Providing Billing Support in WiMAX Mesh Networks

Erlon R. Cruz[1], Daniel Camara[2] and Hélio C. Guardia[1]
[1]Universidade Federal de São Carlos, São Carlos – SP, Brazil
[2]EURECOM, Sophia-Antipolis, France
{erlon_cruz, helio}@dc.ufscar.br, daniel.camara@eurecom.fr

***Abstract* - A huge effort has been applied on the study of Wireless Mesh Networks (WMNs) over the last few years. As part of this effort the IEEE 802.16 Standard for Local and Metropolitan Area Networks specifies a mesh mode of operation. Although several technical aspects of the physical and medium access layers of the standard have been studied, only few works investigate how the WiMAX mesh mode architecture will handle billing aspects and paid access. Here we propose a billing architecture and present an accounting mechanism which allows WISPs to charge its users and also reward those who contribute forwarding packets. We evaluate the accounting mechanism through simulations and show its feasibility.**

***Index Terms*— Billing, Charging, IEEE 802.16, Rewarding Policies, Wireless Mesh Networks, WiMAX mesh.**

I. INTRODUCTION

WIRELESS Mesh Networks (WMNs) have attracted great attention to both academia and industry. However, it is still not clear how users will be charged for using the network. The WiMAX forum estimates that more than 133 millions of people will be using the WiMAX technology by the year 2012. From these more than 70% will be using the mobile implementation of the technology. Without efficient processes for Authentication, Authorization and Accounting (AAA) the management of this volume of users would be a hard, if not impossible, task. This work proposes a cooperative billing process for WiMAX mesh networks, where nodes are rewarded for aiding other nodes to deliver their traffic.

The addition of the mesh operation mode to the IEEE 802.16 [1] standard brought several advantages to this technology, including non line of sight transmission capacity, greater reliability, security, throughput and availability [2].

Contrasting to a point to multipoint (PMP) network, where all the transmissions involve a central entity, in WMNs nodes must cooperate to transmit data through the network. Considering the environment of a Wireless Internet Service Provider (WISP), where private nodes are used to route network traffic, forwarding other node's data involves the consumption of local resources, e.g. power, processing and, mainly, bandwidth. Without any kind of incentive, it is likely that many users may be resistant to sharing their resources with others. On the other hand, it is well known that such selfish behavior can affect the performance of the whole network [3].

The accounting proposal described here aims to stimulate cooperation, persuading users to share resources by assigning credits to those that cooperate with others by forwarding their data. The protocol uses a session based approach designed to discourage nodes fraudulent behavior. The main objective of our proposal is to ensure that the charges and rewards made by the WISP are correct, secure, and fair.

The remainder of this paper is organized as follows: in Section II we present an overview of IEEE 802.16 mesh mode. In Section III we state the main security and performance requirements of our architecture. Then, in Section IV, we explain the accounting scheme. After that, in Section V, the security requirements are put in proof and we show how the architecture overcomes some possible fraud attacks. The evaluation of the billing system is shown in Section VI. The related works are discussed in Section VII. Finally, in Section VIII we present our conclusions.

II. OVERVIEW OF 802.16 MESH MODE

The WiMax mesh mode frames are divided into control and data sub-frames. There are two types of control sub-frames: schedule and network control sub-frame. The network control sub-frame provides the basic functionalities for network attachment and topology management. The schedule control sub-frame controls the transmissions. Scheduling is done by negotiating mini-slots ranges for the traffic demands of each link. All the communications are collision free and done through the links established between nodes. All data transmissions between two nodes are done through one link and the QoS (Quality of Service) is provisioned over links on a message by message basis. Upper layer protocols are in charge of the traffic classification and flow regulation.

A node that wishes to join the mesh network needs to wait until a MSH-NCFG message is detected. When detected, the node is able to establish the synchronization with the mesh network. Once the sponsor node is chosen, the new node uses it to send a MSH-NENT message to the Mesh BS with its registration information. After being authenticated the new node closes the sponsor channel and acquires an IP address using DHCP, only then the new node is able to transmit.

Due to its connection oriented nature, the interconnection between MAC and upper layers is done through a convergence sub-layer (CS). The CS is responsible for mapping upper layer datagrams into connections. This mapping is based on the information and protocol of the datagram. After classified, the datagram is sent as the payload of a mesh MAC frame to the next node on its route. This process is repeated until the packet reaches its destination.

III. TARGET STRUCTURE

This work targets the billing process in a Wireless Internet Service Provider (WISP) environment, as the one depicted in

Fig. 1. The main objective of the WISP network structure is to provide Internet access to fairly static nodes in a well defined and stable region. The WISP domain may be divided into sub-networks where a Mesh Base Station (Mesh BS) acts as a backhaul for the connected set of mesh Subscriber Stations (SS). The Mesh BS is part of the WISP structure and is responsible for providing access to the nodes of the sub-network, organizing and collecting information, Mesh SSs are end user stations, not WISP ones. These stations may, or may not, act as traffic forwarders for other mesh SSs. We assume that all nodes support the mesh operation mode defined by the IEEE 802.16 standard [1]. The AAA Server is responsible for the actions of Authentication, Authorization and Accounting.

As a simplification, we only charge traffic from and to the Internet, SS to SS traffic is not billed. All considered traffic passes through the Mesh BS, that is responsible for keeping track of the transmitted packets and reward the nodes. The WISP is considered trustful and fair, and the billing records are informed to the AAA server using SNMP messages.

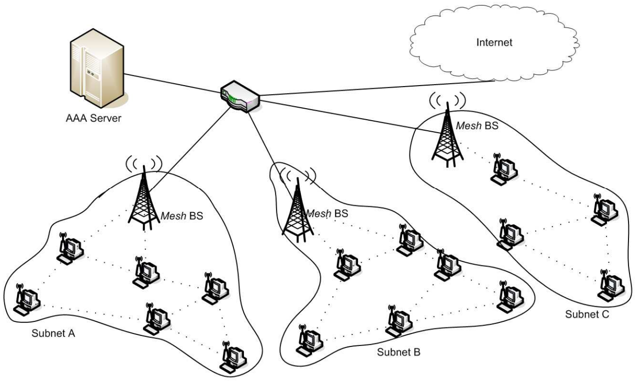

Fig. 1 Billing Scenario

IV. Proposed Archtecture

All packets sent through the network must be accounted to ensure a fair billing and rewarding process. The Mesh BS is the entity in charge of keeping track of the transmissions and nodes taking part on them. Nodes also keep track of their own transmissions but this data has to be confirmed by the Mesh BS. A node must be able to prove the successful transmission of a packet in order to account for it in a billing session. The node's transmission log must be consistent, with the one kept by the BS. This ensures nodes cannot lie about their own transmission history. Even if two, or more, nodes try to overcome this by forging consistently their transmission history, based in its logs the Mesh BS is able to check if all transmissions are really correct. The control traffic is not directly billed, and control messages may pass through any node. However, the volume of control traffic is significantly smaller than data transmission. Nodes also have interest in retransmiting control messages since they are encrypted and may be carrying information regarding their own rewards.

The accounting scheme differs slightly for uplink and downlink, however, both are based in billing sessions as detailed in subsection A.

A. Billing Sessions

A billing session can be seen as a virtual channel established between either the Mesh BS and a SS (downlink - BS/SS), or between a SS and the Mesh BS (uplink - SS/Mesh BS), in which traffic with certain characteristics is sent. Each session is uniquely identified by a session identifier issued by the Mesh BS during the session startup. Packets transmitted in a session are identified by the session identifier plus the packet sequence number.

Each session may have different reward values depending on its Quality of Service (QoS) requirements. The use of differentiated session classes allows the WISP to apply different polices when charging or rewarding a flow, giving differentiated bonus to higher priority flows.

Each session is allowed a maximum inactivity time, and if this value is met the session is closed. The maximum inactivity time value is negotiated during the session startup and may vary according the required QoS and the response time between the SS and Mesh BS.

All session signaling messages are encrypted with a secret key derived from the authorization key received during the nodes authentication process.

Downlink Billing Session

A downlink billing session is started when an Internet packet addressed to an SS reaches the mesh BS. We will use the example displayed in Fig. 2 to explain the downlink billing session. Before forwarding the packet, the mesh BS sends a message (DBS_REQUEST) to SS3 signaling that a downlink billing session will begin.

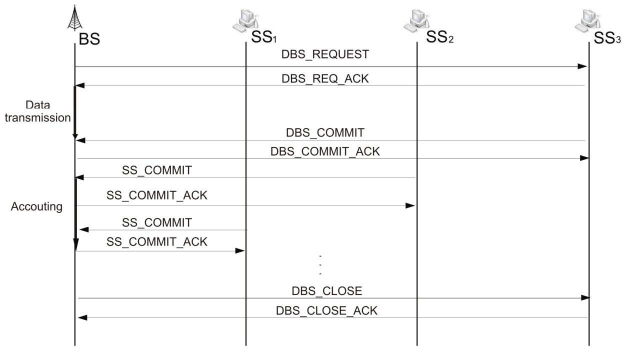

Fig 2. Downlink Billing Session

Upon receiving the confirmation (DBS_REQ_ACK) of SS3, the session is initiated. From that moment on, before sending a packet to SS3, the BS calculates the hash for the data of the packet and stores this hash in a buffer. Each packet will carry along a label that contains its sequence number and the session identifier. The modified packet is then sent, and forwarded by SS1 and SS2 until it reaches SS3. For each received packet, SS3 calculates the hash for the data and stores this value. As the number of the hashes for the session grows, SS3 assembles a message (DBS_COMMIT) and sends it to the mesh BS. After receiving the DBS_COMMIT message, also referred as confirmation commit, BS compares the hashes received with those previously calculated and determines which packets were correctly received by SS3. If the mesh BS does not receive a DBS_COMMIT within a previously agreed period of time, it stops sending messages to SS3.

Before forwarding the packets, the intermediate stations SS1 and SS2 must calculate the hashes and store them as a proof that they forwarded those packets. Periodically, SS1 and SS2 send the BS a message (SS_COMMIT), also referred as claim commit. After comparing the received hashes with the stored ones, the BS replies with a (SS_COMMIT_ACK) message informing which ones, from the received hashes, where checked. The BS ignores any commit message whose hashes were not yet received in a DBS_COMMIT, and confirms only the hashes already verified. The intermediate station will retransmit the unconfirmed hashes using a back off algorithm until the BS sends a DBS_COMMIT acknowledging those hashes or until the maximum number of attempts is reached. In the last case the intermediate stations will not be awarded by the claimed traffic. Again, the BS is considered to be fair and flawless.

The session finishes when no data is transmitted after a period of inactivity. When this happens the BS sends a message (DBS_CLOSE) to the correspondent SS that confirms the receipt of a closing message by sending a DBS_CLOSE_ACK message.

Uplink Billing Session

The uplink billing session is fairly similar to what happens in the downlink. Fig. 3 presents an example of the uplink billing session. This billing session starts when an SS wants to send messages to the Internet.

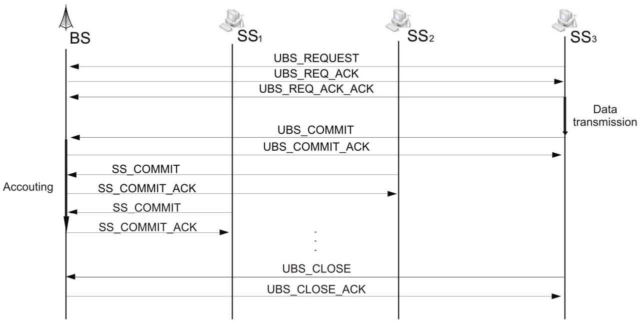

Fig 3. Uplink Billing Session

There are three main differences between uplink and downlink sessions. First, the uplink session is initiate by the SS (UBS_REQUEST). Second, the startup process is, for this case, a three way handshake where the SS sends a confirmation (UBS_REQ_ACK_ACK) regarding the BS request response (UBS_REQ_ACK). This last message informs to SS3 which session ID should be used for this session. The third difference is that the data flow is originated at the SS and headed to the mesh BS and the transmitter station must send the confirmation commit.

B. Billing Mechanism

The billing mechanism is implemented on top of the CS defined by the IEEE 802.16 standard. According to the standard, the CS performs the classification of upper layer PDUs and maps each PDU into a connection data flow. The billing layer is responsible for classifying and grouping data flows into billing sessions. The relation among the modules of the proposed architecture is depicted in Fig 4. The billing layer also manages the creation of sessions, verifies the authenticity of session messages, calculates hashes, assembles commit messages, and in case of the Mesh BS, also verifies the hashes received in commits. The billing layer is divided into three main components.

Session Manager: is responsible for creating the session, for sending, for verifying and for authenticating the session messages.

Policy Manager: is responsible for ensuring the session respects the policies defined by the mesh BS at the start of each session. For example, the BS can define that sessions carrying real time flows have bigger rewarding value than others. This mechanism guarantees that the billing mechanism can assist QoS routing protocols and scheduling algorithms.

Billing Classifier: is responsible for classifying the session received packets. The billing classifier is also responsible for removing the labels of PDUs coming from lower layers and delivering the cleaned PDUs to the upper layers. If the classifier receives a packet from the upper layer and no active session maps the packet, this packet, and all others fitting the same rule, are held until a session can be established by the session manager.

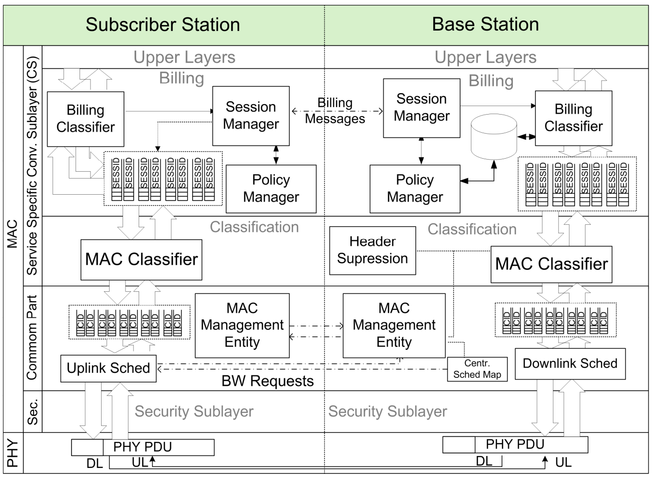

Fig 4. 802.16 CS with billing support

V. Security Analysis

One of the biggest issues related to billing is the security of the system against attacks. Attacks may vary from denial of service to the attempt of forgery, where, in our case, nodes try to obtain more credits than they deserve. This section describes how our system is resilient to forgery, namely: packet rejection, packet injection, packet padding, cyclical routing, repetition attack, over routing attack, denial of confirmation and hash tamper.

Packet rejection: a SS may discard packets that should be forwarded and claim credits for those packets. No SS is obliged to forward the packets of its neighbors; however, if a packet is discarded the node will not receive any reward related the discarded packet. In the same way, if a packet is not delivered, it is not fair to charge the origin for it. The nodes are credited, and charged only when the destination node issues the confirmation commit. If this message is not issued no node may claim any credit related to that specific communication.

Packet injection: a SS may inject packets to a session and claim credits for these transmissions. The only traffic considered for accounting is the one that passes through the Mesh BS, either in the uplink or in the downlink, and if the transmission is confirmed by the destination. If a malicious node inserts a random garbage data packet to the session, the destination will not issue a confirmation for this packet, as it is not what the destination node is expecting for. Thus the malicious node will not be awarded.

Packet padding: an intermediate station may insert bytes into packets in order to increase the number of bytes it forwards. However, the confirmation commit message contains a hash calculated over the transmitted packet, and if this hash does not match the original packet no node is rewarded for the communication.

Cyclical routing: one or more intermediate nodes may conspire to send the same packet through cyclical routes and, in this way, increase their number of sent packets. Each packet is accounted only once for each intermediate node, regardless how many times it was forwarded inside the network and if it passed more than once through a specific node.

Repetition attack: an attacker may retransmit a packet more than once to increase its traffic. Similarly to what happens at the cyclical routing attack, if a node forwards the same packet more than once, the destination will issue only one confirmation commit for the first packet to arrive. Credits are awarded one time only for each packet.

Over-routing attack: an attacker may send a packet through a larger route than the optimal one in order to benefit other nodes. The intention with this attack is to make the WISP reward more stations than the ones really needed for that specific transmission. If more than one route is available, nodes may use alternative routes. However, all nodes have the same routing information, including the Mesh BS. The informal contract states that the shortest route able to guarantee the required QoS parameters should always be used. The Mesh BS may use the shortest path as the reserved budget for sessions. If more nodes were involved in the forwarding process the budget will be divided equally among all the nodes, with a smaller share to each one.

Denial of confirmation: the destination station may avoid sending commits to avoid being charged by the Mesh BS. During the session setup a window value is agreed between the origin and destination. If the destination node does not send a commit until the window is completely filled, the origin stops sending new messages, while the commit message does not arrive.

Hash tamper: commit messages may be routed through stations who did not participate on that specific session transmission. An intermediate station could try to copy the hashes regarding the commit section and claim the rewards for the traffic represented by that hashes. All session messages are sent encrypted with the secret keys negotiated between the BS and an SS, and this prevent nodes to impersonate others.

VI. Evaluation And Simulation Results

In order to analyze the performance of the proposed solution, we have implemented the billing support for the 802.16e mesh mode into the NCTUns network simulator [9]. In our evaluation tests we have used distributed scheduling with fixed routes. The WMN is assumed to operate in a steady state, where links are not established or removed over time. In all scenarios, the simulations were performed both for all nodes using the billing layer (billed system) and for all nodes without billing layer (not billed system) in the same conditions. For the throughput experiments we have used a 1500 bytes TCP flow traffic. For the latency experiments 64 bytes ICMP packets where sent in intervals of 0.2ms.

A. Simulation Metrics

We have considered 7 performance parameters:

i) *initial throughput* is the average throughput of the first 2 MB sent in a simulation. It takes around 150s in simulation time;

ii) *ample throughput* is the throughput measured for the remaining flow. The total time of throughput tests was 500s;

iii) *global throughput* is the combined throughput of downlink and uplink. In this test, bidirectional traffic is sent and there is no separation from initial and ample flows. Simulation time used in this case was of 250s and 3MB were sent in both directions;

iv) *initial latency* is the median latency measured for the first 50 ICMP packets;

v) *ample latency* is the latency measured for the remaining packets sent. For the latency test the simulation time was 400s

vi) *global latency* is the combined latency of downlink and uplink. In this test ICMP packets where sent in both downlink and uplink along 600s of simulation;

vii) *account precision* indicates how precise is the traffic measured by Mesh BS. This metric is perform by comparing the exact amount of traffic generated by the traffic generator with that one measured by Mesh BS.

We have 6 different simulation scenarios where we vary the number of intermediate nodes between the BS and SS from 0 to 10. The evaluated scenarios have 0, 2, 4, 6, 8, and 10 intermediate nodes. The stations were placed, on average, at 250m apart from each other. So for the second scenario, with 2 intermediary nodes, the distance between the BS and SS is, on average, 750m and for the fifth scenario 3000m. With these experiments we want to evaluate the overhead imputed by the billing mechanism on the network. For this reason all nodes are always wiling to cooperate and never try to deceive the billing mechanism.

B. Simulation Results

Downlink and uplink traffic results were collected separately, except for the global test where there is no distinction between uplink and downlink traffic. The vertical bars on the graphs represent the standard deviation for the measures of all the transmissions during the simulation time.

Fig. 5 shows the initial latency for the uplink and downlink sessions with and without the billing support. We can observe that when the number of intermediate nodes increases the difference between uplink and downlink latencies tend to increase. The larger the number of intermediate nodes, the bigger is the impact of the retransmissions of the initial session setup messages on of the billing process. This is expected and we can observe the same behavior in all latency related graphs, Fig. 5, Fig. 6 and Fig. 7. However, the impact of the billing process is small for mesh networks with 6 or less intermediate nodes. This is an interesting result since 6 intermediate nodes is already a fairly large mesh network.

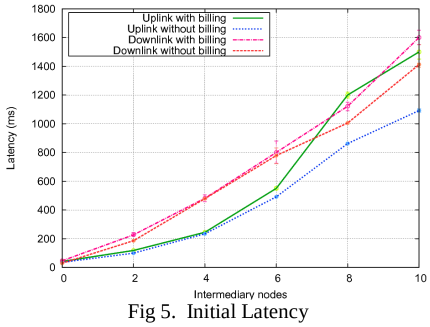

Fig 5. Initial Latency

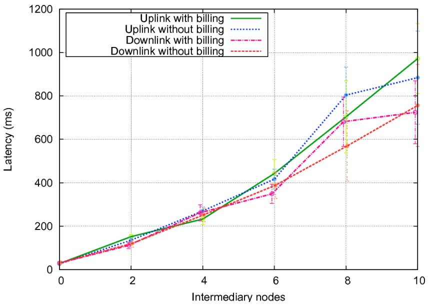

Fig 6. Ample latency

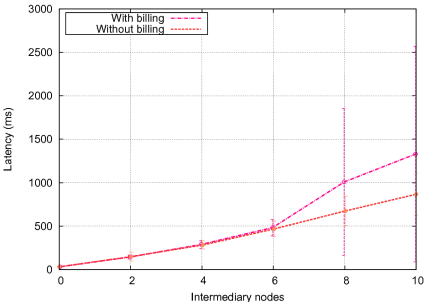

Fig 7. Global latency

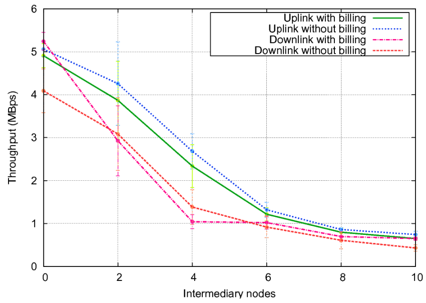

Fig 8. Initial throughput

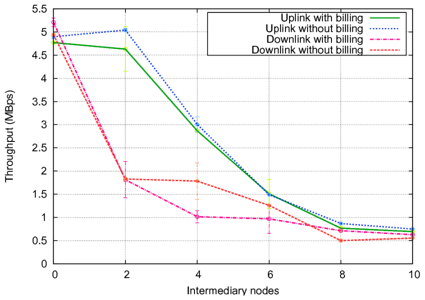

Fig 9. Ample throughput

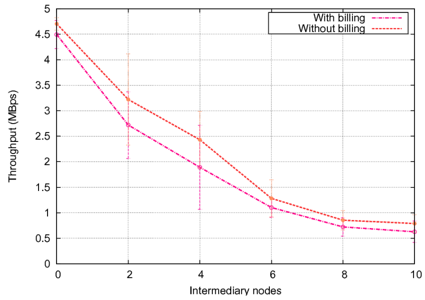

Fig 10. Global throughput

Other interesting fact is that if we compare the graphs in Fig. 5 and Fig. 6, the initial latency values are not expressively bigger than the ones for the ample latency, when the network gets into steady state. This means that the billing startup process does not represent a great overhead, in terms of delay, to the participant nodes.

From the graph in Fig. 6 we can see that the billing mechanism has a small impact over the latency of the packets when the sessions reach steady state. However, when the number of intermediate nodes increases it also increases the traffic and number of lost messages on the network. When we consider all the traffic on the network not distinguishing uplink or downlink, Fig. 7, the latency differences are even smaller for mesh networks up to 6 nodes.

For throughput, shown in Fig. 8, Fig. 9 and Fig. 10, the differences between billed and non billed traffic are also small. The throughput depends heavily on the scheduling mechanism of the network. The used scheduling algorithm gives preference to uplink traffic in detriment of downlink traffic. This is why the throughput values for uplink connections are better than the values for downlink sessions. If we compare the graphs in Fig. 8 and Fig. 9 we can notice a discrepancy between their initial values, but as the number of intermediate nodes increases the discrepancy tend to disappear. The explanation is simple, for the initial packets the load of the network is low, and this enables a bigger throughput for the initial messages. However, while the network gets loaded, and even more when we increase the number of intermediate nodes, the throughput tends to decrease. The global throughput, shown in Fig. 10, is a compromise between the values of uplink and downlink sessions.

Taking the results of global tests (Fig. 7 and Fig. 10) and merging the results of all scenarios, the overall overhead of the billing process accounts for 17.6% in latency and 18% in throughput. In the account precision tests, the traffic measured by Mesh BS has a precision of ±3.5%.

VII. Background And Related Works

Technical issues including infrastructure and aspects related to the AAA (Authentication, Authorization, and Accounting) procedures are exposed in [15].

Several studies ([10],[11],[12]) investigate, the 'selfishness' factor on ad hoc networks. In these studies there are basically two ways to encourage collaboration between nodes in multi-hop networks: incentive policies, where cooperating nodes are rewarded, and repression policies, where selfish nodes are punished in some way.

In [14], Zaghloul *et al.*, the authors propose a billing architecture for cellular backhaul mesh networks. WMNs cellular backhauls pose many technical challenges including timing synchronization for GSM networks, bandwidth reservation techniques, dynamic bandwidth control, and billing. To address some of these challenges, the authors propose a billing architecture using a threshold based bandwidth management algorithm. Even though Zaghloul’s proposal is scalable and suited even for poor implementations of bandwidth reservation algorithms, they focus on cellular networks and do not consider security aspects or rewarding schemes for the participant nodes.

Considering a scenario where several WISPs provide access to its users through mesh networking, Y. Zhang and Y. Fang propose the UPASS, an universal *pass* used for identification, authentication and billing of inter-domain users in WMNs [4]. The charging system UPASS is analogous to current credit card systems. A few certification authorities are used to provided the user a UPASS and make agreements with the WISPs so that they do not need to establish a trust relationship with final users. Through a micro-payment protocol combined with digital signature and hash functions, the UPASS indisputability ensures the charges made by WISPs. This allows users to use the service from several providers, paying them and being rewarded by traffic re-routed without the need to worry about the suitability of the providers. Even though UPASS is resilient to untrustworthy operators, providing means for mutual guarantees for the accounted values, Y. Zhang and Y. Fang do not provide any explanation of how the packets are calculated and how the operator determines which node sent or not the intermediate traffic.

The problem of cooperation in WMNs is also discussed by Salem *et al.* [13]. Considering a scenario where a WISP maintains mesh BSS and network gateways, the authors propose a mechanism to ensure rewards for the stations that forwards packets from neighbors. Thus, the protocol introduces the idea of billing sessions. Before transmitting, a station must configure an end-to-end session, indicating the characteristics of traffic and the route of transmission. Once the session is set, all packets are sent through this session with a label attached. This allows the mesh gateways to control the amount of data transmitted by the stations. All traffic sent and received must be confirmed by the destination station so that the WISP recognizes which packets where really sent and received. Once the receipt is confirmed, all intermediate stations are rewarded. The authors also discuss the various forms of attack that could be raised within the scenario considered and ensure that the protocol is safe against them.

Our work differs from Salem *et al*. one in many aspects, but mainly regarding the target network architecture as they focus on cellular networks and we consider WiMAX mesh networks. The main drawback of their approach is that a billing session is bound to a route. If some node on the route fails a new section must be established; such fact reduces the capability of the network to adapt to route changes or optimizations. They also base their entire billing process only on the packet size and do not consider QoS as a factor on the billing system. Moreover, Salem's approach uses symmetric cryptography, which they argue to be more suited to mobile environments, as they are less computationally intensive. For our scenario the nodes are supposed to have more computational power, even though nowadays even cellular devices have increased considerably their computational capacity. Besides favoring authentication, public key cryptography can always be used for establishing secret keys for encryption purposes.

While providing a theoretical background about the protocols operation, none of these works provides details about which wireless transmission technologies are supported and at which layers of the ISO/OSI reference model their functionalities would be allocated. Besides providing charging and rewarding capabilities to WISPs, our study provides underlying details for its operation in the MAC layer of IEEE 802.16 standard.

VIII. Conclusions And Future Work

This paper presents a billing architecture for WiMAX mesh networks. The main objective of this work is to provide WISPs the capacity to improve the quality of their service by motivating user cooperation through rewards.

The presented simulations show the billing mechanism introduces an acceptable overhead, both in latency and in throughput. These costs were expected as we add some overhead to the data transmission process by introducing the use of encryption routines, mechanisms of establishing sessions, and the insertion and removal of datagram labels. However these values are reasonably low for scenarios with less than 6 intermediary nodes, what is a fair value for WMNs. Despite introducing these overheads, the architecture provides several benefits for both service provider and users. The architecture enables real-time reporting of network traffic, i.*e.*, a user is rewarded immediately after rewarding claims are cleared. Another particularity of our architecture is the ability to assign different rewarding policies for different sessions. When collaborating with a routing algorithm that provides QoS, our method may increase the consistency of services offered.

The experiment section showed that the proposed architecture is fully viable. However, many other aspects can still be further investigated. Benefiting from the example of UPASS, the next steps on this work can be the creation of auxiliary mechanisms to allow mobility of the nodes among different WISPs. We also intend to increase the security of the billing mechanism and decrease its overhead by refining the session protocol, attaching the intermediate nodes IDs to the message. However the costs and benefits of this solution need to be quantified.

References

[1] IEEE Standard 802.16-2004, *"IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems"*, Oct. 2004.

[2] I.F. Akyildiz, X. Wang, W. Wang, *"Wireless Mesh Networks: A Survey"*, Computer *Network*s (2004) 445–487

[3] Fang Y., Lou W., Zhang Y.: *"SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc" Network*s - WCNC 2004 / IEEE Communications Society

[4] Zhang Y. Fang, Y., *"A secure authentication and billing architecture for wireless mesh networks"*. Wireless Networks (2007).

[5] Naouel Ben Salem, Levente Buttyan, Markus Jakobsson, *"A Charging and Rewarding Scheme for Packet Forwarding in Multihop Cellular Networks"*, MobiHoc'03, June 1–3, 2003, Annapolis, Maryland, USA.

[6] M. Jakobsson, J.-P. Hubaux, and L. Buttyan. *"A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks"*. In Proceedings of Financial Cryptography, 2003.

[7] Simple Network Management Protocol (SNMP), http://www.faqs.org/rfcs/rfc1157.html

[8] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer-Verlag, 2002

[9] "*NCTUns Network Simulator and Emulator*", http://nsl.csie.nctu.edu.tw/nctuns.html

[10] S. Zhong, J. Chen, and Y. R. Yang, *"Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks"*, IEEE INFOCON 2003

[11] N. B. Salem, *"Secure Incentives to Cooperate for Wireless Networks"*, PhD Thesis on ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

[12] S. Marti *et al*, *"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks"*, International Conference on Mobile Computing and Networking, 2000

[13] Salem *et al*, *"A Charging and Rewarding Scheme for Packet Forwarding in Multihop Cellular Networks"*, MobHoc'03, 2003

[14] Zaghlou S, Bziuk W., and Jukan ,*"A Scalable Billing Architecture for Future Wireless Mesh Backhauls"*, ICC 2008

[15] Samhat, A.E, Abdi M., "Security and AAA Architecture for WiFi-WiMAX Mesh Network", ISWCS 2007