The Agony of Choice: Behaviour Analysis of Routing Protocols in Chain Mesh Networks

Mohamad Sbeiti and Christian Wietfeld

Communication Networks Institute (CNI), Faculty of Electrical Engineering and Information Technology, Dortmund University of Technology, Germany
{Mohamad.Sbeiti,Christian.Wietfeld}@tu-dortmund.de

Abstract. In recent years, routing in wireless mesh networks has been a focal point of research leading to a profusion of protocol proposals. Choosing the appropriate protocol and finding the optimal parameterization for a given network pose a major challenge in practice. This paper investigates the performance of well-established non-secure routing protocols (such as OLSR, BATMAN and HWMP) and the secure protocol PASER in chain mesh networks. A thorough analysis of the behaviour of the protocols is carried out and parameterization optimizations are derived. The results justifies that reactive or hybrid routing protocols perform better than proactive routing protocols in chain mesh networks having static source-destination pairs and moderate number of forwarding hops. HWMP is the best candidate in such networks in case security is not a concern. Otherwise, due to security flaws of the IEEE802.11 security frameworks as we experimentally show, PASER is a more suitable candidate.

Key words: HWMP, Mesh Networks, Routing Protocols, Secure Routing, Wormhole, Performance Evaluation

1 Introduction

Wireless mesh networks (WMNs) have become a promising technology to achieve high-performance and low-cost ubiquitous network access. WMNs are attracting cellular network operators to substitute long-distance non-line-of-sight cellular links by various mesh links with improved link budgets in order to improve capacity, energy efficiency and performance of the system. Rescue organizations are using mesh networks to establish broadband links to rescue fighters, especially, when infrastructure-based networks fail. Rescue organizations also use WMNs to interconnect autonomous unmanned aerial vehicles (UAVs) in scenarios where uncontrolled emissions of liquid or gaseous contaminants exist.

To establish WMNs, routing protocols are necessary to discover and maintain routes on the fly between all network nodes. There are mainly three classes of mesh routing protocols, namely, proactive, reactive and hybrid. In case of proactive protocols, nodes periodically send routing messages throughout the entire network, regardless of the network traffic, and each node has the routing information of all other reachable nodes in the network. In contrast, reactive protocols are traffic-aware and their overhead is strongly related to the traffic load of the network. Nodes only exchange routing information when a route to an unknown destination is required and only information about active routes is maintained. Hybrid protocols are a combination of both previous routing classes. Hereby, only nodes having a superior role, e.g. gateways, periodically broadcast messages throughout the network.

A profusion of routing protocols of all three classes have been proposed in the last decade [1], such as the well-known protocols OLSR (proactive) [2] and AODV (reactive) [3]. To increase the scalability of OLSR, the freifunk community has released BATMAN and its derivatives [4]. Inspired by AODV, IEEE specified the hybrid protocol HWMP as part of the new mesh standard IEEE802.11s [5]. To achieve a reasonable trade-off between performance and security, we have proposed the reactive routing protocol PASER [6] in earlier work. Given all the protocols, choosing the appropriate protocol and finding the optimal parameterization for a network poses a major challenge on end-users in practice. To this end, we investigate in this paper OLSR, BATMAN, HWMP, and PASER in chain mesh networks as representative of several applications of mesh networks, especially, UAVs in emergency scenarios [7].

The remainder of this paper is organized as follows: A brief review on related work is given in Section II. In Section III, the theoretical throughput of the IEEE802.11g standard [8], which is used as a reference WLAN technology in this work, is calculated and deviations between simulation and real networks are discussed. In Section IV, a thorough performance analysis of the protocols is presented. In section VI, notable simulation results are validated in a real testbed and a routing attack is carried out. Finally, we conclude our contribution and give an outlook on future work in Section VII.

2 Related Work

In recent years, there has been an intensive study of routing protocols for multihop wireless networks. The authors in [1] present a high level comparison of characteristics and complexity of many routing protocols of different classes. They conclude that proactive protocols having flat routing structure do not scale well in general and that the worst case scenario with respect to reactive protocols is when there is no previous communication between source and destination (initial stages). Analogously, the author in [9] indicates that AODV performs better in networks with static traffic while OLSR has advantages in networks with highly sporadic traffic. Based on experimental measurements, the author in [10] reports that proactive protocols perform much better than reactive in semi static topologies. The main reason hereby is, however, the frequently changing traffic destination in the evaluated scenarios and not the topology. Thus, the results of this work matches those of the previously listed studies. In a realistic scenario-based performance evaluation (conference, event coverage and disaster relief), the authors in [11] show that AODV performs better than proactive protocols. Hereby, static source-destination pairs have been considered. Similarly, the authors in [12] denote that AODV performs better than OSLR in military applications with static constant bit rate (CBR) flows. In contrast, other work in the literature such as [13] shows the superiority of proactive routing protocols in case of static CBR traffic. In this paper, we justify, based on a thorough analysis of the protocols behaviour, that reactive or hybrid routing protocols perform better than proactive protocols in mesh networks having static source-destination pairs and moderate number of forwarding nodes. We show that contradictions to this statement are mainly caused by a non fair parameterization of the protocols or by an overload of the network. Among others, we consider the new IEEE mesh routing protocol HWMP in our evaluation, which has been investigated only in few experiments yet and only in reactive mode [14, 15]. On top of that, and analogously to [16] where only HELLO and TC intervals of OLSR were addressed, we derive parameterization optimizations of performance crucial parameters of all the considered protocols in the reference scenarios. Apart from that, we experimentally verify the vulnerability of WPA2 (the security framework in [17]) and the recently proposed security framework in IEEE802.11s against the wormhole attack.

3 Theoretical Throughput of IEEE802.11g

In this section, the theoretical throughput of one IEEE802.11g [8] node is calculated according to the equations and the parameter values provided in Table 1. The latter comprises the throughput values of equations 1 and 2 for a UDP connection in case of different PHY bitrates. These values are necessary to derive the saturation throughput of a network which denotes the state in which a node has always a frame to send. The saturation throughput is considered a threshold of the sender data rates in our evaluation.

Apart from that, for a realistic simulation-based analysis, a special care has been given to the following points: a) According to the IEEE802.11g standard, nodes responding to a received frame shall transmit their control response frame (either CTS or ACK) at the highest rate in the BasicRateSet parameter that is less than or equal to the rate of the received frame and that is of the same modulation class as the latter. While this statement holds in practice, in most simulation tools such as OMNET++ (see next section), CTS and ACK are always transmitted with a static bitrate of, e.g., 1 Mbit/s. This leads to lower saturation throughput in simulation than in practice. Validating the simulation results in practice makes only sense when properly calculating and considering the different throughputs. b) While bitrates are sender-receiver specific in practice, in OMNET++, bitrates are only sender specific. That is, a sender uses only one bitrate to send its frames, regardless of the receiver of the frame and the channel characteristics of the latter. Thereby and to avoid ambiguity, we only consider static bitrates in our analysis. The impact of rate adaptation mechanisms in mesh networks has been well investigated in the literature such as in [18].

Table 1. IEEE802.11g Theoretical Throughput.

IEEE802.11g Throughput Equations.

$$\mathrm{Throughput}_{\mathrm{Basic}} = \frac{\mathrm{Size}_{\mathrm{Packet}}}{\mathrm{T}_{\mathrm{Transmission}_{\mathrm{Basic}}}} \qquad (1)$$

$$\mathrm{Throughput}_{(\mathrm{RTS/CTS})} = \frac{\mathrm{Size}_{\mathrm{Packet}}}{\mathrm{T}_{\mathrm{Transmission}_{(\mathrm{RTS/CTS})}}} \qquad (2)$$

$$\mathrm{T}_{\mathrm{Transmission}_{\mathrm{Basic}}} = \mathrm{DIFS} + \frac{\mathrm{CWmin}\cdot \mathrm{T}_{\mathrm{Slot}}}{2} + \mathrm{T}_{\mathrm{Data}} + \mathrm{SIFS} + \mathrm{T}_{\mathrm{ACK}}$$

$$\mathrm{T}_{\mathrm{Transmission}_{(\mathrm{RTS/CTS})}} = \mathrm{DIFS}+\frac{\mathrm{CWmin}\cdot \mathrm{T}_{\mathrm{Slot}}}{2}+\mathrm{T}_{\mathrm{RTS}}+\mathrm{SIFS}+\mathrm{T}_{\mathrm{CTS}}+\mathrm{SIFS}+\mathrm{T}_{\mathrm{Data}}+\mathrm{SIFS}+\mathrm{T}_{\mathrm{ACK}}$$

$$\mathrm{T}_{\mathrm{Data}}= \frac{\mathrm{PHYHeader}}{1\ \mathrm{Mbit/s}} + \frac{(\mathrm{Size}_{\mathrm{Packet}}+\mathrm{UDPHeader}+\mathrm{IPHeader}+\mathrm{MACOverhead})}{\mathrm{Bitrate}}$$

$$\mathrm{T}_{\mathrm{ACK}}= \frac{\mathrm{PHYHeader}}{1\ \mathrm{Mbit/s}} + \frac{\mathrm{ACK}}{\mathrm{BasicBitrate}}$$

$$\mathrm{T}_{\mathrm{RTS}}= \frac{\mathrm{PHYHeader}}{1\ \mathrm{Mbit/s}} + \frac{\mathrm{RTS}}{\mathrm{BasicBitrate}}$$

$$\mathrm{T}_{\mathrm{CTS}}= \frac{\mathrm{PHYHeader}}{1\ \mathrm{Mbit/s}} + \frac{\mathrm{CTS}}{\mathrm{BasicBitrate}}$$

IEEE802.11g Selected Parameter Values.

T_{Slot}	SIFS	DIFS	CWmin
9μs	10μs	28μs	31
UDPHeader	IPHeader	MACOverhead	PHYHeader [bits]
160bits	160bits	272bits	20 (ERP-OFDM), 192 (DSSS)
ACK	RTS	CTS	BasicRateSet [Mbit/s]
112bits	160bits	112bits	1,11,18
Bitrate [Mbit/s]			
11, 36			

Throughput [Mbit/s]: CBR-UDP with $\mathrm{Size}_{\mathrm{Packet}} = 1460\cdot 8$ [bits].

Applicability	Bitrate [Mbit/s]	BasicBitrate [Mbit/s]	$\mathrm{Throughput}_{\mathrm{Basic}}$	$\mathrm{Throughput}_{\mathrm{RTS/CTS}}$
ERP-OFDM				
Experimental	36	18	20.85	18.38
Simulation	36	1	13.93	7.71
DSSS				
Experimental	11	11	6.94	5.53
Simulation	11	1	6.54	4.74

4 Performance Analysis

In this section, the results of the evaluation of the protocols in the discrete event-based simulation environment OMNeT++ [19] and its INETMANET framework are presented. The behaviour of the protocols is analyzed in static and mobile chain mesh networks, as illustrated in Figure 1. An overview of the protocols' parameters which are crucial for the performance is provided in Table 2. The initial values of these parameters as well as the simulation configuration are depicted in Table 3. The carrier sense range in all scenarios equals 341.8 m. According to the free space propagation model with a path loss exponent of 2.8, this is the maximum distance, in which a node equipped with a wireless interface having a receiver sensitivity of -91d Bm can sense the signal in case the transmitting power is 20 dBm. The SNIR threshold is set to 4 dB, which means that a node simultaneously receiving a signal and an interfering signal with powers (mW) $\mathrm{P}_{\mathrm{Signal}}$ and $\mathrm{P}_{\mathrm{Interference}}$, respectively, is able to recover the signal in case $10\cdot log_{10} \cdot \frac{\mathrm{P}_{\mathrm{Signal}}}{\mathrm{P}_{\mathrm{Interference}} + \mathrm{NoiseLevel}} > 4$. This means, in case the thermal noise is -101 dBm and the noise factor is 9 dB

Table 2. Performance Crucial Parameters of Routing Protocols.

Parameter	Protocol(s)	Description / Refresh Condition
HELLO-Interval	OLSR, PASER	HELLO messages are necessary to establish (OLSR) / refresh (OLSR & PASER) links between neighbours (one-hop) and two-hop nodes.
TC / OGM-Interval	OLSR, BATMAN	Topology control (TC - OLSR) / Originator (OGM - BATMAN) messages are necessary to establish and refresh routes between nodes.
RANN-Interval	HWMP	Interval between two root announcements. In case HWMP is running in reactive mode, this interval is 0.
Neighbour-Hold-Time	OLSR, PASER, HWMP	When this timeout is triggered, the corresponding entry is set as invalid (or deleted). All the route entries for which this neighbour has been next-hop are also set as invalid (or deleted). OLSR & PASER: Timer is refreshed only in case of receiving routing messages from the corresponding neighbour. HWMP: Timer is refreshed upon sending / receiving any frame to / from the neighbour.
Route-Hold-Time	ALL	When this timeout is triggered, the corresponding route entry is set as invalid (or deleted) in the routing table. OLSR & BATMAN: Timer is refreshed only in case of receiving the corresponding routing message. PASER & HWMP: Timer is refreshed every time a node receives / sends any IP-packet (PASER) / frame (HWMP) over the route.
IsLinkLayerFeedback	PASER	Option to (de-)activate the link layer feedback mechanism.

Table 3. Relevant Simulation Parameters.

Network and Traffic Models.

Parameter	Value
Carrier Sense Range [m]	341.8
Transmission Range [m]	267.1
Bitrate [Mbit/s]	36, 11
BasicBitrate [Mbit/s]	1
MAC Layer	IEEE802.11g
Channel Model	Free-space
Simulation Time [s]	100
Traffic Model	CBR-UDP
Packet Size [Bytes]	1460
Network Buffer Size [Packets]	100
Application Start, Stop Time [s]	10, 95

Protocol Configuration Parameters.

Parameter	Protocol(s)	$\text{Initial Value}_{\text{static}}$	$\text{Initial Value}_{\text{mobile}}$
HELLO-Interval	OLSR	1s	500ms
OGM-Interval	BATMAN	1s	500ms
HELLO-Interval	PASER	1s	2s
TC-Interval	OLSR	2s	1s
RANN-Interval	HWMP	0s	2s
Neighbour-Hold-Time	OLSR, PASER, HWMP	12s	12s
Route-Hold-Time	ALL	15s	15s
IsLinkLayerFeedback	PASER	false	true

($\text{NoiseLevel (mW)} = 10^{\frac{(\text{themal noise + noise factor})}{10}}$), the interference range of a link of length 175 m is approximately 277 m and the transmission range equals 267.1 m. That is, all the hidden nodes in the chain networks in Figure 1 lies within the interference range of the corresponding links.

4.1 Static Chain Mesh Networks

In this subsection, the protocols are first evaluated in case of the basic transmission method of the IEEE802.11g standard. Afterwards, the RTS/CTS mode is analyzed. An error-free channel with a fixed bitrate of 36 Mbit/s is used at first.

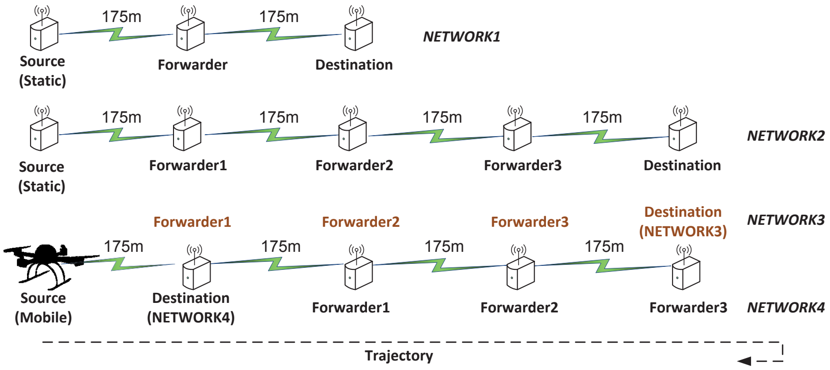


Fig. 1. Evaluated networks.

Error-Free Channel, Without RTS/CTS Seeking for a deep understanding of the protocols' behaviour in chain mesh networks, the protocols are first analyzed in a chain of three nodes and then in a longer chain of five nodes.

1.1) Chain of Three Nodes

The three nodes are placed in a distance of 175 m, as depicted in Figure 1 (network1). Thus, according to Table 1, $\text{Throughput}_{\text{Basic}}$ is 13.93 Mbit/s. The saturation throughput of the sender and forwarder is $\text{Throughput}_{\text{Saturation}_{[\text{S,F}]}} = \frac{\text{Throughput}_{\text{Basic}}}{2} = 6.985$ Mbit/s, because only one of both nodes can transmit at any instance of time. Since there is no hidden nodes in this scenario, $\text{NetworkThroughput}_{\text{optimal}} = \text{Throughput}_{\text{Saturation}_{[\text{S,F}]}} = 6.985$ Mbit/s. The protocols perform in this scenario as following:

OLSR: Collisions solely occur at the forwarder. They are caused by the periodic routing messages of the destination, which arrives at the forwarder while it is receiving data packets from the sender. The collisions lead to route losses at the forwarder and sender in specific intervals, as depicted in Figure 2(a), where the goodput almost drops to 0. These intervals correspond to the OLSR timeouts mentioned in Section III. The routes get recovered again after the sender loses the route to the destination. The UDP packets are then dropped at the sender and thus the routing messages of the destination does not collide anymore.
Figure 2(b) illustrates the goodput in case the data rates are higher than $\text{NetworkThroughput}_{\text{optimal}}$ (e.g., 14 Mbit/s). In that case, the sender will not have enough time (access to the medium) to send all its UDP packets, thus the higher the data rates are the faster the queue of the sender is filled up and the higher number of packet drop occur. Thereby, the goodput decreases to less than the half.

BATMAN: The behaviour of BATMAN in this scenario is quite similar to OLSR. The sole difference is that in BATMAN there is no Neighbour-Hold-Timeout (12s in OLSR). The routes are only deleted when a Route-Hold-Timeout is triggered (every 15s). As a result, the number of route losses in this scenario in case of

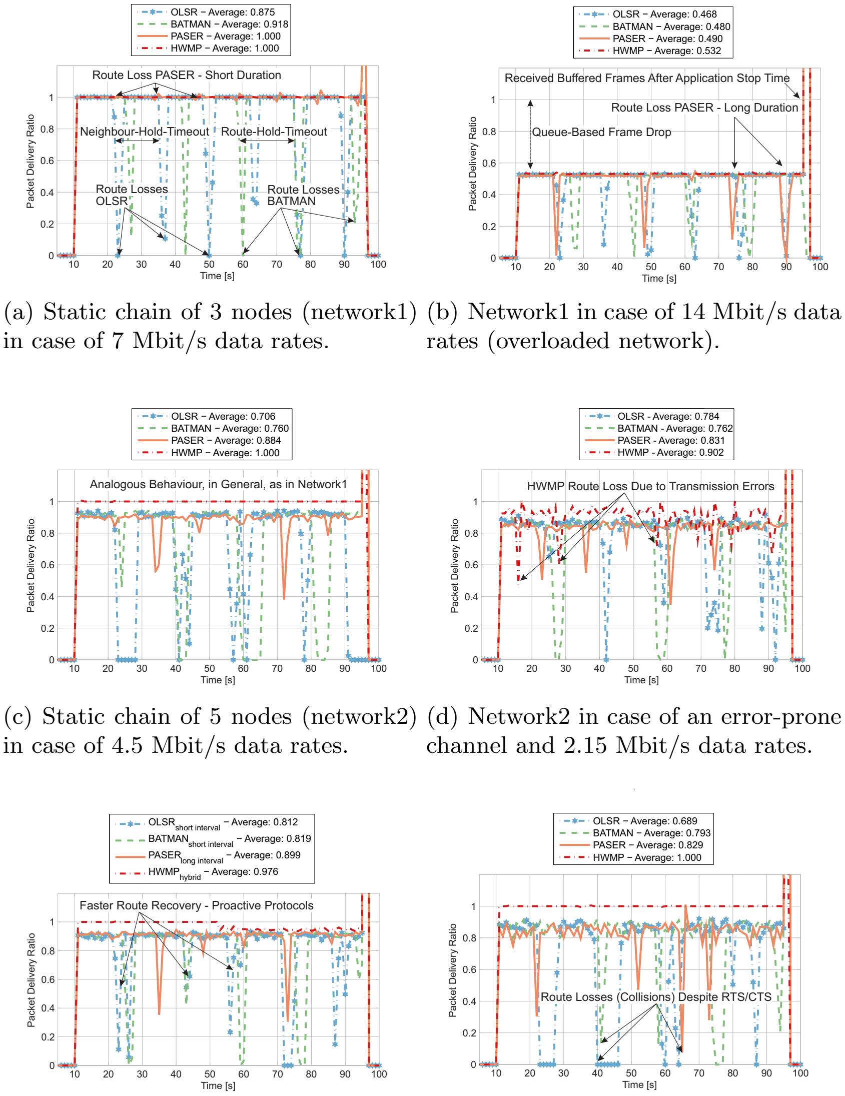
BATMAN is in general lower than that of OLSR, thereby, the goodput in case of BATMAN is slightly higher than that of OSLR, see Figure 2(a).

PASER: Only the collision effect in case of PASER resemble to OLSR and BATMAN. Hereby, HELLO messages of the destination collides with packets send from the sender to the forwarder. As a result, the route from forwarder to destination gets invalid every 12s (Neighbour-Hold-Timeout). However, in contrast to the proactive protocols, PASER is traffic-aware. That is, the sender never loses the route to the destination, because it is receiving HELLO messages of the next hop (forwarder) and it is sending packets over the route (Route-Hold-Timeout will be refreshed). Besides, when the forwarder loses the route to the destination and it receives a UDP packet from the sender, it will buffer this packet as well as the next ones and it will try to repair the route by starting a route discovery towards the destination. While HELLO messages are broadcast messages and they are not retransmitted after collision, the reply of the destination is a unicast message and it will be retransmitted seven times in case of collision. Thus, we see in Figure 2(a) very fast recovery in case of PASER (no falling edges) in comparison with BATMAN and OLSR. Nonetheless, the higher the sending rates of sender are, the longer this discovery might be, since the probability of successful retransmission of the reply message also decreases, see Figure 2(b). Figure 2(a) shows that the traffic-awareness of PASER and its route discovery approach (use of unicast messages) in addition to the queuing mechanism lead to better goodput in comparison with proactive protocols.

HWMP: In contrast to all other protocols, HWMP does not comprise any periodic messages to sense neighbours. The route maintenance is solely based on the link layer feedback (LLF) and on timeouts. That is, only if a unicast frame has been dropped after seven retransmissions or a route timeout is triggered, HWMP will declare the link as broken. Since there are no hidden nodes in this scenario, no collision will occur. Also no timeouts occur because the route validity is updated every time the node sends or receives a frame over the route/path. As a result, no route breaks occur and the performance of HWMP in this scenario is similar to the performance of a network with preconfigured routes. The only difference is that, few packets get queued by HWMP at the sender during the route discovery at the beginning. As expected, Figure 2(b) shows that even in case data rates are higher than $\text{NetworkThroughput}_{\text{optimal}}$, no route losses occur but only queue-based packet drop at the sender.

1.2) Chain of Five Nodes

In this network (Figure 1, network2), $\text{Throughput}_{\text{Saturation}_{[\text{S,F3}]}} = \frac{\text{Throughput}_{\text{Basic}}}{2} = 6.985$ Mbit/s, the sender only contends with forwarder1; forwarder3 contends with forwarder2. $\text{Throughput}_{\text{Saturation}_{[\text{F1,F2}]}} = \frac{\text{Throughput}_{\text{Basic}}}{3} = 4.64$ Mbit/s, fowarder1 contends with sender and forwarder2. The latter contends with forwarder1 and forwarder3. $\text{NetworkThroughput}_{\text{optimal}} \leq 4.64$ Mbit/s because forwarder1 (bottleneck) has one hidden node, namely forwarder3.



(a) Static chain of 3 nodes (network1) in case of 7 Mbit/s data rates.

(b) Network1 in case of 14 Mbit/s data rates (overloaded network).

(c) Static chain of 5 nodes (network2) in case of 4.5 Mbit/s data rates.

(d) Network2 in case of an error-prone channel and 2.15 Mbit/s data rates.

(e) Network2 in case of optimized parameterization and 4.5 Mbit/s data rates.

(f) Network2 in case of active RTS/CTS and 2.5 Mbit/s data rates.

Fig. 2. Packet delivery ratio (PDR) in networks 1 and 2 (static).

OLSR & BATMAN: In case of data rates approx. equal $\text{NetworkThroughput}_{\text{optimal}}$, collisions occur at forwarder1 because forwarder2 is saturated and it is a hidden node for the sender. This produces a domino effect causing collisions, among others, between forwarder1 and forwarder3 traffics as well as between forwarder2 traffic and the routing messages of the destination. As for network1, the collision of the routing messages will lead to route losses and thus to a drop in the PDR (see Figure 2(c)). Note however, that in this network and in case of OLSR, if routing messages of forwarder2 are successfully received by forwarder1 before forwarder2 loses the route to the destination, the sender and forwarder1 will refresh the route to the destination while forwarder2 will lose this route afterwards. This will lead to queue-based packet drop and a delayed recovery of the route due to collisions between UDP packets, ICMP and routing messages. In case of BATMAN, when OGM of destination collides, all nodes will lose the route to forwarder3. The latter will leads to a faster recovery and thus to better PDR in comparison with OLSR (see Figure 2(c)).

PASER: The impact of the design differences of PASER and proactive protocols is the same in this network as in network1. Of course, due to the longer chain, the recovery of the routes takes longer in case of proactive protocols, because they have to wait until the periodic messages are rebroadcasted. In case of PASER, the recovery is faster because PASER is traffic-aware and the reply is unicast. Thereby, PASER achieves better goodput than proactive protocols in this scenario, as illustrated in Figure 2(c).

HWMP: No route breaks occur in case of HWMP. Despite the collision, no transmission errors exist.

Error-Free Channel, With RTS/CTS In case the RTS/CTS mechanism is activated in the chain network of five nodes (Figure 1, network2), $\text{Throughput}_{\text{Basic}}$ decreases to 7.71 Mbit/s, as illustrated in Table 1. Thus, $\text{NetworkThroughput}_{\text{optimal}} \leq \frac{\text{Throughput}_{\text{Basic}}}{3} = 2.571$ Mbit/s. One would expect that in this scenario, due to the RTS/CTS mechanism, routing messages of PASER, OLSR and BATMAN that are broadcasted in the opposite direction of the traffic flow will not collide with the traffic and thus no route breaks will occur between the nodes. However, the results in Figure 2(f) contradict with this theory for the following reasons: Indeed no data packet-based collisions occur in this scenario but rather control frame-based collisions. RTS, CTS and ACK frames of forwarder2 collide with routing messages of the destination. RTS frames of forwarder1 and forwarder3 collide among each other and so on.

Protocols Parameterization As opposed to previous work in [14], a comparison of Figures 2(c) and 2(e) shows that short periodic messages intervals in case of proactive protocols (above a threshold, which depends on the scenario and should be derived using analytical models - in this scenario, it is 500 ms) lead in general to faster reaction on route breaks. This parameterization pays off despite the higher resulting overhead, because it is much more crucial to faster recover from route breaks than producing slightly more collisions of data packets. Figure 2(e) also shows that in case of reactive routing protocols that use HELLO messages such as PASER, long intervals are rather beneficial (in this scenario, it is 2s), since HELLO messages are not used to repair a broken route. Apart from that, as a matter of course, higher timeouts values (below a threshold - see Table 3) are necessary to keep the number of route breaks low in case of all three routing classes. Running HWMP in hybrid mode might lead to unnecessary route changes in this scenario.

Error-Prone Channel, without RTS/CTS In this scenario, a fixed bitrate of 11 Mbit/s is considered in the chain network of five nodes (Figure 1, network2). In that case, $\text{Throughput}_{\text{Basic}}$ is 6.54 Mbit/s, thus, $\text{NetworkThroughput}_{\text{optimal}} \leq 2.18$ Mbit/s. Figure 2(d) shows that error-prone channels lead in general to a decrease of the PDR threshold below 1. It also shows, especially in case of reactive and hybrid protocols relying on LLF, a higher number of route loss such as the case in HWMP. Nevertheless, HWMP still perform the best in this scenario.

Summary for Static Chain Mesh Networks In a chain network having low number of flows, static source-destination pairs and moderate number of forwarding hops, reactive or hybrid routing protocols perform better than proactive protocols and HWMP performs the best. The main drawback of proactive protocols in this scenario, in addition to their non-QoS broadcast messages in the opposite direction of the flow, is that they are not traffic-aware. They always have to wait some timeouts until they consider a route as broken. They do not refresh their Route-Hold-Timeouts when they send or receive data over the routes. Besides, they do not react on ICMP messages.
In addition to the reasons stated in [20], it has been verified that it does not pay off to activate RTS/CTS in multihop networks because of collisions between control frames (and data). It has also been shown that exceeding the network bandwidth capacity leads to high queue-based packets drop regardless of the protocol used as well as longer route recovery time in case of reactive and hybrid protocols. As a matter of fact, overloading the network might lead to more route losses in the latter case since the probability of transmission errors increase. Using mechanisms based on the model proposed in [21] can proactively constraint the number of flows so that the network is never overloaded. Finally, in contrast to HWMP (layer 2), routing messages of OLSR, BATMAN and PASER are not prioritized at the MAC layer, thus, these often spend long time in the queue or they are even dropped in case the queue is full, e.g., at the bottleneck node.

4.2 Mobile Chain Mesh Networks

To understand the behaviour of the routing protocols with respect to mobility, network3 and network4 have been considered, as illustrated in Figure 1 (bottom). In both networks, the mobile node moves along a 875 m path. It has a velocity of 10 m/s. In network3, the mobile node moves towards the destination. In network4, it moves away from the destination. Figure 3 depicts the nodes in the carrier sense range of the mobile node (sender) as well as the nodes in

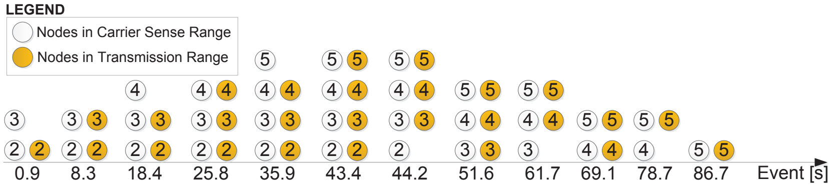


Fig. 3. Nodes in the proximity of sender versus time.

its transmission range (neighbours) versus time. Hereby, node number 2 is the forwarder1 in network3 while it is the destination in network4 and so on. The protocols' configuration is given in Table 3. They perform as follows:

Error-free channel, network3 - decreasing route length Figure 4(a) shows that proactively switching the route is in general beneficial in this scenario. In that case and due to the decrease of the route length, routing timeouts might be avoided (compare PASER and the other protocols in the interval $18.4s \leq t < 25.8s$). Apart from that, the figure shows that OLSR switches the route faster than BATMAN (see $10s \leq t < 18.4s$). In this interval and in case of BATMAN, the sender keeps using the same route (via forwarder1) because of its metric (it only switches the route in case it receives more destination-OGMs via forwarder2 than forwarder1 within a sliding period). In case of OLSR, the sender switches the route to forwarder2 after receiving the corresponding HELLO and TC messages. Thereby, PDR in case of OLSR is higher than that of BATMAN in this phase.

Parameterization of network3 - decreasing route length Short periodic messages intervals in case of proactive protocols are also recommended in this scenario, otherwise, 'ping pong' effects might occur, especially, in case of BATMAN. Hereby, the sender chooses a node as next-hop to the destination while that node chooses the sender as its next-hop. In case of PASER, it is certainly beneficial to turn on the link layer feedback to immediately react on the consequences of the mobility of the node. An important optimization in this scenario with respect to HWMP is to activate the root mechanism at the destination because it enables a fast refresh of the route towards that destination (compare Figures 4(a) and 4(b)). As in the static scenario, it is recommended to keep the timeout values high in this scenario, otherwise, route instability occurs, as depicted in Figure 4(b).

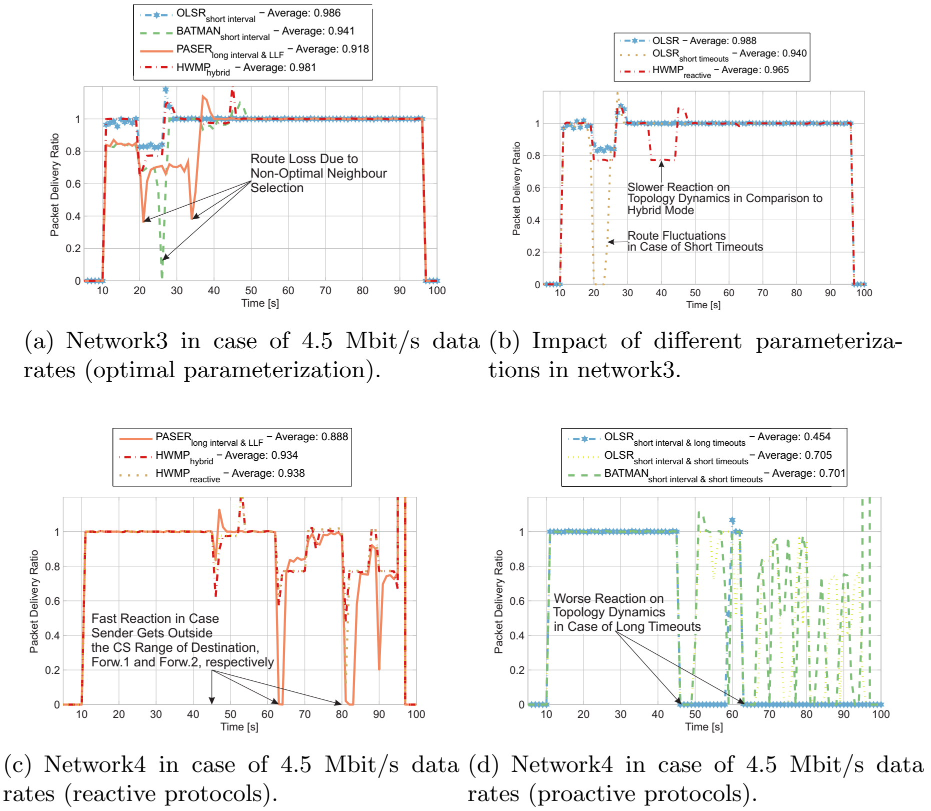
Error-free channel, network4 - increasing route length Figure 4(c) highlights the fast reaction of PASER and HWMP to link breaks due their link layer feedback and their reactive route maintenance mechanism. The figure shows that at t≈45s when the sender gets outside the range of the destination, HWMP and PASER rapidly react and switch the route. The same holds at t≈62s and t≈80s, when the sender loses the route to forwarder3 and forwarder2, respectively. In case of proactive protocols, the sender detects route breaks only when route timeouts are triggered, which also leads in this scenario (short timeouts) to unnecessary route switches (see Figure 4(d)).

Parameterization of network4 - increasing route length keeping the interval of periodic messages low in case of proactive protocols is also beneficial in this scenario, as depicted in Figure 4(d). In case of PASER, it also makes sense here to activate LLF and to configure long HELLO intervals. In case of HWMP, the same holds as in the previous scenario, even though the benefit of running it in hybrid mode is not that obvious in this chain scenario. This benefit increases the longer the route is, since nodes away from the destination will be able to immediately reply to the sender's route request.
Keeping the route timeouts low in case of proactive protocols is indispensable in this scenario. Otherwise, as a matter of course, frequent route timeouts will indeed cause lower route fluctuations at the expense of long route recovery time and thus low PDR (see Figure 4(d)).

Summary for mobile chain networks The same parameterizations can be applied in mobile chain networks as in static networks with respect to periodic messages interval. In case of proactive protocols, timeouts in mobile scenarios by which the number of hops between the sender and destination often increases should be kept low. Otherwise, the same timeouts as in the static scenario might be configured. In PASER, it is imperative to activate the link layer feedback in this scenario. In case of HWMP, it is beneficial to run the protocol in hybrid mode. As in the static scenario, HWMP performs in average the best in this scenario.

5 Experimental Validation and Wormhole Attack

The same experimental testbed as in [14] is used to validate the simulation results of HWMP (wireless-testing.git tree, kernel 3.6). To make sure that the analyzed behaviour generally holds in indoor as well as outdoor environments and regardless of the PHY bitrates as long as the traffic load is below the $\text{NetworkThroughput}_{\text{optimal}}$, we run two different measurements in a real chain of 5 nodes: *a)* indoor, PHY bitrate 36 Mbit/s, application data rate 4.5Mbits; *b)* outdoor, PHY bitrate 11 Mbit/s, application data rate 2.3Mbits.
As in simulation, Figure 5(a) shows that very few route losses occur. It also highlights the decrease of PDR in case of activated RTS/CTS. The figure also reflects $\text{NetworkThroughput}_{\text{optimal}}$ of network2 in case of the indoor measurements. In case of the outdoor measurements, $\text{NetworkThroughput}_{\text{optimal}} \ll \frac{6.94}{3}$ Mbit/s, because in that case the carrier sense range $>$ 2·transmission range. Thereby, $\text{NetworkThroughput}_{\text{optimal}} \leq \frac{6.94}{4} \approx 1.73$ Mbit/s.
So far we have shown that reactive and hybrid protocols perform in general better than proactive protocols in the considered chain mesh networks with HWMP performing the best. However, in case security is a concern and network availability is crucial for the applications running in the network, we now show that HWMP might not be the best choice.



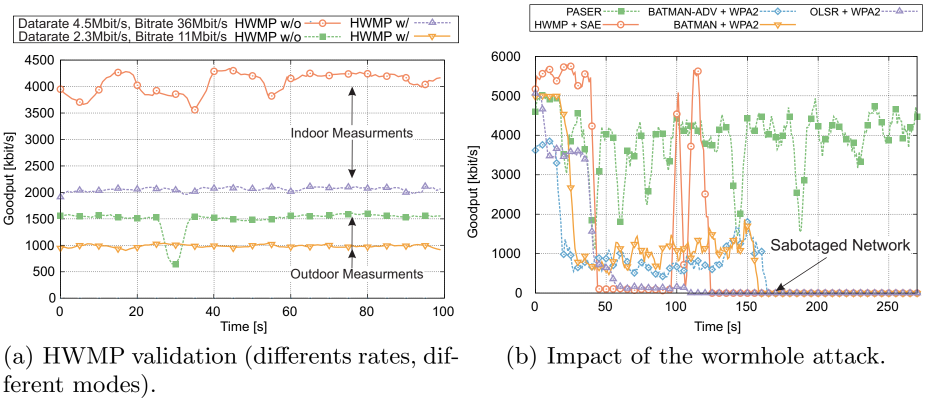
(a) Network3 in case of 4.5 Mbit/s data rates (optimal parameterization).

(b) Impact of different parameterizations in network3.

(c) Network4 in case of 4.5 Mbit/s data rates (reactive protocols).

(d) Network4 in case of 4.5 Mbit/s data rates (proactive protocols).

Fig. 4. PDR in networks 3 and 4 (error-free channel, mobile).



(a) HWMP validation (differents rates, different modes).

(b) Impact of the wormhole attack.

Fig. 5. Validation of HWMP behaviour in network2 and impact of the wormhole attack in a real testbed.

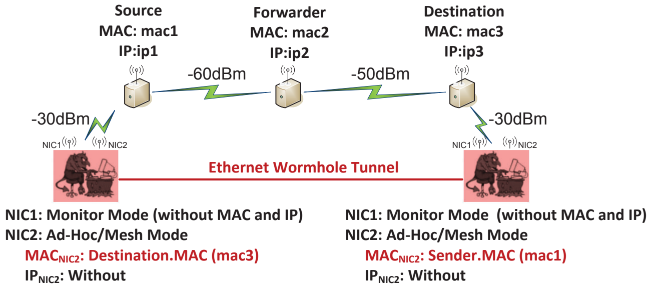


Fig. 6. Setup of the wormhole attack scenario.

5.1 The Wormhole Attack

In a wormhole attack, two malicious nodes connected via fast tunnel transparently forward routing messages faster than legitimated nodes from one area of the network to another one. This causes affected nodes located in different areas to believe they are neighbours and start sending their messages via the wormhole tunnel instead of using legitimated relay nodes. The attacker might than, in worst case, drop all data packets causing a sabotage of the network. It is well known that non-secure routing protocols are prone to this attack as we showed in simulation in previous work [6]. Nevertheless, it has not been yet investigated in practice if a combination of non-secure protocols with standard security mechanisms such as IEEE802.11i-personal mode (WPA2 pre-shared key) [17] or the IEEE80211s' security framework (SAE) [5] can mitigate this attack and it is not known yet what minimal number of relay nodes is necessary for the attack to succeed in that case. To this end, we setup the testbed provided in Figure 6. We considered the worst case scenario from an attacker perspective, that is, there is only one relay node between the sender and destination. The malicious nodes have 2 wireless LAN cards each. The first one is set in monitor mode to capture all frames in the proximity and send them to the other end of the tunnel via Ethernet. Note that since the frames are encrypted and the attacker is only interested to forward routing messages but to drop data packets, the attacker forward the frames based on their sizes. Since routing messages have a relatively small size, the attacker only forward frames having a size less than 1024 Bytes. To acknowledge unicast frames so that legitimated nodes do not notice the attack and since forwarding the ACK frame via the tunnel takes longer time than an ACK timeout, the malicious nodes have another wireless LAN card set in adhoc/mesh mode and having the same MAC address as the legitimated node at the other end of the tunnel. This interface acknowledge each unicast frame it receives. Since ACK frames are never encrypted, regardless if WPA2 and SAE are active or not, the setup works. During the evaluation, the network is operated with auto bitrate (minstrel) and a traffic load below the $\text{networkThroughput}_{\text{optimal}}$. The duration of each measurement is 300 s. For WPA2 pre-shared key, we used hostapd-2012.09.10 and for SAE, we used the cozybit authsae-2013.06.05 implementation. The attack is started after 15 to 20 s of the Iperf-UDP application start time. The results of the evaluation are provided in Figure 5(b). Three observations can mainly be derived from this figure. First, PASER shows to be robust against the wormhole attack. Second, non-secure routing protocols in combination with the IEEE802.11 standard security frameworks are prone to this attack even if there is only one relay node between the sender and destination. Third, how fast the wormhole is established depends on the protocol design. In case of OLSR, since the route quality is the sum of the quality of all one hop links that build the route, the attack occurs the fastest. In case of BATMAN (layer3) and BATMAN-ADVANCED (layer2), the route is selected based on the number of OGMs received within a sliding interval, thus, it takes a bit longer time to use the wormhole tunnel than in case of OLSR. In case of HWMP and due to its airtime link metric, the success of the attack is very fast, however, if routing messages forwarded via the wormhole collide with frames send by the relay node, the legitimated node might switch the route and use the right one for a short period. Nevertheless, this occurs infrequent and the network is considered sabotaged. Bearing this in mind and taking also into consideration that WPA2 pre-shared key and SAE are password-based, which means that revealing the password/key will cause the operator to re-setup the whole network, and since PASER endorses a key management scheme and it is robust against routing attacks, it might be more reasonable to choose PASER for routing in chain mesh networks in case security critical applications are running, instead of HWMP.

6 Conclusion

This paper investigates for chain mesh networks the performance of the well-established non-secure routing protocols OLSR, BATMAN and HWMP as well as the secure protocol PASER. The results justify that reactive or hybrid routing protocols perform better than proactive protocols in chain mesh networks having static source-destination pairs and a moderate number of forwarding hops. The paper shows that HWMP performs the best in the analyzed scenarios in case security is not a concern. However, in case network availability is crucial and due to the security flaws of the IEEE802.11 security frameworks in mesh networks, as we experimentally show, PASER is a more suitable candidate. In future work, we intend to design a novel multi-tier security framework that combines PASER and the IEEE802.11 security frameworks.

Acknowledgment

Our work has been conducted within the AIRBEAM project, which is funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261769. We also acknowledge the Sec2 project, which is funded by the German Federal Ministry of Education and Research (BMBF). We would like to thank Kai Scharwies from the IMST GmbH company for his technical assistance.

References

1. M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” *Elsevier Ad Hoc Networks*, vol. 2, no. 1, 2004.
2. T. Clausen and P. Jacquet, “Optimized Link State Routing (OLSR) Protocol,” RFC 3626, 2003.
3. C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) routing,” RFC 3561, 2003.
4. (2013) Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.). Freifunk Community. [Online]. Available: http://www.open-mesh.org/
5. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11, 2012.
6. M. Sbeiti, J. Pojda, and C. Wietfeld, “Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks,” in *IEEE PIMRC*, 2012.
7. N. Goddemeier, K. Daniel, and C. Wietfeld, “Role-based connectivity management with realistic air-to-ground channels for cooperative uavs,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, 2012.
8. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-2007, 2007.
9. A. Huhtonen, “Comparing aodv and olsr routing protocols,” in *Seminar on Internetworking*, 2004.
10. E. Borgia, “Experimental evaluation of ad hoc routing protocols,” in *IEEE PERCOMW*, 2005.
11. P. Johansson *et al.*, “Scenario-based performance analysis of routing protocols for mobile ad-hoc networks,” in *ACM/IEEE MobiCom*, 1999.
12. J. Hsu *et al.*, “Performance of mobile ad hoc networking routing protocols in large scale scenarios,” in *IEEE MILCOM*, 2004.
13. C. Mbarushimana and A. Shahrabi, “Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks,” in *AINAW*, 2007.
14. J. Pojda *et al.*, “Performance analysis of mesh routing protocols for uav swarming applications,” in *ISWCS*, 2011.
15. J. C. P. Wang, B. Hagelstein, and M. Abolhasan, “Experimental evaluation of ieee 802.11s path selection protocols in a mesh testbed,” in *ICSPCS*, 2010.
16. Y. C. Huang, S. N. Bhatti, and D. Parker, “Tuning olsr,” in *IEEE PIMRC*, 2006.
17. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11g, 2003.
18. R. T. Morris, J. C. Bicket, and J. C. Bicket, “Bit-rate selection in wireless networks,” Masters thesis, MIT, Tech. Rep., 2005.
19. A. Varga and R. Hornig, “An overview of the OMNeT++ simulation environment,” in *SIMUTools*, 2008.
20. K. Xu, M. Gerla, and S. Bae, “How effective is the ieee 802.11 rts/cts handshake in ad hoc networks,” in *IEEE GLOBECOM*, 2002.
21. H. Zhao *et al.*, “Evaluating the impact of network density, hidden nodes and capture effect for throughput guarantee in multi-hop wireless networks,” *Elsevier Ad Hoc Networks*, vol. 11, no. 1, 2013.