VLANs Investigation in IEEE 802.11s Based Wireless Mesh Networks

Youssef Saadi, Bouchaib Nassereddine, Soufiane Jounaidi, Abdelkrim Haqiq

Abstract— ***The virtual local area network (VLAN) technology is a convenient concept to improve the wireless mesh networks performance by eliminating the unnecessary rebroadcasts flooded from stations located outside the mesh BSS.***

Hundreds or even thousands of stations may be located at a IEEE 802 LAN segment which leads to think about broadcasting cost if such segment is bridged to the wireless mesh BSS. The latter is seen as a single broadcast domain from external networks. Consequently, flooding may hinder the transmission of data frames due the broadcasting storm problems.

VLANs is a logical concept that aims to segment a network into different broadcast domains by compartmentalizing users and devices. A bridging solution that carry VLANs traffic along the mesh BSS may reduce the flooding impact on data frames transmission. In this paper, we investigate the VLAN support for IEEE 802.11s. We were motivated by the fact that no specification of VLAN integration has been defined in the draft of IEEE 802.11s.

Keywords—***Flooding, IEEE 802.11s, Multicasting, VLAN, Wireless Mesh Network.***

I. Introduction

Wireless Mesh Network (WMN) is an emerging technology to provide ubiquitous high bandwidth access for a large number of users in a cost-effective, easy, and fast manner. WMNs are particular type of mobile ad hoc network (MANETs) with low mobility, providing improved services and lower infrastructure costs than conventional wireless networks. They are typically self-organized, self-configured, self-healing and self-discovering.

In this study, we focus interest to IEEE 802.11s based wireless mesh networks [1]-[2] which are the next evolution step in IEEE 802.11 Wireless Local Area Networks (WLANs) [3]. They tend to extend wirelessly the coverage area of WLANs by dynamic association of access points (APs).

IEEE 802.11s networks distinguish between different network components as shown in Fig. 1:

Stations (STA): which presents any device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

Access Point (AP): any entity that has station (STA) functionality and provides access to the distribution services (DS), via the WM for associated STAs.

Mesh stations (mesh STAs): they are wireless routers that have mesh capabilities. They forward data frames on the behalf of other mesh STAs according to IEEE 802.11s standard. They constitute a wireless mesh BSS (MBSS) among them (referred to as mesh in the following).

Mesh gates: they are gateways bridging the mesh to external networks (i.e., Internet). They have access to the DS and also implement mesh facility.

The mesh operates like an IEEE 802 LAN segment compliant to IEEE 802.1D. It can be seen as a single broadcast domain for outsider devices (non-mesh stations) and thus can integrate with other 802.11 networks. Mesh gates implement bridging functionalities according to IEEE 802.1D specifications. Any 802.11 network can be interconnected to the mesh via mesh gates.

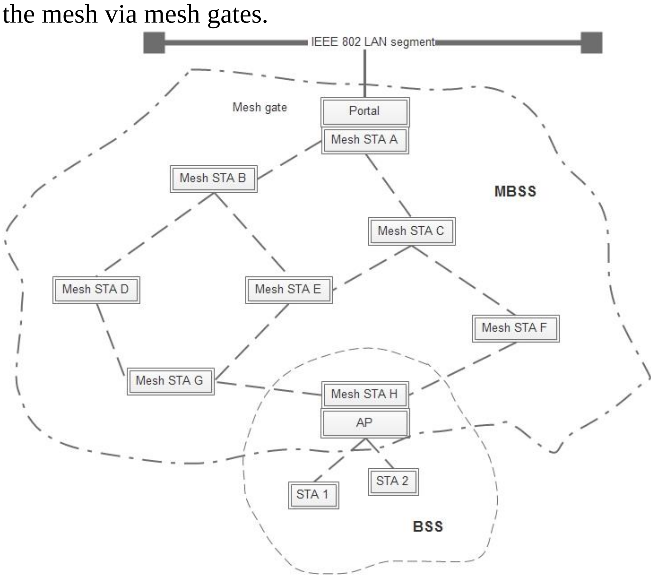

Figure 1. IEEE 802.11s WMN architecture

Flooding is frequent operation in IEEE 802.11s based wireless mesh networks. Actually, routing protocol may flood frequently control packets. In addition, stations may disseminate the messages sent by their deployed broadcast-based applications. This means a great amount of broadcast traffic that flows into the mesh.

Manuscript published on 30 August 2015.
***** Correspondence Author (s)

Youssef SAADI*, Computer, Networks, Mobility and Modeling laboratory, Department of Mathematics and Computer, FST, Hassan 1st University, Settat, Morocco.

Prof. Bouchaib Nassereddine, Computer, Networks, Mobility and Modeling laboratory, Department of Mathematics and Computer, FST, Hassan 1st University, Settat, Morocco.

Soufiane Jounaidi, Department of Mathematics and Computer,Computer, Networks, Mobility and Modeling laboratory, FST, Hassan 1st University, Settat, Morocco.

Dr. Abdelkrim Haqiq, PhD. (Doctorat d'Etat), Professor, Department of Mathematics and Computer, FST, Hassan 1st University, Settat, Morocco.

Thus, if stations are not rationally deployed then the WMN performances may be easily degraded due the broadcast storm problems [4]. One solution to that is to use Virtual Local Area Network (VLAN) concept. VLANs [5] may reduce considerably the broadcast traffic because of authorization on forwarding operation. This means a reduced flooded messages, reduced contention and secure forwarding by only legitimated devices.
If LAN segment is interconnected to a WMN, then additional functionalities must be added to mesh gates to deal with broadcasting.
Mesh gates uses IEEE 802.1D standard to make translation between IEEE 802 and IEEE 802.11s networks.
For example, when a broadcast is performed at LAN segment, it will be translated to a broadcast 802.11s frame format and then flooded through the mesh. It is a complete flooding process involving all mesh components. However, if VLANs are defined, the broadcast frame will reach only concerned devices having same VLAN identity. It is a considerable gain in terms of traffic load and security.
In this paper we introduce VLANs support in IEEE 802.11s networks. We compare our proposition to flooding to get communication improvement efficiency.
The reminder of the paper is organized as follows.
Section 2 introduces the VLAN technology. Section 3 outlines the routing and internetworking concept in IEEE 802.11s based WMN. Section 4 presents some related works. Section 5 proposes the VLAN support in WMN while section 6 presents the simulation model and results. Finally, section 7 concludes this paper.

II. Virtual Local Area Network Concept

A VLAN (Virtual Local Area Network) is a local network of a set of logical users and devices which are connected administratively and defined ports on a switch.
With virtual networks (VLANs) it is possible to overcome the limitations of the physical architecture (geographic constraints, addressing constraints ...) by defining logical segmentation (software) based on combination devices with criteria (MAC addresses, port numbers, protocols, etc.).
VLANs are cost and time effective, can reduce network traffic, and offer an extra measure of security.
By creating VLANs, we create smaller broadcast domains. Only subscribed devices to a particular VLAN identity have the ability to treat the broadcast packets initiated by devices having same VLAN ID. Generally, all communications are managed according to VLAN membership policy based on port members, MAC addresses or IP addresses.
There are two type of VLAN membership:

- Static VLANs which are created by network administrator.
- Dynamic VLANs which are assigned dynamically (software) based on MAC address, protocols and applications.

A switch port can be an access port or a trunk port. An access port vehicles only one VLAN traffic while trunk port belongs to all VLANs.
A trunk link defines the link between two switches to carry all VLANs traffic between them. It is a 100 or 1000 Mbps point to point link. At a time it carries the traffic of 1 to 4094 VLANs.
To identify VLANs switches uses several trunking methods. Mainly the most used ones are Inter-Switch link (ISL) or IEEE 802.1Q tagging.
ISL operates at layer 2 and encapsulates the Ethernet frames by new header and cyclic redundancy check. It is used only for Fast and Gigabytes Ethernet links.
IEEE 802.1q tags the Ethernet frames by new information element to identify the VLAN to which frames belong. Tagging is used through trunk links only and removed when frame forwarding on access ports.
Below in Fig. 2, is shown the IEEE 802.1Q tagging information in the Ethernet frame. In this study we are only concerned by bridging IEEE 802 networks.

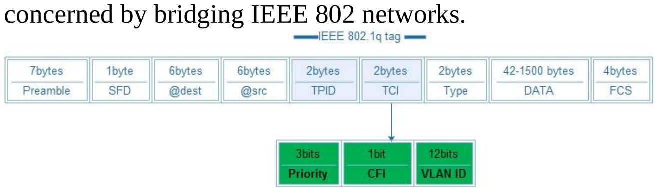

Figure 2. IEEE 802.1Q frame

The TPID (tag protocol identifier) is defined to be equal to 0x8100. It identifies an IEEE 802.1Q tagged frame.
The TCI (tag control information), consists of 12 bits correspond to the VLAN identifier and 4 bits containing metadata used for QoS management.

III. Routing and Internetworking in IEEE 802.11s Based WMN

A. Routing

Routing in IEEE 802.11s based WMNs relies on layer 2 addressing instead of IP addresses. This is why the term “path selection” is preferred to routing. The standard defines a default path selection protocol, namely, Hybrid Wireless Mesh Protocol (HWMP) [6] which provides both reactive path selection derived from the Ad hoc On Demand Distance Vector (AODV) [7] and proactive tree oriented approach. The default metric is, namely, airtime metric and it indicates the link’s overall cost.
In the reactive Radio Metric AODV protocol, the route is established on demand. Indeed when a mesh STA wishes to communicate with another mesh STA that he does not know the path, it initiates a path discovery process to look for an optimized path selection. It broadcasts a path request packet (PREQ) that may cross multiple hops to reach the destination or a mesh STA knowing already a fresh path to this destination. On receiving the PREQ, the destination mesh STA responds the source by sending a unicast path reply packet (PREP) to indicate the reverse path to the destination.
The proactive tree building mode most often used for path selection to gateways (mesh gates). It configures a particular mesh STA as the root of the tree (e.g., bridge linking an external network). It defines two methods to disseminate path information for reaching the root: the first is the proactive PREQ that aims to select paths between the root and all mesh STAs in the network. The second is intended to distribute path selection for reaching the root but actual paths to the root may be built according to the on demand mode.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

B. Internetworking

To integrate the non-mesh stations into path selection, the standard adopts a solution introducing a total of sixth addresses to the IEEE 802.11s data frame (Fig. 3). This is useful when both source and destination are non-collocated non-mesh stations. Non-collocated mesh stations means stations that are not part of the same LAN segment or stations not associated to the same access point.

The frame will keep track of both source and destination, both actually intermediate transmitting and receiving mesh stations and of both source and destination proxies mesh gates.

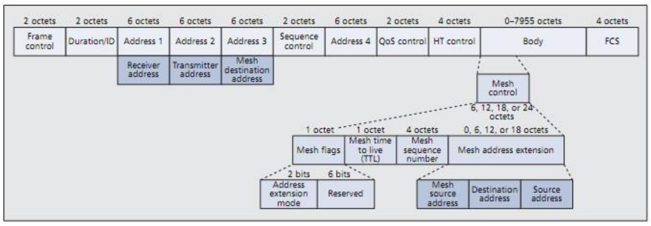

Figure 3. IEEE 802.11s data frame [2]

Each mesh gate or mesh STA with access point facility stores its associated STAs in a so-called “proxy-table”. Proxy mesh gates proxy data frames for non-mesh stations and they learn reactively proxy information when receiving frames from their non-mesh interfaces. To learn about non-collocated non-mesh STAs, some changes were carried to PREQ (Fig. 4) and PREP (Fig. 5) in a similar way as the IEEE 802.11s data frame.

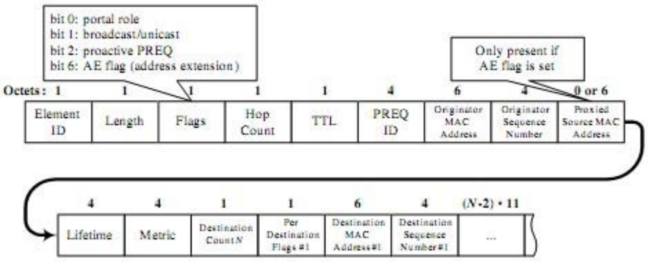

Figure 4. Path Request message (PREQ) [8]

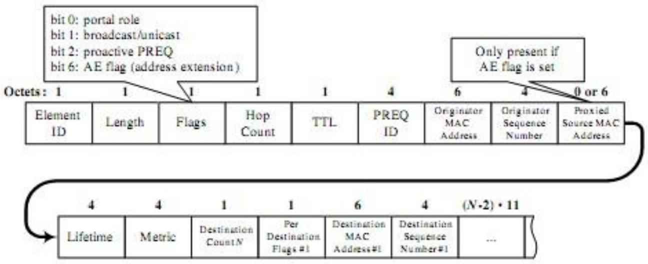

Figure 5. Path Reply message (PREP) [8]

When an originator mesh STA (source proxy mesh STA) attempts to establish a path to a target, it does not know whether the target is a mesh STA located inner the mesh or a station outside. Only when the Originator receives a PREP does it learn if the target is a mesh STA in the mesh or not. It checks the Address Extension (AE) Flag of the PREP, if the latter is set to 1 then it learns the proxied target by checking the proxied destination MAC Address field.

In the same way, the target proxy mesh gate referring to the mesh gate proxying for the target, will learn about source non-mesh stations when receiving a PREQ and checking the AE flag. If it is set then the target mesh gate will learn the proxied source MAC Address.

The IEEE 802.11s standard defined the Gate Announcement Protocol that aims to announce each mesh gates to the other mesh STAs in the MBSS.

Alternatively, when the proactive PREQ or proactive RANN method is used, the mesh gate announce its presence by setting the Gate Role field equal to 1 when sending proactively a PREQ or RANN message.

When the mesh gate uses one of the HWMP proactive path selection methods, the gate announcement protocol is not used. Thus, all mesh stations will be aware of mesh gates existence. Which will be helpful in VLAN support as only the mesh gates are concerned by learning and forwarding VLANs traffic.

C. Multicasting in IEEE 802.11s based WMN

Authors in [9] proposed an efficient multicasting scheme adapted to IEEE 802.11s networks. They simply utilize tree-based path selection information created and maintained by the HWMP to achieve multicasting so no additional path maintenance overhead needs to be generated.

When a new mesh STA want to join a multicasting group it sends a unicast MPC-JOIN frame (Fig. 6) to the root according to the proactive path selection maintained by HWMP. Upon receiving the frame by the next hop (parent node) mesh STA, the latter creates or updates the multicast routing table (Fig. 7) where it mentions the new multicast member (child node). After that it will forward the frame to the root by changing the source MAC Address to itself. By this way a multicasting tree is built.

Multicast group MAC address	Flag	Source MAC address	Destination MAC address

Figure 6. Multicast path change (MPC) message format [9]

A mesh node requesting path invalidation, will unicast an MPC-PRUNE frame with flag set to 0 to the root. Intermediate mesh STAs will perform corresponding changes to the multicast routing table by removing source MAC Address from child member list.

Field	Description
Multicast Group MAC Address	MAC address of the multicast group
Child Member List	list of multicast member among neighbor nodes

Figure 7. Proposed multicast routing table [9]

IV. RELATED WORKS

Few works have been devoted to investigate VLANs in wireless networks and especially in based IEEE 802.11s wireless mesh networks.

Authors in [10] proposed the integration of VLANs into WLAN systems. They investigated the effect of VLAN on WLAN performance in terms of delay and throughput. The simulation results have shown a reduced throughput and delay when using VLANs.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

They found that throughput has been improved using routing protocols like AODV and OLSR [11].
In [12], a study was performed on VLAN's creation and deployment in wireless networks. The study makes suggestions on the better kind of architectures to be used for the best of security requirements.
To avoid attacks on routing and selective forwarding in IEEE 802.11s based WMNs, authors in [13] introduced a differentiated security based on VLAN concept. They defined different protection levels to be assigned to mesh nodes. Frames that assigned certain type of protection will be accepted only by trusted nodes that contain same level of protection. Consequently, data traffic is separated and routing is performed into different protection levels.
Tzu-Chiang Chiang and Ching-Hung Yeh in [14] proposed the forwarding cache VLAN protocol (FCVP) for ad hoc networks. In this scheme the forwarding operation is progressed based on VLAN tags using a forward cache table. The tags are used to forward or filter packets. The simulation results show that FCVP outperforms original flooding process.

V. PROPOSITION OF VLANS SUPPORT IN IEEE 802.11S BASED WMN

It is obvious that to link switches between them through the mesh, the latter must act as virtual trunk port (Fig. 8).
To achieve this, the mesh gate has to be equipped by trunk interface like in switches. And according to IEEE 802.1D specifications, the mesh gate must learn tagged frames and translate them into IEEE 802.11s frames so to be forwarded through the mesh.

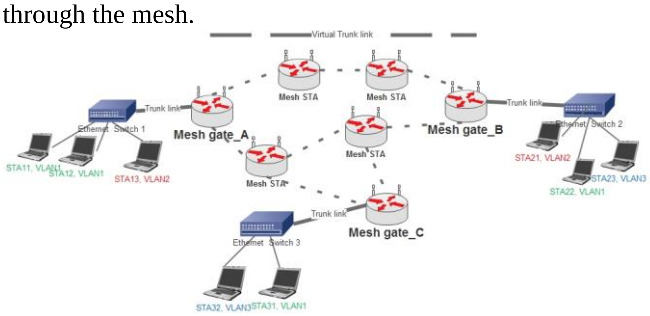

Figure 8. Typical WMN with bridged switches

The mesh will be considered then as link carrying VLANs wirelessly according to multihop communication.
Here below (Fig. 9) an update suggestion on the mesh header of the IEEE 802.11s data frame.

1 byte			1	4	0, 6, 12, 18, or 22 bytes				
Mesh Flags			Mesh Time To Live	Mesh E2E Seq Number	(Optional) Mesh Addressing				
Bit 0 et 1 : Address Extension	Bit 2 : VLAN Flag	Bit 3-7 : Reserved			Address 4	Address 5	Address 6	Vlan IE	
								VPID (2 bytes)	TCI (2 bytes)

Figure 9. Extended IEEE 802.11s mesh header format

The field VLAN ID is the same as in the tagged IEEE 802.1Q frame. The bit VLAN flag will be set to 1 to indicate that the frame is tagged and it concerns a VLAN.
When receiving a tagged frame, the proxy mesh gate will translate the frame and send it by multicasting to other mesh gates connected to the MBSS. Each mesh gate learns about existence of the others according to the mesh gate announcement protocol, or according to gate role field in proactive PREQ or proactive RANN methods as explained earlier. Each receiving mesh gate performs the translation back to the original IEEE 802.1Q frame and transmits it then via trunk port to its interconnected switch.
Obviously, each mesh gate has to inform others if it is proxying a switch. This operation can be done in the announcement phase by setting one bit from reserved ones of the flag field in both PREQ and PREP. If this bit is set, it will indicates that it has an active trunk port. This way all mesh gates become aware of mesh gates bridging switches. This knowledge is important to switch tagged frame to only mesh gates with active trunk ports.
Thus, on receiving a frame belonging to a certain VLAN, the proxy mesh gate will perform translation and send it by multicasting to all mesh gates with active trunk ports. If there is no active trunk port, the frame is simply discarded.
Activation or deactivation of trunk port on mesh gates will trigger respectively a request to join or invalidate a path for a multicasting group.

VI. SIMULATIONS AND RESULTS

In this section we evaluated the proposed bridging solution to carry VLANs traffic through the mesh BSS. We selected a grid topology which is a better choice to consider in wireless mesh networks [15]-[16]. The corners of the grid will constitute the selected 4 mesh gates bridging conventionally wired LAN segments by trunk links to switches. The root mesh STA will be placed in the center of the grid to optimize the number of hops to reach each mesh gate. The simulation aims to compare multicasting process involved in VLANs traffic transport to the broadcasting by flooding operation which present the normal behavior when no VLAN is selected. We opted for the multicasting algorithm presented earlier in section III. C. We studied the average end to end delay and overhead metrics to get network performance improvement.

A. Simulation model

We opted for a square grid mesh topology (Fig. 10). The network is sized 49 mesh STAs. Closed neighbors were distant by 175m so to allow direct communication only by immediate neighbors. To communicate with others a multihop scenario is needed. In order to apply tagging in the wireless mesh network, broadcast traffic will be differentiated by identifiers. Each distinct ID will express the VLAN ID to witch the frame belongs. Thus, on receiving a tagged frame the mesh gate will engage a MPC frames exchange if it has no valid entry in its multicasting table and then it will multicast the frame to the other mesh gates. Indeed, multicasting concerns only mesh gates with active trunk links. In the simulation we have disabled trunking on the mesh gate "D". Each mesh gate will randomly switch to different VLANs ranging from 1 to 5, and will send frames according to a determined data rate (number of frames by unit time). For computation reason we limited the number of frames sent in the network to 400 frames during the simulation time. The chosen rates are 2, 5, 10, 15 and 20 frames per second. To learn the existence of the other mesh gate and to use multicasting, we opted for the RANN proactive mode.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The Table. 1 summaries the simulation parameters.

Table 1. Simulation parameters

Network size	49 (7*7 square grid)
MAC Layer	802.11g
Transmission range	300m
Transmission data rate	54Mb/s
Frame payload	1024bytes
Traffic's type	CBR
Routing protocol	HWMP
RANN interval	3s
Packet Rate	2, 5, 10, 15, 20 frames/s
Simulation time	100s

We have implemented our suggestion using ns-2 [17]. We integrated and updated HWMP source code to take into account internetworking features. We modified the functionalities of both proactive PREQ and RANN modes. We added a module to support multicasting according to section III. C.

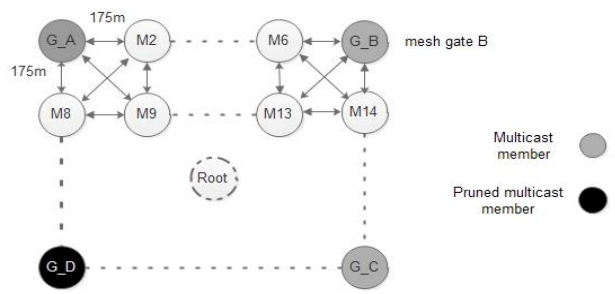

Figure 10. The studied mesh grid network

B. Performance metrics

The studied performance metrics are listed below:

End to end delay: is the time from the first moment of sending a flooding frame until its reception by the last node in the network.

Overhead: is the number of bytes transmitted by unit time. It includes broadcast data frames, HWMP control packets and MPC messages.

C. Results and interpretation

The simulations results are illustrated below in Fig. 11 and Fig. 12.

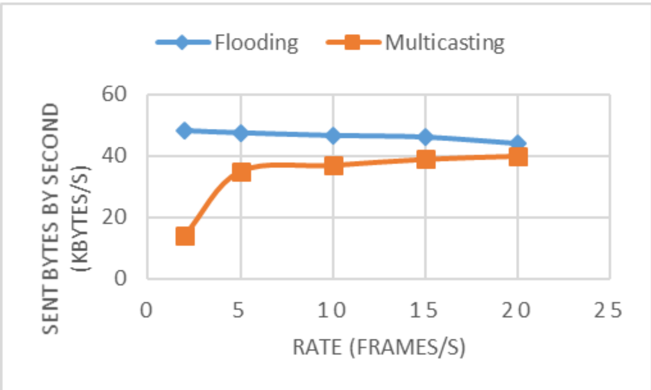

Figure 11. Overhead

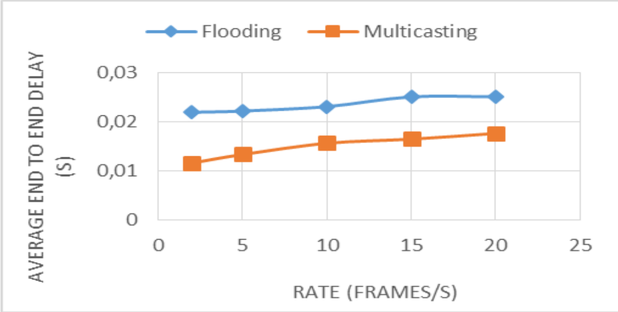

Figure 12. Average end to end delay

The results show that the use of multicasting over mesh gates with active trunk links outperforms the normal dealing with broadcast by flooding operation. The average end to end delay and the overall overhead are improved using VLANs.

The overhead in flooding is decreased when data rate is increased. This is explained by network reachability which is reduced due to the broadcasting storm problems. In the other hand, multicasting maintains increased overhead which is reasonable as all member mesh stations path is maintained by the multicasting tree.

The VLANs decreased overhead in comparison with flooding. Flooding involves all mesh stations in the forwarding process unlike multicasting where only members are involved.

As the contention is less concentrated in multicasting in comparison with flooding, the average end to end delay is considerably improved when using VLANs.

VII. Conclusion

In this paper we introduced an investigation on VLAN support in IEEE 802.11s based Wireless Mesh Networks. As the mesh gates are responsible for bridging the mesh BSS to external networks, a solution to carry VLAN traffic is based on updating the mesh gate functionalities by adding a new support to translate tagged frames based VLAN to IEEE 802.11s frames. To carry VLANs traffic the mesh gates will be the start and end points for a virtual trunk link between switches. VLANs and multicasting to mesh gates will reduce the impact of flooding when outside stations are not compartmentalized according to VLAN concept. The simulation results show the network improvement in terms of average end to end delay and overhead. Future work tends to extend the investigation to more complex simulation scenarios including mobility, scalability and traffic differentiation. Adaptive multicasting membership will be adopted to switch broadcast frames to only concerned mesh gates. A mesh segmentation and VLAN's awareness are needed for this purpose.

References

[1] X. Wang, and A.O. Lim, IEEE 802.11s wireless mesh networks: Framework and challenges, *Ad Hoc Networks 6 (2008) 970–984.*

[2] Hiertz, G.R.; Denteneer, D.; Max, S.; Taori, R.; Cardona, J.; Berlemann, L.; Walke, B., "IEEE 802.11s: The WLAN Mesh Standard," *Wireless Communications, IEEE , vol.17, no.1, pp.104,111, February 2010. doi: 10.1109/MWC.2010.5416357*

[3] IEEE 802.11 Standard Working Group, Draft Standard for Information Technology –Telecommunications and Information Exchange Between Systems – LAN/MAN Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE P802.11-REVma/D9.0, January 2007.*
[4] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, J.-P. Sheu, The broadcast storm problem in a mobile ad hoc network, *Wireless Networks 8 (2/3) (2002) 153–167.*
[5] G. Prakash Pal, S. Pal, “Virtual Local Area Network (VLAN)”, International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 1 Issue10 pp 006-010 January 2013. ISSN 2278 - 0882
[6] IEEE 802.11s Task Group HWMP Specification doc.: IEEE 802.11-06/1778r1 November 2006.
[7] C.E. Perkins, E.M. Belding-Royer, S.R. Das, Ad hoc on-demand distance vector (aodv) routing, IETF RFC3561, July 2003.
[8] Bahr, M., "Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s," Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on, vol., no., pp.1, 6, 8-11 Oct. 2007 doi: 10.1109/MOBHOC.2007.442872.
[9] Sung-Jun Bae; Young-Bae Ko, "Efficient layer-2 multicasting for IEEE 802.11s based wireless mesh networks," Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on, vol., no., pp.109,114, 16-18 June 2010. doi: 10.1109/ICUFN.2010.5547223
[10] S Y. Ameen, S W. Nourildean, “Wireless Local Area Network VLAN Investigation and Enhancement Using Routing Algorithms”, International Journal of Engineering and Advanced Technology (IJEAT), Volume-3, Issue-2, December 2013, ISSN: 2249 – 8958.
[11] Clausen T, Jacquet P, RFC 3626-“Optimized Link State Routing Protocol (OLSR)”, Oct 2003.
[12] Rajul Chokshi and Dr. Chansu Yu, “Study on VLAN in Wireless Networks”, 2007.
[13] T. Gamer, “Differentiated security in wireless mesh networks”, SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks. (2009). DOI: 10.1002/sec.163
[14] Tzu-Chiang Chiang, Ching-Hung Yeh, Yueh-Min Huang, “A virtual subnet protocol for mobile ad hoc networks using forwarding cache scheme”, International Journal of Computer Science and Network Security, Vol. 6 No. 1 pp. 108~115.
[15] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, M. Singh, Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols, in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’05), 2005, pp. 1664–1669.
[16] J. Robinson, E. Knightly, A performance study of deployment factors in wireless mesh networks, in: Proceedings of the IEEE International Conference on Computer Communications (INFOCOM ’07), 2007, pp. 2054–2062.
[17] Kelvin Fall, “The ns manual (formerly ns Notes & Documentation)”, US Berkerley LBL USC/ISI and Xerox PARC, 2010.

Youssef SAADI received the B.Sc. degree in Computer Engineering in 2005 and M.Sc. degree in Systems and Networks in 2008 from Hassan 1st University, Faculty of Sciences and Techniques of Settat (FSTS), Morocco. He has been working as professor of Computer Sciences in high school since 2006, Berrechid, Morocco. Currently, he is working toward his Ph.D. at FSTS. His current research interests are: Wireless Mesh Network Capacity Amelioration, Flooding Operation Improvement, and Study of Mobile Ad hoc Networks.

Prof. Bouchaib Nassereddine is a professor at Faculty of Sciences and Techniques (FSTS), Hassan 1st University, Settat, Morocco. He is an active member of research team RIME at MOHAMMADIA School of Engineers, Rabat, Morocco and he is a researcher in the Computer, Networks, Mobility, and Modelling Laboratory, at FSTS.

Dr. Abdelkrim Haqiq has a High Study Degree (DES) and a PhD (Doctorat d'Etat), both in Applied Mathematics, option modeling and performance evaluation of computer communication networks, from the University of Mohamed V, Agdal, Faculty of Sciences, Rabat, Morocco. Since September 1995 he has been working as a Professor at the department of Mathematics and Computer at the Faculty of Sciences and Techniques, Settat, Morocco. He is the Director of Computer, Networks, Mobility and Modeling laboratory and the Coordinator of the education of Computer Engineering at the Faculty of Sciences and Techniques, Settat. He is also a General Secretary of e-Next Generation Networks Research Group, Moroccan section.