

# **An Enhanced Geographical Routing protocol for Wireless Mesh Networks, 802.11s**

Mariem Thaalbi, Nabil Tabbane  
MEDIATRON LAB, High Communication School of Tunis, Tunisia

## **ABSTRACT**

Wireless Mesh Networks (WMNs) have emerged as a key technology for next generation wireless networking. The performance of these networks depends on routing protocols. IEEE 802.11s is one of the emerged standards designed to build WMNs for the classical standard 802.11. It defines the HWMP (Hybrid Wireless Mesh Protocol) as its default routing protocol which combines the Radio Metric Ad hoc on-demand distance vector (RM-AODV) with a proactive tree building mode. RM-AODV relies on the well known AODV protocol which provides paths by broadcasting path requests. However broadcast to find routing paths consumes much bandwidth and increases the traffic overhead. In this situation broadcast optimization is an ever-present issue. In this paper, the Geographical Hybrid Wireless Mesh Protocol (GHWMP) is presented

## **Keywords**

Wireless Mesh Networks, IEEE802.11s, routing protocol, HWMP, RM-AODV, GHWMP.

## **1. INTRODUCTION**

Mobile and wireless networks knew an unprecedented development these last years. With progress achieved in terms of physical and MAC layers, a new technology has emerged which is Wireless Mesh Networks WMN. The wireless Mesh Networks are composed of a set of wireless nodes communicating in multi-hop. These nodes form the Backbone network to the mobile client stations. Several standards support this technology including meshed WLAN IEEE 802.11s [1], and meshed WMAN IEEE 802.16f [2]. In our paper we will focus our study on the IEEE 802.11s standard. This technology is a recent standard for Wireless LANs 802.11 [3]. It provides a wireless backbone to connect multiple access points.

The wireless and multi-hop concepts in the backbone network reveal the importance of routing protocols in such networks. Therefore, routing in WMNs is an important issue. It must take into account the quality of radio links and ensure good quality services. In our paper, we focus on 802.11s routing mechanisms. We have proposed and implemented a new routing technique for this standard: GHWMP: Geographical Hybrid Wireless Mesh Protocol. We also compared the performance of this protocol compared to the IEEE 802.11s default routing protocol Hybrid Wireless Mesh Protocol (HWMP) [1, 4]. This routing protocol operates on the MAC layer. The HWMP is the combination of a reactive routing protocol which is Radio-Metric AODV

(RM-AODV) [1] derived from the Ad hoc On Demand Vector (AODV) [5] and a tree based routing protocol.

In this paper we propose to use geographical routing protocol instead of RM-AODV to minimize the path discovery mechanism's cost thus to enhance the routing performance in WMNs. HWMP and GHWMP will be evaluated via simulation under NS3 simulator.

This introduction is followed by six sections which present successively the related works, IEEE 802.11s network's overview, the HWMP protocol, the proposed routing protocol, the performance evaluation and finally a conclusion.

## **2. IEEE 802.11s standard**

The working group IEEE 802.11s was formed on May 2004[1]. It aims to standardize the Wireless Mesh Networks in WLANs. In the 802.11s networks, the stations which implement routing algorithm and Meshing functions like Mesh Peering and neighbor discovery are known as Mesh Stations (Mesh STAs) or also Mesh Points (MPs) [1, 6]. These wireless devices interconnect via the radio link to create the WLAN Mesh BSS. The default routing protocol of this standard is Hybrid Wireless Mesh Protocol (HWMP) [1]. This hybrid protocol is the combination of a reactive protocol Radio Metric-Ad hoc On Demand Vector (RM-AODV) [1] and a proactive protocol which is based on tree building algorithm. Another routing protocol was defined by the IEEE 802.11s which is Radio Aware-Optimized link State Routing (RA-OLSR) [1]. Security solutions developed by IEEE 802.11s group define a mutual authentication between MPs, key generation and management, data encryption and attack detection. We will present this standard in more details.

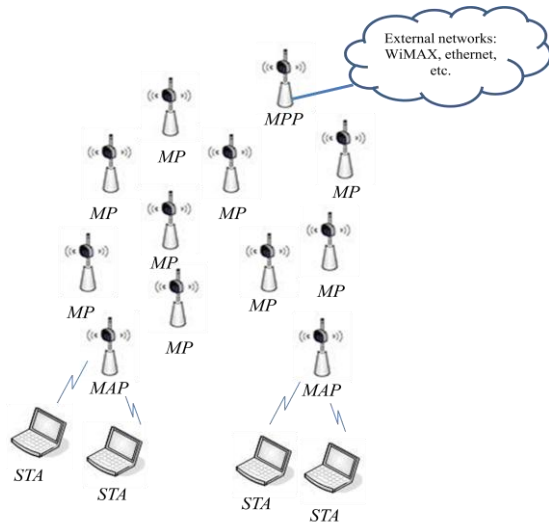
### **2.1 802.11s architecture**

In WMN, the MPs form a wireless backbone for the Simple Stations (STA) [1]. This wireless back-bone is called MeshBSS since the MPs are interconnected according to a mesh topology. Every MeshBSS is identified by a unique MeshID [1].

The Simple Stations don't implement the mesh networking functions. MPs implementing the access point functionalities are called Mesh Access Points (MAP) [1]. These nodes provide the net-work access to the STAs. With this entity the 802.11s insure the compatibility between all other 802.11 standards like 802.11a, 802.11b, and etc.

The Mesh Portal Point (MPP) [1, 6] performs as a gateway and interconnects the 802.11s network to external networks.

The following figure (Fig1) presents the 802.11s network devices:



**Fig 1. IEEE802.11s network architecture.**

All contribution given by the IEEE 802.11s are in MAC layer. The physical layer is kept intact [7]. These MAC modifications will be presented in the next paragraph.

## 2.1 MAC layer improvements

### 2.2.1. Presentation of the 802.11s MAC layer

This layer provides the Mesh networking functionalities including neighbors' discovery, topology formation, media access coordination functions, routing protocol, and interconnection and security functions [1]. The Mesh BSS discovery and formation specifies how a mesh network builds up itself and how the MPs join the network or leave it. To interconnect the mesh network with other networks, MPPs must implement 802.1D standard that defines interconnection structure between different 802 networks. Security in 802.11s network is based on the same principles defined by the IEEE 802.11i standard. The 802.11s standard defines two coordination access method [1]. The first one is Enhanced Distribution Channel Access (EDCA) which is considered the mandatory method. The second one is called Mesh Coordinated Channel Access (MCCA) which is an optional method which optimizes the frames exchange within the MeshBSS. In order to support these features, new frames were defined by the IEEE 802.11s standard, others have been modified by adding new fields such as the Mesh Header field.

### 2.2.2. Improvements of 802.11s MAC layer

In this section we discuss the EDCA and MCCA mechanisms, congestion control method, Common Channel Function (CCF), power management, and synchronization.

- **EDCA:** is the mandatory channel access defined by 802.11s. It was proposed by the standard IEEE 802.11e [8] in order to insure Quality of Service (QoS) in the WLAN networks. It supports differentiated and distributed access to the wireless Medium according to four access categories: Voice, Video, Best Effort and Background.
- **MCCA** [6, 9]: is an optional access method that allows the MPs to access the wireless medium at given times. It's based on reservation protocol via a simple exchange between sender and receiver to determine MCCAOPs (MCCA Opportunities) periods. Each MP maintains and disseminates its information about: a list of all MCCAOPs during which it's either transmitter or receiver and a list of nearby MCCAOPs. This information allows neighboring MPs to avoid overlaps. Once a MP gets a MCCAOP it performs a Clear Channel Access (CCA) and accesses the wireless medium with the highest priority. Its neighbors remain inactive during this period.
- **Congestion control** [9]: is an intra-Mesh mechanism which is implemented in each node. If a MP detects congestion it informs its neighbors. Each MP receiving this congestion message should adjust its transmission rate.
- **CCF** [10]: this mechanism offers multi-channel aspect to the network in order to improve its capacity. It allows negotiation of channel to exchange data between two peers. A common channel is used before switching to a data channel. The data channel is selected by exchanging control frames Request to exchange (RTX) and clear to exchange (CTX) on the common channel between peer MPs.
- **Power management** [9]: While MAPs should remain awake. MPs may optionally have a mechanism for saving power (PS: Power Save). The MPs fully charged can stay awake without interruption to route the traffic more efficiently but when the power level becomes critical, they should switch to a sleep mode to conserve energy.
- **Synchronization** [9]: In the 802.11s is optional. Many MAC functions are based on synchronization like energy saving, CCF, and MCCA. Synchronization is necessary to avoid control frames collisions.

### 2.2.3 Network discovery mechanism

In order to join the IEEE 802.11s network, every MP should discover its neighborhood. This discovery is accomplished by either a Passive scan by listening to beacon frames of its neighbors or Active one by sending request probes. After the discovery of his neighborhood, the MP maintains the MAC addresses of the MPs

candidates in its neighbor table and proceeds to the association. A neighbor MP is considered as a candidate only if it has the same Mesh Profile.

Each MP should at least bear one Mesh Profile [1]. A Mesh Profile consists of:

- MeshID: Mesh BSS Identifier.
- Path Selection Protocol ID: Identifier of the supported routing protocol.
- Path Selection Metric ID: Identifier of the metric used to choose the best path.
- Version: The version of the Mesh Peering protocol used.

If a MP failed to detect its neighbors, it adopts a MeshID and creates its own mesh network [1].

### 2.2.4 Routing IEEE 802.11s

Routing in IEEE 802.11s is also called path selection [1]. It is used to select the optimal path from the transmitter to the receiver. This mechanism operates on the MAC layer and it uses MAC ad-dresses. Two routing protocols were proposed by the IEEE802.11S group:

- Hybrid Wireless Mesh Protocol (HWMP) [1]: is the default mandatory routing protocol. It is inspired by a combination of RM-AODV and tree based routing (TBR). This protocol will be more presented on the next section.
- Radio Aware-Optimized Link State Routing (RA-OLSR) [1]: is an optional routing protocol. It's suitable for low mobility environment which is the case of 802.11s networks. It's based on the OLSR [11] routing protocol which is developed by the IETF MANET working group.

The default routing metric defined by the IEEE 802.11s is Air Link Metric (ALM) [1]. It corresponds to the amount of radio resource consumed during the transmission of a frame. It's computed according to the following formula [12]:

$$c_a = \left[ O_{ca} + O_p + \frac{B_t}{r} \right] \frac{1}{1 - e_f}$$

Where  $r$  and  $e_f$  denote respectively the data rate (Mb/s) and the error rate for a test frame of size  $B_t$ .  $O_{ca}$  represents the channel access overhead,  $O_p$  the protocol overhead.

### 2.2.5 Security in 802.11s network

Security in IEEE802.11s is based on the mechanisms proposed by the IEEE 802.11i [13] which provides a solution for securing 802.11 networks. The 802.11i aims to secure the radio link between the client stations and the Access Points (APs). Other specific features are developed by the 802.11s to insure the security in the MeshBSS, which are:

- Mutual authentication between MPs [1]: when a new MP wants to join a new 802.11s network, it performs a first authentication Mesh Security Authentication (MSA) with a

Mesh Authenticator (MA) in the network. Once the MP gets the necessary keys from the MA, It performs authentication with candidate MPs.

- Protection of management messages exchanged between the MPs such as topology and routing information [1].

## 3. RELATED WORKS

Routing protocols play an important role in WMNs. In order to disseminate routing information in the whole network, most proposed protocols use the flooding approach. IEEE 802.11s group [1] defines the HWMP as a routing protocol which is completely based on the flooding mechanism.

In order to overcome this issue, the authors in [14] proposed the Route Driven Routing (RDR) protocol. The core idea of this protocol is to enable a root MP to provide the best-metric path for any intra-Mesh traffic. According to RDR, root MP must build the whole network topology. When a MP needs to send traffic, the root MP recommend it the optimum on demand path. Based on neighbors' information, the root computes the optimum route for all source-destination pairs using the Dijkstra's algorithm. This protocol gives good performance in fixed and stable networks. However, in dynamic environments the root has to update frequently its network topology to keep suitable paths reliability. Also, the MPs have to send frequently information about its neighbors. In order to reduce the overhead generated by the tree based protocol defined by HWMP, Bae and Koe [15] have proposed to adjust the RANN transmission period. Also, they proposed an algorithm which contains three mechanisms: Alternative Parent Node, Local Repair and RANN solicitation in order to reduce path maintenance cost and path recovery delay. According to RANN mechanism defined by HWMP, any MP can receive same RANN message from different paths, it has to select the parent node which has the smallest ALM to construct a path towards the root MP. With the Alternative Parent Node mechanism proposed in [15], the MP stores also the MAC address of an alternative parent node which is providing the second smallest ALM. The alternative parent node will be useful when the link with the parent node is broken. If the path recovery is failed, the MP executes the Local Repair mechanism. It broadcasts a PREQ in a limited area. In order to achieve this issue the authors limit the TTL field's value of the PREP packet to cover the local area and set its RF and TO bits to 0. If this mechanism failed to repair the path, the RANN solicitation mechanism will be executed in order to rebuild the entire routing tree. HWMP is based on flooding mechanism to build the network topology and to refresh routing information. To solve these problems, Ueda and Baba [16] proposed an initial routing establishment method with greedy forwarding method. The authors define a new address space based on the link state between MPs for the greedy forwarding. Also they proposed a routing method based on addresses in the address space. The source traffic MP chooses a MP closest to destination one. According to [16], the path recovery mechanism still not defined.

Despite flooding mechanism degrades the radio link quality and creates important overhead traffic. Other

routing mechanisms didn't provide accurate information about the network topology especially in dynamic environments.

Routing protocols in WMNs deployment stills an open issue for researchers today. To the best of our knowledge there are no many propositions to the routing protocols in dynamic and changing WMN environment.

## 4. HWMP

HWMP is a kind of hybrid routing protocol operating on the layer 2 on the OSI model. It builds proactive paths to the root MP thanks to the tree based routing and reactive paths between the MPs inside the same MeshBSS according to the RM-AODV routing protocol. The use of these two routing mechanisms depends on the presence of a root MP.

HWMP defines several control messages which are: Path Request (PREQ), Path Reply (PREP), Root Announcement (RANN), and Path Error (PERR) [1]. It uses sequence numbers as a mechanism to avoid loop formation.

### 4.1. Reactive Mode

This mode is based on the RM-AODV [1] protocol which is an extension of AODV [5]. It operates on the layer two and holds MAC addresses. It adopts the ALM as a metric to choose the best path and not the hop count like the AODV protocol. The ALM is a cumulative metric.

RM-AODV is a reactive routing protocol where the source MP initiates a path discovery when it has data packets to send. The source MP broadcasts a PREQ packet containing information about the source and destination MAC addresses, the initial metric, and the source sequence number.

Depending on the sequence number field, intermediate MPs can set up a reverse path to the source and broadcast the PREQ packet after modifying the metric field.

In case where the source MP allows gratuitous replies (by setting Target Only (TO) flag to 0 in the PREQ) intermediate MPs, which have available path to the destination, send PREP to the source. Otherwise only the destination sends a PREP. Upon receiving PREP, the source sets up a bidirectional link to the destination.

In RM-AODV, routing tables' entries for active routes are updated only when routing packets containing "fresh information" are received. Route table entries are deleted after Active Route Timeout and PERR packets are broadcast by MPs in case of link failures.

### 4.2 Proactive Mode

The proactive mode aims to disseminate on the whole MeshBSS the information how to reach the root MP. HWMP defines two mechanisms to realize this function. The first uses proactive PREQ packet [1], intended to

mesh network in a proactive manner. The second uses the RANN packet [1], intended to distribute routing information to reach the root MP but the paths can be set up in a reactive manner. Both mechanisms are detailed below.

#### 4.2.1 Proactive PREQ mechanism

In order to build the tree, according to this mechanism, the root MP sends periodically a proactive PREQ. This request contains a destination address field set to the broadcast address, a metric field initialized to zero by the root MP, a TO bit set to 1 and a RF (replay and forward) bit set to 1 in order to propagate the PREQ to the entire network.

MPs receiving the Proactive PREQ create or update its path entry to the root MP. Also they modify the Proactive PREQ by updating the metric field and send it to their neighbors.

Each MP may receive multiple copies of the Proactive PREQ, each one traversing different paths from the root MP. Once the MP has chosen the best path, it may send PREP to establish a bidirectional path with the root MP. Sending PREP depends on the Proactive PREP bit included on the PREQ. The following diagram shows the behavior of each MP according to the status of this bit.

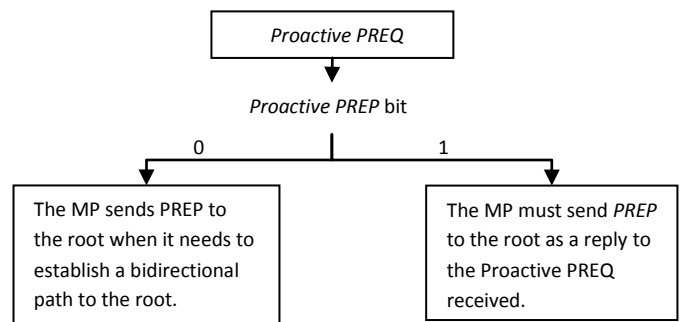


Fig 2. MP behavior according to the Proactive PREP bit.

#### 4.2.2 RANN mechanism

The root MP broadcasts periodically a RANN on the MeshBSS in order to refresh the routing information to it. The information contained in the RANN is used to distribute the paths costs leading to the root MP. As every control packet, the RANN will be processed by the MPs only if it has a sequence number greater or equal to that recorded on its routing table and providing a better metric value.

Every MP receives RANN, it rebroadcasts it to all its neighbors and so on till the RANN packet reaches all the MPs in the MeshBSS. Each MP chooses the best path and sends a PREQ to the root MP along this path. The root MP sends PREP as a reply to each received PREQ in order to establish a bidirectional link. The PREQ establishes the reverse path from the root to the MP and the PREP sets up the forward path from the MP to the root.

## **5. GEOGRAPHICAL HYBRID WIRELESS MESH PROTOCOL**

HWMP is a hybrid routing protocol which adopts a reactive mode based on the flooding mechanism to find a path to the destination. In our paper, we improve and optimize the behavior of the reactive mode. We keep the proactive mode intact and the tree based routing will be retained.

### **5.1 GHWMP Overview**

In GHWMP, when a MP has data packets to send, it requests the root MP about its destination.

If the destination is outside the MeshBSS, the root MP will be responsible for forwarding data packets from source to destination. If the source and destination belong to the same network, the root MP sends to the source the information needed to reach the destination. While the root MP transmits the data packets from the source to destination, the source MP establishes a reactive path to the destination better than the proactive one.

The main idea of GHWMP is to utilize a geographical routing protocol in the reactive mode in-stead of the RM-AODV protocol in order to support the mobility and decrease the overhead load in the network.

All the MPs are equipped by a Global Positioning System (GPS) [17]. In the learning network phase, all the MPs consult the GPS in order to determine their geographic coordinates. As in HWMP, the root MP sends periodically a RANN or a proactive PREQ in order to announce its presence, and the MPs must include their geographic coordinates and their velocity in the reply packet. In order to not overload the network with these sized packets, only the MPs which changed their positions will include their geographical information in the reply. Otherwise the MPs will adopt the same packet reply used in HWMP.

In order to optimize the overhead traffic in the network, a location database will be centralized in the root MP. This database will contain the geographic information received by the root from the different MPs in the network as a reply to its RANN or proactive PREQ.

When a source MP wants to find its destination node, it sends a PREQ to the root MP in order to know if the destination is inside or outside the MeshBSS. Upon receiving this PREQ, the root MP consults its location database and it sends to the source the geographic location of the destination MP if the destination is inside the same network. Based on this location information, the source MP try to find a valid path to the destination according to a reactive geographical routing protocol inspired from the Location Aided-Routing protocol (LAR) [18]. LAR is a reactive and geographic routing protocol that exploits the cinematic parameters of mobile nodes (like speed, direction, location, etc.) in order to optimize the route discovery process by reducing the diffusion zone of the control messages.

### **5.2 First Network initialization phase**

All MPs belonging the MeshBSS, consult the GPS system in order to acquire their location information. The root MP broadcasts periodically a proactive PREQ or RANN containing its geographic coordinates. Any MP receiving this packet from different paths chooses the best path (like in HWMP) and replies the root across this path by encapsulating its geographic coordinates in the reply packet. The root collects the routing and location information from the replies it receives and updates its location database.

According to GHWMP, the MPs consult the GPS only once time when it joins the MeshBSS. To refresh their coordinates, the MPs will approximate their current coordinates from previous ones. Since GHWMP adopts the Random Way Point (RWP) mobility model. In this model, the MP randomly chooses a destination called waypoint according to a direction  $\alpha$  and moves towards it in a straight line with a constant velocity, which is selected randomly from 0 to  $V_{max}$ . After it reaches the waypoint, it pauses for some time called Tpause and then repeats the same procedure.

In case of fixed backbone, the coordinate's approximation mechanism will be disabled in order to reduce the processing capabilities of the MPs.

### **5.3 Path discovery**

All MPs desiring to send data packets begins by examining its cache to find a valid path to the destination. In the absence of such path, the source MP performs a path discovery process. It requests the root MP in order to know if the destination is inside or outside the MeshBSS. In case where the destination is outside, GHWMP will have a similar behavior to HWMP. The root will transmit the data packets from source to destination. In case where the destination is inside the network, the root MP will extract the geographic information of the destination from its location database and encapsulate them in the PREP which will be sent back to the source. Also, it transmits the data packets from source to destination till the source finds a better reactive path. Based on the geographic coordinates of the destination and the source, the MP source computes the forwarding zone where the PREQ will be broadcasted. This approach allows reducing the overhead traffic generated by a path discovery. In fact, the PREQ will not be broadcasted in the whole network like in RM-AODV but it will be only transmitted in a limited area called forwarding zone. This zone will be defined according to the LAR Box routing protocol. The forwarding zone is composed by two zones: the expected zone and the requested zone.

### 5.3.1 Expected zone

The Expected zone is the geographic area in which a source MP estimated to find its destination MP at a given moment using its location information in earlier time. The determination of the expected zone requires some additional information such that the maximum or average speeds of the destination node and its movement direction. If at time  $t_1$ , the source MP  $S$  knows the average speed  $v$  of the destination MP  $D$  and its location in earlier time  $t_0$ , so the expected zone is the circle with a radius  $R = v(t_1 - t_0)$ , centered around the location of  $D$  at time  $t_0$ . The Fig 3 shows the expected zone of the MP  $D$ .

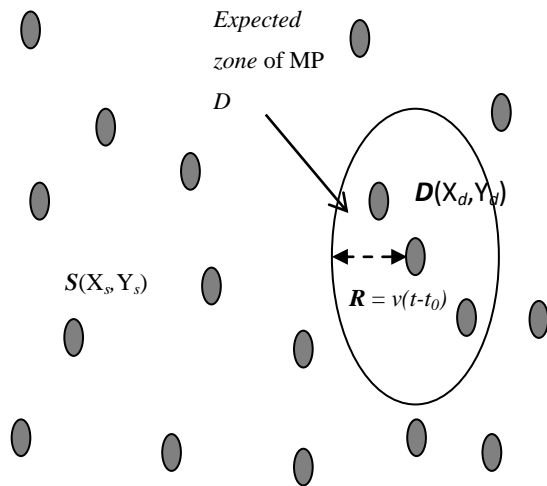


Fig 3. MP D Expected zone.

### 5.3.2 Request zone

The request zone is the geographic area in which the PREQ will be broadcasted. This zone must include at least the expected zone and the source MP. The LAR Box defines the request zone as the smallest rectangle that covers the current position of the source MP and the expected zone. The Fig 4 represents the requested zone of the MP  $D$ .

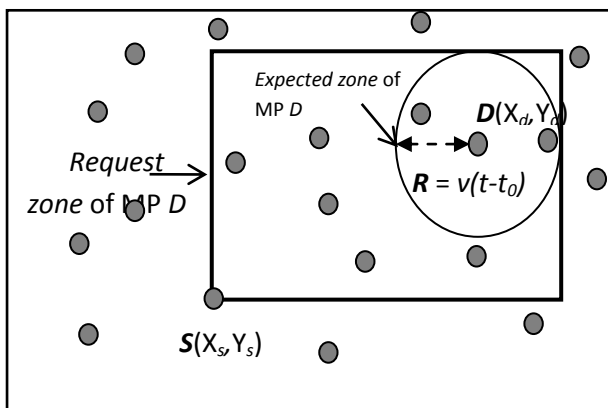


Fig 4. Request zone of the MP Destination.

## 5.4 Link failure management

GHWMP adopts a link failure management approach similar to LAR Box. Any intermediate MP detecting a

link failure updates its routing cache and sends a PERR towards the source. However this PERR may takes a long time till it arrives to the source node which causes a routing performance decrease. This can be reduced if the intermediate MP detecting the link failure performs a path discovery by using its own location and the destination ones.

## 6. EVALUATION STUDIES

### 6.1 Simulations environment and performance criteria

We will show performance comparison between HWMP and our proposed GHWMP protocol done under NS3 simulator [19, 20].

We will study three different scenarios: the first one studies the routing protocols behavior vs. mobility, the second one studies the routing protocols scalability, and the third one studies the behavior of HWMP and GHWMP vs. the network load increase. For all scenarios, we consider a rectangle area where the MPs are uniformly deployed. Each MP has a transmission range of 150m. The root MP is located on the top left corner of the simulation area. The duration of simulation was fixed to 100s. Link speed was set to 54 Mbps. Parameters of the IEEE 802.11s network used during simulation are shown in Table 1.

Table 1. 802.11s parameters.

Parameter	Value
Coverage Radius	150 m
Radio Propagation Model	Two- RayGround
Frequency	5 GHz
Propagation Model	LogDistancePropagation LossModel
Simulation Duration	100s

Voice over IP (VoIP) traffic was simulated. The traffic flows parameters are shown on Table 2.

Table 2. Simulated traffic parameters.

Packet size	160 bytes
Delay interval	20 ms

To evaluate the performance of different routing protocols, we calculate the following criteria: Throughput, transmission delay, jitter, packet loss rate and traffic Overhead (ToH).

- Throughput: is the average rate of successful data delivery over a communication channel

per unit time. It is measured in Kbits per second (Kb/s).

- Transmission delay: is an important parameter to evaluate the QoS of real time traffic. It is the time taken for a packet to be transmitted across the MeshBSS from the source MPP to the destination MPP.
- Jitter: is the time variation between packets arriving. It is an important parameter for VoIP traffic, where it should be as short as possible.
- Packet Delivery Rate: is defined as the ratio of the data packets delivered successfully to destination nodes and the total number of packets generated for those destinations. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the better performance is obtained in the network from routing protocol. The packet loss rate parameter allows determining the lost packet rate compared to those sent.
- Traffic overhead: describes how many routing packets for path discovery and path maintenance need to be sent in order to propagate the data packets. It specifies the traffic overhead induced by the routing protocol in the network. Traffic Overhead is defined as the ratio of transmitted routing packets and received data packets. It determines the performance in congested networks. If a protocol needs to send many routing packets, it will most likely cause bottleneck/congestion, collisions and delay in large networks.

## 6.2 Proposed scenarios and simulation results

### 6.2.1 Mobility

In order to analyze the wireless mesh network in mobile environments, we customized a MeshBSS containing twenty MPs. We simulated a communication between 802.11b network and WIMAX network traversing the 802.11s network. The MeshBSS was considered as a network interconnection between the source and destination networks. We focused only on the intra-mesh traffic between the two MPPs. To study the behavior of different routing protocols in a mobile environment, the MPs will move according to the RWP mobility model. The nodes velocity  $V_{max}$  will vary from 0 to 30 m/s, the direction  $\alpha$  was fixed to zero and  $T_{pause}$  was fixed to 2s. Table 3 resumes these different parameters.

Nodes mobility causes dynamic and random topology changes. This constraint is a challenge to overcome on WMNs. In fact, the movement of nodes can affect the validity of paths and causes the broadcast of control packets in order to repair or build new paths. The strategy of GHWMP tries to minimize this significant overhead traffic by reducing the forwarding zone of control messages. To highlight the impact of mobility on

the performance of HWMP and GHWMP protocols, we choose to deploy 20 MPs and vary their speed for a network load of 10 %. We simulate one traffic between two MPs.

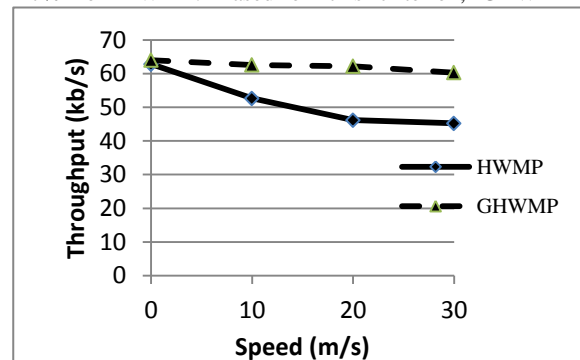
**Table 3. Mobility scenario parameters.**

Parameter	Value
Mobility Model	Random Way Point
Direction : $\alpha$	0
Pause Time: $T_{pause}$	2 s
Velocity: $V_{max}$	0, 10, 20 et 30 (m/s)
MPs number	20 MPs

### a. Throughput

Fig 5 shows the throughput evolution according to the average speed of the MPs of the MeshBSS. We note that GHWMP provides a stable data rate regarding the average speed of the backbone MPs. When the moving speed of the MPs increases significantly from 20 m/s to 30 m/s the throughput provided by GHWMP remains relatively intact. This shows that GHWMP which is inspired from LAR Box routing protocol is well adapted to frequent changes in network topology caused by the MPs mobility.

Increasing the average speed from 0 m/s to 30 m/s induces throughput degradation of 6% for GHWMP and 27% for HWMP. Based on this criterion, GHWMP



**Fig 5. Throughput evolution vs backbone mobility.**

performs better than HWMP in mobile environments.

### b. Packet Loss rate

Figure 6 shows the variation of packet loss rate provided by HWMP and GHWMP based on the MPs average speed. We remark that the PLR: Packet Loss Ratio of the two protocols increases when the mobility speed increases. Indeed, when the speed increases the paths became unavailable. As a result, several path discoveries are initiated and several data packets stored in buffers are deleted after a specific timeout. In addition, packet loss during transmission becomes high because of paths broken.

We conclude that the GHWMP offers better results than HWMP, since it adopts a path recovery mechanism. Any MP detecting a link failure sends a PERR to the source and seeks for a new valid path to the destination. While in HWMP, when a MP detects a link failure it generates a PERR to the source node which is the only network entity having to find a path to the destination by performing new path discovery mechanism.

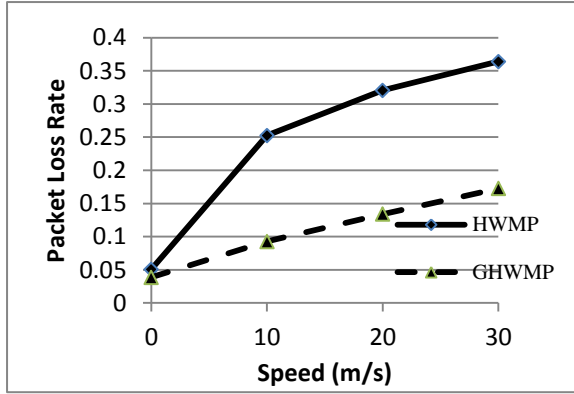


Fig 6. Packet Loss Rate variation in mobile scenario.

#### c. Transmission delay and jitter

Figure 7 illustrates the variation of transmission delay between the source MP and destination one. We remark that HWMP provides high transmission delay. In fact, according to HWMP every MP wishing to find a path to the destination must consult the root MP and wait for its reply in order to perform the reactive path discovery according to RM-AODV. GHWMP provides shorter transmission delay than HWMP since it is based on geographic routing. Each MP transmits packets to its neighbor which is closest to the destination.

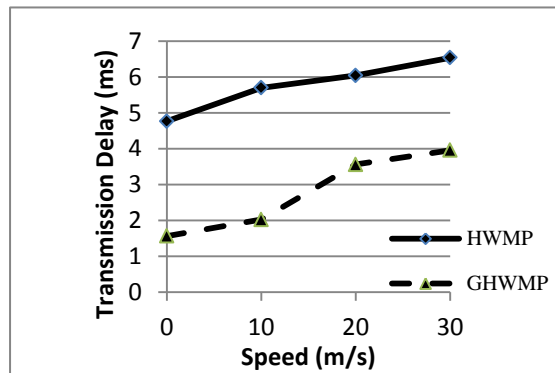


Fig 7. Transmission Delay.

Figure 8 shows the jitter variation according to the backbone mobility. We notice that HWMP provides the highest jitter. This is due to the consultation of root MP each time the procedure of finding path to a destination node is launched. In HWMP, when a link failure occurs a new path discovery procedure must be initiated by the source MP. GHWMP offers the shortest jitter since it adopts a path repair mechanism.

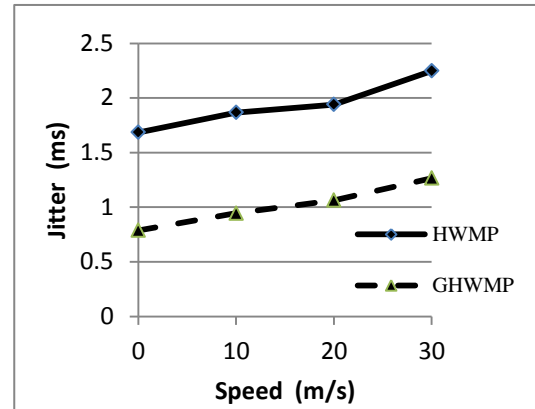


Fig 8. Jitter variation.

#### d. Traffic Overhead

Figure 9 shows the traffic overhead evolution regarding the MPs mobility. We see that Traffic overhead increases with nodes mobility. Indeed, when mobility speed increases, routing data re-quires more control messages to build and to repair paths. From figure 7, we note that HWMP traffic overhead increases significantly when the speed increases from 0 to 30 m/s. We note that GHWMP reduces the traffic overhead compared to HWMP. In fact, GHWMP requires limited broadcast overhead to find routing paths. We note that our proposed routing protocol offers stable overhead values when the backbone speed increases. We conclude that GHWMP is well adapted to mobile and changing WMN deployments. From the curves, it's very clear that GHWMP outperforms HWMP in mobile environment.

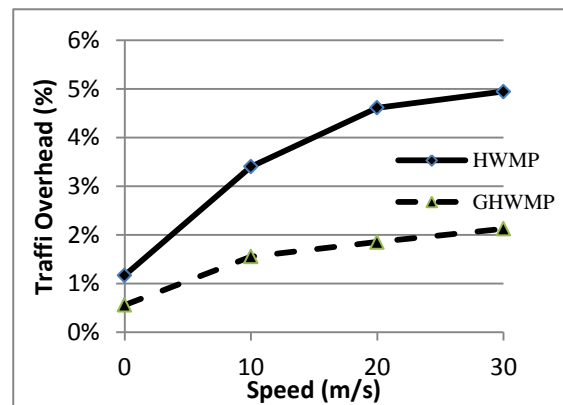


Fig 9. Traffic Overhead evolution.

#### 6.2.2 Scalability

In order to study the scalability of different routing protocols, we adopted a fixed MeshBSS, where all the MPs are static. The simulation area was fixed to 500\*200 m<sup>2</sup> and we varied the number of nodes deployed on the network. All the MPs are fixe. This MeshBSS operates as

a backbone between the source and destination network. We simulate a single traffic flow from the source MP to destination MP.

#### a. Throughput

Figure 10 shows the throughput evolution depending on the number of MPs deployed on the Mesh BSS. We note that different protocols have similar behavior when the number of MPs is up to twenty. When the number exceeds twenty GHWMP offers 35% better throughput than HWMP. HWMP was designed with an objective to include 32 MPs [21] in the MeshBSS. We notice that the HWMP throughput decreases when the number of MPs exceeds 20 MPs. The GHWMP throughput slightly decreases when the MPs number exceeds 24.

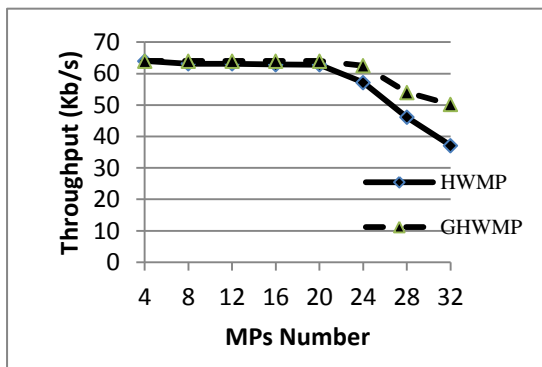


Fig 10. Throughput evolution.

#### b. Packet Loss rate

Fig11 shows the packet loss rate (PLR) variation depending on network density. We note that the network density affects the PLR because of the increase of hop numbers between the source and destination MP. In HWMP, the packet loss rate increases significantly when the number of MPs deployed in the network exceeds 20. In fact, when the number of hops between source and destination increases the path quality degrades because of the adapted metric ALM which is a cumulative metric.

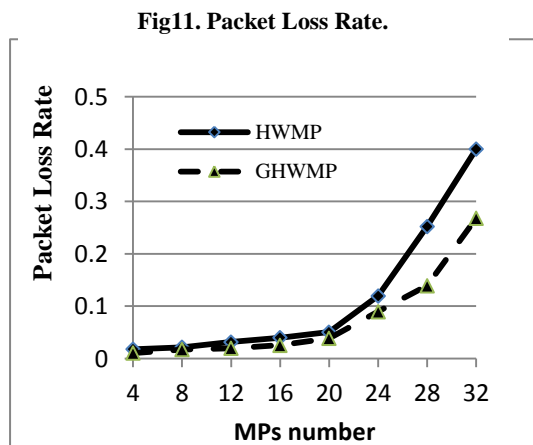


Fig11. Packet Loss Rate.

#### c. Transmission delay and jitter

Fig 12 shows the transmission delay evolution regarding the MPs number increase. We note that the network density affects the transmission delay. Higher the MPs number is higher the transmission delay becomes. In HWMP, when the network become dense the root consultation and path discovery processes become slower. In GHWMP, the forwarding zone computing time needed by the source MP and the time taken by intermediate MP to verify its appartenance to the forwarding zone increases the transmission delay required by packets to reach their destination MP.

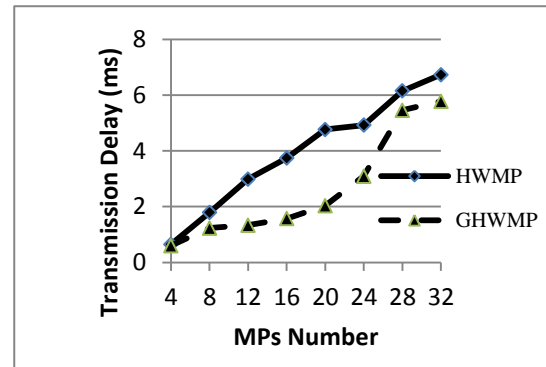


Fig 12. Transmission Delay.

Fig13 shows the jitter variation regarding the network density. We note that the network density increase affects dramatically the performance of different protocols. But we remark that GHWMP is 28% better than HWMP.

#### d. Traffic Overhead

Fig 14 shows the traffic Overhead evolution according to the increase of MPs number in the network. We note that when the MPs number in the MeshBSS increases the traffic Overhead in-creases. GHWMP is more scalable than HWMP. Also, we remark that GHWMP reduces the traffic overhead.

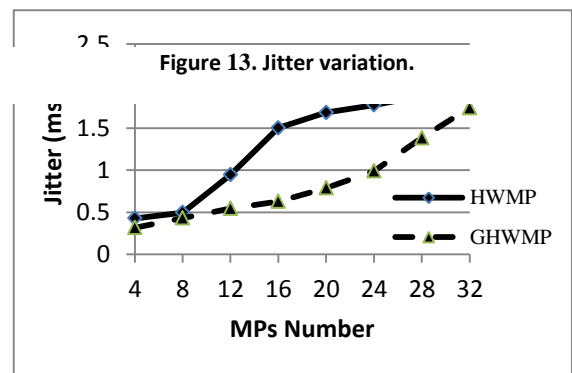
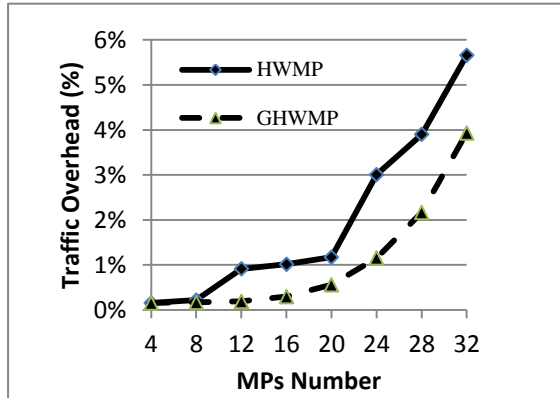


Figure 13. Jitter variation.



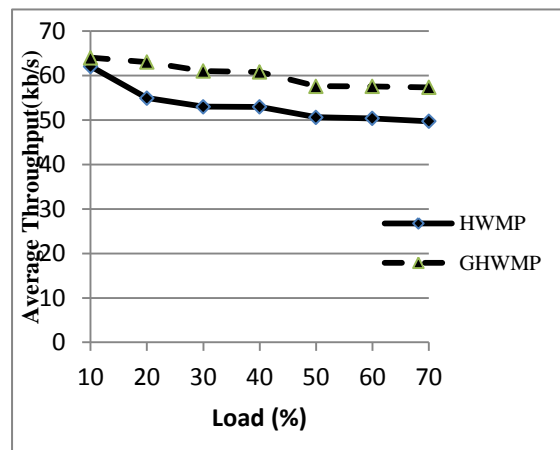
**Fig14. Traffic Overhead as a function of MPs number.**

### 6.2.3 Load increase

In this scenario, we adopted a fixed MeshBSS. The simulation was conducted on a 400\*500 m<sup>2</sup> area with twenty MPs deployed uniformly. We will increase the traffic load carried on the network by increasing the number of active MPs. An active MP is a node capable of exchanging traffic with another one. We assume intra-Mesh traffic, where the source and destination belong to the same network.

#### a. Throughput

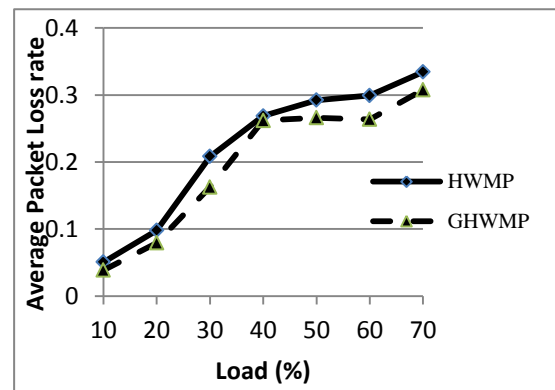
Fig 15 shows the average throughput evolution according to the load increase. When the load increases from 10% to 70% the average throughput drops by 11% for GHWMP and by 23% for HWMP.



**Fig 15. Throughput evolution.**

#### b. Packet Loss rate

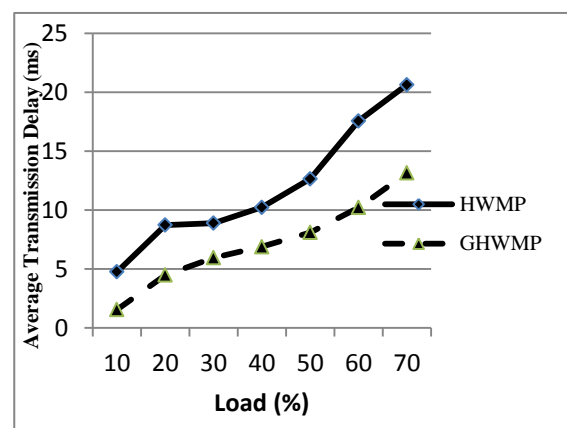
Fig 16 shows the average Packet Loss rate evolution depending on load increase. We remark that the PLR increases considerably when the load increases because the network becomes more congested. We note, also, that HWMP has the highest Packet loss ratio. This result is due to the amount of traffic overhead generated by this routing protocol which is based on flooding. Indeed an increase in the number of control and data packets affects the links quality and increases loss rate of data especially in high loaded network. We also note that GHWMP is slightly better than HWMP.



**Fig 16. Packet Loss Rate evolution.**

#### c. Transmission delay and jitter

Fig 17 shows the average transmission delay evolution depending on load increase. We note that the load increase degrades the average transmission delay for both protocols especially HWMP. When the network load increases from 40% to 70% the transmission delay increases to reach 22 ms but with GHWMP it didn't exceed 13 ms.



**Fig 17. Transmission Delay.**

Fig18 shows the average jitter variation depending on network load increase. From this figure, it is clear that the average jitter increases with the network load increase. Indeed, more the network is loaded, data and control traffic generated become important. As a result,

the network becomes increasingly congested. We also note that the GHWMP is much better than HWMP.

#### d. Traffic Overhead

Figure 19 shows the variation of Traffic overhead generated by HWMP and GHWMP according to the network load. We note that traffic overhead increases when the network load increases. We conclude that these two protocols have similar behavior regarding the network load increase. GHWMP outperforms slightly HWMP when the load is inferior to 40% or between 50% and 70%.

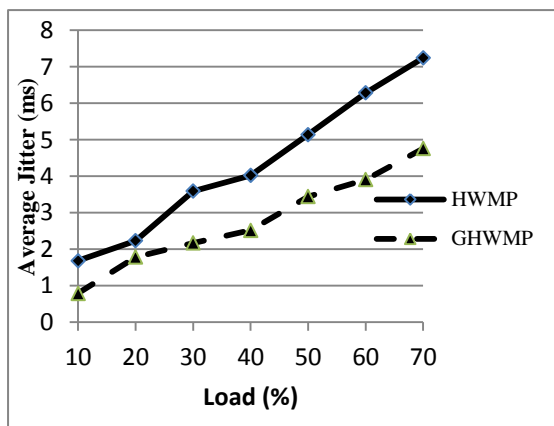


Fig 18. Jitter variation.

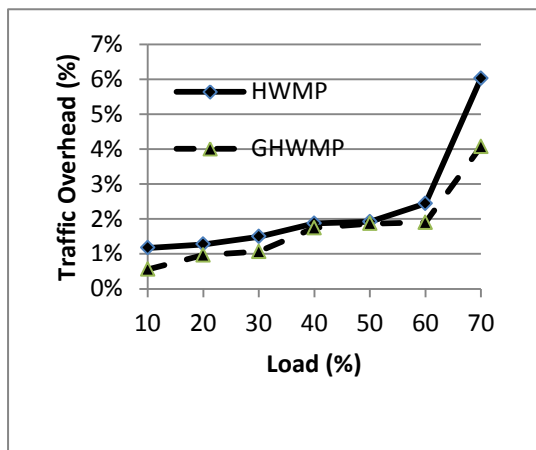


Fig 19. Traffic Overhead evolution.

## 7 CONCLUSIONS

In this paper, we proposed GHWMP protocol to reduce routing overhead traffic exchanged among MPs when RM-AODV protocol is used for intra-Mesh traffic in IEEE 802.11s network.

GHWMP adopts a geographical routing mechanism for its reactive mode. It uses the location information of MPs, provided by GPS, to determine and limit the zone in which the source expects to find the destination. Its main purpose is to reduce the overhead traffic and to provide efficient routing in mobile WMNs.

A performance comparison between HWMP and GHWMP was conducted in this paper. Simulation results reveal that GHWMP outperforms HWMP with higher throughput, lower packet loss rate and transmission delay. Compared to HWMP, GHWMP provides efficient routing in mobile and changing environment WMN. In addition, GHWMP is completely compatible with IEEE 802.11s standard. Furthermore, our simulation results show that HWMP can't support more than twenty MPs in the network.

As a next step, our proposed protocol can be extended to any mobility model. Also, we plan to study routing in Multi-channel and Multi-radio WMNs in order to ameliorate the QoS provided by Mono-channel and Mono-radio IEEE 802.11s networks and ensure a suitable load balancing between different radio channels.

## REFERENCES

- [1] Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment 10: Mesh Networking, IEEE Unapproved draft P802.11s/D3.0, March 2009.
- [2] IEEE Std 802.16f. Amendment to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems, December 2005.
- [3] IEEE, "802.11 standard: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," 2007, standard.
- [4] Ricardo C. Carrano, Luiz C. S. Magalhães, Débora C. Muchaluat Saade and Célio V. N. Albuquerque, IEEE 802.11s Multihop MAC: A Tutorial,

- Communications Surveys & Tutorials, IEEE, issue 99,p. 1-16, May 2010.
- [5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF Internet Std. 3561, July 2003.
  - [6] Xudong Wang and Azman O. Lim, "IEEE 802.11s wireless mesh networks: Framework and challenges", Ad Hoc Networks, vol.6, August 2008
  - [7] Michael Bahr, Proposed routing for IEEE 802.11s WLAN mesh networks, WICON '06: Proceedings of the 2nd annual international workshop on Wireless internet, 2006.
  - [8] IEEE 802.11 WG, Draft Supplement to standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment 8:Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/D13.0, Nov. 2005.
  - [9] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer, L. Berlemann, "Principles of IEEE 802.11s," IEEE ICCCN'2007, Honolulu, Hawaii, USA, 13-16 August 2007.
  - [10] Bernhard H. Walke, Stefan Mangold, and Lars Berlemann, "IEEE 802 Wireless Systems Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence", John Wiley, Ltd, 2007
  - [11] T. Clausen, and P. Jacquet, "Optimized Link State Routing Protocol", IETF Internet Std. 3626, October 2003.
  - [12] J.Camp et E.Knightly, "The IEEE 802.11s Extended Service Set Mesh Networking Standard", IEEE Communications Magazine, August 2008.
  - [13] Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE P802.11i/D10.0, April, 2004.
  - [14] Azman Osman Lim , Xudong Wang , Youiti Kado , Bing Zhang, A hybrid centralized routing protocol for 802.11s WMNs, Mobile Networks and Applications, v.13 n.1-2, p.117-131, April 2008.
  - [15] Sung-Jun Bae, Young-Bae Ko, An Efficient Proactive Tree Building Scheme for IEEE 802.11s based Wireless Mesh Networks, 2009 IEEE VTS Asia Pacific Wireless Communications Symposium (IEEE VTS APWSC 2009), Ewha Womans University, Seoul, Korea, August 20-21, 2009.
  - [16] Kazunori Ueda, Ken-ichi Baba, Proposal of an Initial Route Establishment Method in Wireless Mesh Networks, SAINT '09 Proceedings of the 2009 Ninth Annual International Symposium on Applications and the Internet.
  - [17] Tomasz Imieliński , Julio C. Navas, GPS-based geographic addressing, routing, and resource discovery, Communications of the ACM, v.42 n.4, p.86-92, April 1999.
  - [18] Young-Bae Ko , Nitin H. Vaidya, Location-aided routing (LAR) in mobile ad hoc networks, Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, p.66-75, October 25-30, 1998, Dallas, Texas, United States.
  - [19] NS3 simulator, version 3.6, [www.nsnam.org](http://www.nsnam.org).
  - [20] Flow Monitor patch, Gustavo Carneiro, Pedro Fortuna, and Manuel Ricardo, "FlowMonitor - a network monitoring framework for the Network Simulator 3 (NS-3)", Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools, Pisa, Italy, 2009
  - [21] IEEE, "P802.11s draft d3.02, draft amendment to standard IEEE 802.11: ESS mesh networking," 2008, standard.