Flooding-Based Network Monitoring for Mobile Wireless Networks

Christian Sauer[1], Maja Sliskovic[1], and Marco Schmidt[2]
[1] SEW-Eurodrive GmbH&Co.KG, 76646 Bruchsal, Germany
[2] University of Applied Sciences Bochum, 42579 Heiligenhaus, Germany
Email: {Christian.sauer.w, maja.sliskovic}@sew-eurodrive.de; marco.schmidt@hs-bochum.de

Abstract —The monitoring and online analysis of computer networks is a wide field of research, covering many applications from constant load determination of high-performance wired networks to connection-oriented measurements in different QoS applications. QoS-enabled routing in mobile ad-hoc networks (MANETs) is the most common application for network monitoring in dynamic wireless network topologies. We describe three example applications requiring the monitoring of connection reliability, transmission delay and the network topology. The presented set of applications shows similarities in the used communication network. A network monitoring system used in such network has to have specific properties. We surveyed a number of existing protocols and propose an additional system for network monitoring in mobile wireless networks. We implement and test a Flooding-Based Network Monitoring (FBNM). The impact of flooding-based systems on primary communication using the same wireless medium is tested using the implemented system. The delay of message transmission multi-hop networks is analyzed.

Index Terms—Network monitoring, mobile nodes, intermittent connections, multi-hop relay

I. Introduction

Network monitoring aims to measure parameters of connections within a communication network, with the goal to capture and analyze the performance of the network. We present a flooding-based network monitoring system for mobile wireless networks. We start by generalizing the type of application our system is meant to be used in, followed by three examples of such applications. We extract the requirements for an applicable network monitoring system from the generalized description in order to verify the applicability of our system.

For a generalized version of the examined application, we consider a group of mobile nodes in an unknown environment. All of these nodes are equipped with radio communication devices and communicate using a wireless network. The nodes act autonomously while being supervised by one or more static nodes. All nodes can utilize peer-to-peer or multi-hop communication. A mobile node is described as connected to the network, if a direct or multi-hop route to the static node exists.
Some of the examined applications can include critical communication from the static node to mobile nodes (e.g. fire alarm). This critical information must be transmitted within 100 ms and with a reliability of at least 98 %. The existence of such a connection to all mobile nodes can never be guaranteed in a changing environment. Therefore the mobile nodes must additionally detect the lack of a sufficient connection to a stationary device within a determined time span (e.g. 1 s). The connections state should be reported to the static node in regular intervals.

Wild fire detection, continuous vitals monitoring and the control of mobile robot fleets are three examples for the previous general description. In forest fire detection, for example it is of great interest to detect the disconnection of sensors as soon as possible, since disconnected sensors would lead to a delayed detection of fires if the fire originates in the affected part of the forest. Mobile wireless sensor networks with ad-hoc network capabilities can be used for health monitoring in non-critical situations. In this application, it might be of great interest of the medical staff and the patient to be informed if the current health information can no longer be transferred to a central data sink. A third application is the usage of mobile devices in industrial automation. In such an application, a central control unit might issue an alarm, which requires the mobile nodes to transfer to a safe state. Such time critical applications require the continuous monitoring of connection parameters.

After describing the application and the resulting requirements for an applicable network monitoring system, we continue to categorize the type of network monitoring, that is required. First, we identify the route parameters that are of interest. In our applications these are: the message delay (1-way-latency) and the reliability/packet loss of a route. The system must be able to monitor the routes from one central node (e.g. data sink, central control unit) to all nodes in multi-hop range. The routes must be monitored permanently. Since the continuous existence of communication cannot be guaranteed, the network monitoring system must actively send messages to avoid time spans without monitoring. The system needs to work in mobile wireless networks. Disconnections by single nodes are not predictable but may not affect the general monitoring functionality. The results of the monitoring have to be provided to the central node and in parts to all mobile nodes of the network, too. Additionally all networks in the aforementioned examples are used to transport data, which is further described as primary communication.

Manuscript received March 8, 2019; revised September 4, 2019.
Corresponding author email: Christian.sauer.w@sew-eurodrive.de.
doi:10.12720/jcm.14.10.876-883

TABLE I: COMPARISON TO RELATED TYPES OF NETWORKS

Field of Research	Monitored …			Required Network	Purpose
	Connections	Duration	Characteristics		
QoS-enabled MANET routing	One	During transmission or route establishment	Throughput End-to-end delay Jitter	Peer-to-peer Manet	Guaranteeing connection quality for application layer
Backbone Balancing (ISP)	All	Permanent	Throughput Delay Load	Wired Backbone	Load Balancing in network infrastructure
WSN Management	All	Permanent or on event	Connection Date Throughput	Wireless Dense Static	Tool for management, debugging and use of WSN
MSN	-	-	-	Mobile Wireless Sparse	Sensor Measurements Data Exchange
Required	All One-to-Many	Permanent	End-to-End delay Reliability	Wireless Sparse Mobile	Checking connectivity from and to one node

The impact of the network monitoring on the throughput of the primary communication should be minimal.

We continue this work by giving an overview of research topics featuring the measurement and online analysis of computer networks in section II and check if they match our previously described criteria. In section III we describe the network monitoring system we implemented to fulfil the set requirements. Section IV contains implementation specific details, as used in the considered application. Continuing in section V, we describe performed tests of the proposed system and its performance and conclude the work in chapter VI.

II. RELATED WORK

We surveyed a number of systems that include monitoring of different types of networks. A summary of the examined technologies can be found in table I.

The most common application for network monitoring and measuring of connection parameters are Quality of Service (QoS) supporting protocols. This field of research experienced steady growth in the last decades. The central goal of QoS is the delivery of content and services to network devices, while fulfilling application specific connection requirements [1]. For a long time QoS had the central goal to ensure the quality of voice transmissions, subsequently an early focus was on transmission delay and jitter, the central performance metrics for this application. During the last decade the demand for the delivery of media data to wireless mobile devices grew exponentially and additional requirements like transmission throughput and support for wireless cell networks were presented [2]. Furthermore a wide variety of QoS routing strategies were introduced, that can operate in mobile ad-hoc networks without network infrastructure [3]-[5]. QoS-enabled routing protocols for mobile ad-hoc networks are capable of operating without network infrastructure. However, they are not designed to monitor all connections continuously, and they do not scale well with the number of disconnections in the ad-hoc network. This makes them especially unsuited for usage in applications, where communication between all nodes is not always present. The management of a robot fleet is one example of this. Therefore, they are not suitable for the considered applications. Most QoS routing strategies do not support optimization for monitoring multiple connections from one end-point at once. Additionally, many MANET variants of QoS routing check transmission characteristics only during route discovery, maintenance or selection, but do not support permanent monitoring of multiple routes or connections. Adding such capabilities would cause a major overhead and lead to increased congestion on the wireless medium, which is to be avoided in the examined applications. Network Monitoring is also an important tool for Internet Service Providers (ISP) in the context of network management [6], [7]. It allows tracking of the customers received performance and load balancing in the network. This type of monitoring is explicitly optimized for permanent monitoring of the complete network and minimizing the interference with primary communication. However, these monitoring mechanisms are almost all designed exclusively for wired networks. While some strategies might be transferable to wireless connections, their performance would degrade if subjected to the expected rapidly changing network topology. This must be considered when examining applications like vitals monitoring, where the nodes move with humans. SNMP and CMIP are examples for the existing monitoring protocols [8].

The Monitoring of wireless Sensor Networks (WSN) is one part of the general task of WSN management [9], [10]. Additionally, the management contains installation assistance, debugging capabilities, data analysis, visualization and other functionalities. There are noticeable overlaps between WSN network monitoring and the considered applications. These similarities include monitoring of most relevant network characteristics, a very similar topology and permanent monitoring. However, wireless sensor networks usually

consist of static sensor nodes. Due to the dynamic nature of mobile networks and network environments, we expect vastly more disconnections during network operation. Furthermore, we expect our network to be rarely fully connected, which contrasts most WSN applications. While such systems might be adaptable to permanent monitoring in the wildfire example application, they would cause major communication overhead in mobile networks, like mobile nodes in industrial applications.

Mobile Sensor Networks are special variants of wireless sensor networks [11], [12]. In this work, these are most suitable to be compared to the considered applications. The proposed system is transferable to enhance management solution for such networks. The sparse and mobile nature of these networks complicates this task. Some routing solutions from MSN use opportunistic routing strategies from delay tolerant networks for data transfer [13].

As seen in Table I and the previous descriptions some of the examined technologies, like ISP network monitoring fulfils all of the requirements, but are not applicable for the type of network present in the examined applications. Other technologies, like mobile sensor networks, are very similar to the example application, but do not offer the required functionality and monitoring capabilities.

III. Monitoring System Concept

Inspired by strategies used in delay tolerant network routing, we propose Flooding-Based Network Monitoring (FBNM) to fulfil the set requirements. The system is able to continuously monitor all connections from one or more static node to all mobile nodes in regards to their connection parameters (packet error rate and latency). It is suitable to be used in the described applications.

Because of the fast changes in topology, FBNM is inspired by the epidemic routing strategy, known from delay tolerant networks [14]. This decision is based on the assumption that epidemic routing offers an optimal solution in regards to message dissemination and communication delay, when disregarding storage or bandwidth limitations [15]. FBNM does not store data, therefore the first assumption is true. In this work we will focus on the second assumption and analyze the impact of the limited wireless bandwidth we observe in reality.

In the proposed system, the static node sends test messages to the network with defined intervals. These messages are sent as broadcasts. A node is described as connected, if it receives these test message. Any connected node rebroadcasts a received test message if following three conditions are met:

- **Hop-Limit** - The test message is relayed if a hop-limit of 10 hops is not yet reached.
- **Delay-Limit** - A message is not relayed if it is older than 100 ms.
- **Uniqueness** - Every test message is relayed only ones by any node. Not relaying copies of known messages keeps the network loop-free.

The test messages contain fields to determine the relevant characteristics. A Hop-Count is compared to the set Hop-Limit. A time-of-sending field in combination with the local system time of the receiver is used to determine the delay on a route. A sequence number is sent to guarantee uniqueness and to detect missing messages and messages received in a changed or reversed order. This strategy results in the network topology pictured in Fig. 1.

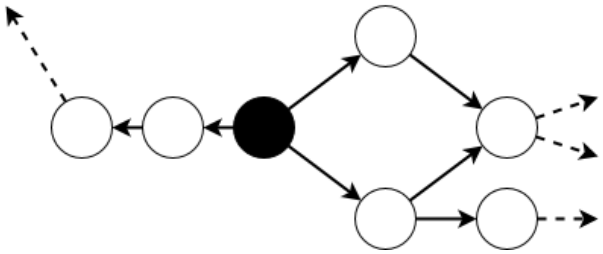

Fig. 1. Topology of test message phase creating a meshed tree. Figure shows test message source (black) and network nodes (white) with the dissemination of test messages over partly redundant routes

In the event of a test message relay the relaying node also appends its own information (address, location, time of relaying and status information) to the test message before rebroadcasting it. Every test message that is passed through the network therefore contains its travelled path. By receiving a test message, all nodes can not only evaluate their own connection status, but also determine a return route to the test message source. This is used to send feedback messages from the network nodes back to the source. This feedback system is meant to enable the test message source to observe and monitor network parameters of the connected nodes and thus the resulting network.

With the proposed feedback system, each node creates feedback messages with a fixed frequency. The process of creating the feedback includes the analysis of all received test messages for their experienced delay, the observed packet loss and the most reliable route back to the test message source.

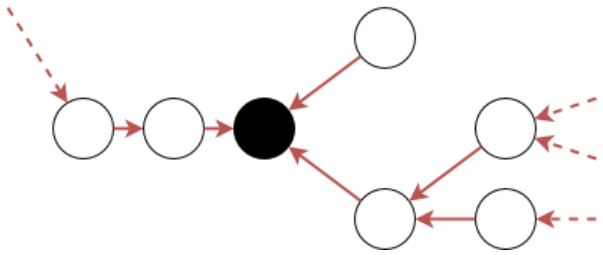

Fig. 2. Collection of feedback messages at the test message source (black) during the feedback phase. The topology has a tree structure without meshed elements

The mobile node then selects a return route based on the determined routes' reliability (determined by packet loss). We assume, that the network topology does not change between the detection of the route during the test message phase and it's usage in the feedback phase. In certain applications, like UAV networks, alternations to the feedback creation frequency are necessary for this

assumption to be true. The feedback system employs a source route mechanism [16]. This means, that the feedback contains the entire route, from the sending node to the test message source. Since the route for the feedback is known, the messages do not need to be broadcast. The reply topology is shown in Fig. 2. This reduces the overall load for the wireless medium during the feedback stage. It can be used to minimize the number of transferred copies. This strategy is not suited for the test message stage because that stage relies on the creation of copies by the broadcast mechanism of the wireless medium.

Each mobile node senses the current status of connection properties to neighboring nodes within a one-hop neighborhood by receiving their rebroadcast test messages and the resulting feedbacks.

The implemented network monitoring system is independent from the used wireless technology. It only requires the ability to send broadcasts or broadcast-like messages and peer-to-peer messages without relying on network infrastructure. It was adapted to use multiple, incompatible wireless technologies at the same time, too. However this requires gateways between different communication technologies, therefore creating parallel network structures. These gateways can either be the test message source or one or more network nodes. The implemented scenario can be seen in Fig. 3.

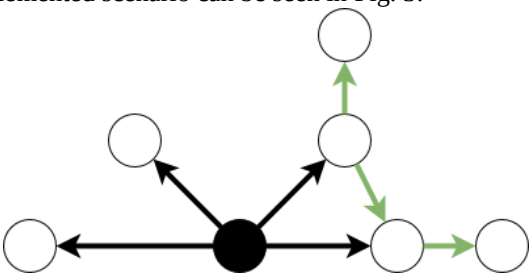

Fig. 3. Implementation of parallel communication using FBNM. High range communication (IEEE 802.11) in black and low range communication (LRC) in green.

Such a division in network traffic might be especially useful in avoiding congestion of any wireless medium. We will examine these benefits in future work.

IV. Implementation

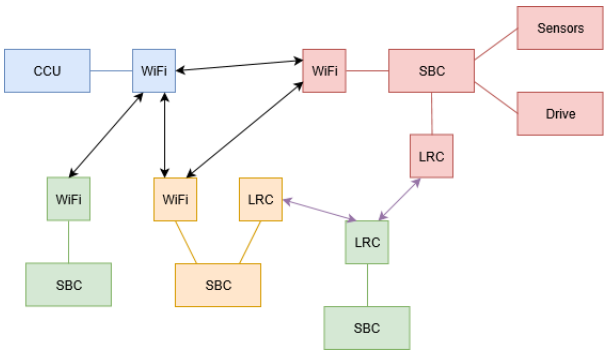

Fig. 4. Example for the implemented network

For the implementation of the FBNM protocol and the presented network scenarios, the Click router framework [17] was used. The implementation uses a number of portable nodes, which used a commercial IEEE 802.11 b/g/n WLAN solution in ad-hoc mode utilizing the 2.4-GHz ISM-band to connect all nodes. A part of the resulting network is shown in Fig. 4.

The Central Control Unit (CCU) is connected to a WiFi interface, creating the static node i.e. the test message source. It broadcasts test messages (black arrows) via WiFi to portable nodes (green). Some nodes are altered, by including additional communication interfaces (yellow) or drive systems (red). The normal nodes contain a WiFi interface or low range communication device (LRC) and a Single Board computer (SBC) to receive, process, and store messages. The advanced nodes are equipped with an LRC and a WiFi interface, which they can use to relay messages between these networks. The last type of node is equipped with additional sensors and actuators.

Based on considered applications a test message generation frequency between 100 Hz and 0:2 Hz was tested. Feedback messages are generated with a lower frequency. The reason is, that the feedback relaying phase requires more resources than the test message relaying phase. During the test message relaying phase each node receives x copies of the test message and edits and relays only exactly one of these. During the feedback phase however, every node receives y feedbacks and sends y + 1 feedback messages, adding its own feedback. Fig. 5 shows this increased number of messages. During the test message phase any node sends only one frame, which is relayed as a broadcast only once. The creation of ”copies” is accomplished by the broadcasting nature of the wireless communication. During the feedback phase, the messages are not sent as broadcasts, but as unicasts. Therefore this results in more individual telegrams, that need to be transferred over the medium. The feedback generation frequency was set between 10 Hz and 0:02 Hz. Higher frequencies in test message and feedback generation allow more precise monitoring of the connections between the nodes, while slower frequencies interfere less with other wireless communication. The reason for the reduced interference is the lowered load on the wireless medium. The impact of these parameters is shown in the following section. The system was implemented using an unaltered version if IEEE802.11, which included the media access control, in particular Listen Before Talk (LBT) and the exponential backoff mechanism. The performed tests include influences of these features in the measurement of transmission delays.

In order to calculate the message delay we need to synchronize system clocks of all nodes with the test message source. This is done by using NTP[1]. Nodes can detect clock desynchronization and synchronize once they are in direct neighborhood to the test message source. Feedback messages are marked by a flag if the contained information is calculated by an unsynchronized node, to

[1] Network Time Protocol

warn the user about possibly misleading data. The clock drift of the used devices required resynchronization after approximately 30 minutes to 3 hours. The usage of real-time-clocks might drastically reduce the need for resynchronization. In outdoor applications a GPS clock can be utilized for this purpose.

The Fig. 11 shows the process of normal usage, relaying, connection loss and the reestablishment of this connection. In this short test the receiver was moved along the green line from the test message source (purple), passing by the relaying node (red) to reach an end-point out of range of both and return back to the test message source. Fig. 11 displays the number of hops, measured transmission delay and transmission reliability, as logged by the receiver. The results show, that with decreasing connection quality and increasing number of relays, we could observe the expected increase in delay and decrease in connection reliability. In all cases the detection of deteriorating connection quality was fast and fulfilled the set requirements.

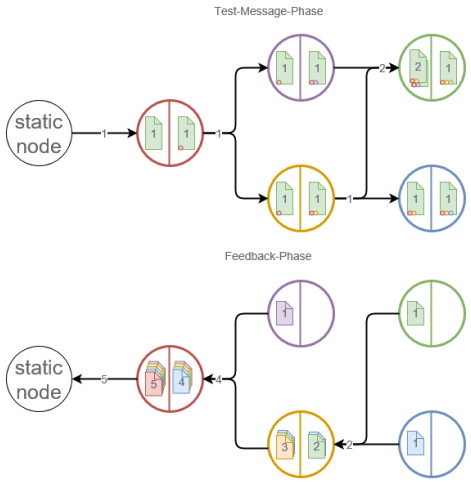

Fig. 5. Message copies during test message phase and feedback phase of FBNM. Example shows additional load on the wireless medium during the feedback phase.

V. Testing

After confirming the general functionality of FBNM (see Fig. 11), we tested three aspects of the FBMS using the implementation described in the previous section. Firstly, we tested the general functionality of the proposed system using different network scenarios of mobile and static nodes in varying environments with up to 10 nodes. After confirming the general functionality of the system we determined the correlation between the number of relays of a message and it's experienced delay. It was verified, that the set hop-limit of 10 hops and the acceptable delay for safety critical information of 100 ms are compatible. Lastly, we needed to determine the impact of the proposed monitoring system on primary communication in the same wireless medium.

The proposed system was successfully tested in office environments, industrial applications and outdoor scenarios. Test messages were sent every 10 - 5000 ms. This enables us to detect disconnections within the same time. Due to interferences and collisions in the wireless medium, the fast frequency of test messages (test messages every 10 ms) shows decreased performance in networks with larger number of nodes.

The correlation between number of hops and delay was tested with an altered version of the proposed system. This was necessary, since a 10-hop-relay using IEEE 802.11 would require an experiment with up to 1 km total length. In order to avoid this, we removed the requirement of uniqueness from the relay check (see section III). This creates loops in the network. The resulting topology is shown in figure 6. The following results were measured using one test message source and two mobile nodes within direct transmission range.

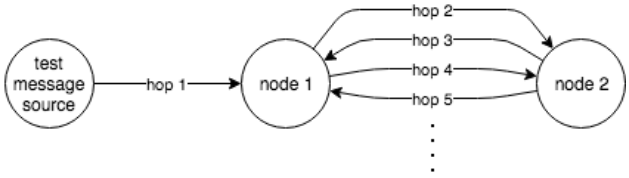

Fig. 6. Modified FBNM for 10 hop topology. Showing relaying of test message from the test message source left) to a pair of mobile nodes (right).

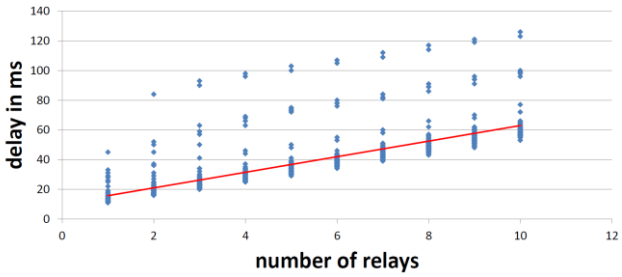

Fig. 7. Delay per hop using FBNM. Measured for 3000 test messages. Including linear regression showing average delay.

As seen in Fig. 7, about 99% of the measured delay was below the limit of 100 ms. However, we did observe a small number of relays with highly increased delays. The cause for this is the exponential back-off of the used IEEE802.11. Since the system is meant to be used in varying environments, which might including unknown parallel usage of the wireless spectrum, such interferences must be expected. We have observed that a 10-hop Ad-Hoc network using FBNM can fulfil the requirements extracted from considered applications.

Compared to other monitoring systems [7] the proposed system has the disadvantage that we actively send messages to test the quality of connections. Other systems can passively monitor existing network traffic. This was required for the proposed system, since we need to detect disconnections within 1 s, but cannot guarantee the presence of communication for every second. Therefore we examined the impact of FBNM on primary wireless communication on the same channel. We compared the throughput of the primary communication in three scenarios. In the first FBNM is not running, creating our reference throughput. In the second scenario FBNM was used with 2 nodes sending test messages once per second. These parameters were selected to create a

scenario with equivalent density of nodes compared to the considered applications. In the last scenario 5 nodes use FBNM with 10 test messages per second. This scenario is meant to be a stress test and result in a high number of interferences/collisions in the wireless medium. All three scenarios were tested for about 10 hours at comparable times of day. The throughput of the network was measured between two of its nodes. One of the nodes will continuously generate TCP frames with 1500 bytes of payload for the other node. We obtain the network throughput by counting the number of frames we can successfully transmit within a second. The three test scenarios are illustrated in figure 8. In this figure the test message source is shown in black. The test network traffic is illustrated by a black arrow, while the traffic, caused by FBNM is marked by red arrows. Thicker connections symbolize more traffic, i.e. higher number of transferred packets.

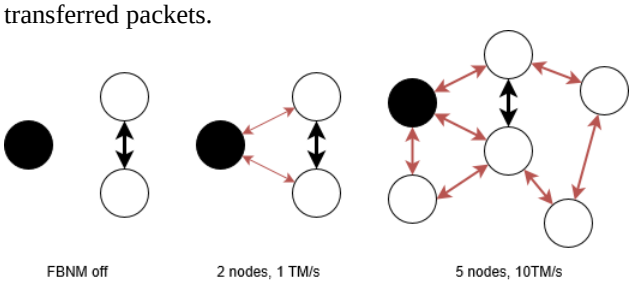

Fig. 8. Three experimental scenarios for observation of the impact of FBNM on parallel communication. Static node (source of test messages) shown in black, mobile nodes in white. FBNM communication represented by red connections with the thickness signaling the larger number of packets on the wireless medium. In black the primary communication used for throughput measurements.

As shown in Fig. 9 and 10 the three scenarios had the expected impact on the throughput of the primary communication. In the reference scenario an average throughput of 34.9 Mbit/s was measured. In the second scenario the throughput was slightly decreased by about 0.53 %. The last scenario yielded a more pronounced reduction in throughput of about 8.3 %. Additionally we have observed that the introduction of a high channel saturation increased the delay measured by FBNM by up to 100 %.

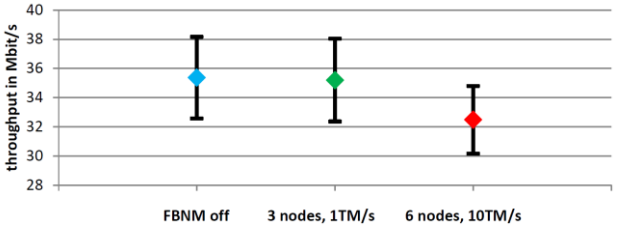

Fig. 9. Reduction in throughput in primary communication showing average and variance (TM/s: test messages per second)

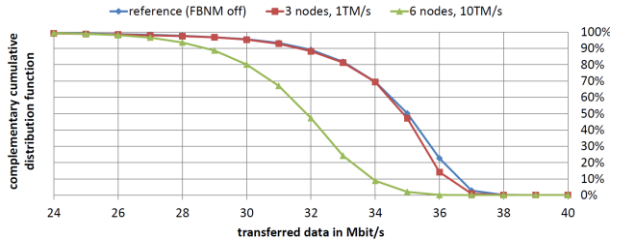

Fig. 10. FBNM impact on primary communication. Complementary cumulative distribution function for throughput. Diagram shows three scenarios: network monitoring system turned off, 3 nodes using 1 test message per second (TM/s) and 6 nodes using 10 test messages per second.

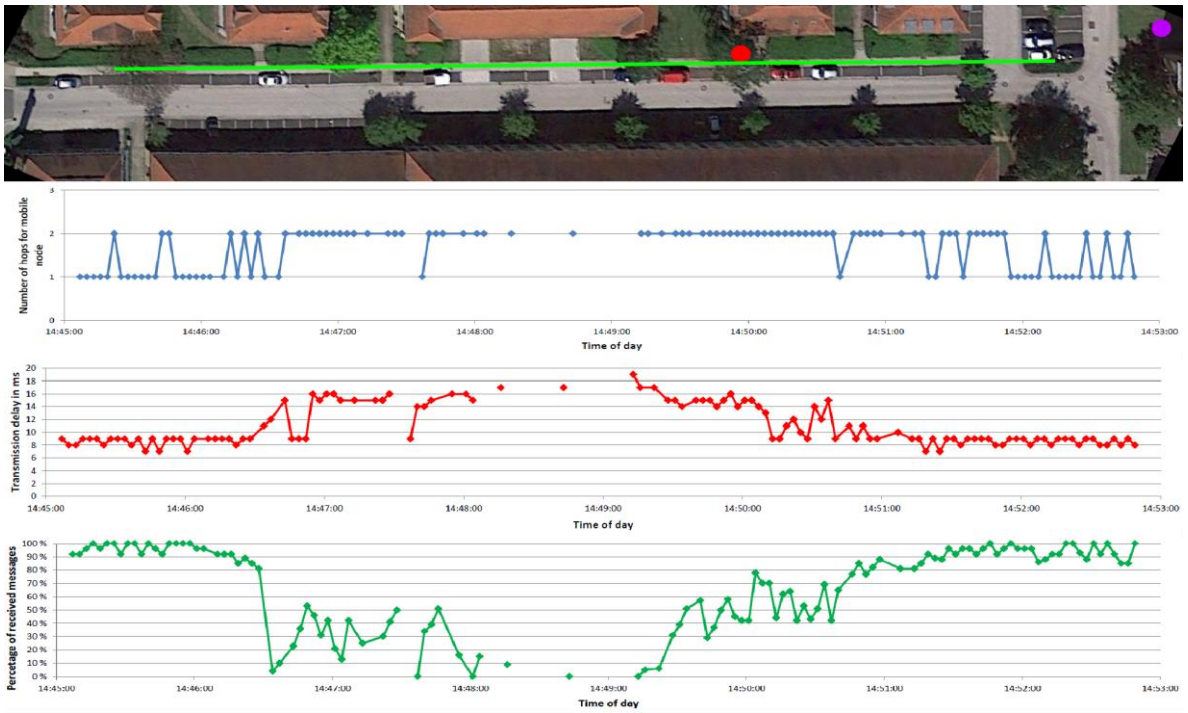

Fig. 11. Aerial view of a simple test scenario and measured number of hops, one-way latency and packet delivery rate. The receiver was moved along the green line from the test message source (purple) past the relaying node (red) to an end-point out of range of both and back to the test message source.

Based on these observations two possible improvements to the performance of FBNM in regards to experienced delay and reduced impact on primary communication are suggested. First, FBNM should be modified to use existing communication for monitoring, if such is present. Test messages would only be sent, if no communication is present on a channel. Second, the media access control of the used communications interface should be altered to improve the performance, by specializing it for considered applications.

VI. Conclusion

In this work we presented a set of applications requiring the measurement and observation of connection parameters. We surveyed a number of network protocols developed for measurement of connection parameters in different applications. After comparing the properties of these protocols, a flooding-based network monitoring, inspired by routing strategies known from delay tolerant networks, was proposed. We implemented the flooding-based network monitoring and measured its functionality and impact on parallel data exchange on the same wireless channel.

The performed measurements show that FBNM meats the required goals regarding measurable delay and impact on primary communication. We plan to verify this results for networks with larger number of nodes. Additionally we show, that FBNMs impact on the throughput of parallel communication on the same wireless channel is minimal for considered use cases. Since the content of the periodic messages has no influence on the congestion in a wireless medium, here presented results are transferable to other systems that utilize periodic messages. Since our experiments showed that a congested medium can increase the delay experienced by the FBNM, an additional focus will be set on the parallel usage of non-interfering mediums to alleviate congestion.

Further work will include optimizations and testing of the proposed system under various conditions and in more varied environments. Especially the system behavior in dense networks and obstructed indoor environments is of interest for industrial automation applications.

References

[1] C. Aurrecoechea, A. T. Campbell, and L. Hauw, "A survey of qos architectures," *Multimedia Systems*, vol. 6, no. 3, pp. 138–151, 1998.

[2] T. R. M. Rahman and N. B. Patil, "Evaluation of mobile network planning strategy with routing protocol support," *International Journal*, vol. 9, no. 1, 2018

[3] P. Mohapatra, J. Li, and C. Gui, "Qos in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 10, no. 3, pp. 44–53, 2003.

[4] G. Gebreslassie, L. M. I. Sheela, and S. R. Grace, "Analyzing and optimizing of quality of service management in flying ad hoc networks," *International Science and Technology Journal*, 2018.

[5] H. Xiao, W. K. G. Seah, A. Lo, and K. C. Chua, "A flexible quality of service model for mobile ad-hoc networks," in *Proc. Vehicular Technology Conference Proceedings*, 2000, pp. 445–449.

[6] R. G. Cole and J. H. Rosenbluth, "Voice over ip performance monitoring," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, pp. 9–24, 2001.

[7] Y. Tsang, M. Coates, and R. D. Nowak, "Network delay tomography," *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2125–2136, 2003.

[8] D. Gavalas, D. Greenwood, M. Ghanbari, and M. O'Mahony, "Advanced network monitoring applications based on mobile/intelligent agent technology," *Computer Communications*, vol. 23, no. 8, pp. 720–730, 2000.

[9] W. L. Lee, A. Datta, and R. Cardell-Oliver, "Network management in wireless sensor networksm," in *Handbook of Mobile Ad Hoc and Pervasive Communications*, 2006, pp. 1–20.

[10] M. Turon, "Mote-view: A sensor network monitoring and management tool," in *Proc. Second IEEE Workshop on Embedded Networked Sensors*, 2005, pp. 11–17.

[11] D. A. Manolecu and E. Meijer, *Mobile Sensor Network*, July 2013.

[12] A. Howard, M. J. Matari ć, and G. S. Sukhatme, "Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem," in *Distributed Autonomous Robotic Systems*. Springer, 2002, pp. 299–308.

[13] Y. Wang and H. Wu, "Delay/fault-tolerant mobile sensor network (dft-msn): A new paradigm for pervasive information gathering," *IEEE Transactions on Mobile Computing*, vol. 6, no. 9, 2007.

[14] S. Ali, J. Qadir, and A. Baig, "Routing protocols in delay tolerant networks-a survey," in *Proc. 6th International Conference on Emerging Technologies*, 2010, pp. 70–75.

[15] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, "Prioritized epidemic routing for opportunistic networks," in *Proc. 1st International MobiSys Workshop on Mobile Opportunistic Networking*, ACM, 2007, pp. 62–66.

[16] D. B. Johnson, D. A. Maltz, J. Broch, *et al.*, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad Hoc Networking*, vol. 5, pp. 139–172, 2001.

[17] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek, "The click modular router," *ACM Transactions on Computer Systems*, vol. 18, no. 3, pp. 263–297, 2000.

Christian Sauer researches industrial applications for mobile robots. He specializes in the wireless communication networks of these robots

Maja Sliskovic researches localization and wireless communication of mobile systems at SEW-Eurodrive.

Marco Schmidt leads a team of researchers at the Bochum University of applied Sciences. He and his team focuses on robotics and space technology