications (Mobicom) for their support and the German Research Foundation (DFG) for their kind funding.

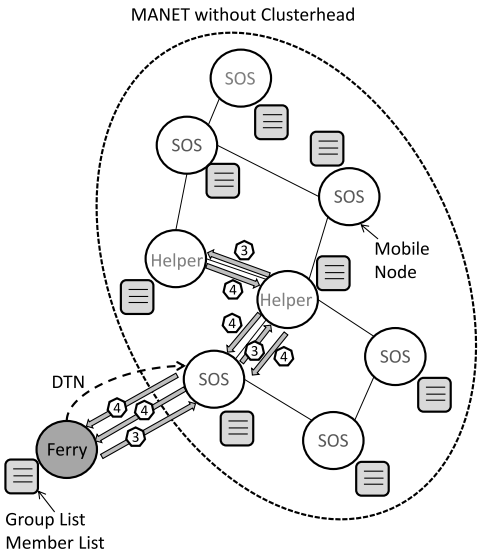

Figure 6: Multicast message delivery after group member discovery

Bibliography

[AL09] S. Ahn, Y. Lim. A Modified Centralized DNS Approach for the Dynamic MANET Environment. In *9th International Symposium onCommunications and Information Technology (ISCIT)*. Pp. 1506 – 1510. Sept. 2009.

[AM09] R. Agarwal, M. Motwani. Survey of clustering algorithms for MANET. *International Journal on Computer Science and Engineering (IJCSE)* 1:98–104, 2009. http://arxiv.org/ftp/arxiv/papers/0912/0912.2303.pdf

[AMZO09] A. Afanasyev, K. Mayoral, Z. Zhu, S. Y. Oh. DTCAST: Delay and Disruption Tolerant Multicasting Protocol. *Proceedings of the 11th Youth Technological Conference "High Technologies and Intellectual Systems"*, Apr. 2009.

[CK11] S. Cheshire, M. Krochmal. Multicast DNS (IETF Internet-Draft). Feb 2011. Expires: 18 August 2011.

[ETE03] P. Engelstad, D. Thanh, G. Egeland. Name Resolution in On-Demand MANETs and over External IP Networks. In *International Conference on Communications (ICC)*. Pp. 1024 – 1032 vol.2. May 2003. doi:10.1109/ICC.2003.1204507

[FSS+12] T. Finke, J. Schroeder, S. Schellenberg, M. Hager, J. Seitz. Address Resolution in Mobile Ad Hoc Networks using Adaptive Routing. In *Seventh International Conference on Systems and Networks Communications (ICSNC)*. Pp. 7–12. Nov. 2012.

[JPK04] J. Jeong, J. Park, N. Kim. DNS Name Service based on Secure Multicast DNS for IPv6 Mobile Adhoc Network. In *6th International Conference on Advanced Communication Technology (ICACT)*. Volume 1, pp. 3 – 7. Feb. 2004. doi:10.1109/ICACT.2004.1292818

[LSSI05] J. Liu, D. Sacchetti, F. Sailhan, V. Issarny. Group Management for Mobile Ad Hoc Networks: Design, Implementation and Experiment. In *6th International Conference on Mobile Data Management (MDM)*. Pp. 192–199. May 2005.

[MAH00] S. Mäki, T. Aura, M. Hietalahti. Robust Membership Management for Ad-hoc Groups. In *5th Nordic Workshop on Secure IT Systems (NORDSEC)*. Oct. 2000.

[Moc87] P. Mockapetris. Domain Names - Concepts and Facilities. RFC 1034 (Standard), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[MP04] M. Maleki, M. Pedram. Lifetime-Aware Multicast Routing in Wireless Ad Hoc Networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*. Volume 3, pp. 1317 – 1323. Mar. 2004. doi:10.1109/WCNC.2004.1311633

[NK10] S. C. Nelson, R. Kravets. For Members Only: Local and Robust Group Management in DTNs. *5th ACM Workshop on Challenged Networks (CHANTS)*, pp. 5–12, Sep. 2010.

[NS09] Z. Narmawala, S. Srivastava. MIDTONE: Multicast in Delay Tolerant Networks. In *4th International Conference on Communications and Networking in China (ChinaCOM)*. Pp. 1–8. Aug. 2009.

[PBD03] C. Perkins, E. Belding-Royer, S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.

[RP00] E. Royer, C. Perkins. Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing. July 2000. http://tools.ietf.org/html/draft-ietf-manet-maodv-00

[SBH+13] S. Schellenberg, P. Begerow, M. Hager, J. Seitz, T. Finke, J. Schroeder. Implementation and Validation of an Address Resolution Mechanism using Adaptive Routing. In *27th International Conference on Information Networking (ICOIN)*. Pp. 95 – 100. Jan. 2013.

[YLSG02] Y. Yi, S.-J. Lee, W. Su, M. Gerla. On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks. November 2002. http://tools.ietf.org/html/draft-ietf-manet-odmrp-04