

A Bridging-based Solution for Efficient Multicast Support in Wireless Mesh Networks

Yassine Hadjadj-Aoul, Seán Murphy and Liam Murphy
UCD School of Computer Science and Informatics
University College Dublin, Belfield, Dublin 4, Ireland

Abstract—Wireless mesh networking is a promising, cost effective and efficient technology for realizing backhaul networks supporting high quality services. In such networks, multicast data are transmitted blindly without any mechanism protecting data from loss, ensuring data reception, and optimizing channel allocation. The multicast services may undergo, then, very high data loss ratio which is exacerbated with the number of hops. In this paper, we propose a Reliable Multicast Distribution System (RMDS) to optimize multicast packets transmission in bridged networks. Relying on a modification of the IGMP snooping protocol, RMDS enables reliable services provisioning support in common wireless mesh networks. In particular, RMDS only exploits the local knowledge of a particular node to compute the multicast tree, which significantly reduces the signalling overhead in comparison with network layer and overlay solutions. Simulation results elucidate that RMDS optimizes resources' allocation by reducing significantly the network load, the media access delay and the data drop rate compared to the classical approach, which is based on the combination of spanning tree algorithm and IGMP snooping protocol.

Index Terms—Reliable, Multicast, IGMP Snooping, Mesh Networks, Bridged Networks.

I. INTRODUCTION

Wireless mesh networking is an emerging, cost effective and efficient technology for realizing backhaul networks supporting high quality services. The multi-hop wireless network architecture of Wireless Mesh Networks (WMN) enables efficient coverage of large areas with only few interconnections with the wired infrastructure. Furthermore, WMNs auto-organize and auto-configure themselves which eventually results in reduced up-front cost and lower network maintenance costs for operators. Nevertheless, there are still many open issues in the design of WMN. One of the most important one in such resource constrained networks is to support multicast services.

Multicasting is an efficient way to deliver data simultaneously to a set of destinations since it avoids redundant and useless transmissions [9]. This not only allows additional bandwidth saving but also reduces energy consumption, a very desirable feature for many Wireless Multi-Hop Networks. In such networks, multicast data are broadcasted after detecting that the channel has been idle during a period of time equal to the *DIFS* period plus a random back-off time. This means that the multicast data are transmitted blindly without any mechanism protecting from loss (e.g. RTS/CTS handshake) and without any guarantee of reception (e.g. Acknowledgement ACK). Moreover, the basic CSMA/CA mode used for

multicast increases the hidden terminal problem since it does not perform any channel allocation. The multicast services may undergo, then, very high loss ratio which is exacerbated with the number of hops. Consequently, the support of reliable multicast is not only a desirable feature but a substantial necessity to the success of such services.

The issue regarding reliable multicast transmission in WMN has been extensively discussed [9][3]. To create optimal multicast trees, however, a prerequisite for those schemes is global information of the network topology, impelling them to operate at network or application layers. Obviously, they are unsuitable for wireless bridged networks, where packets handling is performed below the IP layer. Also, in this context, the nodes knowledge of the topology is limited to the local neighborhood. This makes the creation of multicast trees impossible following the upper layer standard.

The few existing bridging-based solutions which are based on a combination of the spanning tree algorithm and the IGMP snooping protocol, exploit the shortest path to the gateway. These approaches focus on reducing the nodes' cost regardless of that of the total tree. In this paper, we propose a novel Reliable Multicast Distribution System (RMDS) to optimize multicast packets transmission in bridged networks. Relying on a modified version of the IGMP snooping protocol, RMDS enables reliable services provisioning support in common WMN. This novel scheme, which only exploits the local knowledge of a particular node to compute the multicast tree, optimizes the tree's cost while significantly reducing the signalling overhead, compared to overlay and network layer solutions.

The reminder of the paper is organized as follow: Section II discusses the related works on reliable multicast architectures in WMN. Section III provides the key components of the proposed reliable multicast protocol. Section IV portrays the simulation setup and discusses the obtained results. Finally, the paper concludes in Section V with a summary recapping the main advantages and achievements of the proposed scheme.

II. BRIEF OVERVIEW OF RELIABLE MULTICAST ARCHITECTURES IN WMN

Reliable multicasting in Multi-Hop networks can be designed in different ways. Existing reliable multicast techniques can be broadly classified according to the layer which provides the multicast service, i.e., Overlay-based multicast schemes (e.g. Application layer), Wireless Routers-based multicast

schemes (e.g. Network layer) or Wireless bridging-based multicast schemes (e.g. Link layer).

The issue regarding network layer's reliable multicast transmission in WMN has been extensively discussed [9]. These approaches can be further divided into two categories: MAC-enabled Reliable Multicast [2] and FEC/ARQ coding for Reliable Multicast [8]. By exploiting the broadcasting advantage, the network-based multicast solutions allow scalable communications. This induces, however, less efficiency and unreliable transmissions since the data are transmitted at a basic service rate and without channel allocation beforehand. To improve reliability, handshake-based approaches were proposed. These approaches improve the network performance when very few loss is experienced by the receivers [12]. When the loss ratio is high, FEC/ARQ-based techniques are more effective even if they lead to increased end-to-end delay [6].

In Overlay Multicast (OM), the overlay network which is formed by the nodes participating in the multicast data transmission rely on unicast delivery and does not require any multicast network layer support [4], [11]. Compared to network-based multicast, overlay multicast is more reliable while it allows the use of higher data rates. Nevertheless, the signalling overhead augmented with the peer-to-peer transmission of multicast traffic lead to some performance issues over the network layer-oriented solutions. This drawback disappear, however, in large scale networks since the overlay tree cost decreases as the level of the host in the overlay increases [3].

The problem of link layer multicasting over WMN has not been discussed in depth in existing literature. In such networks, the multicast data are simply flooded to the immediate vicinity of the node. Each intermediate node retransmit, then, the multicast packets which consumes lot of bandwidth and may lead to congestion. To ensure loop-free topology while preserving the quality of MAC services, the Rapid Spanning-Tree Protocol (RSTP) which supersedes the Spanning-Tree Protocol (STP) was standardized in MAC bridges [5]. RSTP defines a tree that spans all the nodes in an extended network while preventing undesirable loops by placing redundant ports in a backup state. This protocol improves the bridges performance by restraining the flooding of data packets to non redundant links only. Further, the RSTP tree allows connecting each node within the extended network to the root¹ using the shortest path. The efficiency of multicast is, however, limited in such networks. Indeed, the multicast packets are flooded to all the nodes as the multicast MAC address is never used as source (e.g. Source pruning behavior). To restrain the multicast traffic to only the end stations registered to that multicast group, the authors in [13] proposed the IGMP Snooping protocol. A similar protocol, named GARP (Generic Attribute Registration Protocol) Multicast Registration Protocol (GMRP), was proposed and included as a part of the IEEE standard 802.1D [5]. The basic idea behind each of these protocols is to get information of multicast group and their members at

¹The root in wireless networks is not selected randomly as in wired networks; it is, indeed, represented by the Mesh Portal (MP).

layer two. In such architecture, the bridges are responsible of keeping track of the set of multicast groups for which active members currently exist. This permits suppressing the transmission of multicast packets on links where no valid recipients is reachable. Lacking a global view of the network, the multicast tree construction in bridged networks is not optimal, which makes the bridging-based solutions not suitable in large scale networks. When the number of hops is limited to two or three hops, the link layer multicast tree converge to the optimal multicast tree, which makes such solutions more suitable in small scale networks. In such configuration, the reduced overhead along with the possibility of exploiting higher data rates without modifying the standardized MAC layer make bridging-based solutions more viable.

III. RMDS: RELIABLE MULTICAST DISTRIBUTION SYSTEM

A. System overview

In this paper, a mesh network which provides coverage in a metropolitan area is considered. In addition to the ability to support best effort applications such as city-wide ubiquitous Internet access, this network will provide enhanced services such as Voice over IP and Multimedia applications. The main focus, in this work is to support reliable multicast services such as: Announcements or Safety alert broadcasting (100% reliability) and Multicast streaming of video services (not guaranteed 100% reliability).

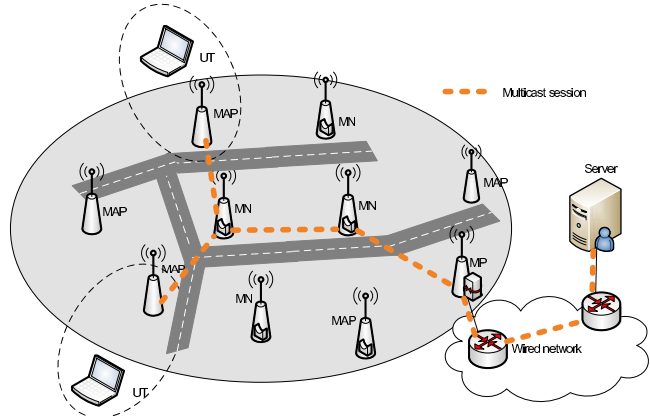


Fig. 1. General overview of the network.

As mesh networks are resource constrained, we assume that the mesh backbone is a multichannel, multi-radio system resulting in greatly increased backbone capacity. Fig. 1 illustrates the scenario under study here. The network comprises of:

- User Terminals (UTs) which connect to the mesh network;
- Mesh Access Points (MAPs) which provide access to the UTs and form part of the mesh backbone;
- Mesh Nodes (MNs) which do not provide UT access but relay traffic within the mesh;

- Mesh Portals (MPs) which provide connectivity between the mesh backbone and a wired infrastructure.

B. Problem formulation

The problem of calculating the optimal multicast trees at network or application layers is fundamentally different from the problem of calculating it at the link layer. Indeed, a global knowledge of the network topology is available above the network layer. This makes the deduction of efficient multicast trees easier than in link layer where only a local view is available.

As stated in the related work section (see section II for more details), the link layer approaches proposed in the literature exploit spanning tree-based protocols to construct the multicast trees. Spanning tree meets the design objectives of unicast traffic since the shortest path is only related to a particular destination. The shortest path for multicast traffic concerns, however, a set of destinations making the spanning tree unsuitable for such traffic. Indeed, optimizing the path from each destination to the mesh portal may increase the total cost of the tree, which may reduce the total bandwidth while increasing the contentions. To overcome these issues while solving the multicast traffic reliability problem, we propose a new link layer algorithm which minimizes the multicast trees' cost while reducing the hidden node problem.

Note that the Multiple Unicast (MU) approach is adopted in the core network to guarantee the multicast traffic reliability. Besides, the proposed algorithm relies on the IGMP snooping algorithm [13] in order to restrain the multicast traffic only to the nodes registered to that multicast group.

1) *Problem parameters:* As the proposed link layer protocol relies on unicast delivery to provide reliable multicast, each node in the wireless mesh network can transmit using the highest rate in contrast with network layer protocols.

To simplify the network model, let us consider the wireless mesh network topology in the form of an undirected graph $G = (V, E, W)$, where V is the set of nodes, E is the set of duplex links between pairs of nodes and W is the set of weights² of edges in E . Let $d(v_i, v_j)$ be the euclidian distance between the nodes $v_i, v_j \in V$. An undirected edge $e_{ij} = e(v_i, v_j) \in E$ exists if and only if $d(v_i, v_j) < r$, where r is the range of the lowest transmission rate. We also assume that a multicast session consists of one source node s and a set D of m destination nodes belonging to V (e.g. $D = \{d_k | d_k \in V, k \in [0, m]\}$).

Let Ψ be a set of multicast trees. Each multicast tree $\psi_i \in \Psi$ which is implemented using unicast in our use case, is composed of a set of sub trees T having the same source s and reaching disjoint subsets of destination nodes $D_i, D_i \subseteq D$. The sub trees contains no repeated edges and no repeated nodes (e.g. Cycles are not supported). Moreover, their collection must covers all the nodes registered into a particular multicast session.

We can express these conditions by the following equation:

$$\Psi = \{\psi_i | D_i \in \psi_i \wedge D_i \subseteq D\} \quad (1)$$

where:

$$\begin{cases} \bigcup_{i=1}^N D_i = D \\ \bigcap_{i=1}^N D_i = \{\phi\} \end{cases}$$

where N represents the total number of sub trees $t_i \in T$ implicated in the construction of the multicast tree.

In the following, the sub tree length which represents the number of edges implicated in the construction of the sub tree $t_i \in T$ is denoted by P_i . P_i can represent other metrics such as the link's weight to meet other design objectives. In this case, P_i is represented by the following equation:

$$P_i = \sum_{e_{kl} | \forall e_{kl} \in t_i} w_{e_{kl}} \quad (2)$$

where $w_{e_{kl}} \in W$ denotes the weight of the edge $e_{kl} \in E$ between the nodes $v_k, v_l \in V$. Accordingly, P_i represents the sum of the edges' weight of the subtree t_i .

Note that in order to reduce the general problem's complexity, we dissociate in the following the problem of determining the optimal multicast trees and the problem of channels assignment in multi-radio nodes. The impacts of channel assignment could be integrated easily through modifying the links' weight.

2) *Design objective:* Given the parameters and variables defined in section III-B1, the objective function of the optimal wireless multicast trees planning problem can be written as follow:

$$\min \sum_{i=1}^N P_i \quad (3)$$

C. RMDS algorithm description

As the multicast tree construction problem has been shown to be NP-complete, we propose in this section a heuristic algorithm to build multicast trees.

In opposition with network layer solutions, which consider a global knowledge of the network, it is assumed below that each wireless node knows only its one hop neighbors using the periodic beaconing, for example. It is also assumed that there is no global knowledge of the network topology except the number of hops to the gateway. In bridged networks, this information is easily available by bridges at the bootstrap phase.

The following notations are used in the Function 1 which computes the next hop to the gateway and the Algorithm 2 which calculates the optimal multicast tree:

- *Curr* and *NextHop*, which represent the current node in the tree and the next hop towards the gateway, respectively;
- $\langle node \rangle .NeighborsList()$, which represents a member function of *node*, $node \in V$, returning a list of its neighbors, which are determined at the bootstrap phase;
- $\langle node \rangle .DefaultHop$, which represents a member variable of *node*, $node \in V$, whose value is equal to the

²The weight in the paper is represented by the number of hops to the MP. This metric could be changed to reach other design objectives.

neighbor through which the gateway is reached using the shortest path;

- $\langle node \rangle .HopsCount$, which represents a member variable of $node$, $node \in V$, whose value is equal to the minimal number of hops required to reach the gateway. Each particular node can easily detect its proper $HopsCount$ and its neighbors $HopsCount$ through using a spanning tree-like mechanism;
- G , which represents a particular multicast group;
- $\langle node \rangle .Member(G)$, which represents a member function of $node$, $node \in V$, that returns *TRUE* if $node$ is a member of the group G . In the Ad-Hoc case, a particular node can retrieve these values based on overhearing IGMP/MLD packets sent by its neighbors. In multi-channels use case, this values could be retrieved by overloading the beacons with the current multicast sessions or by using a signalling protocol;
- $\langle node \rangle .Join(G)$, which represents a member function of $node$, $node \in V$, that allows $node$ to join the group G ;
- $Root$, represents the MP which is the source of the multicast traffic for the WMN.

Function 1 Next_hop_selection

Input: $Curr \in V$

Output: $NextHop \in V$

```

NextHop ← Null;
for all  $n_j$  such that  $n_j \in Curr.NeighborsList()$  do
  if ( $n_j.Member(G)$ ) then
    if ( $Curr.DefaultHop = n_j$ ) then
      NextHop ←  $n_j$ ;
      return NextHop;
    else
      if ( $NextHop = Null$ ) then
        NextHop ←  $n_j$ ;
      else
        if ( $n_j.HopsCount < NextHop.HopsCount$ )
          then
            NextHop ←  $n_j$ ;
          end if
        end if
      end if
    end if
  end for
if ( $NextHop = Null$ ) then
  NextHop ←  $Curr.DefaultHop$ ;
end if
return NextHop;

```

The design principle of Algorithm 2 is to determine a self configured multicast tree allowing end-users to join and leave a particular multicast tree dynamically. Rather than considering all the wireless nodes to compute the next hop, as achieved in wireless router-based solutions, we only consider the immediate vicinity of the particular node, which

reduces considerably the computational complexity of next hop selection. As described in the optimal multicast path calculation algorithm, the multicast tree is computed from the destinations towards the *Root* in contrast with spanning tree-based algorithms.

The RMDS starts when a particular Access Point (AP) receives the *IGMP/MLD.Response* signaling packet from end-users requesting to join a particular group. Each node, within this distributed algorithm, executes the next hop selection function after receiving such signalling packets. However, if a node is already a member of the multicast group it just updates its path's time stamp and exploits its previously calculated next hop. The *IGMP/MLD.Response* packet is, then, forwarded to the selected node until reaching the *Root* or until reaching a node belonging to the multicast group. This mechanism allows the creation of a multicast path from different destinations to the source. The multicast path is updated automatically when receiving other *IGMP/MLD.Response* messages which allows adapting to topology variation. When no end-users is subscribed to the multicast group, the AP stop immediately the multicast packets forwarding. The multicast packets' forwarding is interrupted for the other node when no *IGMP/MLD.Response* message is received during a certain amount of time or when receiving the *IGMP/MLD.Leave* message which allows reacting to end-users leaving the multicast group.

Algorithm 2 RMDS: Optimal multicast path calculation

```

for all  $d_i$  such that  $d_i \in D$  do
   $Curr \leftarrow d_i$ ;
  if ( $!Curr.Member(G)$ ) then
     $Curr.Join(G)$ ;
    while ( $Curr \neq Root$ ) do
       $NextHop \leftarrow Next\_hop\_selection(Curr)$ ;
      if ( $!NextHop.Member(G)$ ) then
         $NextHop.Join(G)$ ;
      end if
       $Curr \leftarrow NextHop$ ;
    end while
  else
    print The path already exist;
  end if
end for

```

IV. PERFORMANCE EVALUATION

The purpose of this section is to evaluate the performance of RMDS using simulations conducted with Matlab [7] and Opnet [10] environments. RMDS is compared to GMRP, which uses the IGMP Snooping algorithm [13] to restrain the multicast traffic to the multicast members. The simulations focus on the abilities of our proposal to quickly construct an optimal multicast tree with only local information while improving wireless resources utilization.

A. Simulation model

In this section, we present the simulation parameters, describe the envisioned network architecture and the test scenarios. We first simulate 49 nodes (e.g. bridges) placed uniformly in a plane of 800×800 meters. The radio propagation range is 200 meters. We first construct a complete graph connecting these nodes in function of the distance (see gray lines in Fig. 2). The gateway (e.g. portal) is then selected automatically as the nearest node to the centroid³.

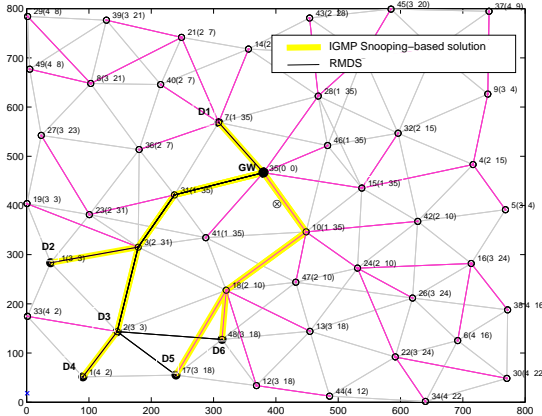


Fig. 2. Randomly generated network topology (use case under study).

Two scenarios are considered in the performance evaluation: a scenario with an IGMP Snooping-based solution and another with RMDS. We test the system under homogenous traffic conditions using a constant bit rate multicast source from a server located behind the gateway (MP). The simulations were performed during 1800s, a duration long enough to capture and study the behavior of RMDS.

In order to avoid loops in our bridged network, we compute the minimum spanning tree on that graph, which is described by the pink lines in Fig. 2. The signalling packets disseminated by the spanning tree algorithm allows the nodes to not only have the minimal number of hops to reach the gateway and the default next hop to the gateway, but also to have a local knowledge on the neighbors, which is used in our proposed protocol.

B. Simulation results

In this section, we present the simulation results to illustrate the performance of our RMDS algorithm. We use then the topology described in Fig. 2 to explain in more details the difference between our proposal and the classical approach which perform multicast at layer two based on the spanning tree and IGMP snooping as well. In this topology, the set of destinations $D = \{D_1, D_2, D_3, D_4, D_5, D_6\}$ is selected randomly using a dense mode selection.

³The centroid is represented by the symbol \otimes in Fig. 2.

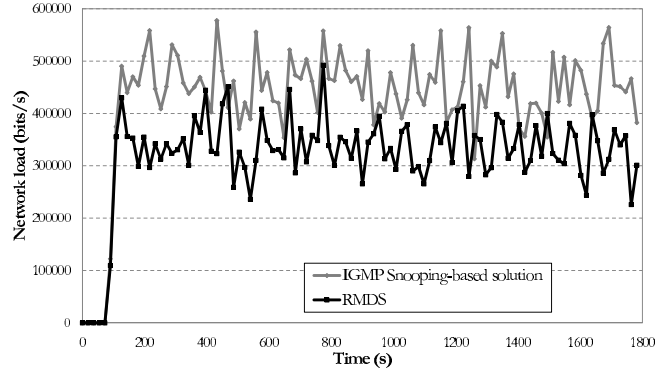


Fig. 3. Network load.

Figs. 3 and 4 depict the variations of the average network load and the media access delay measured when using the classical approach and the RMDS scheme, respectively. Fig. 3 indicates that the conventional IGMP snooping-based scheme consumes substantially higher bandwidth than RMDS. In fact, as depicted in Fig. 3, the aggregated network load with RMDS is 25.15% lower than the classical approach. This is a consequence of the reduction of the global multicast tree cost by joining the multicast tree through an already connected neighbor. However, this comes at the price of an augmentation of the end-to-end delay, since the number of hops to the gateway may increase for some particular nodes. The end-to-end delay is increased, in the simulated scenario, by approximately 3.31%, which is limited compared with the benefits of our approach. On the other hand, the network load reduction has a direct consequence on the media access delay experienced in Fig. 4. RMDS barely reaches an average access delay of $0.09ms$ while the conventional scheme reaches $0.12ms$. This corresponds to a 23.42% gain in the media access delay.

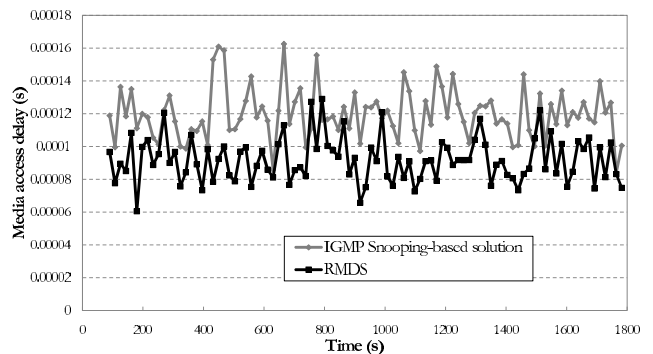


Fig. 4. Media access delay.

Figs. 5 and 6 represent the average data drop rate and the goodput experienced by the classical approach and the RMDS scheme, respectively. It is obvious from Fig. 5 that the conventional scheme exhibits significantly high packet drops. It should be noted that the discard of a packet is mainly due to buffer overflow and exceeded transmission retry threshold.

Thus, unlike the conventional approach, RMDS achieves relatively reduced data drop rate. This is a consequence to the reduction of the network load, which significantly reduce the contention at the wireless channel. In fact, as depicted in Fig. 5, the aggregated data drop rate with RMDS is 21.89% lower than the classical approach.

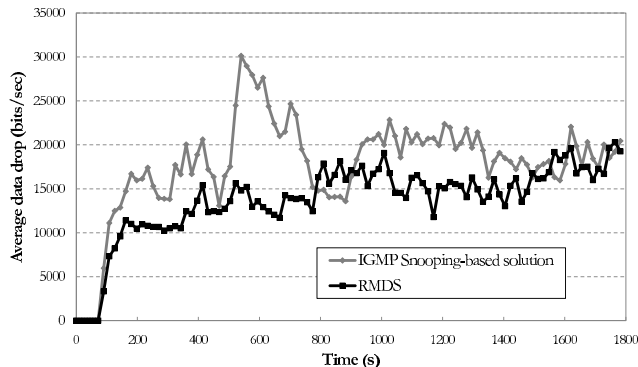


Fig. 5. Average data drop rate.

Another important observation is that the conventional approach leads to an important degradation of the goodput, as depicted in Fig. 6. This is a direct consequence of the packets loss rate experienced by the intermediate ad hoc nodes. The RMDS scheme achieves approximately an average data rate of 72.81kbits/s while the conventional approach barely reaches 65.98kbits/s per destination. This corresponds to an improvement of 10.35%.

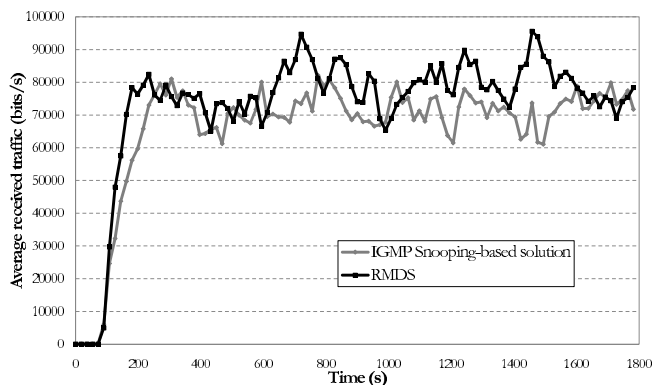


Fig. 6. Average received traffic.

V. CONCLUSION

In this paper, we have studied the problem of reliable multicast provisioning in WMNs particularly in wireless bridged networks. Specifically, we proposed a novel algorithm, called RMDS, to optimize the construction of multicast trees at link layer by solely exploiting nodes' local knowledge. The proposed scheme is different from conventional methods as it reduces the global cost of the multicast tree while dynamically adapts to topology variation. The RMDS tracks the IGMP/MLD signalling of its neighbors to enforce different

next hop selection towards the gateway. Extensive simulations showed that by considering only the immediate nodes' vicinity, RMDS significantly outperforms the existing approaches in terms of cost on multicast tree construction, load of the network, media access delay, data loss and goodput.

ACKNOWLEDGMENT

This work was partially funded by the European Commission within the 7th Framework Program in the context of the ICT project Carrier-Grade Mesh Networks (CARMEN) [1]. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the CARMEN project or the European Commission.

REFERENCES

- [1] Carmen. CARrier grade MESH Networks. ICT Project of the EU 7th framework program, <http://www.ict-carmen.eu/>.
- [2] A. Chen, D. Lee, and P. Sinha. Efficient multicasting over large-scale w lans through controlled association. *ELSEVIER Computer Networks*, Vol. 53(1):Pages 45–59, 2009.
- [3] S. Fahmy and M. Kwon. Characterizing overlay multicast networks and their costs. *IEEE/ACM Transaction on Networking*, Vol. 15(2):Pages 373–386, 2007.
- [4] C. Gui and P. Mohapatra. Overlay multicast for manets using dynamic virtual mesh. *SPRINGER Wireless Networks*, Vol. 13(1):Pages 77–91, 2007.
- [5] IEEE. IEEE standard for local and metropolitan area networks media access control (MAC) bridges. *IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998)*, pages 1–269, June 2004.
- [6] D. Koutsonikolas and Y. C. Hu. Exploring the design space of reliable multicast protocols for wireless mesh networks. *ELSEVIER Ad Hoc Networks*, In Press, Corrected Proof:–, 2008.
- [7] Matlab. <http://www.mathworks.com/>.
- [8] A. Nafaa, T. Taleb, and L. Murphy. Forward error correction strategies for media streaming over wireless networks. *IEEE Communications Magazine*, Vol. 46(1):Pages 72–79, January 2008.
- [9] U. T. Nguyen. On multicast routing in wireless mesh networks. *ELSEVIER Computer Communications*, Vol. 31(7):Pages 1385–1399, 2008.
- [10] OPenNETworks. Opnet 15, <http://www.opnet.com/>.
- [11] G. Rodolakis, A. Laouiti, P. Jacquet, and A. M. Naimi. Multicast overlay spanning trees in ad hoc networks: Capacity bounds, protocol design and performance evaluation. *ELSEVIER Computer Communications*, Vol. 31(7):Pages 1400–1412, 2008.
- [12] W.-S. Si and C.-Z. Li. RMAC: A reliable MAC protocol supporting multicast for wireless ad hoc networks. *SPRINGER Journal on Comput. Sci. Technol*, Vol. 20(5):Pages 702–712, 2005.
- [13] J. Wang, L. Sun, X. Jiang, and Z. Wu. IGMP snooping: a VLAN-based multicast protocol. In *IEEE International Conference on High Speed Networks and Multimedia Communications (5th HSNM'02)*, pages 335–340, Jeju Island, Korea, July 2002.