

2017-11

# Performance analysis of WMN routing protocols for disaster networks

Tchinda, AP

<http://hdl.handle.net/10026.1/13395>

---

10.1109/scvt.2017.8240309

2017 IEEE Symposium on Communications and Vehicular Technology (SCVT)

IEEE

---

*All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.*

# *Performance Analysis of WMN Routing Protocols for Disaster Networks*

A. Paguem Tchinda, G. Frick, U. Trick and A. Lehmann

Research Group for Telecommunication Networks  
Frankfurt University of Applied Sciences  
Frankfurt/Main, Germany  
Email: {paguem, frick, lehmann, trick}@e-technik.org

A. Paguem Tchinda and B. Ghita

Centre for Security Communications and Network Research  
University of Plymouth  
Plymouth, United Kingdom  
Email: {auberlin.paguemtchinda, bogdan.ghita}@plymouth.ac.uk

**Abstract**—This paper evaluates the performance of the routing protocols HWMP, Babel and B.A.T.M.A.N. advanced for disaster networks. The evaluation is performed using a virtual environment so that the obtained results are similar to the expectations of a real world testbed. According to the specific requirements in disaster situations, three different scenario categories are implemented. The focus of the scenarios defined in the first category is to evaluate the behavior of the protocols inside a static network. The focus in the second category is to test their performance after dynamic processes. The focus in the last category is to predict the behavior of the routing protocols inside a large network expected after a disaster. The obtained results can be interpreted as follows: in the first category, the results obtained by HWMP and B.A.T.M.A.N. advanced are similar. Both protocols take the variations in the link throughput into consideration for their routing operations. In the second category, the protocol HWMP shows the most promising results concerning dynamic processes inside the network. The results obtained in the last category show that none of the examined protocols is appropriate for large networks, with the exception of Babel, which can be modified to support a large number of clients and routers. Because none of the examined routing protocols can fulfil the requirements in disaster situation, a new network architecture is proposed, which combines the advantages of two routing protocols to address the existing routing challenges.

**Keywords**—WMN; routing protocols; disaster networks

## I. INTRODUCTION

Wireless mesh Network (WMN) has been presented in [1], [2] and [3] as suitable architecture for communication recovery after a natural disaster. Due to the self-organisation and configuration character of such a network, it can be built few hours after the disaster in order to produce a quick response and coordinate rescue operations. The WMN routers necessary to build the disaster network are brought and dispersed in the disaster area by helpers of a protection organisation. In a previous publication [4] the requirements of WMN routing protocol in such scenarios have been defined. Based on these requirements, a classification was provided from which the protocols HWMP, Babel, and B.A.T.M.A.N. advanced are the most promising. This paper follows on the work by providing a comparison between the three protocols. The aims of the

implemented scenarios are to evaluate the behavior of the routing protocols in static networks, to test their ability to produce a quick response after dynamic changes, and to test and to predict their performance inside large networks. The paper is structured as follows: section 2 introduces to the routing mechanisms, packet types and metrics in HWMP, Babel and B.A.T.M.A.N. advanced. In section 3, the behavior of the protocols by common operations is tested. This is done based on two tests, first one to evaluate whether differences in the link quality can affect the routing decision and the second one to find out if existing traffic can affect the routing decision. The performance of the routing protocols by dynamic processes is analysed in section 4. The tests look at the delay for three milestones: establishing an alternative path for a running flow that is interrupted due to a router loss, making a new coming node reachable by other mesh participants, and making a new coming node a complete part of the mesh, which routes existing flows. In section 5, the influence of the network size on the protocol performance is analysed. Section 6 presents an optimised network architecture and explains its benefits with the focus on the energy consumption as key requirement for communication network with battery supplied devices. This paper presents the first evaluation of the three routing protocols using the general Linux implementation and the described scenarios focused on disaster. The proposed architecture can be used to solve many issues in WMN.

## II. ROUTING PROTOCOLS

Routing protocols are an important research domain in WMN. Due to the self-organisation and configuration character of a WMN, finding a path between two mesh participants has proved to be particularly difficult. Depending on the time, when the path is determined, these protocols can be shared into three groups: proactive, reactive and hybrid. Another classification differentiates between distance vector and link state protocols. By link state protocols each node periodically broadcasts update messages containing information about connection to its neighboring nodes (interface, link cost). These messages are forwarded to all mesh participants. Based on this information each node calculates the shortest path to a given destination, typically using Dijkstra's algorithm [11]. Due to the limited router

computational resources and the difficulties in updating topology information, link state protocols have shown their limits for large WMNs. For distance vector protocols, each router periodically sends update messages that contain its routing table (information about the costs to all known destinations and their costs). Each neighboring router receiving this message updates its routing table and selects the originator of the message as next hop to reach a given destination, when the announced cost is better than current one. A complete knowledge of the network topology as well as intensive path computation are not required. This mechanism is used by the protocols HWMP, Babel and B.A.T.M.A.N. advanced that are discussed more detailed in this section.

#### A. HWMP

The Hybrid Wireless Mesh Protocol (HWMP) was standardised in IEEE802.11s [6]. It is a layer 2 routing protocol. That means, it uses MAC instead of IP-addressing for packet delivery. It is also a hybrid protocol because it allows each mesh participant to use proactive, reactive or a combination of both mechanisms for path discovery. During the reactive process, which is tested in this paper, each node willing to communicate with another one inside the mesh network starts a path request (*PREQ*). This request is broadcasted by neighbouring routers up to the destination. The routers between the source and the destination router, which receive the *PREQ*, learn the shortest path to the initiator of the request. Then the reply from the destination can be send as unicast path reply (*PREP*) to the initiator of the communication. If a mesh participant is configured to work proactively, it periodically broadcasts a root announcement (*RANN*) or a path request (*PREQ*). Each router which receives this message, ignores it if the metric that it contains, is worse good than the current metric to reach the initiator, or selects the neighbouring router which has send this message as next node to reach the root one and broadcast the message, if the metric is better than the current metric or the sequence number is newer. To determine the best path quality between two routers, HWMP uses the airtime link metric. The airtime link metric is calculated as follows:

$$COST = \frac{1}{(1 - e_p)} \left( O + \frac{B_t}{R} \right) \quad (1)$$

It is given by the ETX metric (see following subsection equation (2)), which is corrected through the multiplication with another factor. The new factor takes the cost (delay) of the channel access  $O$  as well as the test frame size  $B_t$  and the data rate  $R$  used by the router to transmit the test frame into consideration.

#### B. Babel

Babel is a proactive layer 3 routing protocol that was defined in RFC6126 [7]. Babel messages are defined using the Type-Length-Value (TLV) model and are transported inside UDP packets. To reduce the protocol overhead multiple Babel messages can be combined and send inside one UDP packet. Each Babel router periodically broadcasts a Hello message.

This message is received only by routers, which are located in the range of the transmitter and will not be forwarded. Hello messages are used for the neighbour discovery and for the estimation of the link quality. The metric used in Babel is a variant of the expected transmission count (ETX) metric:

$$COST = \frac{1}{(1 - e_p)} \quad (2)$$

$e_p$  is the packet error probability. It is calculated by the router, which gets the Hello message on the base of information it contains. The calculated packet error probability is transmitted to the sender by using an I-Heard-You (*IHU*) message. Additional to the *Hello* and *IHU* messages each router periodically broadcasts *Update* messages. For each known subnetwork and its metric, one *Update* message is generated. Each neighbouring router, which receives this message updates its routing table if the update is feasible and accordingly broadcasts the message. If a router wants to communicate with a given prefix and the information in the routing table is not up-to-date enough, it can use a *Route* or a *Seqno Request* to request and update this information.

#### C. B.A.T.M.A.N. advanced

The Better Approach To Mobile Adhoc Networking advanced (B.A.T.M.A.N. advanced) is a layer 2 proactive routing protocol [8]. Each B.A.T.M.A.N. advanced node periodically broadcasts an originator message (*OGM*) with an incrementing sequence number. Each mesh participant which receives an *OGM* updates its path table. Then it broadcasts the message only if it was received from the neighbouring router which is currently selected as next hop to reach the original initiator of the *OGM*. To select the best next node to reach a given originator, each *OGM* contains a Transmission Quality metric field (TQ). Its value is updated by each router before they forward the *OGM*. The new value is calculated on the basis of the normalised link local transmission quality multiplied by a link asymmetry penalty.

$$COST = \frac{RQ}{EQ} \quad (3)$$

$RQ$  is the fraction of *OGMs* received during a given time frame (window size) from the neighbour router and  $EQ$  is the fraction of own *OGMs* rebroadcasted by the given neighbour router. The developers of B.A.T.M.A.N. advanced IV assume that *OGMs* propagate faster over a non-overloaded path or a path with less packets loss. B.A.T.M.A.N. advanced attaches an additional headers from up to 32 Byte on all frames working over the network in order to perform its forward operations.

In B.A.T.M.A.N. advanced V, the developers try to decouple maintenance operations like neighbour discovery or link metric calculation from the spread of information necessary for the routing process. *OGMs* are no longer used to determine the path quality. The metric used in B.A.T.M.A.N. advanced V is based on the measured throughput. *OGMs* are used to transmit routing information over the mesh. This information is contained inside a list of one or more fields attached to the *OGM* message. These fields are structured using the Type Version Length Value (TVLV) model.

### III. ROUTING PROTOCOLS PERFORMANCE IN STATIC NETWORK SCENARIOS

In this section, the WMN routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V are evaluated regarding two network scenarios. The first scenario consists of the path selection for a data transfer, when the maximal throughput of the existing paths is different. The second scenario consists of the path selection, when the best path is overloaded. For performing those scenarios, a virtual environment has been used. The environment is based on a Linux host using Docker for realizing the routers as a container, the kernel module mac80211\_hwsim for realising the router's IEEE 802.11 radios and wmediumd [5] for emulating different transmission powers between the wireless interfaces of the routers. The network topology used to perform the scenarios is shown in figure 1. It consists of 10 routers. The RSSI value is set to -90 and -81dBm so that the maximum bitrate is 5.5 and 24Mbps respectively. Table I summarizes the default configurations of the protocols, which are used during the realisation of the scenarios.

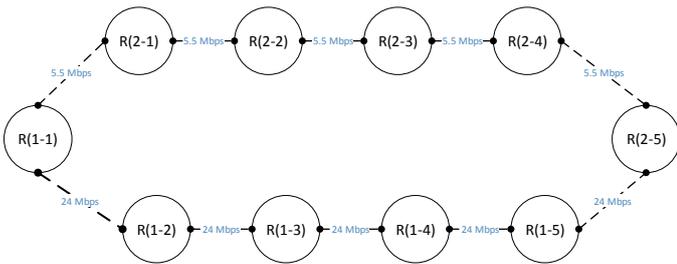


Fig. 1. Mesh-Topology with ten mesh routers

TABLE I. ROUTING PROTOCOLS CONFIGURATION

Routing Protocol	Configuration
HWMP	Configuration modus: reactive PREQ interval: 4s Beacon frame interval: 1s
Babel	Version: babeld-1.8.0-6-g16ae1f9 Hello interval: 4s IHU interval: 12s Update interval: 16s
B.A.T.M.A.N. Advanced IV	Version: batman-adv-2017.2 OGM interval: 4s
B.A.T.M.A.N. Advanced V	Version: batman-adv-2017.2 OGM interval: 4s

#### A. Influence of the link quality

When building a WMN in a disaster area, it can be assumed that the distance between mesh participants is not the same overall. The data transmission between two neighbouring routers is also influenced by different factors such as the used IEEE 802.11 standard or the disaster environment. Therefore, it is impossible to have the same link conditions between all routers in the WMN. Due to these differences, significant changes are expected in the maximum data rate. To overcome this issue, the routing protocol must consider the available bandwidth between the source and the destination router. To test this, the network topology in figure 1 is used. After the router configuration, a waiting period is used to make sure that all routing updates were performed (this is important in the case of proactive protocols), the maximum throughput between

routers R(1-1) and R(2-5) was measured using the Linux tool iperf3 by simulating a 90second UDP data transfer. The process was repeated 10 times for each protocol and the next transit router was determined. The obtained results can be interpreted as follows:

- The routing protocol HWMP considers the maximum bandwidth of the available paths. The UDP packets are therefore routed via router R(1-2) in all 10 tests.
- The routing protocol Babel balances well between the two alternative paths. The next router is selected depending on the path that was learned first. The Hello messages used by Babel to determine the link quality are sent to the broadcast address. In WLAN, messages sent to the broadcast address are transmitted using the lowest possible data rate (1 Mbps in this scenario). Because no packet loss is registered at this rate, the protocol cannot differentiate between the path over R(1-2) and the one over R(2-1). Furthermore, the routing protocol Babel implements a mechanism to avoid unnecessary route changes. A route change is only occurring if the new route has a significantly better metric.
- The Routing mechanism and metric used by B.A.T.M.A.N. advanced IV leads to the same problem. Unlike Babel, B.A.T.M.A.N. advanced IV lacks of a strategy for avoiding frequent route changes, the selected route can change more than once during a 90s transmission.
- The metric of B.A.T.M.A.N advanced V is based on the measured throughput. It therefore selects in all cases the router R(1-2) as next router to reach R(2-5).

#### B. Influence of existing flows

Another issue in WMN is the network traffic load. The routing protocol must consider existing traffic and selects an alternative route if the best one is overloaded at the time of the path establishment. The tests were performed on the network topology from Figure 1, as before, but introducing cross-traffic. Firstly, a UDP data transfer was simulated between R(1-3) and R(1-4). The required bitrate for this transfer was set to 24 Mbps so that the link between these two routers was overloaded (the maximum bitrate was set to 24 Mbps on layer 1 using wmediumd). Secondly, a second UDP flow was simulated between R(1-1) and R(2-5), 30s after the first one was started. It was expected that the new flow would be routed over R(2-1) as long as the first stream between R(1-3) and R(1-4) is running. The experiment was repeated 10 times. The obtained results can be summarised as follows: using HWMP and B.A.T.M.A.N advanced V, the data stream is routed over R(1-2) by all 10 tests like in the previous scenario. This indicates that the existing data stream between R(1-3) and R(1-4) does not affect the new communication. By Babel the path over R(1-2) is selected 6 times and the one over R(2-1) 4 times. The same result is obtained with B.A.T.M.A.N advanced IV. Here, the selected path can change more than once during the transmission.

#### IV. ROUTING PROTOCOLS PERFORMANCE IN DYNAMIC NETWORK SCENARIOS

Unlike common ad hoc networks where the mobility plays an important role, dynamic processes are not the focus in a WMN. However, they are an important part of the use cases in disaster situations. In this section the ability of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V to react to the loss or the integration of new devices is going to be tested and evaluated.

##### A. Router loss

A common scenario in disaster situation is the loss of an existing mesh router due to events such as aftershocks. As the devices of the disaster network are battery-supplied, lack of energy can also lead to the loss of a router. To react to this aspect of a lost router, all data flows via the lost router must be redirected within a short period of time. In this subsection, the time required for discovering an alternative path is going to be analysed. To reach this goal the network topology in figure 1 is used and an ICMP data transfer is simulated between the routers R(1-1) and R(2-5). The interval between ICMP Requests was 10ms. After 30s the router R(1-3) was shut down and the time difference between the last ICMP packet sent via R(1-2) (old path) and the first packet sent via R(2-1) (new one) was measured with Wireshark. The result is shown in table II (a). The protocol HWMP is the fastest and needs 0.2s to find an alternative path. This is due to the PERR frames generated by the neighbouring routers of R(1-3) after it leaves the mesh. The protocols B.A.T.M.A.N. advanced IV and V need 4.5s in average. This is due to the interval of 4s between the *OGMs*. The worst result is delivered by Babel (21.6s) and is based on the low frequency of routing updates (15s).

##### B. Router availability

An existing mesh can be extended by including new routers. In this subsection, the delay needed by the router R(1-1) to reach the router R(2-5) after it was started and becomes available, is going to be investigated. The test was performed using the *ping -f* command. The duration between the first frame sent by R(2-5) after it joins the mesh and the first ICMP packet that it replied, was measured. The results are resumed in table II (b). HWMP also shows the best result in this scenario with an average duration of 0.2s. For the protocols B.A.T.M.A.N. advanced IV and V, this procedure requires 6 and 3s respectively. Babel takes the most time (18s) to establish a communication between R(1-1) and R(2-5). This can be explain through the duration necessary for the association between R(2-5) and its neighboring routers and the low frequency of routing updates.

##### C. Router integration

One main objective of the integration of a new router inside an existing mesh is to improve the network performance. In this scenario, the mesh consists of the network topology in Figure 1, except for router R(1-3), which initially does not participate to the mesh. A UDP data stream was simulated between R(1-1) and R(2-5). After 30s, the router R(1-3) joins the mesh and the experiment measured the

delay until the routing protocols discovered the existence of a better path. Table II (c) summarises the results obtained by the test. The results can be interpreted as follows:

- The routing protocol HWMP requires 5s to redirect the UDP stream. This value can be explained through the duration necessary for R(1-3) to discover its neighbouring routers and the interval of the periodic PREQ send by R(1-1).
- The data stream is not redirected by Babel (No obtained results (-) in the table). Due to the metric implemented by Babel, the protocol cannot make a difference between the paths over R(1-2) and R(2-1). The data stream is already transmitted over R(2-1) when R(1-3) connects to the mesh. Due to the implemented mechanism to avoid unnecessary route changes in Babel, this path is used for total duration of the transmission.
- The result obtained by B.A.T.M.A.N. advanced IV should be the same as by Babel. However, because the protocol does not implement a mechanism to avoid multiple route changes, the selected path can change more than once after the integration. The selected route changes after 44s in average.
- A complete integration including the redirection of the UDP stream is possible using B.A.T.M.A.N. advanced V. After the new router joins the mesh, the update procedure is started. This process requires approximately 5s.

TABLE II. TEST RESULTS – ROUTER LOSS – ROUTER AVAILABILITY - ROUTER INTEGRATION

	HWMP	Babel	Bat. Adv. IV	Bat. Adv. V
Duration <sup>a</sup> [s]	0.20±0.09	21.63±1.96	4.75±0.35	4.48±0.30
Duration <sup>b</sup> [s]	0.23±0.15	18.16±2.41	5.99±0.61	2.55±0.33
Duration <sup>c</sup> [s]	5.27±0.25	-	44.37±7.88	4.97±0.28

<sup>a</sup> ICMP stream interruption duration after the router R(1-3) has left the mesh

<sup>b</sup> Necessary duration to reach a new router after that it connects to the mesh

<sup>c</sup> Necessary duration for the complete integration

#### V. ROUTING PROTOCOLS PERFORMANCE IN LARGE NETWORKS

In this section, the results obtained in the previous part are used to predict the behaviour of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V in large networks. Figure 2 shows the network topology. It consists of a  $n \times m$ , grid. The SNR is set to the same value for all links over network so that the maximum bandwidth between neighbouring nodes is 24 Mbps on Layer 1.

##### A. Network throughput

For the first test, the TCP throughput between the routers R(1-1) and R(n-n) was measured with iperf3. The obtained results are summarised in table III. It shows a strong dependency between the network size and the measured throughput. There are two reasons for the observed dependency. First, the communication across multihop paths leads to a deterioration of throughput, as described in [10]. The authors conclude that the path throughput is

approximately proportional to the inverse of the number of hops. Second, the huge number of packets generated by the routing protocol lead to a further deterioration of the path throughput. This explains the differences obtained by the tested protocols. The routing protocol HWMP, which generates the smallest number of routing packets, has the better result. However, when the traffic inside the mesh network increases, the expected performance decrease because for each active data transfer a periodic PREQ is broadcasted by the originator of the communication. This PREQ is forwarded by all mesh participants. The obtained results show that the routing protocols B.A.T.M.A.N. advanced IV and V should not be used inside a network with more than 36 routers. The test fails for large network by both protocols ((-) in the table III). The measured bandwidth also decreases by Babel. This is due to the growing number of updates needed to be transmitted, when the network size increases.

TABLE III. TCP THROUGHPUT DEPENDING ON THE NETWORK SIZE

Network size	4	9	16	25	36	49	64	81	100
HWMP [Mbps]	8.3	4.2	3.4	3.5	3.2	2.4	2.0	1.6	1.4
Babel [Mbps]	8.3	4.3	3.9	2.5	2.1	0.6	0.6	0.025	0.003
Bat. Adv. IV [Mbps]	8.1	3.8	3.1	1.8	1.0	0.4	0.01	-	-
Bat. Adv. V [Mbps]	8.0	3.8	3.0	1.6	0.8	-	-	-	-

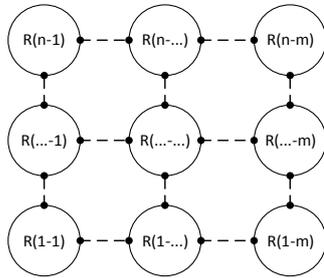


Fig. 2. Mesh grid

### B. Router loss

In this subsection, the delay observed by the redirection of the network traffic is measured. The aim of this test is to determine the effect of multiple failures regarding the performance of the communication path. The network topology used previously is maintained. An ICMP data transfer is running between the routers R(1-1) and R(n-n). After a waiting time of 30s, the major part of routers were disconnected, so that only one path was available between both routers. This means the number of damages on the communication path increases with the network size and therefore with the path length. The time necessary for the router R(1-1) to find an alternative path was documented. The test was repeated 10 times and the results are summarised in table IV. The best result is obtained by HWMP, with a recovery time under 2s for a network size below 25 routers. This is due to the generated error messages after a router loss. For B.A.T.M.A.N. advanced V no dependence could be detected between the distance (increasing with the network

size) and the delay necessary for a path recovery. By B.A.T.M.A.N. advanced IV a huge variation is detected and the path recovery could not be observed in large network. The recovery time is above 10s for the Babel protocol and increases with the network size.

TABLE IV. PATH AVAILABILITY DEPENDING ON THE NETWORK SIZE

Network size	4	9	16	25	36	49	64	81	100
HWMP [s]	0.06 ±0.003	0.5 ±0.3	1.5 ±0.7	1.8 ±0.4	4.1 ±1.6	3.8 ±0.5	4.4 ±0.5	3.7 ±1.5	-
Babel [s]	12 ±3	12 ±4	13 ±1	16 ±5	20 ±6	30 ±9	39 ±6	46 ±7	43 ±10
Bat. Adv. IV [s]	1.8 ±2.4	3.2 ±2.6	5.7 ±3.0	9.4 ±5.9	15.8 ±5.7	16.2 ±6.0	-	-	-
Bat. Adv. V [s]	4.5 ±0.3	4.3 ±0.3	4.6 ±0.4	4.5 ±0.6	4.8 ±0.2	-	-	-	-

## VI. OUTLOOK AND CONCLUSION

In this paper, the performance of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V was tested for disaster networks. In section 3, the performed analysis shows that the protocols HWMP and B.A.T.M.A.N. advanced V consider the path bandwidth by their routing operations. However, none of the examined protocols considers the influence of existing data transfers and implements load balancing to improve the network capability. Concerning the protocol performance after dynamic processes presented in section 4, the routing protocol HWMP has shown the best results. In the last section the performance of the protocols were examined for their scalability feature and it was concluded, that although the protocol Babel shows the best results concerning the network throughput none of the examined protocols can be used to build a large network like necessary for the communication after a disaster. This is due to the huge number of routing protocol packets generated in such a network. One solution can be to use a multiple cluster network like proposed in [9]. But such a network has two major inconvenients: first the hierarchical architecture is not desirable in disaster network due to the single point of failure and the need of a network administrator for the network configuration and secondly the routers which are configured as cluster head (CH) require huge computing and network capacity because all the network traffic has to transit them.

This paper presents a new network architecture to overcome this issues. The proposed architecture is shown in figure 3 and consists of two layers (basis layer and overlay layer). The basis layer is built with wireless routers which run a layer 2 routing protocol (e.g. HWMP). On the top of this an overlay layer is implemented. It provides IP routing functionalities (e.g. using the Babel protocol). From the point of view of an IP router running on the overlay layer of the proposed architecture, the network is fully meshed. Nodes in this layer do not have to deal with link quality changes or hardware router loss. Each cluster build a subnetwork. In the following subsections, the benefits of the proposed network architecture are going to be discussed more in details. Its advantages are presented by addressing two specific communication cases (intra and inter cluster communication). In the last subsection, suggestions are made for the realisation of the proposed architecture.

### A. Intra cluster communication

If a client connected to the router R(1-1) wants to communicate with another client connected to R(3-3) inside the same cluster/subnetwork, the communication is established using a layer 2 routing protocol. A cluster-id can be attached by the first router to each broadcasted frame so that the generated frames are not forwarded by mesh nodes outside the cluster. The proposed architecture is scalable, because the generated broadcast frames are no longer forwarded by all mesh participants but only by routers inside the cluster. Energy can be saved by each WMN node through the smaller number of transmitted routing packets and the overall network throughput increases.

### B. Inter cluster communication

If a client connected to R(1-1) wants to communicate with a client connected to R(6-6), which is not part of its cluster/subnetwork, it first sends the packets to its gateway represented by R(2-2), which uses the proactive layer 3 routing protocol to forward the packets to the next IP router R(5-5). This can be considered as a one hop communication in layer 3. In fact, the router R(2-2), creates a connection with the router R(6-6) on the MAC basis using the layer 2 protocol. The broadcast messages generated by routers hosting layer 3 routing functionalities like R(2-2) use the default cluster-id, so that its broadcast messages are relayed by all mesh participant independent of their cluster. This means the layer 2 routing protocol (e.g. HWMP), which is implemented in the underlying layer of the proposed architecture, is responsible for the path establishment between R(2-2) and R(5-5). As shown in the previous sections (III and IV) the established path (e.g. using HWMP) takes care of the link throughput and can provide a quick answer to network changes like router loss. Furthermore, due to the resulting aggregation of the inter cluster data stream (only one path is used for the communication between two clusters), the number of hardware routers used to transmit data packets is reduce and new optimisation opportunities are created. One example can be to reduce the duration of the sleeping mode by routers, which participate to a inter cluster communication to improve the network throughput and to increase the sleeping duration by other routers to save power. Another advantage of the proposed network architecture for inter cluster communications is the possibility to implement multi path communications. R(2-2) can send data packets to R(5-5) using two hop paths in addition to the direct one. This can be used to increase the network throughput or reduce packet loss.

### C. Proposed implementation

According to the results presented in this paper, the choice of HWMP as layer 2 routing protocol working on the first layer of the proposed network architecture and Babel as layer 3 routing protocol working on the second layer can be a suitable solution. Furthermore, due to the full meshed nature of the overlay IP network, periodic hello and IHU messages are no longer required. Additionally, the usage of a technology like network function virtualization (NFV) to implement routing functionalities on layer 2 of the proposed network

architecture can improve the network performance and increase the network life. As an example, a Babel router, which represents the cluster head, can be implemented as a virtual network function. Its position in the cluster could be changed (live migration) depending on the router which generates the most important inter cluster traffic or depending on the remaining router energy. The migration of the cluster heads leads to a change in the selected routes for the inter cluster communication and therefore a better distribution of the network load/power consumption. An NFV orchestrator has to be used to manage the dynamic configuration of the network and dynamic build new clusters inside the WMN. The NFV orchestrator also allows a fast recovery, when a mesh node running a Babel router shuts down unexpectedly.

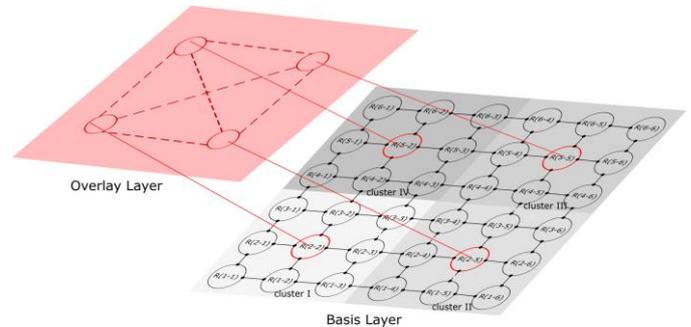


Fig. 3. Optimised network architecture to solve routing issues in disaster scenarios

### REFERENCES

- [1] A. Lehmann, A. Pagueu Tchinda and U. Trick, "Optimization of Wireless Disaster Network through Network Virtualization," Eleventh International Network Conference (INC 2016), pp. 165-170, 19-21 July 2016.
- [2] A. Yarali, B. Ahsant und S. Rahman, "Wireless Mesh Networking: A Key Solution for Emergency and Rural Applications," Advances in Mesh Networks, 2009. MESH 2009. Second International Conference on, vol., no., pp.143-149, 18-23 June 2009.
- [3] M. Portmann and A.A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Application," IEEE Internet Computing, vol. 12, no. 1, pp. 18-25, 2008.
- [4] A. Pagueu Tchinda, A. Lehmann, and U. Trick, "Untersuchung von Wireless Mesh Network-Routing-Protokollen für den Einsatz in Netzen für Katastrophengebiete," Mobile communication conference, ITG-Fb. 263: Mobilkommunikation.
- [5] "Bcopeland Wireless Medium Simulator (wmediumd)," 2017. [Online]. Available: <https://github.com/bcopeland/wmediumd>.
- [6] Institute of Electrical and Electronics Engineers, "HWMP Protocol specification," Mai 2009
- [7] J. Chroboczek, "The Babel Routing Protocol," RFC 6126, April 2011
- [8] "B.A.T.M.A.N. Advanced," 2017. [Online]. Available: <https://www.open-mesh.org/projects/batman-adv/wiki>
- [9] D. Kaushal, G. Niteshkumar, B. Prasann K. and V. Agarwal, "Hierarchical cluster based routing for wireless mesh networks using group head," International Conference on Computing Sciences (ICCS), Phagwara, pp. 163-167, 2012.
- [10] J. Marchang, B. Ghita, and D. Lancaster, "Hop-Based dynamic fair scheduler for wireless Ad-Hoc networks," 2013 IEEE International Conference on Advanced Networks and Telecommunications Systems
- [11] E. W. Dijkstra, "A note on two problems in connexion with graphs." Numerische Mathematik, pp. 269-271, 1959

