MDRP: A Content-aware Data Exchange Protocol for Mobile Ad Hoc Networks

Stephan Eichler [#1]

[#]*Institute of Communication Networks, Technische Universität München*
Arcisstr. 21, D-80290 München, Germany
[1]s.eichler@tum.de

***Abstract*— Information exchange and content distribution is the main task of Mobile Ad Hoc Networks (MANETs). However, most of the communication protocols suggested in the literature follow conventional routing strategies to exchange messages. A data exchange mechanism solely using the content as the basis for communication relations is yet missing. In our work we identify the need for a content-aware message routing protocol and explain the scenario where such a protocol can be applied. Further we outline the new content exchange protocol called Mobile Data Request Protocol (MDRP) and explain the main protocol steps. The new protocol is then evaluated using the OMNeT++ simulation environment. The presented simulation results in the paper prove the functionality of MDRP in different scenarios. We close with a conclusion highlighting the advantages of the protocol over conventional routing concepts.**

I. Introduction

Using ad hoc communication technology to distribute information in mobile environments will become very common in the future. The use cases for ad hoc communication range from primarily static Sensor Networks to highly Mobile Ad Hoc Networks (MANETs) in vehicular environments. The common use in all scenarios is the distribution or exchange of information. The use of ad hoc communication provides means to exchange data in a fully distributed and self-organized fashion, which is especially well adapted to spontaneous, unplanned communication settings.

The primary data exchange mechanisms suggested for MANET environments is a routing-based data exchange, while in Vehicular Ad Hoc Networks (VANETs) the use of broadcasting techniques is dominating. Many different routing protocols have been proposed in the last years [1], dealing with different MANET scenarios and challenges. The existing approaches can be categorized into three categories: *flat*, *hierarchical*, and *Geo-based* routing. The protocols of each category have specific scenarios and settings where they work best, however, all of them have in common that the routing mechanism is not connected to the requested data in any way. A network setting where routing and data content are somewhat connected is in Peer-to-Peer (P2P) networking for file exchange on the Internet. In this setting the user doesn't care from which peer the data is transferred, only the respective content is crucial.

The nature of P2P is also relevant in different MANET and especially VANET settings[1]. A node might require a specific information, however, it does not know from which node to request it. Hence, a conventional routing protocol can not fulfill the task of retrieving the data, therefore, a specific *content-aware* data request protocol is needed. For any solution suggested for this use case the specific limitations existing in MANETs have to be considered, leading to a highly adapted solution. The main limitation relevant for a protocol design is the limited network capacity in MANETs. Hence, a protocol should be able to retrieve the desired content with as few requests as possible. Thus, a simple broadcast-based request solution is not feasible, as it would use up most of the available bandwidth.

In this paper we present one solution to the given problem: The Mobile Data Request Protocol (MDRP) is a request-based data exchange and distribution protocol, which is optimized for MANET environments supported by gateway nodes. The remainder of the paper is structured as follows. In Sec. II the scenario for MDRP and the protocol are introduced. In Sec. III the simulation environment and the results are presented. The related work and further reading are given in Sec. IV. The paper concludes with Sec. V.

II. Content Distribution using MDRP

A. Motivation and General Idea for Content-aware Routing

Especially in a VANET, where most data exchanges are unrequested and broadcast-based, the use of a conventional routing protocol is useless and of no much help. But solely relying on the broadcast-based data distribution is not sufficient in some situations, since a node might need specific information which however is currently not broadcast by any of the surrounding nodes. In this case it would be useful to be able to send a request to the neighbors or the network environment in general asking for the required information.

While most content is not directly addressable by nodes as is, since its existence is only known to nodes that already received the respective data, it can become addressable by introducing e.g. content categories. An example for such a category could be the current parking capacity in a given city, the traffic conditions in a certain area, or the support and status information for the supporting security architecture needed in a vehicle-to-vehicle (V2V) communication system. Introducing content categories, therefore making information directly addressable for a content-aware protocol, will reduce the load on the network. Hence, the content can be distributed

[1]We use MANET as a synonym for VANET in the following.

in an optimized fashion compared to a simple broadcast solution.

The term *content-aware* stands for any routing or data distribution protocol which itself relates to the content it transports. In the case of MDRP content-awareness exists in two ways. First the content is used similar to a network address and secondly the protocol is constantly aware of which content the node currently requested to be able to gather the respective data from incoming packets.

Basically, a content-aware routing mechanism can be realized in any MANET scenario. Nevertheless, a few requirements have to be fulfilled to implement such a mechanism. In addition, some scenarios are more beneficial for content-aware routing than others. In our scenario we use gateway nodes that distribute content. Each gateway node is connected to both the ad hoc network and the backend network hosting the content servers. Besides the initial content distribution, the gateways are also used to optimize the success rate of content requests. Each request is sent with a geographical direction. The direction is always towards the closest gateway of the requesting node. Since the gateways are omniscient due to the direct connection to the content servers, the request does not have to be flooded throughout the whole network. To be able to find the closest gateway an announce mechanism is required making gateway information available to nodes. For this purpose the mechanisms proposed in [2], [3], [4] can be used. In the protocol version outlined in Sec. II-B each node needs to have the information of at least one gateway. However, a protocol without using gateway nodes would also be feasible with slight changes.

B. The Mobile Data Request Protocol

In the following section we will introduce the functionality of the Mobile Data Request Protocol (MDRP). We differentiate between *nodes* and *gateways*. While a gateway is the origin of content it will distribute data initially. In addition it can be the final peer in a content request process, the peer providing the content at last. The regular nodes can either be a requesting node or a forwarding node.

Neighborhood discovery: Before a node can start to request content or handle incoming requests it needs knowledge of its current neighborhood. Each node holds a table with the neighbor information containing node positions. The table is updated based on both incoming messages and the use of Hello-messages. If the table entries are older than a given threshold (t_{age}) and no messages have been received, the node starts sending Hello-messages to update the neighbor information. The neighborhood is divided into four sectors (see Fig. 1), which helps to reduce the number of nodes that react to a request.

Request process: If a node needs to request content it first looks up the closest gateway from its database and identifies the sector in which the gateway is positioned. In the second step the neighbor database of the respective sector is searched. If the sector contains nodes the request is sent, relevant only for the nodes located in the selected sector. However, if the sector contains no nodes or a first request has not been answered after a wait-time (t_{wait}), the adjacent sector to the right is added to the list of recipients. This process is continued until all sectors are in the list of recipients (see Fig. 2). A node receiving a request, first checks if it can provide the requested content. If this is the case it replies directly, addressing the sector where the request came from. Otherwise the request is forwarded to neighbors in the direction of the gateway. Again the sector management introduced above is used. In Fig. 1 an example for a communication process is shown. A reply is always sent directly after the request has been received, while the message forwarding is slightly delayed. This enables the protocol to detect the replies and halt the forwarding process to reduce the network load.

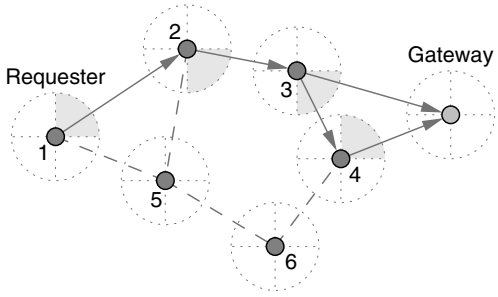

Fig. 1. Message path towards a gateway using MDRP

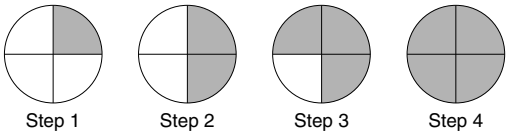

Fig. 2. Sectorization used by MDRP

Reply process: Any node in the network along the path towards the gateway can reply to a received request, provided that it has the respective content. If no node along the path towards the gateway can reply, the gateway is the assured content source, being able to provide any requested content. During a request process, like the one shown in Fig. 1, each intermediate node saves the incoming requests and its originating sector in a reply table. This helps to forward the replies to the designated area in the network. As soon as the corresponding content reply has been forwarded the entry in the reply table is deleted. The reply table is constantly reviewed to age entries and delete them accordingly. In the case where a request is replied by both an intermediate node (e.g. node 4) and the gateway, the next upstream node(s) sharing both reply paths act as a filter. Only the first reply received will be forwarded. Due to the deletion of the respective reply table entry after the first reply has been handled, all following replies can not be routed and are therefore deleted. This is beneficial, since the request has already been replied to, hence, the network load due to multiple replies is reduced to a minimum.

Expanding request messages: Since a request can travel multiple hops until a gateway is reached (see Fig. 1), it is likely that intermediate nodes also have requests to send. MDRP

allows to expand received requests and attach additional content requests. This has no implications on the request process itself, however, the reply process has to be adapted slightly. Each node expanding a request has to scan the incoming replies for the desired content. If the requested content is contained in a received reply, the node takes out the content and forwards the reduced content reply message towards the remaining receivers. This feature makes MDRP content-aware.

Large content replies and fragmentation: Since content replies can become larger than the Message Protocol Data Unit (MPDU) of the used wireless transmission technology, for example conventional IEEE 802.11 Wireless Local Area Network (WLAN) uses a MPDU-size of 2346 B [5], [6]. Hence, a fragmentation mechanism is required, to be able to send larger content messages using several smaller packets. MDRP handles each request and reply pair coherently. The requesting node selects a request-ID, which then identifies the full protocol process until its completion. The first packet of a reply process contains status information on the reply. This includes the request-ID, content size, and the number of fragments. Each of the following packets contains the request-ID and the respective fragment sequence number. The requesting node can then collect all fragments, re-request potentially lost fragments, and combine the parts to the desired content.

C. Security Considerations for the Protocol

Security is a required component in most wireless communication systems [7]. Hence, also for MDRP security features are required. In this paper we will not outline the full security setup required for MDRP due to space limitations, however, we will present the most important mechanisms.

As a trust basis we suggest a Public Key Infrastructure (PKI) with certificates [8], [9], each node owns at least one certificate to identify itself and its messages to other nodes. All messages exchanged by MDRP are digitally signed, therefore, a recipient can verify and identify them as a valid message sent by a trustworthy sender. Messages not persisting these checks or messages not signed at all will not be processed further by the protocol.

Very crucial is the integrity of the exchanged content. Content providers hold special certificates, enabling them to initially distribute content. Receiving nodes can validate content using the known certificate chain of the PKI. Thus, a content provider *always* has to digitally sign content packets to ensure their integrity. Since MDRP can also be used to exchange confidential data between a node and a gateway directly, a Diffie-Hellman key agreement scheme [10] is integrated in the request/reply mechanism. Using the exchanged shared key all content can then be encrypted.

Since all content packets are digitally signed by the content provider and receivers save the content together with the signature, any previous receiver can become provider for the respective content. The slight overhead in storing the signatures in addition to the content can be justified by the feature that any node can reply to a request.

III. Simulation and Evaluation

To test and evaluate MDRP we implemented the protocol in a simulation environment. In this section we outline the details on the simulator and the settings used and we present simulation results.

A. Simulation Environment and Settings

The simulation environment we used was OMNeT++ in combination with the Mobility Framework (`http://www.omnetpp.org/`). The simulation area was set to 1000 m $\times$ 1000 m. The radio propagation model was the Free-Space model with the pathloss coefficient α set to 2.5, leading to a radio range of about 100 m. The overall message size was set to 200 B. The Hello-message interval was set to 2 s. The nodes moved at an average speed of 15 m/s using the Random-Waypoint model. For all simulations we did 20 independent simulation runs and calculated the 95% confidence intervals for the results.

In the simulations the gateway provided three different content categories. The nodes tried to receive all three categories during the maximum simulation time of 600 s. Where not stated otherwise we used one gateway node in our scenarios.

B. Simulation Results

First of all we looked at the general functionality and the performance of the new protocol. The simulations proved that MDRP is well suited to distribute content in mobile wireless networks. In Fig. 3 the time required to distribute *all* three content packets to all network nodes depending on the node density is plotted, with increasing node density the distribution time reduces exponentially. Due to the higher density the connectivity increases, hence, messages can be distributed much better. Our protocol uses this effect very well to its own benefit.

The second issue we looked into was the number of hops a content packet travelled until it reached the requesting node. The maximum, minimum, and average number of hops the content travelled are plotted in Fig. 4. In all scenarios the minimum number of hops is one. More interesting is the maximum and average number of hops for different densities. The average ranges between two and ten hops. The results

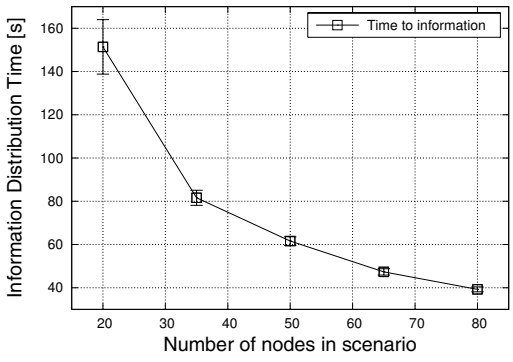

Fig. 3. Time to fully distribute information

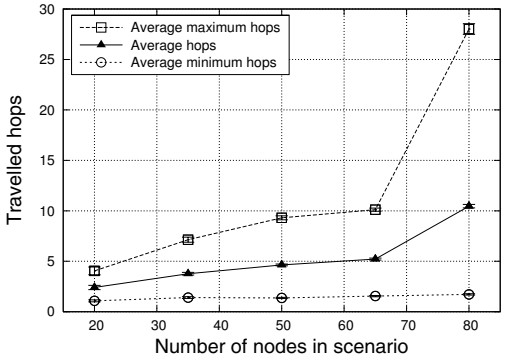

Fig. 4. Number of average travelled hops

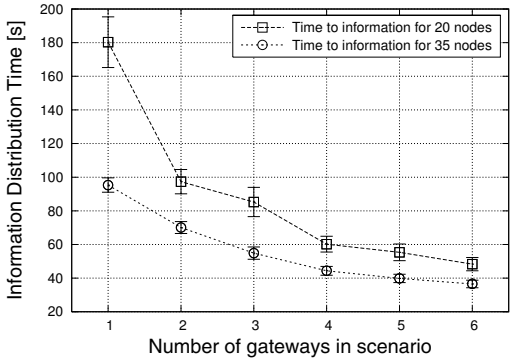

Fig. 6. Influence of gateway density on information distribution

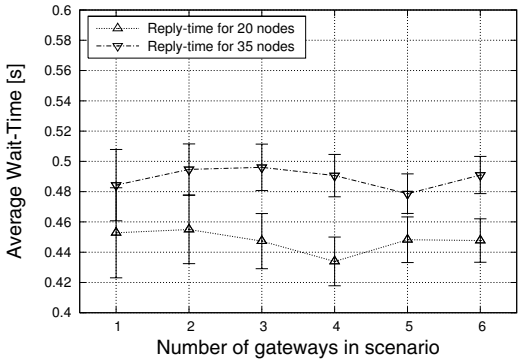

Fig. 7. Influence of gateway density on wait-times

plotted in Fig. 4 include all content exchanges that occurred during the simulation time. In the beginning of a simulation run the hop distance is longer than after some time has passed, since no content has already been distributed at the start of the run. In a more dense scenario the probability of a fully connected network is higher, therefore, longer multihop paths to a gateway are more likely. This leads to the increased travel distance shown in the plot, while the distribution time can be decreased (see Fig. 3).

The third parameter we evaluated is the reaction time for a successfully answered request. This is the time between the moment a request has been sent until the corresponding response is received. The results for two different settings, either only the gateway may answer a request or also nodes may reply to a request if they can provide the content, are presented in Fig. 5. It can clearly be seen in the plots that allowing intermediate responses made by regular nodes reduces the reaction time up to 0.15 s. For the given scenario with one gateway the reaction time is below 1 s for all simulated node densities. The increase of the reaction time for higher densities can again be explained by the higher probability for longer paths. In addition the higher density leads to a significant increase of the packet collisions on the channel, which also results in a longer reaction time.

An important issue is the density of gateways required for

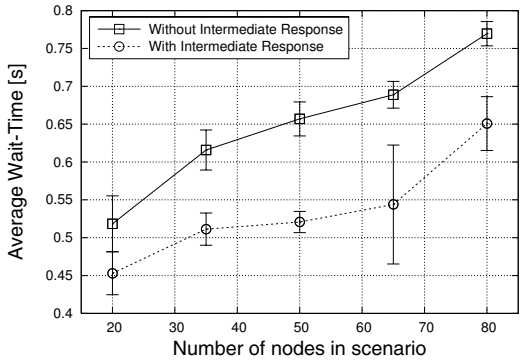

Fig. 5. Reaction times for the Mobile Data Request Protocol

MDRP to work properly. In the previous results the functionality using simply one gateway has been proven. However, the question arises if more gateways can increase the performance of the protocol significantly. First we looked at the content distribution time (see Fig. 6), which decreased exponentially with increasing gateway density. The effect can also be seen if the node density is increased, however, the effect weakens for an increased node density. Thus, especially for low density network settings even a slight increase of the gateway density can reduce content distribution times.

Looking at the reaction times, the increase of the gateway density does not clearly show an effect in either direction. In Fig. 7 simulation results for two node densities are shown. The average reaction time for the scenario with 20 nodes is almost constant at 0.45 s while for the second scenario with 35 nodes the average value is slightly higher at 0.49 s. We assume that using an optimized placement of the gateway nodes on the simulation area will lead to a reduction of the reaction times with increased gateway densities.

IV. Related Work

A multitude of alternatives for routing in MANETs has been proposed in the literature. Here, we given an overview on the directly related work used for defining MDRP.

In [11] Carzaniga et al. introduced the concept and system design of content-based networking. Nodes are no longer

addressed by unique network addresses, however, so-called *receiver-predicates* (comparable to our content classes) are used. The authors outline their subscription and publishing mechanisms and how they connect to routing in a network very thoroughly. The authors extended their concept and suggested a content-based routing protocol in [12]. The protocol uses broadcast trees based on the predicates of content-based networking to forward requests and replies. The routing protocol does exchange routing information just like most known routing protocols, replacing network addresses with predicates connected to content.

Besides the content-based networking the MDRP concept relates closely to geocasting concepts. In geocast protocols nodes are addressed by their position or area around their position rather than a network address [13]. Ko et al. present in [14] a geocasting concept for location-based multicast. In their concept data is flooded to a defined geographical region using positioning in the nodes. Closely related to our forwarding scheme is the Greedy Perimeter Stateless Routing (GPSR) protocol presented in [15]. Again, the protocol uses the nodes position to forward messages, however, the protocol is in no way content-aware. Thus it is more of a conventional routing mechanism simply based on positions. Another geocast-based multicast protocol is GeoTORA [16] which is a geographic extension to the TORA routing protocol. A good overview on different geocasting mechanisms has been presented in [17].

In addition to geocasting concepts MDRP also relates to the Zone Routing Protocol (ZRP) presented in [18]. The ZRP is a hybrid routing protocol; it uses so-called routing zones around each node which are updated proactively. Routes beyond the zone need to be set up using a reactive mechanism.

V. Conclusion

With the Mobile Data Request Protocol (MDRP) we presented a novel routing concept especially suited for MANETs. MDRP is a content-aware data exchange protocol, specifically addressing content not nodes. In the current protocol setup it relies on gateway nodes providing content initially and in all cases where no close by neighbor can provide the respective content. The protocol uses geocast mechanisms to optimize the distribution of content requests towards the closest gateway node.

Our simulation results prove the functionality of MDRP. Even with low gateway densities the protocol can distribute content fast and efficiently. This new routing concept is especially useful in networks where content can be categorized and directly addressed. This is the case in VANETs for example. Since vehicles know about their route they can specifically request information an the respective roads/areas. A second use case for MDRP is to distribute status information on a request basis. This can be usefull for e.g. status information of a PKI. Compared to routing protocols like Ad hoc On-Demand Distance Vector Routing (AODV) or ZRP our protocol generates lower network load and distributes information with similar reaction times.

In further research activities we will further evaluate and improve the protocol. The next step will be to find optimal gateway densities and distributions for MDRP. In addition, we are working on a gateway announcing mechanism to better inform nodes about gateways close by.

References

[1] H. Xiaoyan, X. Kaixin, and M. Gerla, "Scalable routing protocols for mobile ad hoc networks," *IEEE Network*, vol. 16, no. 4, pp. 11–21, July 2002.

[2] M. Michalak and T. Braun, "Common gateway architecture for mobile ad-hoc networks," in *Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services*, Jan. 2005, pp. 70–75.

[3] M. Bechler, L. Wolf, O. Storz, and W. Franz, "Efficient discovery of internet gateways in future vehicular communication systems," in *Proceedings of the 57th IEEE Semiannual Vehicular Tecnology Conference (VTC 2003 Spring)*, Apr. 2003. [Online]. Available: http://www.ibr.cs.tu-bs.de/users/bechler/myPublications/marc_BSFW03.pdf

[4] J. Xi and C. Bettstetter, "Wireless multihop internet access: Gateway discovery, routing, and addressing," in *In Proceedings of the International Conference on Third Generation Wireless and Beyond*, May 2002.

[5] LAN/MAN Standards Committee, *Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, IEEE Computer Society, Sept. 1999.

[6] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116–126, Sept. 1997.

[7] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[8] C. Schwingenschlögl and S. Eichler, "Certificate-based key management for secure communications in ad hoc networks," in *Proceedings of the 5th European Wireless Conference: Mobile and Wireless Systems beyond 3G*, Feb. 2004.

[9] R. Perlman, "An overview of pki trust models," *IEEE Network*, vol. 13, no. 6, pp. 38–43, Nov. 1999.

[10] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[11] A. Carzaniga and A. L. Wolf, "Content-based networking: A new communication infrastructure," in *Proceedings of the NSF Workshop on an Infrastructure for Mobile and Wireless Systems*, ser. Lecture Notes in Computer Science, no. 2538. Springer-Verlag, Oct. 2001. [Online]. Available: http://serl.cs.colorado.edu/~carzanig/cbn/

[12] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in *Proceedings of IEEE INFOCOM*, Mar. 2004.

[13] J. C. Navas and T. Imielinski, "Geocast – geographic addressing and routing," in *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*. New York, NY, USA: ACM Press, 1997, pp. 66–76.

[14] Y.-B. Ko and N. H. Vaidya, "Geocasting in mobile ad hoc networks: Location-based multicast algorithms," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, 1999.

[15] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*. ACM Press, Aug. 2000.

[16] Y.-B. Ko and N. H. Vaidya, "GeoTORA: A protocol for geocasting in mobile ad hoc networks," in *Proceedings of the 8th International Conference on Networking Protocols (ICNP)*, Nov. 2000.

[17] X. Jiang and T. Camp, "A review of geocasting protocols for a mobile ad hoc network," in *Proceedings of the Grace Hopper Celebration (GHC)*, 2002.

[18] Z. J. Haas and M. R. Pearlman, *Ad Hoc Networking*. Addison-Wesley Longman Publishing Co., Inc., 2001, ch. ZRP: A Hybrid Framework for Routing in Ad Hoc Networks, pp. 221–253.