Original scientific paper

Resilient Multipath Routing Protocol to Enable Hazardous event Monitoring with Wireless Sensor Network

Bálint Á. Üveges, *Student Member, IEEE,* Máté Lőrincz, and András Oláh, *Member, IEEE*

***Abstract* — With the growing impact of climate change, the occurrence of hazardous spatial events increases. Wireless sensor networks are suitable to sense, monitor, and report such events in remote or inaccessible locations. Hazardous events are rare compared to the network's lifetime, thus maintaining its consistency must be realized energy efficiently. During the impact, the network must monitor the event with precision, and report the incidence, while mitigating the loss of perishing nodes.**

To fulfill these requirements, we propose the Self-healing Multipath Routing Protocol that is based on the Heterogeneous Disjoint Multipath Routing Protocol and introduces application-specific extensions to improve network stability, resiliency, and failover. To realize the monitoring of spatially extended hazardous events we introduce an event-based, application-level protocol.

To evaluate the routing protocol, we perform simulations utilizing a cellular automaton-based wildfire model as the spatial event and provide measurement results including delivery ratio, consumed energy, and protocol-specific metrics.

***Keywords* — Failover, Hazardous environment, Multipath, Resiliency, Self-healing, Wireless sensor networks.**

I. Introduction

THE demand to sense, monitor and report life-threatening hazardous spatial events increases: natural phenomena related to climate change, such as wildfires or floods are more intense every year, while catastrophes caused by human failure, including oil spills or chemical leaks in natural or artificial environments continue to happen regularly.

Wireless Sensor Networks (WSN) consist of battery-powered computing, sensing, and communicating devices, that are capable of monitoring both indoor and outdoor areas and detecting different natural and artificial events. By utilizing wireless communication, WSN devices, also known as nodes, can convey this information via their neighbors to a distinguished node called a sink, from where the information is transferred to the user. Depending on the equipped sensors and the density of the nodes, a WSN can sense temperature, humidity, gases, luminosity, pressure, and other physical phenomena. Via wireless communication, sensed information can be propagated without perceptible delay, which enables the user to react to events effectively. Due to their relatively low price per node, WSNs are suitable to monitor events that can damage or destroy affected sensing devices.

Hazardous event monitoring poses diverse and contradictory requirements against WSNs:

1) Event frequency: Although these events have fatal effects on living organizations and the environment, their occurrence is rare compared to the network's lifetime. As a result, a WSN must minimize energy consumption related to network maintenance during eventless periods.

2) Autonomous operation: As a natural consequence of the monitored event's rarity and spatial occurrence, the network must operate autonomously without or with minimal supervision. To minimize the need for human intervention, it is expected that the network bears self-organizing capabilities.

3) Event extent and direction: The extent of the monitored phenomena can change over time, in many cases towards a specific direction. An oil spill spreads along the current or wave activity, while a wildfire's direction is influenced by wind, terrain vegetation, and slope. A WSN shall be capable of not just detecting the event, but closely monitoring its evolution both spatially and temporally. The conveyed information can support the user forecast the event's future behavior, which assists disaster-relief activities.

4) Event severity and alerting: Depending on the monitored event's nature, it is expected that the occurrence is reported within a specific time limit to mitigate or suppress the hazard effectively. This poses a delay requirement on the network, that naturally contradicts energy consumption requirements.

5) Damages: The network must possess the capability to reorganize itself to convey information to the user, even if a significant number of nodes are terminated.

Paper received May 10, 2023; revised July 19, 2023; accepted July 28, 2023. Date of publication August 08, 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Nataša Nešković.

This paper is revised and expanded version of the paper presented at the 30th Telecommunications Forum 2023 [1].

This research was supported by the National Research, Development and Innovation Office of Hungary through the grant TKP2021-NVA-27.

Corresponding author Bálint Á. Üveges is with the Faculty of Information Technology and Bionics, Pázmány Péter Catholic University, Práter utca 50/A, 1083 Budapest, Hungary (phone: +36209369527; e-mail: uveges.balint.aron@itk.ppke.hu).

Máté Lőrincz is with the Faculty of Information Technology and Bionics, Pázmány Péter Catholic University, Práter utca 50/A, 1083 Budapest, Hungary (e-mail: lorincz.mate@itk.ppke.hu).

András Oláh is with the Faculty of Information Technology and Bionics, Pázmány Péter Catholic University, Práter utca 50/A, 1083 Budapest, Hungary (e-mail: olah.andras@itk.ppke.hu).

A. Wildfire monitoring

Wildfires are a specific subclass of hazardous events. According to the advance report published by the European Commission's Joint Research Centre on Forest Fires in Europe, Middle East, and North Africa in 2021, 1.1 million hectares of area burnt down due to wildfires [2]. WSNs provide a feasible solution for wildfire monitoring when near real-time sensing is required.

The field of WSN-based wildfire monitoring is a thoroughly researched area. Doolin and Sitar performed field testing with sensor nodes during prescribed burning and analyzed sensing and structural degradation aspects [3]. Lutakamale and Kaijage performed a case study in Tanzania with their proposed WSN network, where ZigBee was the communication protocol of choice [4]. Antoine-Santoni et al. provided a performance analysis of an XMesh-based WSN during wildfire, where the nodes were equipped with fire-resisting insulation [5]. Somov provided an overview of WSN-compatible sensors and sensing techniques [6], while AL-Dhief et al. further enhanced the Location-Aided Routing Protocol to adapt to wildfire monitoring scenarios [7]. While most proposed systems consider node failures, extensive node malfunction and its effect on monitoring capabilities were not investigated. Also, energy-efficient, but reliable operation during eventless periods is not reflected in protocol designs.

B. Multipath routing

Nodes in a WSN network that cover a spatially extended area, do not have a direct connection to the sink. To convey information from a distant node, multi-hop communication is required, which defines a sequence of nodes, also known as a path, via packets can be transmitted to the sink [8]. Every path is vulnerable to node failures, that can render the given node disconnected.

A commonly used technique to enhance a multi-hop WSN's reliability is to establish multiple paths towards the sink, that is to increase the connection's redundancy available to a node [9]. Depending on the structure of the constructed paths available to a node, it is possible to further classify multipath networks:

1) Node-disjoint paths: Two paths are considered node-disjoint if they do not share a common node, not concerning the source and the destination. While such paths provide the highest grade of redundancy, in a sparse network it is challenging to establish node-disjoint paths to every node.

2) Link-disjoint paths: Paths are classified as link-disjoint if they share common nodes, but the sequences of nodes are not identical. In wireless networks, where link establishment is considered less expensive compared to wireline networks, such compromise in redundancy is only feasible if the network is sparse, or common nodes bear special properties.

3) Partially disjoint path: Paths share common node sequences and differ only in selected parts. Such paths provide a solution when redundancy is needed only in a spatially limited area of the network. Examples of all three path variants are depicted in Fig. 1.

Routing protocols with the aim to establish multipath WSNs are studied in detail in the literature. Ganesan et al. proposed the Braided Multipath Routing (BMR) Protocol [10],

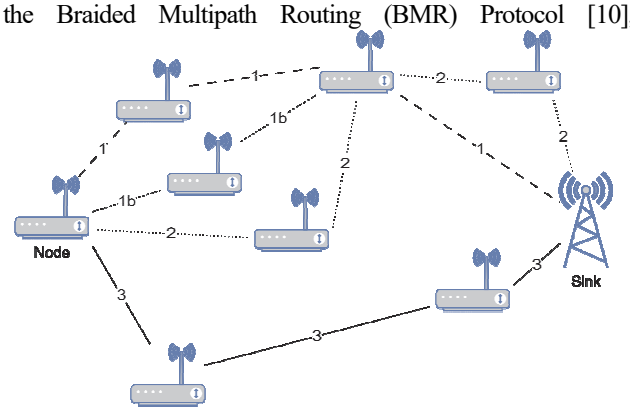

Fig. 1. Multipath scenarios between Node and Sink: node-disjoint (1, 3), link-disjoint (1,2), and partially disjoint (1, 1b) paths.

which establishes partially disjoint paths by "braiding" paths around an initial, primary path. Deb et al. developed Reliable Information Forwarding using Multiple Paths Protocol (ReInForM) [11], with the goal to achieve predefined reliability using multiple paths: the protocol constructs link-disjoint paths between a given node and the sink and performs packet repetition based on local metrics to achieve reliability.

Radi et al. introduced the Low-Interference Energy-Efficient Multipath Routing Protocol (LIEMRO) [12], a routing protocol establishing node-disjoint, energy, and interference-aware paths. Optimized for network lifetime and throughput, the protocol performs load balancing on available paths when sending data packets.

Maimour investigated interference-aware multipath routing by extending existing routing protocols, such as Maximally Radio-Disjoint Multipath Routing (M2R2) with interference-aware metric and interference-zone marking to minimize interference between node-disjoint paths [13]. Fu et al. developed the Environment-Fusion Multipath Routing Protocol (EFMRP) [14] to perform routing on node-disjoint paths utilizing a multi-dimensional potential field. The dimensions, such as node-sink distance, residual energy, and environment enable the protocol to avoid potential danger zones, such as wildfires, that would decrease reliability.

Moussa et al. analyzed the performance of Multilevel, Heterogeneous Disjoint Multipath Routing Protocol (HDMRP) and Enhanced Ant-based QoS-aware routing protocol for Heterogeneous Wireless Sensor Networks (EAQHSeN) involving wildfire events and node failures [15], although their scenarios did not consider node damages and wildfire propagation.

The contribution of this paper is the HDMRP-based routing protocol called Self-Healing Multipath Routing Protocol (ShMRP), which utilizes various failure prevention and mitigation techniques to maintain connectivity during node failures caused by hazardous events, such as wildfires. Both ShMRP and a proposed application-level wildfire monitoring protocol are described in Section II, while the simulation environment and results concerning packet delivery, energy

consumption, and communication redundancy are detailed in Section III. Section IV concludes the paper by addressing protocol limitations and future directions.

II. Protocol Description

A. Application Protocol

Wildfire sensing and reporting are realized by an application-level protocol. The protocol distinguishes two states: *steady* and *emergency*. Every node starts its lifecycle in steady state, where periodic sensor readings are performed. Report messages are sent towards the sink with low frequency, i.e., every 24 hours to signal environmental and network conditions. If the sensor readings indicate wildfire, the node enters emergency state and starts sending periodic event messages towards the sink with high frequency, i.e., every 3 minutes, indicating wildfire. Parallel to that the node in emergency state also broadcasts an emergency message to neighboring nodes, periodically. A node receiving an emergency broadcast message also enters emergency state, however it does not re-broadcast the message itself. It is assumed that nodes in emergency state are destroyed, and the network is partially redeployed during damage control. Due to this assumption, a transition from emergency to steady state is not defined. The state transition from steady to emergency state is depicted in Fig. 2 in Sequential Function Chart format (SFC) [16].

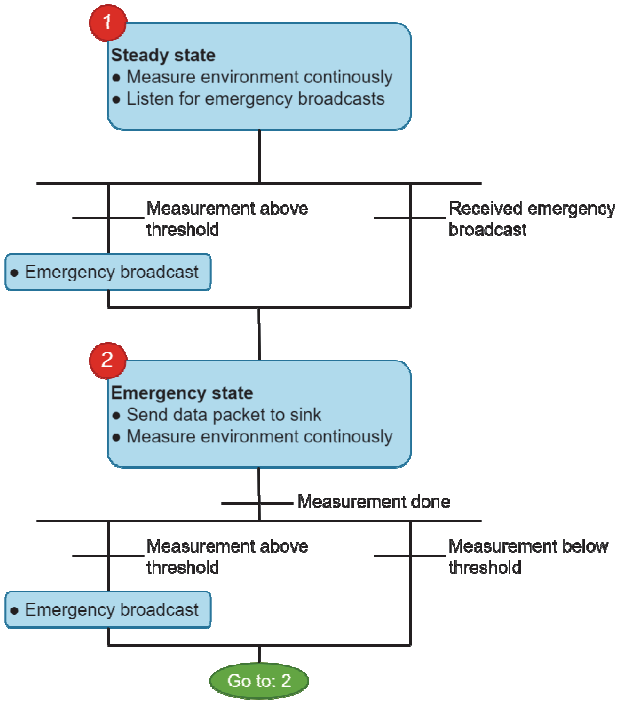

Fig. 2. The switch from steady to emergency state in SFC.

B. Heterogeneous Disjoint Multipath Routing Protocol

HDMRP, proposed by Hadjidj et al. is designed to exploit nodes with unlimited energy during the construction of a multipath network [17]. The protocol constructs node-disjoint paths, that can intersect at distinguished nodes, if present in the network.

In an HDMRP network, nodes are either battery-powered sensor nodes or master nodes, with unlimited power supply. Depending on the communication-wise distance from the sink, a node's *role* is *root*, if it is the sink's neighbor, *sub-root*, if it is a root's neighbor or *non-root*, if it is any other node.

HDMRP employs a sink-initiated, round-based path construction mechanism by broadcasting a route request message (*RREQ*) to its neighbors:

$$RREQ = \left(R, S, P_{id}, len, N_{mas}\right), \tag{1}$$

where R is the round number, S is the sending node's identifier, P_{id} is the path identifier, *len* is the number of nodes along the path and N_{mas} is the number of master nodes along the path.

The *RREQ* message is first received by root nodes, which update the relevant fields and repeat the broadcast. Once a sub-root receives the *RREQ* message, it assigns its identifier as the P_{id} and repeats the broadcast. If the *RREQ* is received by a non-root or non-sub-root node, the node enters learning state. The learning state ends if a pre-defined learning timer, called t_l expires. During the learning state, the node processes every received *RREQ* message and stores or updates the indicated path, if it is not yet received or the cost function yields a lower value for the new *RREQ*, respectively. The cost function is defined as:

$$f_{cost}\left(RREQ\right) = \frac{RREQ.len}{RREQ.nmas}. \tag{2}$$

Once the t_l timer expires, the node enters the relaying state and its behavior depends on the possessed capabilities: A master node broadcasts every learned path via *RREQ*, while a sensor node broadcasts only one, that is selected randomly. A possible realization of an HDMRP-based network is depicted in Fig. 3a.

Energy-node-disjoint paths maintain the disjoint property until they reach a sub-root node, while the number of available paths is limited by the number of sub-roots.

C. Self-healing Multipath Routing Protocol

While HDMRP provides a solid foundation to establish multiple energy-node-disjoint paths towards the sink from every node of the network, it does not specify any dynamic behavior, e.g., how to detect failing paths or how to adapt to node failures. In the following sections, several enhancements and extensions are proposed, that together with HDMRP bear the name ShMRP.

1) RSSI-based Route Request filtering: To increase path reliability, nodes in the learning state reject *RREQ* messages that do not exceed a certain RSSI value. While RSSI is not considered a definitive indicator of link quality, *RREQ* messages exceeding a certain RSSI value do result in more stable links.

2) Automatic Repeat Request with Hop-by-Hop Transfer: To ensure packet delivery, the Automatic Repeat Request (ARQ) protocol is introduced [18]. To minimize the communication overhead, the network layer realizes a connectionless, but reliable packet transfer. ARQ is realized between every node participating in the path, i.e., the transfer of a data packet is always confirmed between

two nodes if ARQ was requested in the original message. Such a mechanism requires buffering in every node, which increases overall memory usage and introduces additional delay.

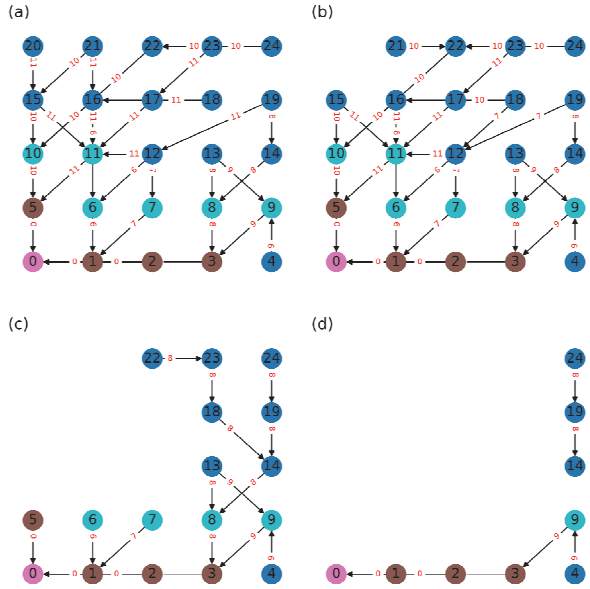

Fig. 3. Multipath network created and maintained by ShMRP – Initial setup (a), Single node failure after 10 minutes (b), Multiple node failures after 137 minutes (c), Disintegration after 207 minutes (d) due to wildfire. Sink, root, and sub-root nodes are colored pink, brown, and cyan respectively.

3) Path reselection: If ARQ-based packet transfer fails between two nodes and there are other paths available to the sender, it randomly selects a new path and retries.

4) Message categories: Event messages are sent with a higher frequency compared to report messages. While every report message is delivered with ARQ, in case of events only every n^{th} message is secured with ARQ. Increased quality of service for report messages is needed, since their rate is relatively low during eventless periods, while they convey information about the network's status.

5) Path failure and reconstruction: It is expected that during wildfire several nodes fail. Such a scenario can also cause path failure and render certain nodes disconnected from the sink. To mitigate such a scenario a failure message is delivered to the sink that triggers a new round of *RREQ* to re-establish the connection to unreachable nodes.

During path construction nodes have the possibility to discover their neighbors by capturing *RREQ* messages independent of their own state. If a node detects path failure via the ARQ protocol, it randomly selects a neighbor that is not a member of the failing path and sends a *PATH_FAILURE* message. If the node did not discover any corresponding neighbor, the failure message is sent to a random neighbor. A node, receiving a failure message forwards that towards the sink using the existing paths ensuring the delivery with ARQ. Once the sink receives a failure message, it broadcasts a new *RREQ* message indicating a new round to heal the network. The behavior of reconstruction is demonstrated in Fig. 3.

III. Results

A. Simulation environment and setup

To implement and simulate the application protocol, HDMRP, and ShMRP, we chose the OMNeT++/Castalia framework. To provide a comparison we also implemented a restricted flooding algorithm, described in [8]. To efficiently simulate wildfire propagation, a cellular automaton-based wildfire model was implemented, published by Freire and DaCamra [19]. The source code of the protocols, the wildfire model coupled with the framework is published online [20]. TMAC was chosen as MAC protocol with Immediate Retry on Collision, CC2420 as Radio Transceiver with 0 dBm TX power, while the collision model was set to additive interference. The path loss exponent was set to 2.2, while sensor nodes had 18720 Joules (J) of initial energy.

B. RSSI-based Route Request filtering

Related simulation scenarios lasted 20 minutes, with 64 nodes on a square area of 2.56 hectares, deployed in an 8x8 grid topology. Every node generated 3 messages per minute, while the packet delivery ratio (PDR) was measured at the sink, which was in the north-east corner. Results summarized in Table 1 show that although a high RSSI value yields high PDR, it also increases power consumption and reduces the number of available paths per node. While lower RSSI values have a positive effect on available paths, power consumption increases as established paths become less reliable.

Table 1: RSSI-based *RREQ* filtering

RSSI (dBm)	PDR	Consumption per node (J)	Average path per node
-86	100%	18.8	1.01
-87	99%	16.3	1.25
-88	99%	17.0	1.40
-89	99%	16.4	1.91
-90	99%	16.6	1.86

C. Network scaling analysis

ShMRP's scaling capabilities were evaluated with quadratic node numbers, ranging from 4x4 to 10x10. The nodes were deployed in a square grid, with 22 meters as the square's side length. The simulation lasted 4 hours, with report messages sent by every node every 2^{nd} minute, and the sink was in the north-east corner.

As expected in the case of a multi-hop network, with the increase of network size the PDR decreases due to increasing hop count and inter-node routing. Simulation results for 16 nodes show 100% PDR, while for 100 nodes a slight decrease can be observed to 97.4%, as shown in Fig. 4a.

In the case of average path per node, an interesting phenomenon could be observed: while the overall tendency is decreasing, in the case of a 36-node network the path per node reaches a local maximum, which can be also seen in Fig. 4b. This can be attributed to the network size and the sub-root to non-sub-root ratio: In case of a 25-node network the ratio is 0.53, while in case of a 36-node network it is 0.56. A network of 36 nodes is large enough to host a significant number of sub-roots, which ultimately define the maximum number of paths, but small enough

not to let the network form segments, where only a limited number of paths are available. Radio communication also intensifies with higher node numbers. As a result, the average consumed energy per node increases from 138 J to 151 J, as depicted in Fig. 4c.

To measure the effect of non-uniform node placement, randomized node deployments were evaluated on a 100-node network. Every node's x and y positions were altered compared to the grid spacing with a uniform distribution and compensated with the given randomization quotient. As shown in Fig. 4d, a more random node placement had a positive effect on the average number of paths available to a node. The result suggests that with a less rigid deployment, ShMRP can disseminate path information more effectively, resulting in more redundant connections.

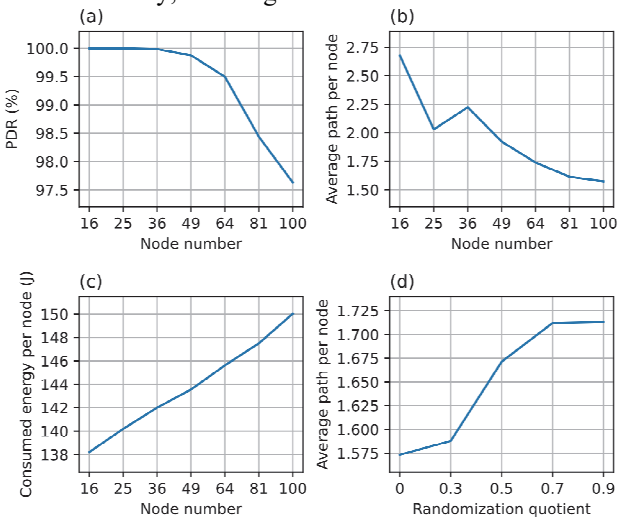

Fig. 4. Effect of network size on PDR (a), path per node (b), consumed energy per node (c) and effect of placement on path per node (d).

D. *Steady state analysis*

A comparative analysis of ShMRP was performed in a steady state, i.e., without wildfire present. To investigate the dynamic behavior of the *RREQ* mechanism, a static routing was introduced, where five paths were pre-generated, with nodes connecting only to a single path. Restricted flooding, static rooting, HDMRP, and ShMRP were compared on a 100-node network, deployed on a 4.84 ha square area, in a 10x10 grid topology. The simulation lasted 4 hours, during which report messages were generated every 3rd minute. Results, where 10% of nodes were master, are shown in Table 2. HDMRP significantly exceeded static routing PDR-wise, which clearly shows that the broadcast-based *RREQ* mechanism can construct reliable paths. As expected, Flooding's energy consumption was the highest, while static routing came second, due to pre-defined, but unreliable routes. While ShMRP is tailored to cope with significant node failures, it was able to improve PDR compared to HDMRP. The slight increase in energy consumption is attributed to failure messages and reorganization, while the decrease in average paths per node is linked to interference caused by the constant traffic even during construction.

By projecting consumption results to a single message and assuming daily one message with 1.4 mWh idle consumption in between, the estimated network lifetime for Flooding is 435 days. In the case of static routing, HDMRP, and ShMRP the value increases with 25 days, 65 days, and 59 days, respectively.

TABLE 2: STEADY STATE, 10% MASTER NODE

Protocol	PDR	Consumption per node (J)	Average path per node
Flooding	90.4%	172.0	N/A
Static routing	74.0%	162.8	1
HDMRP	97.4%	148.9	1.65
ShMRP	97.5%	151.5	1.51

An identical scenario with zero master nodes showed a 1% increase in energy consumption in the case of HDMRP, but only 0.06% in the case of ShMRP. Individual node consumption analysis revealed that HDMRP and ShMRP achieved a less fluctuating depletion of nodes compared to static routing. Placing the sink in different positions, such as map center or edge did not affect ShMRP's PDR-wise performance over HDMRP.

E. *Emergency state analysis*

To evaluate ShMRP's performance during hazardous events, different scenarios were executed, placing the sink in different positions on the map and initiating wildfires in varying locations. Fire propagation parameters were tuned to destroy approximately 20% of the nodes. Node number and topology were identical to Section III.D. PDR was measured for event messages generated every 2nd minute, while every 10th message was delivered with ARQ.

As shown in Table 3, ShMRP outperformed Flooding in the majority of the cases PDR-wise and in all cases consumption-wise. In the case of centered fire nests, Flooding was able to deliver higher PDR. This result is attributed to the sink-fire proximity: The fire destroys path-interim nodes near the sink, rendering certain nodes disconnected for a significant amount of time before the healing mechanism resolves the situation.

TABLE 3: EMERGENCY STATE

Sink and fire location	PDR		Consumption (J)	
	Flooding	ShMRP	Flooding	ShMRP
West edge, South-East	83.9%	88.9%	105.9	80.9
Center, North-East	77.7%	82.1%	251.6	184.9
North-West, North-East	81.8%	87.8%	251.2	191.2
Center, South-West	81.6%	88.0%	203.2	155.7
West edge, South-West	84.2%	87.2%	201.8	153.5
West edge, Center	90.5%	83.6%	100.1	78.5
North-West, Center	88.0%	82.3%	100.1	78.7

To simulate a potentially real scenario, a 100-node network was deployed with an overlay on an existing map excerpt, covering a 4.84 ha square area. Nodes were placed randomized in a 10x10 grid, with the sink in the south-east corner, and 10% master node amount. Each master node was placed in the vicinity of the hiking route, assuming the presence of infrastructure, as depicted in Fig. 5. The fire nest was in the north-west corner and destroyed 19 nodes. In the case of ShMRP the event message PDR was 96.7%, with 262 J average energy consumed per node and 1.44 average path per node, while in the case of Flooding the PDR reached 94.9% with 417 J average consumption. The potential network topology realized by ShMRP is shown in Fig. 5.

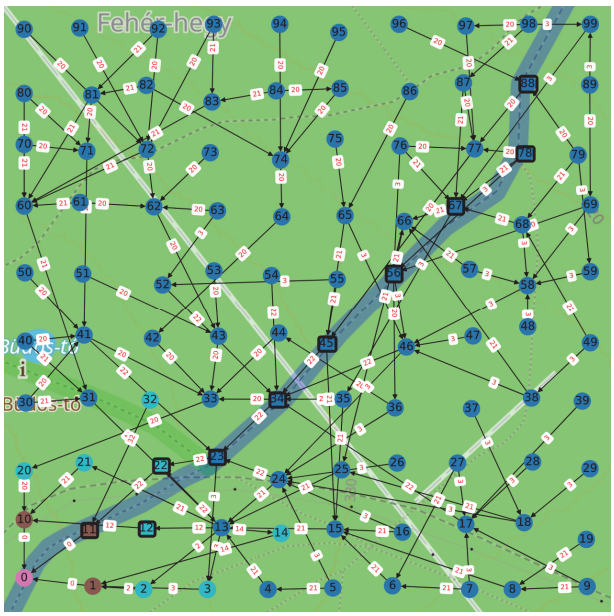

Fig. 5. Potential network deployment with ShMRP on map excerpt from Börzsöny mountain range, Hungary. Master nodes are denoted with rectangular shapes.

IV. Conclusion

In this paper, we introduced the HDMRP-based Self-healing Multipath Routing Protocol tailored to assist hazardous event monitoring with WSN an application-level protocol to monitor wildfire events. ShMRP's scaling capabilities were investigated, and the protocol was analyzed from PDR and energy consumption point of view in comparison with Restricted Flooding, static routing, and HDMRP. ShMRP's performance was also evaluated during wildfire activity and compared with Restricted Flooding. Potential network deployment outdoors with environmental constraints was presented and evaluated as well. Results show that ShMRP is able to maintain relatively high PDR without a perceptible increase in consumption during eventless periods, and also during hazardous events with the loss of a serious number of nodes.

Limitations can be observed in ShMRP's centralized and global reconstruction mechanism: while in Section III.D. it is shown that the mechanism improves PDR, it should be noted, that the activation in steady state is a sign of sensitivity to transient failure events, which results in unnecessary messaging, changes in network topology and energy consumption.

To address these issues and to improve topology management and link quality control our future research goal is to study localized and decentralized path failover utilizing link quality and hazard metrics, that could result in a more reliable network even during hazardous event monitoring. The sink could exploit actual event and node-specific packet rate information to schedule network reconstruction that neither disrupts the communication too frequently nor delays centralized intervention to a point, where important network metrics drop below a tolerable level from the application point of view.

References

[1] B. Á. Üveges, M. Lőrincz, and A. Oláh, "Self-healing Multipath Routing Protocol to assist Wireless Sensor Network based Hazardous Event Monitoring," in *2022 30th Telecommunications Forum (TELFOR)*, 2022, pp. 1–4. doi: 10.1109/TELFOR56187.2022.9983752.

[2] J. San-Miguel-Ayanz *et al.*, *Advance report on wildfires in Europe, Middle East and North Africa 2021*. European Commission, Joint Research Centre, 2022. doi: doi/10.2760/039729.

[3] D. M. Doolin and N. Sitar, "Wireless sensors for wildfire monitoring," in *Smart Structures and Materials 2005: Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems*, M. Tomizuka, Ed., SPIE, 2005, pp. 477–484. doi: 10.1117/12.605655.

[4] A. S. Lutakamale and S. Kaijage, "Wildfire Monitoring and Detection System Using Wireless Sensor Network: A Case Study of Tanzania," *Wireless Sensor Network*, vol. 09, no. 08, pp. 274–289, 2017, doi: 10.4236/wsn.2017.98015.

[5] A. Teo, G. Singh, and J. C. McEachen, "Evaluation of the XMesh Routing Protocol in Wireless Sensor Networks," in *2006 49th IEEE International Midwest Symposium on Circuits and Systems*, Aug. 2006, pp. 113–117. doi: 10.1109/MWSCAS.2006.382221.

[6] A. Somov, "Wildfire safety with wireless sensor networks," *ICST Transactions on Ambient Systems*, vol. 11, no. 10–12, p. e4, Dec. 2011, doi: 10.4108/trans.amsys.2011.e4.

[7] F. T. AL-Dhief *et al.*, "Forest Fire Detection Using New Routing Protocol," *Sensors*, vol. 22, no. 20, 2022, doi: 10.3390/s22207745.

[8] A. Förster, "Introduction to Wireless Sensor Networks," A. Förster, Ed., John Wiley & Sons, Ltd, 2016, pp. 77–97. doi: https://doi.org/10.1002/9781119345343.ch5.

[9] S. Chaudhari, "A survey on multipath routing techniques in wireless sensor networks," *International Journal of Networking and Virtual Organisations*, vol. 24, no. 3, pp. 267–328, 2021, doi: 10.1504/IJNVO.2021.115818.

[10] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, Oct. 2001, doi: 10.1145/509506.509514.

[11] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," in *28th Annual IEEE International Conference on Local Computer Networks, 2003. LCN '03. Proceedings.*, 2003, pp. 406–415. doi: 10.1109/LCN.2003.1243166.

[12] M. Radi, B. Dezfouli, S. A. Razak, and K. A. Bakar, "LIEMRO: A Low-Interference Energy-Efficient Multipath Routing Protocol for Improving QoS in Event-Based Wireless Sensor Networks," in *2010 Fourth International Conference on Sensor Technologies and Applications*, IEEE, Jul. 2010. doi: 10.1109/sensorcomm.2010.89.

[13] M. Maimour, "Interference-aware multipath routing for WSNs: overview and performance evaluation," *Applied Computing and Informatics*, vol. 16, no. 1/2, pp. 59–80, Jan. 2018, doi: 10.1016/j.aci.2018.03.002.

[14] X. Fu, G. Fortino, P. Pace, G. Aloi, and W. Li, "Environment-fusion multipath routing protocol for wireless sensor networks," *Information Fusion*, vol. 53, pp. 4–19, 2020, doi: https://doi.org/10.1016/j.inffus.2019.06.001.

[15] N. Moussa, A. E. B. E. Alaoui, and C. Chaudet, "A novel approach of WSN routing protocols comparison for forest fire detection," *Wireless Networks*, vol. 26, no. 3, pp. 1857–1867, Nov. 2018, doi: 10.1007/s11276-018-1872-3.

[16] I. E. Commission and others, "International Standard IEC 61131-3: 2013: Programmable Controllers." Part.

[17] A. Hadjidj, A. Bouabdallah, and Y. Challal, "HDMRP: An Efficient Fault-Tolerant Multipath Routing Protocol for Heterogeneous Wireless Sensor Networks," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Springer Berlin Heidelberg, 2012, pp. 469–482. doi: 10.1007/978-3-642-29222-4_33.

[18] G. Fairhurst and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)," RFC Editor, Aug. 2002. doi: 10.17487/rfc3366.

[19] J. G. Freire and C. C. DaCamara, "Using cellular automata to simulate wildfire propagation and to assist in fire management," *Natural Hazards and Earth System Sciences*, vol. 19, no. 1, pp. 169–179, 2019, doi: 10.5194/nhess-19-169-2019.

[20] B. Á. Üveges, "Wireless sensor network based wildfire monitoring with application-specific multi-path routing." Zenodo, 2023. doi: 10.5281/ZENODO.7885417.