Future Generation Computer Systems 92 (2019) 593–603

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Design and experimental performance analysis of a B.A.T.M.A.N.-based double Wi-Fi interface mesh network

Luca Davoli *, Antonio Cilfone, Laura Belli, Gianluigi Ferrari

Internet of Things (IoT) Lab, Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124 Parma, Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Research Unit of Parma, Parco Area delle Scienze, 181/A, 43124 Parma, Italy

HIGHLIGHTS

- Enhancement of the functionalities of a mesh node through a dual interface approach.
- Integration of mesh-unaware clients in a WMN through the AP interface of the mesh nodes.
- Efficient inter-interface (external/mesh) routing to provide Internet access to mesh-unaware clients.
- Evaluation of an efficient smart parking monitoring system.
- Performance evaluation of a multi-hop communication in mesh networks.

ARTICLE INFO

Article history:
Received 14 October 2017
Received in revised form 12 January 2018
Accepted 8 February 2018
Available online 17 February 2018

Keywords:
IoT
WSN
Mesh networks
B.A.T.M.A.N.
Double interface

ABSTRACT

Mesh networks and, in particular, Wireless Mesh Networks (WMNs) are gaining a growing interest because of their scalability, robustness, and ease of deployment. These characteristics make WMNs suitable for several applications, such as distributed sensing, monitoring, and public safety. In this paper, we describe a novel WMN implementation based on the use of low-cost double Wi-Fi interface embedded IoT-oriented devices. At each node, one interface provides external connectivity, whereas the other interface is used to create a mesh backbone. On the mesh side, the Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) routing algorithm is used to route the traffic flows from external clients (possibly towards an Internet gateway), which can be IoT nodes and/or mobile nodes (e.g., smartphones and tablets). After providing a description of the architecture and relevant implementation details, we carry out an extensive experimental campaign to evaluate the WMN performance, especially in terms of the trade-off between throughput and number of hops.

1. Introduction

Nowadays, in the context of mesh networking, an important role is played by Wireless Mesh Networks (WMNs), in which nodes composing the network itself can all connect to each other through multiple hops. In a WMN, each node composing the backbone of the network operates not only as a host, but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destination endpoints. One of the main advantages of WMNs is that they do not need an infrastructure: the deployment phase, thus, is faster, less expensive and less invasive with respect to networks (either wired or wireless) that operate in a centralized way and need infrastructures. Another advantage of WMNs is that, inside these networks, it is possible to modify the composition of the network itself, by adding, removing or changing the positions of the nodes in a seamless way for the final user. In fact, if the topology changes, a WMNs can re-organize itself leaving the users unaware of these changes.

The organization process of a WMN is handled by a routing protocol, whose aim is to discover and determine the best routes, according to link-based or route-based metrics (e.g., throughput, link quality, number of hops) applied to the traffic flows. Therefore, traffic flows in WMNs behave similarly to the way packets travel around the Internet: data flows hop from one host to another one until they reach their given destination. Dynamic routing capabilities, included in each Internet device, allow this to happen [1,2].

Over the past years, the potential of WMNs has continuously grown, becoming a reality in several scenarios. Moreover, the community supporting mesh networks is extremely active in conducting studies and adapting standards development and additional researches. An example is BattleMesh [3], an annual event that

* Corresponding author at: Internet of Things (IoT) Lab, Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124 Parma, Italy.
E-mail addresses: luca.davoli@unipr.it (L. Davoli), antonio.cilfone@unipr.it (A. Cilfone), laura.belli@unipr.it (L. Belli), gianluigi.ferrari@unipr.it (G. Ferrari).

https://doi.org/10.1016/j.future.2018.02.015
0167-739X/

aims at bringing together people from across the world to test the performance of different routing protocols for ad-hoc networks through a *Wireless Battle of the Mesh*.

Thanks to the ease of deployment and scalability, mesh systems, also including those based on radio technologies different from Wi-Fi, had their main applications in military, public safety, surveillance and distributed sensing [4–7], where the geographic area that needs to be covered is not easy to be accessed.

In general, the clients of a WMN could be of two types. The first type is represented by conventional clients with the same radio technologies as mesh routers, that can directly communicate with mesh nodes. The second type is represented by clients using radio technologies different from that of the WMN. These clients require intermediate mesh nodes (e.g., mesh routers) as "intermediaries" towards the Internet. In this way, mesh routers establish peer-to-peer overlay backbone networks for these client mesh nodes. In this type of architecture, mesh nodes constitute the actual network to perform routing and configuration functionalities, as well as providing end-user applications to customers. Hence, a mesh router is not required for these types of networks. A hybrid WMN is the combination of infrastructure and client meshing. Mesh clients can access the network through mesh routers, as well as directly communicating with other mesh clients.

In the last decades, despite the massive efforts in analyzing and developing WMNs, there has not been a mass market deployment of this class of networks. This is due to the fact that end-users are more interested in general-purpose applications, where high bandwidth and open access to the Internet are essential requirements. To foster the use of WMNs, a suitable solution may be to move to new paradigms in which multi-hop networks are not isolated and self-configured but, rather, can be used as a flexible and low-cost extension of pre-existing wired infrastructures [8].

In this paper, we propose a novel WMN architecture, based on double Wi-Fi interface mesh nodes. At each node, one Wi-Fi interface is used to provide access to the WMN, as an Access Point (AP) for external clients, whereas the other Wi-Fi interface is used to create a wireless mesh backbone with the other mesh nodes. Among available routing algorithms for the internal mesh networking we selected the Better Approach To Mobile Ad-Hoc Networking (B.A.T.M.A.N.) advanced routing algorithm [9]. This choice is mainly motivated by the fact that B.A.T.M.A.N. is a Layer-2 algorithm: in this way, each backbone mesh node acts as a switch with direct knowledge of the radio channel. Moreover, B.A.T.M.A.N. has the following attractive features: (i) it is more robust than other protocols, such as Optimized Link State Routing Protocol (OLSR) [10] or Ad-Hoc On Demand Distance Vector (AODV) [11], since it does not transmit any packet in the absence of a route towards its intended destination; (ii) it has a buffer, in order to avoid data loss in the case of link failure; and (iii) it is already available in the Linux kernel.

B.A.T.M.A.N. has been developed by the German Freifunk community [12] to overcome the limitations of the OLSR, such as the presence of routing loops or the relatively long time needed during route discovering. Although B.A.T.M.A.N. is specifically designed to fit WSN scenarios (and, therefore, is also attractive for Internet of Things (IoT) applications [13]), we show that it can effectively be used also to support mobile communications (namely, to provide connectivity to smartphones and/or tablets). Even though B.A.T.M.A.N. mesh networking is not compliant with the IEEE 802.11s specifications, our proposed mesh networking approach allows to provide transparent connectivity to external devices equipped with IEEE 802.11b/g/n radio interfaces—these devices are the vast majority of commercial mobile devices.

The rest of the paper is organized as follows. In Section 2, background information on the standards and the protocols used in mesh networking is provided. Section 3 contains a comprehensive analysis of current implementations of WMNs presented in the literature. Section 4 describes the details of our WMN implementation. In Section 5, we propose an application scenario and provide experimental performance evaluation results. Finally, in Section 6 we draw our conclusions.

2. Background

2.1. IEEE 802.11s

We first recall the main characteristics of IEEE 802.11s [14], which represents the reference Wi-Fi mesh standard. This allows to better understand, in a comparative way, the characteristics of B.A.T.M.A.N., as well as to highlight differences and similarities among the two approaches.

2.1.1. IEEE 802.11s basics

The demand for larger wireless infrastructures has led, in the last decade, to the development of an amendment of the IEEE 802.11 [15] standard designed for Wi-Fi mesh networks, namely IEEE 802.11s [16]. This amendment introduces new frame forwarding and routing capabilities at the MAC layer, together with new inter-working and security techniques, in order to support mesh capabilities. The IEEE 802.11s standard does not change L1 (PHY layer) of IEEE 802.11, but just modifies L2 (MAC layer). The most important novelty is that the traffic routing is performed at L2 instead of L3 (network layer). The MAC layer needs to have an accurate knowledge of its "radio neighborhood:" in order to perform efficient routing, the nodes must take into account the quality of wireless links to/from their neighbors. In this way, the implementation of routing policies at L2 makes this approach transparent to higher layer protocols.

In an IEEE 802.11s mesh network there are, as expected, different logical components. Besides a sufficient number of Mesh Points (MPs), composing the mesh backbone, there are other MPs with augmented functionalities. One type of enhanced MPs act as APs for classical IEEE 802.11 stations and are denoted as Mesh APs (MAPs), while there exist other components, denoted as Mesh Portal Points (MPPs), which act as gateways towards an external (typically wired) network.

For this reason, each entity composing the mesh network relies on a specific ISO/OSI stack implementation.

2.1.2. IEEE 802.11s topology formation

Similarly to other network protocols, IEEE 802.11s relies, for topology formation, on the exchange of small-size messages denoted as beacons. The mesh station's beacon carries information about the mesh network and helps other mesh stations to detect and join the mesh network their self. The discovery of the mesh stations is based on: (i) the observation of the beacon frames (passive scanning); or (ii) the transmission of probe frames (active scanning). Once a mesh station has found a suitable peer, it uses the Mesh Peer (Link) Management (MPM) protocol [15] to establish a peer link with another mesh station.

After the discovery/peering phase, beacon messages are periodically transmitted and used for topology maintenance and synchronization. Upon receiving beacon messages, the nodes obtain information about the current status of their neighborhood and, then, on the topology: in this way, they can refresh their connectivity associations, updating them when necessary (e.g., due to mobility needs). In particular, peering is maintained as long as mesh stations are in the range of each other and share the same mesh profile.

2.1.3. IEEE 802.11s routing algorithm

All the devices inside a mesh network use the same path metric and routing protocol. IEEE 802.11s defines default solutions for both, which, however, can be replaced by other solutions. The default metric, called "airtime metric", indicates the total cost of a link by taking into account some parameters such as data rate, overhead or frame error rate, measured on a frame of 1 KByte—for an accurate definition of the airtime metric, see [17]. The default routing algorithm is the Hybrid Wireless Mesh Protocol (HWMP) [18]. HWMP is based on the AODV protocol combined with a proactive tree-based solution, in which a mesh station (typically a station that acts as MPP) propagates routing messages to all mesh stations, in order to establish and maintain the links.

2.2. B.A.T.M.A.N.

2.2.1. Basics

B.A.T.M.A.N. is a proactive L2 routing protocol for WMNs. It keeps information about the existence of nodes in the mesh network that are accessible via single-hop or multi-hop communication links. The B.A.T.M.A.N. approach consists in allowing each node to determine, for each destination in the mesh network, a node which represents its best next-hop, which can be identified as gateway to communicate with the destination node, without requiring the knowledge of the complete route. In this way, there is no need of transmitting and keeping information about the whole topology at each node, as each node performs routing independently from the other ones. Therefore, each node needs to keep updated, for each destination, the best next-hop; this reduces significantly the amount of control traffic and makes synchronization faster.

In order to perform the discovery of its neighbor, every B.A.T.M.A.N. node periodically broadcasts an OriGinator Message (OGM), corresponding to a 12 byte UDP payload (for a total packet size equal to 52 bytes, including IP and UDP headers). The OGM has relevant information, such as a sequence number which is expedient to distinguish new OGMs and to guarantee that OGMs are counted twice and, potentially, if a node is a gateway towards Internet or not. In this way, each node informs its link-local neighbors about its existence [9].

Due to the need to maintain B.A.T.M.A.N. protocol as light as possible, each B.A.T.M.A.N. packet is encapsulated in a single UDP data packet and consists of an OGM and zero or more attached Host Network Announcement (HNA) messages—HNA is a message type used to announce a gateway to a network. The formats of the OGM and the HNA message are shown in Figs. 1(a) and 1(b), respectively.

B.A.T.M.A.N. uses, as the default path metric, the Transmission Quality (TQ) metric, which is based on Expected Transmission Count (ETX) [19], to find a trade-off between a short route, in terms of hops, and a (potentially) long route with good links. In order to perform the discovery of its neighbors, each node periodically broadcasts an OGM, thereby informing its link-local neighbors about its existence, and counts the OGMs received from a given neighbor: the number of received OGMs by a given neighbor is denoted as Receive Quality (RQ). The calculation of the RQ value takes place by using a sliding window of 64 bits size (which leads to 2^{64} possible entries). The sliding window keeps track of the last received sequence numbers of OGMs and the current received from each node in the network. The in-window sequence numbers are those which fit in the window below the current sequence number. If an out-of-range sequence number is received, it is set as the current sequence number and the sliding window is moved accordingly. Sequence numbers that are not in the sliding window any more, are deleted. Neighbors re-broadcast received OGMs so that nodes more than one hop away get information about the existence of far nodes. In order to avoid overcrowding the network, each node resends only OGMs from its neighbor with the best TQ metric. In particular, a B.A.T.M.A.N. node evaluates the TQ metric of a neighbor as the fraction of its OGMs that are correctly received by this neighbor as:

$$TQ = \frac{EQ}{RQ}$$

where EQ is the Echo Quality of a certain node A, which is measured counting the received broadcasts of its own messages within the sliding window. Finally, the best hop is determined applying penalties for asymmetric links and taking into account the number of hops needed to reach the destination node.

2.2.2. Gateway node in B.A.T.M.A.N.-based mesh networks

As stated before, a B.A.T.M.A.N. node can announce itself as a *gateway* (GW) towards Internet. According to this, a B.A.T.M.A.N.-based mesh network could be seen as a network composed by a few mesh nodes that act as GW-servers and other nodes that will act as GW-clients.

A GW-client node tunnels all IP packets with a destination address that matches the default route to Internet, through a selected GW node (that can be both a GW-server or a GW client). Thus, the GW-client node encapsulates Internet traffic into an UDP/IP datagram and forwards the encapsulated data to the selected GW node. Then, the GW node identifies the encapsulated packets based on the port number of the outer UDP header and, finally, extracts the original packet and forwards it to its original destination.

For encapsulation purposes, a GW-client node must set the outer IP header's source and destination addresses to the originator addresses of the GW-client and the GW-server, respectively. If the size of the original IP packet does not fit into the payload section of the outer UDP datagram, the packet is dropped. For this reason, if virtual interfaces are used to integrate an implementation of the B.A.T.M.A.N. protocol into a network environment, then the Maximum Transfer Unit (MTU) of the virtual interface should be set to the maximum payload size of the inner UDP datagram.

2.3. Security aspects in B.A.T.M.A.N

As in IEEE 802.11s, the security in B.A.T.M.A.N. protocol can also be enhanced using common encryption and authentication technologies, in order to ensure that routing information is accepted only from trusted nodes [20]. In order to increase the level of security, all information on the physical layer itself may also be encrypted. However, the encryption is not a primary goal of B.A.T.M.A.N, which is a routing algorithm. B.A.T.M.A.N.'s protocol design inherently limits the impact of different attacks.

In the network, a B.A.T.M.A.N. node knows the existence only of nodes that are in its communication range. In other words, a node's topology view is limited to a single-hop horizon and not to the entire network topology. Regardless of this visibility constraint, B.A.T.M.A.N. accepts packets from arbitrary sources and builds its routing tables by analyzing the statistics of all received OGMs.

3. Related work

Research in WMNs has been very active in the last years, because of their applicability in all situations in which wired infrastructures are not feasible or unattractive. In particular, B.A.T.M.A.N. has been widely investigated and compared with other routing protocols, such as AODV, OLSR, Dynamic MANET On-demand (DYMO) and open80211s (which is an implementation of the IEEE 802.11s standard [21]). The comparison has been carried out both through simulations and real implementations [22,23]. In particular, B.A.T.M.A.N. has been compared, in the context of Mobile Ad-hoc NETworks (MANETs), with AODV investigating the effect of

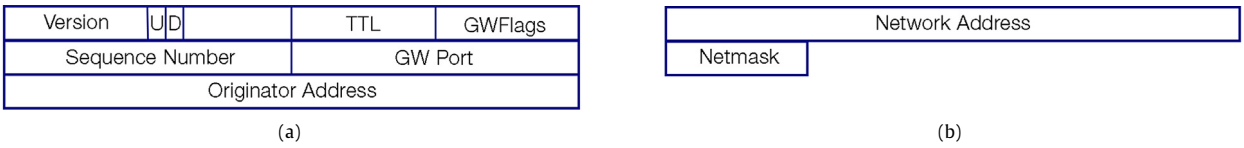

Fig. 1. Packet formats: (a) OGM and (b) HNA message.

mobility and topology variations on the performance of both routing protocols through experiments in a real environment [24]. The obtained results show that, when routes change often, B.A.T.M.A.N. outperforms AODV: this is mainly due to the fact that AODV introduces delays (likely due to its reactive routing nature) and does not buffer traffic packets. Nevertheless, this deployment is composed by nodes that are in direct visibility and are more powerful than Smart Objects (SOs) typical of IoT environments [25].

Another relevant aspect for the selection of the appropriate routing protocol is the impact of the number of hops on the system performance. Considering B.A.T.M.A.N. and AODV, focusing on the quality of multi-hop routes and evaluating the performance with different indicators (e.g., packet loss rate, delay and reachability), B.A.T.M.A.N. outperforms AODV in all the cases where multi-hop communications are required [26]. Moreover, B.A.T.M.A.N. can overcome the shortcomings proper of OLSR, such as the routing loops, long time to discover routes and the absence of packet buffering [27].

Considering an experimental testbed composed of a grid of Wi-Fi nodes close to each other, the obtained results show that B.A.T.M.A.N. outperforms OLSR in terms of delay, throughput, and other metrics [27]. Moreover, B.A.T.M.A.N. outperforms OLSR even in a real-world WSN implementation, with nodes in direct visibility [28] and under a heavy traffic condition.

An interesting comparison is between B.A.T.M.A.N. and open80211s. For what concerns the performance of both protocols, in terms of recovery time and route stability in specific situations and in a controlled environment, even under the use of commercial devices, under static scenarios, B.A.T.M.A.N. has the best performance. However, in the presence of node failure, open80211s seems to recover more rapidly than B.A.T.M.A.N. [29].

Finally, B.A.T.M.A.N. has been adopted in outdoor WMN, for weather monitoring [30]. In this scenario, mesh networking represents a good approach to the design of data harvesting systems in terms of network reachability, Received Signal Strength Indicator (RSSI) level, and data rates. It is remarkable that laptops are used as end-devices, making the applicability of the obtained results limited.

Most of the results presented in the works outlined above are based on simulations or real implementation in controlled testbeds. The main common characteristic of all those implementations is that B.A.T.M.A.N. devices have a single Wi-Fi interface, which simultaneously supports mesh network traffic and provides external connectivity. Moreover, there is no reference to the integration of external clients without mesh capabilities. Our work goes one step further, by designing, implementing, and analyzing a B.A.T.M.A.N.-based WMN composed of nodes equipped with two separate Wi-Fi interfaces. This has the advantage of enabling non-B.A.T.M.A.N. nodes to join the WMN as end-clients and leaving them completely unaware of the actual topology of the "internal" mesh backbone.

4. Mesh network implementation

As stated at the end of the previous section, the aim of the proposed work is the implementation and experimental performance analysis of a WMN which: (i) is based on a wireless backbone of B.A.T.M.A.N. nodes; and (ii) allows the integration of non-B.A.T.M.A.N. devices as external clients which send traffic to the Internet through a MP denoted as MPP (we borrow the IEEE 802.11s notation). In the proposed architecture, every backbone MP is implemented using a Raspberry Pi 3 (RPi) board [31], equipped with two Wi-Fi interfaces.

More in detail, the proposed architecture can be described as a juxtaposition of networks:

- a backbone network, which forwards data (towards proper destinations, e.g., the MPP) and operates in the radio channel centered at 2.412 GHz (namely channel 1 of IEEE 802.11b standard) and with a transmission power of 7 dBm;
- an access network per MAP, operating in the radio channel centered at 2.437 GHz (namely channel 6 of IEEE 802.11b standard), with transmission power of 7 dBm and providing an "access bridge" between end-users and the mesh backbone.

The proposed WMN architecture is shown in Fig. 2.

In the following, the overall architecture will be described considering two macro blocks, which can be separated depending on the used Wi-Fi interface: the internal B.A.T.M.A.N.-based mesh (backbone) network, composed by MPs, and a set of non-B.A.T.M.A.N. (i.e., mesh-unaware) client nodes. It is important to observe that, in the proposed architecture, all MPs are, in practice, MAPs, in order to enable clients' connection.

4.1. B.A.T.M.A.N-based backbone network

The backbone mesh network, formed by blue dotted links in Fig. 2, is composed of a MPP and one or more B.A.T.M.A.N. MAPs. The MPP, acting as a gateway, is the unique wired node, namely the only one with a direct connection to the Internet through an Ethernet cable. The MPP and each MAP are equipped with two wireless interfaces:

- the on-board Wi-Fi interface of the RPi, denoted as `wlan0`, is used as the network interface to execute B.A.T.M.A.N., in order to build the backbone network among all MAPs and the MPP;
- an additional network interface, denoted as `wlan1` and implemented on top of a TP-Link TL-WN722N [32] USB adaptor, is used to provide the MPs with Access Point (AP) features. Thanks to the *hostapd* daemon [33], each MP can create an IEEE 802.11b/g/n Wireless Local Area Network (WLAN) which external mesh-unaware clients (e.g., regular smartphones or tablets) could attach to, in order to connect to the Internet.

Since an attractive extension (currently under investigation) of the proposed architecture is the introduction of roaming among the backbone nodes, the MPP is the only node running a DHCP server, whose aim is to distribute IP addresses to the mesh interfaces (`wlan0`) of all MAPs. The distribution of IP addresses to nodes that are farther than one hop is obtained through the presence of some specific daemons, namely DHCP relays, running on the mesh interface of MAPs. In this way, when a new MAP joins the network and asks for an IP address, an intermediate MAP – except for the case of a new MAP with direct visibility to the MPP – forwards this request to the MPP, that releases a new IP address and transmits it to the requester.

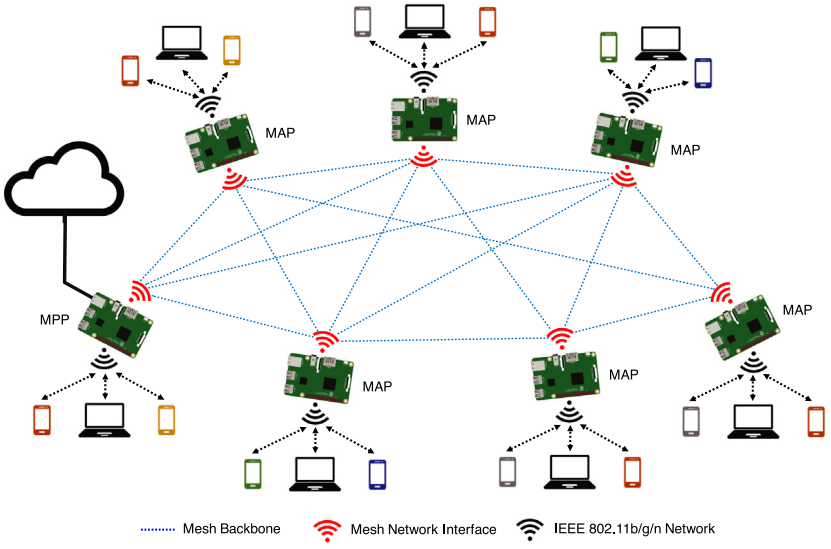

Fig. 2. Proposed multi-hop mesh network architecture with double interface Wi-Fi nodes.

Table 1
Backbone mesh network configuration.

	Interface	Network	IP class	Services
MPP	`wlan0`	Mesh	192.168.3.0/24	DHCP Server, *batctl*
	`wlan1`	Client	192.168.2.0/24	DHCP Server, *hostapd*
MAP	`wlan0`	Mesh	Assigned by DHCP (192.168.4.0/24)	DHCP Relay, *batctl*
	`wlan1`	Client	192.168.2.0/24	DHCP Server, *hostapd*

In Table 1, the network configurations of B.A.T.M.A.N. MPP and MAP are shown, with reference to the associated (addressable) IP classes and the services that running on their network interfaces.

Similarly to what was defined for the `wlan1` interface of the MPP, in order to provide the connectivity to non-mesh clients, each MAP runs (i) a *hostapd* daemon on its `wlan1` interface, turning this NIC into an AP and an authentication server, and (ii) a DHCP server, which is used to assign IP addresses to external non-B.A.T.M.A.N. (mesh-unaware) clients.

In order to route properly the traffic coming from non-mesh external clients, as well as to allow these clients to connect to the Internet, in the proposed architecture the Linux *iptables* are used. The following routing rules have been defined in the MPP:

- the traffic coming from `wlan0` and `wlan1` is sent on the Ethernet interface, namely `eth0`;
- the traffic coming from `eth0` is sent on `wlan0` or `wlan1` only in the presence of already established traffic flows.

4.2. Non-B.A.T.M.A.N external clients

As previously anticipated, in the proposed B.A.T.M.A.N.-based mesh network architecture also non-mesh external clients can attach to the backbone WMN to reach the Internet. These nodes, generally corresponding to smartphones, tablets, or PCs, have to simply connect to the Wi-Fi network provided through the `wlan1` interface of the nearest MAP. Due to the presence of DHCP management functionalities, together with other ones implemented in the mesh network, external non-B.A.T.M.A.N. clients can connect in a transparent way, without performing any additional configuration or installing specific software.

5. Performance evaluation

In this section, a brief introduction on the experimental scenario defined for the performance evaluation is done, followed by the description and the analysis of the obtained results.

5.1. Experimental scenario

As a representative and relevant application scenario for WMNs, here we consider smart monitoring of parking areas in a city. As shown in Fig. 3, the proposed scenario is characterized by the presence of different parking zones that have to be monitored: each of these "islands" is composed of different parking lots, each monitored by a device equipped with a sensor and a short-range radio interface (e.g., IEEE 802.15.4). Moreover, due to the intrinsic constraints of these devices, each parking sensor sends its parking data (namely, presence/absence of a car) to a more powerful node, denoted as Monitoring System (MS). The MS, implemented with a RPi, can perform local processing (in a Fog Computing fashion [34]), and is also equipped with a camera, in order to stream the environmental situation. Therefore, the MS has to send the data received from its monitored parking zone to a system, denoted as Data Aggregator Station (DAS), which is responsible of collecting data from different MSs. The DAS, in turn, can process the received data and, then, forward them to (logically) centralized repositories (e.g., to Cloud services [35]), in order to enable centralized monitoring (e.g., in a control room) and advanced analytics and security [36] on the overall data (according to a Big Data perspective [37]). Since it can be assumed that parking zones are generally located in different areas of a city, it is thus reasonable to assume that, in these cases, a direct link among the MS and a DAS does not exist. In these cases, multi-hop communications become mandatory and, in the proposed architecture, they are enabled by the deployment of several Repeaters between MSs and DASs.

With reference to the proposed network, the DASs are MPPs, while the MSs and the Repeaters are MAPs connected in a WMN. The choice of enabling an MS to be a MAP aims at enabling end-users to monitor the situation of the selected parking [38], to navigate on Internet while they are inside one of the enabled parking islands, and providing Internet navigation for external clients that are in the coverage area of each Repeater. This has the advantage of providing a service for the collectivity, while, in the presence of bottlenecks or infrastructure problems, the network administrators could downgrade the Repeaters from MAPs to MPs, thus relieving this traffic load for a limited time.

Fig. 3. Multi-hop scenario of interest with highlighted parking areas (in green). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

5.2. Experimental performance metrics

In order to experimentally evaluate the performance of the proposed WMN, we first consider the traffic data exchanged among core MAPs and between external non-B.A.T.M.A.N. external clients and backbone MAPs. In particular, our ultimate goal is to investigate the impact of the number of hops on the system performance. The *iperf* tool [39] has been chosen, among different available traffic generators, due to its simplicity. With *iperf*, both TCP and UDP traffic can be generated.

For jitter and packet loss calculation, the UDP packets generated by *iperf* contain, among their fields, a timestamp and a sequence number (denoted as *pcount* by *iperf* notation) inside the payload sent by the sender to the receiving server, that is listening on port 5001. Once the UDP server receives the datagram, it extracts from the payload the timestamp, useful for jitter estimation, and the sequence number, needed for packet loss calculation. More in detail, the *iperf* traffic generator calculates the jitter by comparing the timestamp, contained into the packet, and the current time, in order to estimate the current delay, denoted as $D_{current}$. Then, the calculation of the difference $|D_{current} - D_{previous}|$ between $D_{current}$ and the delay calculated in the previous time interval, denoted as $D_{previous}$, is useful for the jitter estimation, since the difference cancels the clock in-sync between the client sender and the server receiver [40]. This has the additional advantage that synchronized clocks are not required, since the source packet delta times are known. Moreover, this computation does not require knowledge of the round-trip time.

5.3. Experimental results

In case of a network composed by nodes arranged in a linear topology,[1] the data rate at the nth hop can be approximated as R/n, where R is the source data rate (dimension: [bps]) [41]. The value R/n can be thus considered as an upper bound for the data rate, under the assumptions that: (i) each node can communicate only with its two neighboring nodes; and (ii) the relay node waits to receive the whole packet stream (associated, for example, with an image transmitted by the source) and, then, forwards it to the next node, rather than forwarding each single incoming packet of the stream. In a real-world mesh deployment, however, any node can communicate with more than two nodes. This can be considered as a worst case scenario, in which the data rate at the nth hop can be approximated as $R/2^{n-1}$.

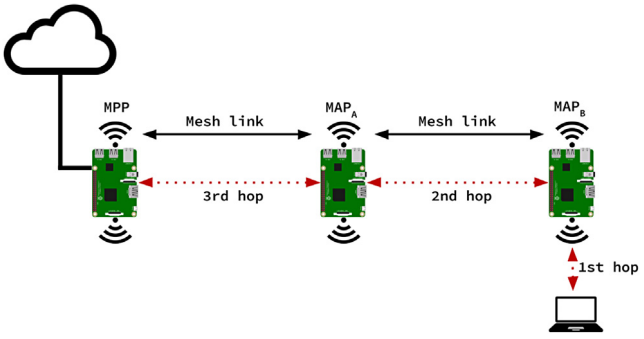

Fig. 4. Multi-hops communication test scenario with 3 hops.

In order to understand the impact of the number of hops on the data exchange between external non-B.A.T.M.A.N. clients and MAPs, we perform two different tests:

- without multiple-hops between the originator node and the target node;
- with multiple-hops between the external client and the target MAP.

In both cases, we carry out different experimental evaluations considering both TCP and UDP traffic and, for each transport protocol, testing single-hop and multi-hop communications for varying values of the network load. As already mentioned, we use *iperf* as traffic generator tool, activating the *iperf* server on the MP gateway node and running *iperf* in client mode on the specific external non-B.A.T.M.A.N. client device, as shown in Fig. 4.

Concerning the link quality, we adopt two types of links with received powers in the range of $-73 \div -75$ dBm: the first link is the one between the MP and its closest MAP, denoted as MAP_A in Fig. 4 and identified by the IP address `192.168.3.253`, with MAP_A having a received power of -75 dBm; the second link is the one between MAP_A and the farthest MAP, denoted as MAP_B in Fig. 4 and addressable with the IP address `192.168.3.252`, with MAP_B having a received power from MAP_A of -75 dBm.

5.3.1. TCP performance evaluation

In order to experimentally evaluate the performance of the proposed WMN in case of TCP traffic sent from an external mesh-unaware client, we perform a set of short tests, each with a duration of 60 s, and a set of long ones, each with a duration of

[1] This is meaningful for a multi-hop route in a network with a general topology, the only difference being the higher multiple access interference experienced in a general network.

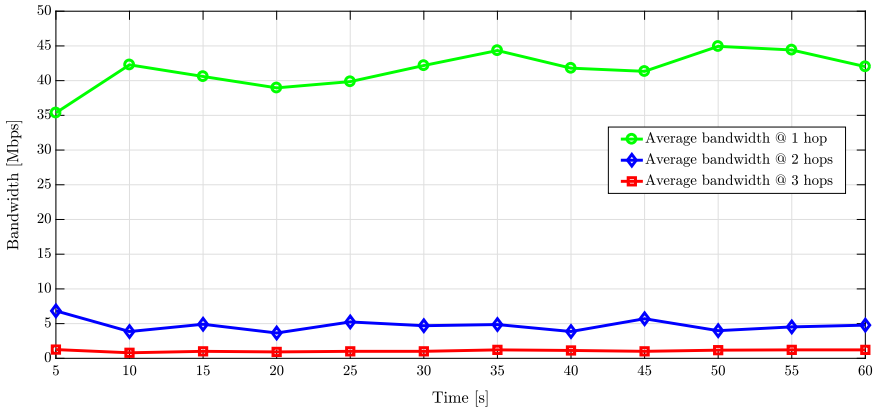

Fig. 5. Average throughput values, obtained in short time duration (60 s) tests, in the presence of TCP for various values of the number of hops.

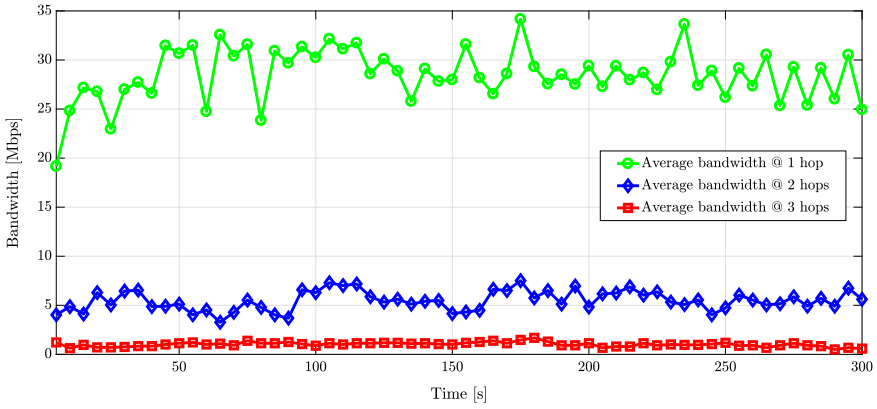

Fig. 6. Average throughput values (dimension: [Mbps]) obtained in long time duration (300 s), multi-hop TCP tests.

300 s. In Fig. 5, the results, in terms of average throughput (dimension: [Mbps]) obtained conducting short term tests, are shown. In Fig. 6, the experimental results, in terms of average throughput obtained with long term tests, are shown.

From the results in both Figs. 5 and 6, it is possible to observe that for each communication hop there is a scaling factor of $4 \div 5$. In other words, our experimental results predict that the throughput decreases as a function of the number of hops n, as $1/4^{n-1}$, rather than $1/2^{n-1}$, as predicted by theoretical results for linear topologies. This degradation is due to various reasons, including: control traffic, including TCP ACK flows and congestion control mechanisms; and the quality of the radio links [42].

Owing to the above considerations, we performed further experimental tests, in order to show that, in the presence of equal quality links, a single-hop link does not always represent the best communication choice. In the following, we present two illustrative cases (shown in Figs. 7 and 8) with two single-hop communication routes compared with one two-hop communication route.

- In Fig. 7, we compare the results, in terms of average throughput (dimension: [Mbps]), obtained conducting short term tests with: (i) a single-hop link with received power of -51 dBm; (ii) a single-hop link with received power of -75 dBm; and (iii) a two-hop route with received powers (in the two links) of -51 dBm and -59 dBm, respectively.
- In Fig. 8, we compare the results, in terms of average throughput (dimension: [Mbps]), obtained conducting short term tests with: (i) a single-hop link with received power of -63 dBm; (ii) a single-hop link with received power of -83 dBm; and (iii) a two-hop route with received powers (in the two links) of -63 dBm and -58 dBm, respectively.

In Fig. 9, we compare the results, in terms of average throughput (dimension: [Mbps]), obtained conducting short term tests with: (i) a single-hop link with received power of -83 dBm; (ii) a single-hop link with received power of -75 dBm; (iii) two-hop routes with received power (in the two links) of -63 dBm and -58 dBm, respectively; and (iv) two-hop routes with received powers of -51 dBm and -59 dBm, respectively.

From the results in Figs. 7 $\div$ 9, it can be observed that the inclusion of an intermediate B.A.T.M.A.N. mesh node can make the information transfer (from the originator node to the destination) more robust, leaving the external clients unaware of the existence of the WMN. In fact, even though the system performance in a multi-hop scenario is usually affected by the interaction between TCP ACK flows and congestion control, the performance, in the proposed scenario with two hops associated with good quality links (with received powers equal to -51 dBm and -59 dBm) is similar to that observed in the scenario with a single hop and received power of -75 dBm. Therefore, the addition of one hop does not have a critical impact on the system performance.

5.3.2. UDP performance evaluation

In order to test the performance of the proposed WMN in case of UDP traffic sent from an external non-B.A.T.M.A.N. client, we perform different tests, each with short duration (60 s) and bandwidth set to 1 Mbit/s, in order to measure jitter and packet loss ratio. In Fig. 10, the experimental results, in terms of jitter (dimension: [ms]), are shown in the case of 1, 2, and 3 hops. In Fig. 11, the performance results, in terms of packet loss ratio (adimensional), defined as the percentage (with respect to the total number of transmitted packets) of packets which are lost, are shown.

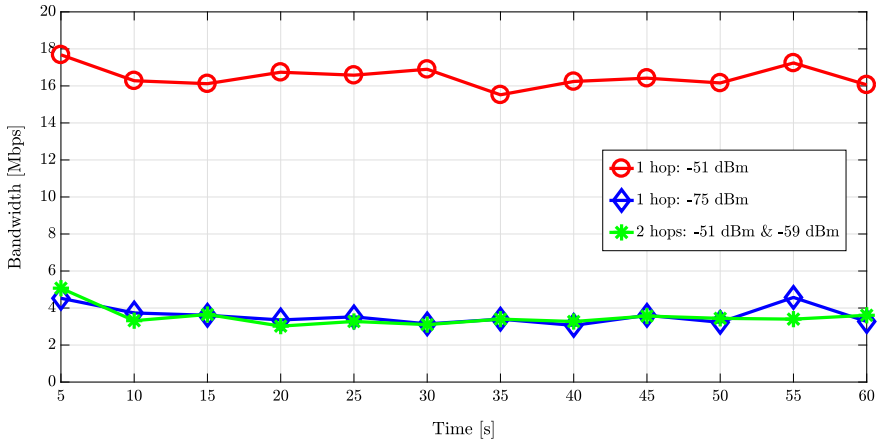

Fig. 7. Average throughput values, obtained in short time duration (60 s) tests, in the presence of TCP for various values of the number of hops and received power, in the range of −51 ÷ −75 dBm.

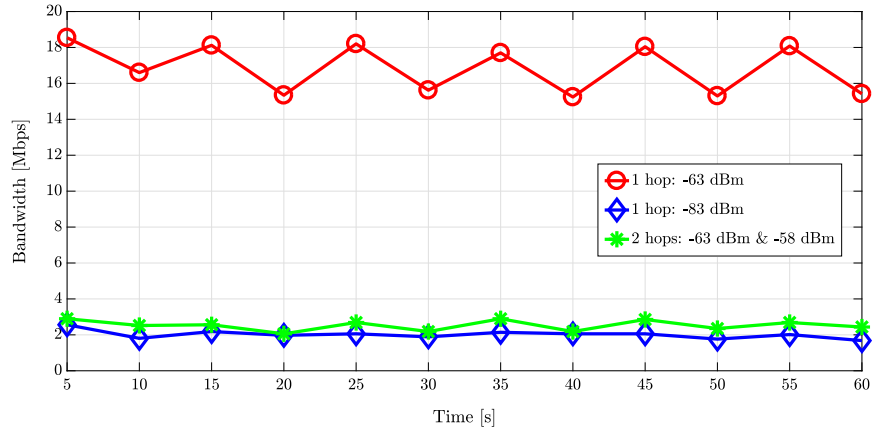

Fig. 8. Average throughput values, obtained in short time duration (60 s) tests, in the presence of TCP for various values of the number of hops and received power, in the range of −58 ÷ −83 dBm.

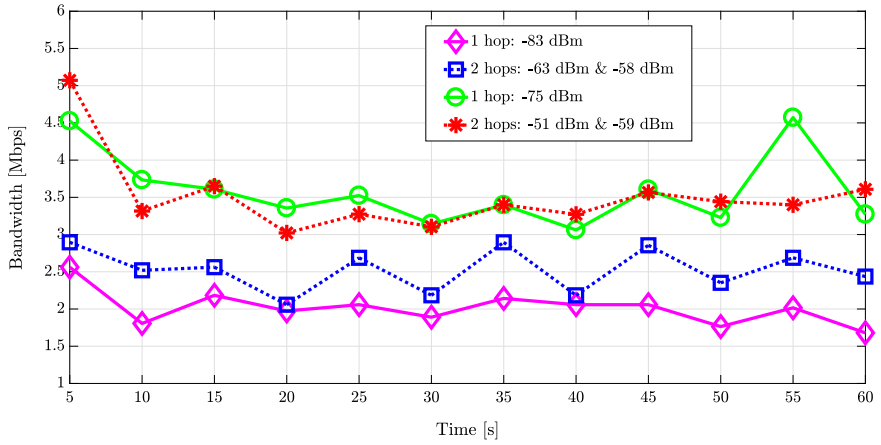

Fig. 9. Average throughput values, obtained in short time duration (60 s) tests, in the presence of TCP for various values of the number of hops and received power, in the range of −51 ÷ −83 dBm.

It can be observed that both jitter and packet loss ratio statistics are influenced by the number of hops in the communication network. More in detail, the jitter gradually increases with the number of hops. At a fixed number of hops, it is quite constant in the cases with a single hop and two hops, except for a spike in the seventh test of two-hop configuration—this is likely an outlier. Therefore, it can be concluded that the jitter has the higher variability in the three-hop experiment. Finally, from the results in Fig. 11, it is possible to observe that the packet loss is heavily affected by the number of hops. In fact for single- and two-hop configurations, the packet loss is negligible, being very close to a value of 0%. However, in the case with three hops, the packet loss ratio is significantly

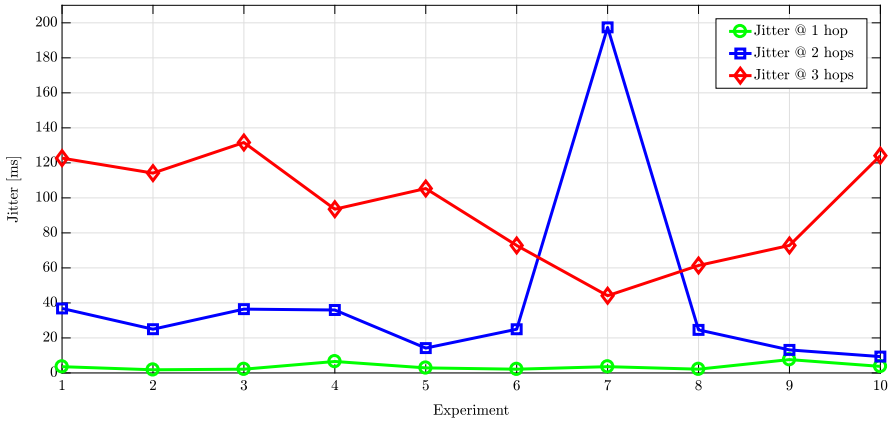

Fig. 10. Jitter over short time duration (60 s) tests, in the presence of UDP transmission. Various values of the number of hops are considered.

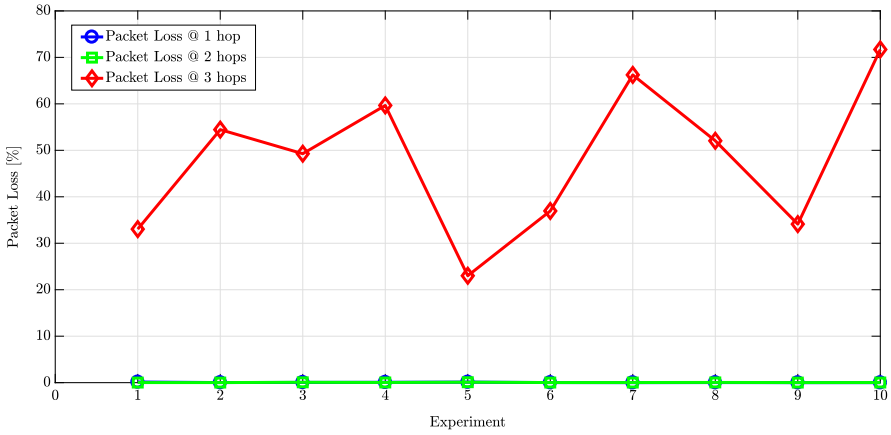

Fig. 11. Packet loss ratio over short time duration (60 s) tests, in the presence of UDP transmission. Various values of the number of hops are considered.

higher that those obtained in the other two setups. This behavior is likely due to both in the link quality, which (as intuitively expected) affects UDP traffic more than TCP traffic.

6. Conclusion and future works

Mesh networks – in particular WMNs – represent a very active research topic and, in the last years, are becoming a reality. In this paper, we have proposed and experimentally analyzed a novel WMN with double Wi-Fi interface nodes: one interface is used to create the backbone mesh network, where B.A.T.M.A.N. is the used routing algorithm; the other one is used by each node, acting as an AP, to create its own WLAN in order to provide connectivity to external non-B.A.T.M.A.N. clients.

Our results show that the proposed WMN can transparently integrate non-B.A.T.M.A.N. nodes as clients also in multi-hop scenarios. All the evaluation tests have been performed adopting backbone nodes implemented on top of RPi boards, properly setting various transmission parameters (e.g., transmission power, hop penalty, manual routing table modification), in order to test the behavior of the WMN in different topology conditions, from single-hop to multi-hop connectivity. By relying on *iperf* as traffic generator tool, an experimental performance analysis with TCP and UDP has been carried out. Our results show that, for varying link quality, the performance degrades, as a function of the number of hops, as $1/4^{n-1}$ (rather than $1/2^{n-1}$, as predicted by the theory). At the third hop, our worst case, we obtained a value of 1 Mbps, an higher jitter and an high packet loss; this is a limit if we are considering applications for smartphones (e.g., video streaming) but it does not affect communications regarding IoT application [43], where the bandwidth requirement is lower, a small delay can be tolerated, and the loss of information can be handled re-sending data if needed (also using constrained application protocols [44]). Moreover, in the presence of equal quality links, our results show that a single-hop link does not always represent the best communication choice. In fact, the inclusion of an intermediate B.A.T.M.A.N.-aware mesh node can make the information transfer (from the originator node to the destination) more robust, leaving the external clients unaware of the existence of the backbone WMN.

An extensive experimental evaluation, involving a larger number of mesh nodes and non-B.A.T.M.A.N. external clients (e.g., smartphones) is an attractive future development. Furthermore, the investigation of the flexibility of the proposed mesh architecture, considering nodes of different manufacturers and with different hardware technologies, also represents an interesting development.

Acknowledgments

This work was supported by Reios s.r.l. (Italy). The authors would like to thank Fabio Pozzi (with Reios) for technical support. The authors are also indebted to Massimo Viglione and Maria Chiara Lorena (both with Reios) for their constant drive.

References

[1] S. Salsano, L. Veltri, L. Davoli, P. Ventre, G. Siracusano, PMSR –Poor man's segment routing, a minimalistic approach to segment routing and a traffic engineering use case, in: 2016 IEEE/IFIP Network Operations and Management Symposium, NOMS, 2016, pp. 598–604. http://dx.doi.org/10.1109/NOMS.2016.7502864.

[2] L. Davoli, L. Veltri, P. Ventre, G. Siracusano, S. Salsano, Traffic engineering with segment routing: SDN-based architectural design and open source implementation, in: 2015 Fourth European Workshop on Software Defined Networks, EWSDN, IEEE, 2015, pp. 111–112. http://dx.doi.org/10.1109/EWSDN.2015.73.

[3] Wireless Battlemesh. URL http://battlemesh.org/.

[4] J.P.T. Moore, J.N. Bagale, A.D. Kheirkhahzadeh, P. Komisarczuk, Fingerprinting seismic activity across an Internet of Things, in: 2012 5th International Conference on New Technologies, Mobility and Security, NTMS, 2012, pp. 1–6. http://dx.doi.org/10.1109/NTMS.2012.6208718.

[5] K. Han, D. Zhang, J. Bo, Z. Zhang, Hydrological monitoring system design and implementation based on IOT, Phys. Proc. 33 (2012) 449–454 2012 International Conference on Medical Physics and Biomedical Engineering (ICMPBE2012). http://dx.doi.org/10.1016/j.phpro.2012.05.088.

[6] G.R.C. Andrés, CleanWiFi: The wireless network for air quality monitoring, community Internet access and environmental education in smart cities, in: 2016 ITU Kaleidoscope: ICTs for a Sustainable World, ITU WT, 2016, pp. 1–6. http://dx.doi.org/10.1109/ITU-WT.2016.7805708.

[7] A. Kandhalu, A. Rowe, R. Rajkumar, C. Huang, C.-C. Yeh, Real-time video surveillance over IEEE 802.11 mesh networks, in: Real-Time and Embedded Technology and Applications Symposium, 2009. RTAS 2009. 15th IEEE, IEEE, 2009, pp. 205–214.

[8] R. Bruno, M. Conti, E. Gregori, Mesh networks: commodity multihop ad hoc networks, IEEE Commun. Mag. 43 (3) (2005) 123–131.

[9] A. Neumann, C. Aichele, M. Lindner, S. Wunderlich, Better Approach to Mobile Ad-hoc Networking (B.A.T.M.A.N.) Draft - Openmesh MANET Routing. Networking Group Internet-Draft, 2008.

[10] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), RFC 3626, Internet Engineering Task Force, 2003. URL http://www.rfc-editor.org/rfc/rfc3626.txt.

[11] C. Perkins, E. Belding-Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, Internet Engineering Task Force, 2003. URL https://www.ietf.org/rfc/rfc3561.

[12] (2018) Freifunk, URL https://freifunk.net/.

[13] L. Davoli, L. Belli, A. Cilfone, G. Ferrari, Integration of Wi-Fi mobile nodes in a Web of Things Testbed, ICT Express 2 (3) (2016) 96–99 Special Issue on {ICT} Convergence in the Internet of Things (IoT). http://dx.doi.org/10.1016/j.icte.2016.07.00.

[14] G.R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, B. Walke, IEEE 802.11s: The WLAN mesh standard, IEEE Wirel. Commun. 17 (1) (2010) 104–111. http://dx.doi.org/10.1109/MWC.2010.5416357.

[15] IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012, 2012, pp. 1–2793. http://dx.doi.org/10.1109/IEEESTD.2012.6178212.

[16] IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking, IEEE Std 802.11s-2011, 2011, pp. 1–372. http://dx.doi.org/10.1109/IEEESTD.2011.6018236.

[17] J.D. Camp, E.W. Knightly, The IEEE 802.11s extended service set mesh networking standard, IEEE Commun. Mag. 46 (8) (2008) 120–126. http://dx.doi.org/10.1109/MCOM.2008.4597114.

[18] S.M.S. Bari, F. Anwar, M.H. Masud, Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks, in: 2012 International Conference on Computer and Communication Engineering, ICCCE, 2012, pp. 712–716. http://dx.doi.org/10.1109/ICCCE.2012.6271309.

[19] D.S.J. De Couto, D. Aguayo, J. Bicket, R. Morris, A High-throughput Path Metric for Multi-hop Wireless Routing, in: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, MobiCom '03, ACM, New York, NY, USA, 2003, pp. 134–146. http://dx.doi.org/10.1145/938985.939000.

[20] L. Davoli, Y. Protskaya, L. Veltri, An anonymization protocol for the Internet of Things, in: 2017 International Symposium on Wireless Communication Systems, ISWCS, 2017, pp. 459–464. http://dx.doi.org/10.1109/ISWCS.2017.8108159.

[21] open80211s project. URL http://open80211s.org/.

[22] S. Marinis Artelaris, Performance Evaluation of Routing Protocols for Wireless Mesh Networks (Ph.D. thesis), Linnaeus University, Department of Computer Science, 2016 URL http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-49745.

[23] G. Vadim, G. Oleg, K. Leonid, K. Mihail, P. Sergey, An experimental comparison of dynamic routing protocols in mobile networks, in: 2014 11th International Conference on Informatics in Control, Automation and Robotics (ICINCO), vol. 02, 2014, pp. 775–782.

[24] E. Kulla, M. Ikeda, L. Barolli, R. Miho, Impact of source and destination movement on MANET performance considering BATMAN and AODV protocols, in: 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, 2010, pp. 94–101. http://dx.doi.org/10.1109/BWCCA.2010.54.

[25] L. Davoli, L. Belli, A. Cilfone, G. Ferrari, From Micro to Macro IoT: Challenges and Solutions in the Integration of IEEE 802.15.4/802.11 and Sub-GHz technologies, IEEE Internet of Things J. PP (99) (2017) 1–1. http://dx.doi.org/10.1109/JIOT.2017.2747900.

[26] D. Seither, A. König, M. Hollick, Routing performance of wireless mesh networks: A practical evaluation of BATMAN advanced, in: 2011 IEEE 36th Conference on Local Computer Networks, 2011, pp. 897–904. http://dx.doi.org/10.1109/LCN.2011.6115569.

[27] D. Johnson, N. Ntlatlapa, C. Aichele, A simple pragmatic approach to mesh routing using BATMAN, 2008. URL http://hdl.handle.net/10204/3035.

[28] A.A.B. Almamou, R. Wrede, P. Kumar, H. Labiod, J. Schiller, Performance evaluation of routing protocols in a real-world WSN, in: 2009 Global Information Infrastructure Symposium, 2009, pp. 1–5. http://dx.doi.org/10.1109/GIIS.2009.5307052.

[29] R.G. Garroppo, S. Giordano, L. Tavanti, Experimental evaluation of two open source solutions for wireless mesh routing at layer two, in: IEEE 5th International Symposium on Wireless Pervasive Computing 2010, 2010, pp. 232–237. http://dx.doi.org/10.1109/ISWPC.2010.5483777.

[30] N.M. Anas, F.K. Hashim, H. Mohamad, M.H. Baharudin, M.P. Sulong, Performance analysis of outdoor wireless mesh network using B.A.T.M.A.N. advanced, in: 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD, 2015, pp. 1–4. http://dx.doi.org/10.1109/SNPD.2015.7176189.

[31] Raspberry Pi. URL https://www.raspberrypi.org/.

[32] TP-Link TL-WN722N: 150Mbps High Gain Wireless USB Adapter, URL http://www.tp-link.com/us/products/details/TL-WN722N.html.

[33] hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS authenticator. URL https://w1.fi/hostapd/.

[34] L. Belli, S. Cirani, L. Davoli, G. Ferrari, L. Melegari, M. Picone, Applying security to a big stream cloud architecture for the Internet of Things, Internat. J. Distri. Syst. Techno. 7 (1) (2016) 37–58. http://dx.doi.org/10.4018/IJDST.2016010103.

[35] L. Belli, S. Cirani, L. Davoli, L. Melegari, M. Mónton, M. Picone, An open-source cloud architecture for big stream iot applications, in: Interoperability and Open-Source Solutions for the Internet of Things: International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, September 18, 2014, Invited Papers, Springer International Publishing, 2014, pp. 73–88. http://dx.doi.org/10.1007/978-3-319-16546-2_7.

[36] L. Davoli, L. Belli, L. Veltri, G. Ferrari, THORIN: An efficient module for federated access and threat mitigation in big stream cloud architectures, IEEE Cloud Comput. PP (99) (2017) 1–1. http://dx.doi.org/10.1109/MCC.2017.455155318.

[37] L. Belli, S. Cirani, L. Davoli, G. Ferrari, L. Melegari, M. Montón, M. Picone, A Scalable big stream cloud architecture for the Internet of Things, Int. J. Syst. Serv.-Oriented Eng. 5 (4) (2015) 26–53. http://dx.doi.org/10.4018/IJSSOE.2015100102.

[38] L. Belli, S. Cirani, L. Davoli, A. Gorrieri, M. Mancin, M. Picone, G. Ferrari, Design and deployment of an IoT application-oriented testbed, Computer 48 (9) (2015) 32–40. http://dx.doi.org/10.1109/MC.2015.253.

[39] iPerf - The ultimate speed test tool for TCP, UDP and SCTP. URL https://iperf.fr/.

[40] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, RFC 1889, Internet Engineering Task Force, 1996.

[41] Solving the wireless mesh multi-hop dilemma, 2015. URL http://www.strixsystems.com/products/datasheets/strixwhitepaper_multihop.pdf.

[42] O. Gurewitz, V. Mancuso, J. Shi, E.W. Knightly, Measurement and modeling of the origins of starvation of congestion-controlled flows in wireless mesh networks, IEEE/ACM Trans. Netw. 17 (6) (2009) 1832–1845. http://dx.doi.org/10.1109/TNET.2009.2019643.

[43] S. Cirani, L. Davoli, G. Ferrari, R. Leone, P. Medagliani, M. Picone, L. Veltri, A scalable and self-configuring architecture for service discovery in the Internet of Things, IEEE Internet of Things J. 1 (5) (2014) 508–521. http://dx.doi.org/10.1109/JIOT.2014.2358296.

[44] S. Cirani, L. Davoli, M. Picone, L. Veltri, Performance evaluation of a SIP-based constrained peer-to-peer overlay, in: 2014 International Conference on High Performance Computing Simulation, HPCS, 2014, pp. 432–435. http://dx.doi.org/10.1109/HPCSim.2014.6903717.

Luca Davoli is a Postdoctoral Research Associate at the Internet of Things (IoT) Lab, at the Department of Engineering and Architecture of the University of Parma, Italy. He received his Dr. Ing. (Laurea) degree in Computer Science from the University of Parma, Italy, in 2013. In 2017, he received his Ph.D. in Information Technologies at the Department of Information Engineering of the same university. His research interests are Internet of Things, Power Line Communications, Pervasive Computing, Big Stream, Mobile Computing and Software-Defined Networking. He is an IEEE Member.

Antonio Cilfone is a member of the Internet of Things (IoT) Lab at the Department of Engineering and Architecture of the University of Parma and, since November 2016, he is a Ph.D. Student in Information Technologies at the University of Parma, Italy. He received his Master of Science in Communication Engineering (summa cum laude) in March 2016 from the University of Parma, Italy. His research interests are Internet of Things, Routing Algorithm, and Mesh Networks.

Laura Belli is a Postdoctoral Research Associate at the Internet of Things (IoT) Lab, at the Department of Engineering and Architecture of the University of Parma, Italy. She received her Dr. Ing. (Laurea) degree in Computer Science from the University of Parma, Italy, in 2011. In 2016, she received her Ph.D. in Information Technologies at the Department of Information Engineering of the same university. Her research interests are Internet of Things, Pervasive Computing, Big Stream, Database Integration, Mobile Computing.

Gianluigi Ferrari received the Laurea (summa cum laude) and Ph.D. degrees in electrical engineering from the University of Parma, Parma, Italy, in 1998 and 2002, respectively. Since 2002, he has been with the University of Parma, where he is currently an Associate Professor of Telecommunications (with National Scientific Qualification for Full Professorship since 2013), and also is currently the Coordinator of the Internet of Things (IoT) Laboratory, Department of Engineering and Architecture. His research interests include signal processing, advanced communication and networking, and IoT and smart systems. He has authored extensively in these areas. He is co-founder and President of things2i s.r.l., a spin-off company of the University of Parma dedicated to IoT and smart systems. He is an IEEE Senior Member.