MESH 2013

The Sixth International Conference on Advances in Mesh Networks

ISBN: 978-1-61208-299-8

August 25-31, 2013

Barcelona, Spain

MESH 2013 Editors

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania

Sandra Sendra Compte, Universidad Politécnica de Valencia, Spain

MESH 2013

Foreword

The Sixth International Conference on Advances in Mesh Networks [MESH 2013], held between August 25-31, 2013 in Barcelona, Spain, built on the previous editions to address the most challenging aspects for designing and deploying mesh networks.

The wireless mesh networks came to rescue the challenging issues related for predicting the location of a user and choosing the position of access points in wireless distributed systems. Basically mesh networks guarantee the connectivity through a multi-hop wireless backbone formed by stationary routers. There is no differentiation between uplink and downlink, but performance depends on the routing protocols. There are several challenging issues for properly exploiting wireless mesh networks' features, such as fast-link quality variation, channel assignments, performance, QoS-routing, scalability, slow/high speed mobile users, service differentiation, and others.

We take here the opportunity to warmly thank all the members of the MESH 2013 Technical Program Committee, as well as the numerous reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to MESH 2013. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the MESH 2013 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that MESH 2013 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in mesh networks.

We are convinced that the participants found the event useful and communications very open. We hope Barcelona provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city.

MESH 2013 Chairs:

MESH Advisory Chairs

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Petre Dini, Concordia University, Canada / China Space Agency Center - Beijing, China
Andreas J. Kassler, Karlstad University, Sweden

MESH 2013 Industry Liaison Chairs
Michael Bahr, Siemens AG - München, Germany
Vladimir Sulc, Microrisc s. r. o. - Jicin, Czech Republic

MESH 2013 Research/Industry Chairs
Mathilde Benveniste, Wireless Systems Research/En-aerion, USA

MESH 2013 Publicity Chair
Sandra Sendra Compte, Universidad Politécnica de Valencia, Spain

MESH 2013 Special area Chairs
Ad Hoc
Karoly Farkas, University of West Hungary / Budapest University of Technology and Economics, Hungary
WiMax
Jens Myrup Pedersen, Aalborg University - Aalborg Øst, Denmark
QoS/Routing
Mats Björkman, Mälardalen University, Sweden
Testbeds
Stefan Bouckaert, Ghent University - IBBT, Belgium
João Paulo Barraca, University of Aveiro, Portugal

MESH 2013

Committee

MESH Advisory Chairs

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Petre Dini, Concordia University, Canada / China Space Agency Center - Beijing, China
Andreas J. Kassler, Karlstad University, Sweden

MESH 2013 Industry Liaison Chairs

Michael Bahr, Siemens AG - München, Germany
Vladimir Sulc, Microrisc s. r. o. - Jicin, Czech Republic

MESH 2013 Research/Industry Chairs

Mathilde Benveniste, Wireless Systems Research/En-aerion, USA

MESH 2013 Publicity Chair

Sandra Sendra Compte, Universidad Politécnica de Valencia, Spain

MESH 2013 Special area Chairs

Ad Hoc
Karoly Farkas, University of West Hungary / Budapest University of Technology and Economics, Hungary

WiMax
Jens Myrup Pedersen, Aalborg University - Aalborg Øst, Denmark

QoS/Routing
Mats Björkman, Mälardalen University, Sweden

Testbeds
Stefan Bouckaert, Ghent University - IBBT, Belgium
João Paulo Barraca, University of Aveiro, Portugal

MESH 2013 Technical Program Committee

Copyright Information

Table of Contents

Blue Bridge and Linkage

Connecting Africa through 802.11, Bluetooth and Raspberry Pis

Curtis Sahd and Hannah Thinyane
Department of Computer Science
Rhodes University
Grahamstown, South Africa
{curtissahd@gmail.com, h.thinyane@ru.ac.za}

***Abstract*—Public Switched Telephone Networks (PSTNs) are predominantly comprised of proprietary protocols and are not well suited to integration with the ever expanding Voice over IP (VoIP) network. PSTNs have evolved from analogue circuit switched systems and purely fixed line services, to the digital and mobile realms, but still remain proprietary. With the advent of wireless technologies and the explosion in VoIP services, the combination of these two technologies results in a large number of integration possibilities and inter-connection of systems. In this paper, we show how existing technologies can be used in the creation of community telephone networks. Specifically, we provide an overview of our system (Blue Bridge), which performs the bridging of Bluetooth and IEEE 802.11 wireless. We also provide an overview of the associated lightweight hybrid protocol (Linkage), which delivers status updates and data transmissions.**

Keywords-Bluetooth bridging; Community telephone networks; Linkage; Raspberry Pi; Wireless mesh networks

I. INTRODUCTION

Wireless Mesh Networks (WMNs) and VoIP have become key players in IP-based telephony services and have revolutionized the industry in terms of cost, geographically constrained infrastructure and service, and interoperability between devices [6].

WMNs can be defined as dynamic self configuring networks in which all nodes have the ability to route traffic directly to the endpoint, or via a multi-hop path. The network is dynamic, which enables it to deal with nodes entering the network, as well as nodes leaving the network due to node failure or connectivity issues [8]. WMNs are comprised of two types of nodes: mesh routers and mesh clients [1]. Mesh routers provide similar functions to traditional wireless routers, except that they provide more routing functions which are suited to WMNs. Mesh routers achieve the same coverage as traditional routers, but with less transmission power, by means of multi-hop communications [1]. Mesh clients can also work as routers, but do not have gateway or bridge functionality as found with mesh routers. WMN architecture is an important consideration when determining how and where the WMN should be implemented. WMN architecture can be classified according to three primary implementations: infrastructure WMNs, client WMNs, and hybrid WMNs [2]. The backbone of an Infrastructure WMN is predominantly comprised of mesh routers with which mesh clients associate.

Client WMNs provide peer-to-peer network functionality, and are mostly comprised of mesh clients which perform the routing of packets.

Hybrid WMNs are a combination of Infrastructure and Client WMNs, with the infrastructure being comprised of both mesh routers and mesh clients [2].

The concept of WMNs has been around for quite some time, and the development of protocols which enable the efficient functioning of these networks has been a core focus area. Since the inception of VoIP, the way in which we communicate has drastically changed, enabling long distance phone calls at a fraction of the cost when compared to previous years. Although easily and universally accessible, VoIP communication has traditionally taken place with somewhat limited mobility, with instances such as calls being made from fixed landlines and scattered wireless hotspots. There still exists a heavy reliance on mobile networks utilizing proprietary protocols, and with the cost of data being close to that of calls, the reality of reliable VoIP communication over mobile networks is an optimistic idea. Over and above the cost of data communications on mobile networks, the filtering and throttling of VoIP protocols on these networks is not an uncommon practice [7] [12]. Extensive development of the IEEE 802.11 wireless protocol has taken place and drastically increased the ease with which we are able to communicate, as well as the general mobility of people and services. IEEE 802.11 wireless technology provides reliable mobile communication with equipment costs being a fraction of those encountered with traditional radio networks.

A community, city, and even country wide WMN running open standards can prove to be a feasible solution in providing cost effective communication along with ease of integration and expandability.

As such, we propose the implementation of a WMN-based Community Telephone Network (CTN), which enables communication for Bluetooth and IEEE 802.11

ISBN: 978-1-61208-299-8

wireless clients by means of distributed bridging nodes (*Blue Bridges*) and a lightweight protocol enabling Push To Talk (PTT) communication and signaling (*Linkage*). Section II provides an overview of the Bluetooth protocol and the benefits it provides in the South African context, as well as the associated constraints. Section III introduces PTT systems and provides a brief overview of how they aid in minimizing scalability concerns and constraints inherent in the Bluetooth protocol. Section IV, then introduces CTNs and outlines the benefits of such networks as well as a brief literature review of the common issues encountered with these networks. Section V builds on the ideas introduced and discussed in the aforementioned sections and discusses the various components of our prototype system (*Blue Bridge*). Section VI provides an in depth discussion of the functioning of our hybrid notification and communication protocol (*Linkage*). Future work is discussed in Section VII and this paper is then concluded in Section VIII.

II. BLUETOOTH OVERVIEW

Bluetooth is a low powered, low cost, and short range wireless Radio Frequency (RF) technology, which operates in the unlicensed 2.4 GHz Industrial Scientific Medical (ISM) frequency range [9]. Bluetooth is comprised of three classes ranging from 1m to 100m. Bluetooth was originally developed to alleviate the problems caused by incompatible connectors, and also as a cable replacement technology [3].

Although, while very limited in terms of bandwidth and scalability, Bluetooth proves to be a widely adopted protocol in South Africa, with a large portion of the population not able to afford IEEE 802.11 wireless enabled mobile phones.

Bluetooth communication is typically used in Wireless Personal Area Networks (WPANs), which are best suited to ad hoc communication between devices within close proximity of one another. Piconets are the most common type of Bluetooth WPAN, and enable communication between a maximum of 7 active slave nodes and 1 master node. Master nodes control the ability of slave nodes to transmit on the channel [4].

The obvious drawback of Piconets is the maximum number of nodes which are able to simultaneously communicate. The total available bandwidth for Class 2 Bluetooth chips (commonly found in mobile devices) is 800 kb/s, which severely limits Bluetooth in terms of scalability [4]. PTT-based communication requires minimal bandwidth and also places a low memory footprint on constrained devices such as those commonly used throughout impoverished communities in South Africa. The next section provides a brief overview of PTT systems.

III. PUSH TO TALK COMMUNICATION SYSTEMS

PTT communication is a well-known system used in two way radios, which eliminates the need for call signaling procedures encountered in traditional cellular calls. PTT calls can be established between two users, or alternatively, in group communication, between multiple users [2]. PTT-based communication systems prove to be considerably more cost effective than cellular or landline-based services in that charges are only deducted for the time used while speaking, and not for the elapsed time of the call.

Some of the benefits of IP-based PTT systems include: faster communication and less call setup overhead, group communication, integration with existing applications on LANs, unlimited range and improved costs [12]. PTT-based systems can be compared to instant messaging systems in that communication is instant and requires minimal call setup and signaling. Apart from faster communication than traditional systems, PTT systems provide group communication, which proves to be incredibly cost effective in organizations consisting of teams of employees. One of the major drawbacks of two way radio communication is the range at which communication can occur. LAN-based PTT systems overcome the range limitation of traditional radio network PTT systems and integrate with existing network infrastructure and software.

LAN-based PTT systems prove to be a cost effective solution to communication in the African context, and as such we have chosen a PTT-based system for the implementation of our CTN.

The next section introduces WMN-based CTNs and shows the relationship between the number of hops and supported calls on the network.

IV. COMMUNITY TELEPHONE NETWORKS

The idea of VoIP communications over IEEE 802.11 wireless networks is by no means a novel one, and the benefits of such implementations are well researched with plenty of optimizations available [6]. For the purposes of this research, we will define CTNs as those which are run by the community, for the community, consisting of open protocols, and subscribed to with very little or no cost. We envision the architecture of CTNs, to be comprised of either fixed wireless access points spanning the area of the community concerned, or WMNs where clients participating in the CTN are an extension to the network and its functionality.

In the case of WMN-based CTNs, it is important to understand the effect of multiple hops between clients on the efficient functioning of the network. Ganguly et al. [6] found that eight calls are supported when each call utilizes a single hop on a 2 Mb/s wireless link en route its destination. They observed that as the number of hops increased from one to four on the 2 Mb/s wireless link, the number of supported calls decreased from eight to one. They suggest, that reason for the drastic drop in the number of supported calls is in converse relation to the number of hops. This can be attributed to the following: 1) a decrease in the User Datagram Protocol (UDP) throughput as a result of self interference; 2) large amount of packet loss due to the increased number of hops and the subsequent need for forwarding; 3) a high protocol overhead for the small VoIP packet sizes (20 bytes for IEEE 802.11 IP/UDP/RTP). They suggest two approaches which reduce the effects of multiple hops on the number of simultaneous calls supported: packet aggregation and packet header compression. They found a 200% - 300% increase in the capacity by implementing these methods.

Due to the dynamic creation and association capabilities of WMNs, they are ideal for peer-to-peer-based systems and are thus very suitable as the underlying platform for CTNs. As seen in [1] and [6], the main constraint regarding WMNs is the number of hops and the throughput each hop is capable of carrying.

Apart from being limited by the number of hops and available bandwidth, WMNs and Bluetooth often suffer from a large number of lost packets which are related to the interference caused by the plethora of devices operating in the 2.4 GHz frequency range. With an overview of PTT systems and CTNs, the next section introduces *Blue Bridge*, and demonstrates the important role it plays in the creation of cost effective CTNs in the South African context.

V. BLUE BRIDGE

Blue Bridge aims to combine the Bluetooth and IEEE 802.11 wireless protocols across a series of Raspberry Pi [11] computers, in an effort to create a CTN using existing technologies. Due to the transmission limitations of the Bluetooth protocol, we propose the implementation of *Blue Bridge* on multiple Raspberry Pi computers in order to create an array of Bluetooth hotspots. People within range of the Bluetooth hotspots will be able to connect to the CTN and in turn place calls to other parties connected via Bluetooth or IEEE 802.11 Wireless.

In order to avoid a large amount of broadcast traffic in an already bandwidth constrained network, we found it necessary to centralize client specific information on the Centralized Authentication and Accounting Server (CAAS).

Figure 1 shows architecture of our proposed CTN:

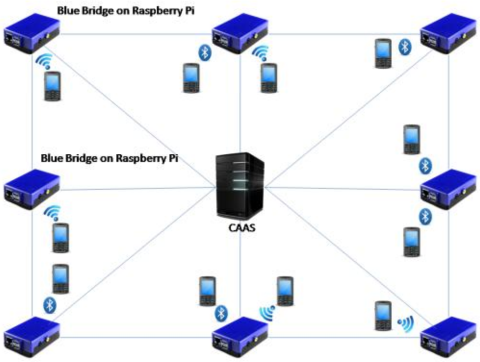


Figure 1. CTN Architecture

From Figure 1, it can be seen that multiple *Blue Bridges* form the infrastructure of the WMN. Bluetooth and IEEE 802.11 wireless clients connect to the CTN through nearby *Blue Bridges*. The CAAS minimizes broadcast traffic by centralizing the status of each client, as well as which router each client is currently associated with. In the event of clients moving between hotspot locations, updates are sent to the CAAS with the newly associated access point address and the status of the client. Multiple IEEE 802.11 wireless clients are able to associate with each *Blue Bridge*, however, a total of 7 active Bluetooth clients are able to communicate with each *Blue Bridge* due to constraints inherent in the Bluetooth protocol.

Connections can be made to and from *Blue Bridges* via the external Bluetooth and IEEE 802.11 Wireless interfaces attached through the USB ports on the Raspberry Pi. Figure 2 provides an overview of the internal structure of each *Blue Bridge* and shows how connections on the same interface as well as varying interfaces are bridged:

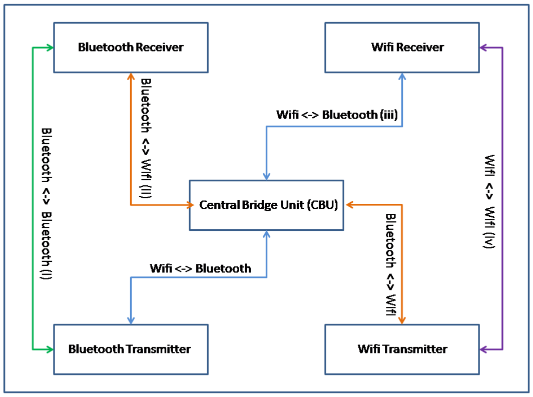


Figure 2. *Blue Bridge* Architecture

From Figure 2, it can be seen from step (ii) that incoming Bluetooth connections (via the Bluetooth Receiver) are sent to the Central Bridge Unit (CBU), which performs the necessary bridging and compression and forwards the data and control packets to the called party on the IEEE 802.11 wireless interface (IEEE 802.11 Wireless Transmitter). Since the concerned *Blue Bridge* is connected to other *Blue Bridges* via the WMN, incoming Bluetooth connections can be connected to any other client on the network without encountering typical range limitations inherent in the Bluetooth protocol. Incoming connections via the IEEE 802.11 wireless interface can similarly be bridged with clients on the attached Bluetooth interface.

In the event where two clients connected to the same *Blue Bridge* via the Bluetooth interface want to communicate, a connection from the calling party is first made to the *Blue Bridge* which then forwards the connection to the called party. This process can be seen in Figure 2 (i). In terms of enabling communication between clients communicating with one another via Bluetooth, there is no need for the *Blue Bridge* to perform any bridging functions or be involved with the communication process at all. With that said, a number of advantages of routing calls/communication via the *Blue Bridge* exist: the ability to perform authentication and accounting functions, which provides useful statistics for network and call monitoring; the ability to create and participate in group calls where clients are distributed across the CTN. There are of course disadvantages of routing local connections via the *Blue Bridge*: since the Bluetooth Master (Bluetooth interface of each *Blue Bridge*) communicates with other locally connected Bluetooth clients, the bandwidth is divided among each connected client and thus reduces the quality of calls;

and increased processing requirements are placed on each *Blue Bridge*.

An SDL diagram of the functioning of the Blue Bridge can be seen in Figure 5. The process can be outlined as follows: the *Blue Bridge* listens for and accepts new connections. Upon accepting a connection the *Blue Bridge* attempts to find the routing information and status of the called client locally (and if not found locally, the CAAS is queried, as seen in Figure 4). This process is illustrated by (a) in Figure 5. Upon finding the routing information for the destination device, the *Blue Bridge* determines the interface from which the data should be sent (as seen in b). If the destination device is connected via the IEEE 802.11 wireless interface, data is forwarded between the concerned devices (as seen in steps c and d). However, if the destination device is connected via the Bluetooth interface, the number of active connections needs to be determined (as seen in g). If the number of active Bluetooth connections is less than or equal to 7, then data is forwarded between the participating devices (as seen in h). In the event where the number of active connections is greater than 7, the *Blue Bridge* terminates the connection and sends the "calling" status to the CAAS as well as the client (not depicted in Figure 5).

With an overview of *Blue Bridge* and how it performs the bridging of the Bluetooth and IEEE 802.11 Wireless protocols, the next section introduces our signaling and voice payload protocol, *Linkage*.

VI. LINKAGE

Although each *Blue Bridge* performs the bridging between the IEEE 802.11 wireless and Bluetooth protocols, without the ability for *Blue Bridges* to communicate, the CTN would cease to exist. We therefore propose *Linkage*, which facilitates inter-communication between *Blue Bridges* and between each *Blue Bridge* and the CAAS. *Linkage* is a lightweight hybrid (UDP and TCP) protocol, which performs the following functions: determining status updates and which *Blue Bridge* each client is currently associated with; informing the CAAS of new clients connected at each *Blue Bridge*; informing the CAAS of existing clients associating with new *Blue Bridges*; status updates between clients, and between *Blue Bridges* and the CAAS; and the transportation of traffic between *Blue Bridges* and clients.

Traditional voice communication is generally session-based, which means that communication between clients and servers is request-response-based. Since voice communication is essentially the transmission of voice data from one client to another and the subsequent playback of this voice data at the receiving end, we decided to abandon the traditional session-based model of voice communication. As such, packets are transmitted from one client to another (via *Blue Bridges*) in a best effort attempt without the need for exchange of information between clients.

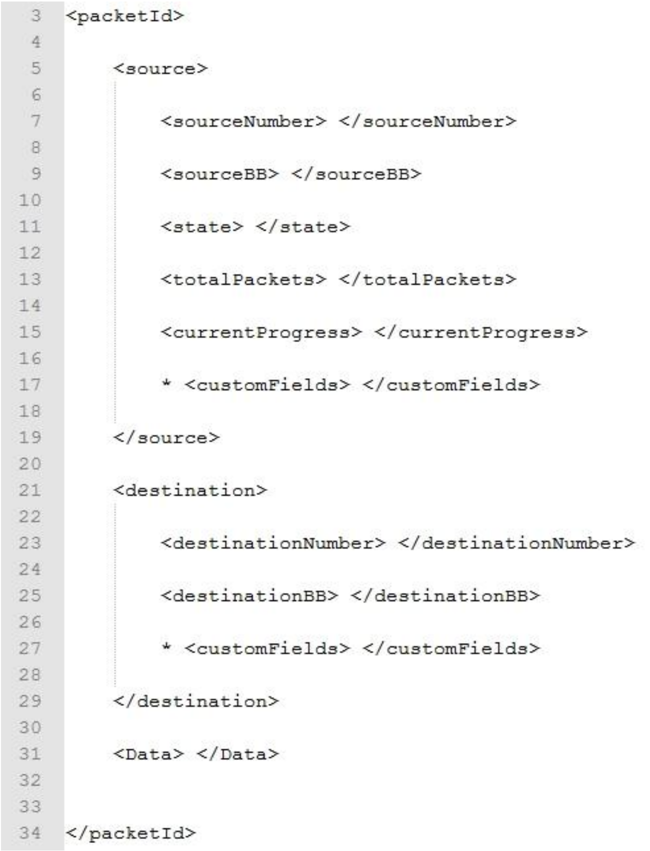
We envision a CTN, to be one in which all protocols are open and easily expandable. As such, we designed *Linkage* in such a way that it can be extended beyond its original function (transportation of voice data between *Blue Bridges* and clients) and transport various other types of traffic by means of custom field addition in the protocol structure.

In order for communication between clients to take place, the following processes are followed:

1. The calling client communicates with the CAAS to determine which *Blue Bridge* the destination client is currently associated with.
2. Once the calling client has knowledge of the destination *Blue Bridge*, it then sends data (voice data in the case of our CTN) via *Linkage* to the destination *Blue Bridge*.
3. Upon receipt of voice data the concerned *Blue Bridge* utilizes the information contained within *Linkage* to route the packet to the destination client.
4. The destination client can then respond to the calling client by utilizing information contained within *Linkage*.

In order to better understand how *Linkage* performs the necessary functions required for the implementation of a CTN we provide an overview of the protocol structure and the components used throughout the process above.

Figure 3 shows the structure of *Linkage* packet*:*



```
<packetId>

    <source>

        <sourceNumber> </sourceNumber>

        <sourceBB> </sourceBB>

        <state> </state>

        <totalPackets> </totalPackets>

        <currentProgress> </currentProgress>

        * <customFields> </customFields>

    </source>

    <destination>

        <destinationNumber> </destinationNumber>

        <destinationBB> </destinationBB>

        * <customFields> </customFields>

    </destination>

    <Data> </Data>


</packetId>
```

Figure 3. Linkage packet structure

Due to the nature of our CTN and for the purposes of efficiency, we utilized the UDP protocol as the underlying protocol for communication between the clients and *Blue Bridges*, and the TCP protocol for communication between *Blue Bridges* and the CAAS. UDP was chosen as the primary protocol between clients and *Blue Bridges* due to the fact that potential lost packets would only result in a decrease in audio quality and would not cause the CTN to cease functioning. TCP was chosen as the preferred protocol for communication between *Blue Bridges* and the CAAS to ensure reliable conveyance of client status information, new client registrations, and reporting of statistical data.

For the purposes of client and *Blue Bridge* communication, we propose the addition of the following fields to the UDP protocol: *Linkage* specific fields, and the payload data field which carries the voice data. In cases where *Linkage* is used merely for informational transfer, the payload data field is left empty.

From Figure 3, it can be seen that the *Linkage* fields are as follows: the packet ID field; client source information; and client destination information.

The PacketID field uniquely identifies each packet for the purposes of accounting, and returned routable responses.

The client source is comprised of the telephone number of the calling client; the IP address of the source *Blue Bridge;* the current state of the client; the total number of packets being transmitted during the voice communication session (if applicable); the current progress of the voice transmission (if applicable); and any additional number of custom fields. The current progress, and total number of packets for the voice communication session, play an important role in optimizing the CTN in that they allow the CAAS to change the status of communicating clients as soon as the voice transmission is complete. These fields also ensure that statuses are updated in the event of lost packets.

The client destination is comprised of the telephone number of the called party, the IP address of the destination router with which the called party is associated; and then any additional custom fields. Due to changing IP addresses, the client telephone numbers serve as the main identifier for communication in the CTN.

A. Statuses and Notifications

In order for the CAAS to be notified of new clients joining the CTN, the above *Linkage* packet is ideal in that new clients can encapsulate their telephone number, and the *Blue Bridge* with which they are associated, as well as their current status. In order to minimize network congestion and unnecessary strain on clients, *Blue Bridges* are required to inform the CAAS of new client associations as well as changes in client statuses. A client can have the following statuses: available; calling; and offline.

It is important to notify calling clients of the status of called clients, so as to avoid engaged calls being mistaken for non-existent clients. An example of this would be, where Client A attempts to call Client B and Client B is currently participating in another call. As such, we have implemented a status field so as to notify the CAAS of the statuses of communicating clients. This scenario can be seen in Figure 4:

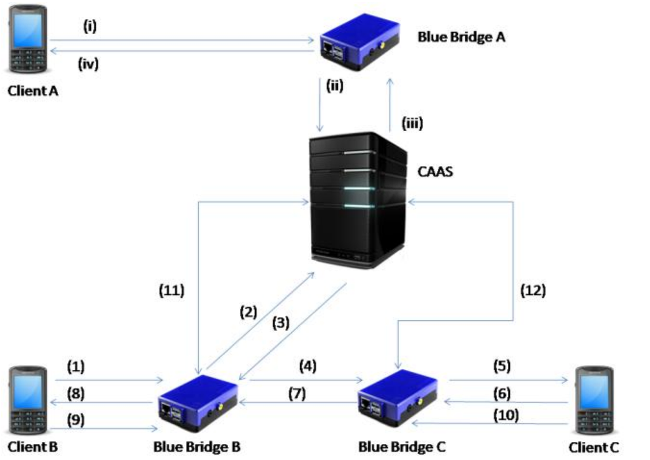


Figure 4. Typical communication session

From Figure 4, Client B and Client C are in a communication session with one another. Client A attempts to call Client B by querying Client B's information from Blue Bridge A (shown as (i) above). Since Blue Bridge A does not have any information pertaining to Client B, it then queries the CAAS for this information (show as (ii) above). The CAAS retrieves Client B's status from the database, and determines that Client B's status is "calling". The CAAS then alters the status field of the *Linkage* packet to "calling" and notifies Blue Bridge A (shown as (iii) above). Blue Bridge A then notifies Client A that Client B is engaged and terminates the connection (shown as (iv) above).

A typical communication session between Client B and Client C can be seen in Figure 4. The communication process begins with Client B querying Blue Bridge B for information pertaining to Client C. The *Linkage* packet sent to Blue Bridge B contains the first media packet to be transmitted to Client C. Since Blue Bridge B does not contain any routing information pertaining to Client C, it strips and stores the voice data temporarily while it attains this routing information from the CAAS (steps 2 and 3). If the CAAS determines that the status of Client C is "available" it updates Client C's status to "calling", which will prevent unnecessary call setup when other clients try to call Client B or C while in the "calling" state.

Throughout the attainment of Client C's routing information, Client B continues to transmit voice data to Blue Bridge B. Blue Bridge B records packet information in a local MYSQL database which references the stored Adaptive Multi-Rate (AMR) media files. Once Blue Bridge B has determined the necessary routing information of Client C, it processes the stored queue of media data and transmits the packets to Blue Bridge C (as seen in step 4). Since Blue Bridge C has a local record of Client C being associated with it, packets can be sent directly to Client C without the need to obtain routing information from the CAAS (as seen in step 5). Blue Bridge C's local database is then also updated with the routing information of Client B. In order to eliminate the storage of non-current client routing information, the local database of Blue Bridges is purged every 10 minutes. Client

C is then able to respond to Client B by sending the voice data to Blue Bridge C (as seen in step 6) which forwards the packet to Blue Bridge B (step 7). Blue Bridge B in turn forwards the data to Client B (step 8). Since both Blue Bridge B and C contain the necessary routing information, communication between Clients B and C then takes place via Blue Bridges B and C (independent of CAAS queries and updates).

When Client B is done communicating with Client C, a status packet (stripped of all voice data) is sent to Blue Bridge B (step 9), which then updates the local database of the status of Client B. Blue Bridge B then notifies the CAAS of the status update (the two way arrow in the diagram indicates a TCP connection, which ensures delivery of the packet - step 11). Similarly, Client C, Blue Bridge C, and the CAAS perform the necessary updates and termination of the communication session as seen in steps 10 and 12.

B. Lost Packets

Since *Linkage* is a best effort based protocol operating across interference prone wireless protocols, the likelihood of lost packets is quite high. In order to minimize the effect of lost packets on the functioning of the CTN we transmit the state the client is currently in; the total number of packets to be transmitted; and the current progress of the transmission from each client transmitting data to its associated *Blue Bridge*. The last packet transmitted from either client contains the "available" state, which notifies the concerned *Blue Bridge* that the client is not participating in a communication session.

In the event where the last packet is lost, the associated Blue Bridge is able to determine when the communication session should have ended based on the total number of packets and the last noted progress. The concerned Blue Bridge then terminates the connection and changes the status of the client to "available

VII. Future work

Although channeling all communication through *Blue Bridges* may result in increased delays throughout the CTN, this type of architecture allows for the system to be extended by providing group calling functionality. This is made possible by Blue Bridges forwarding voice packets to everyone in a particular group. By enabling group broadcasts on Blue Bridges, processing requirements of constrained client handsets is reduced. The ability to provide instant messaging functionality, and create community polling and support systems are other possible extensions. Community polling is particularly useful in areas where there is a shortage of staff. This allows the community to inform the municipality of areas which require attention. These polling systems could also provide benefits for the security and emergency industries, providing a means for people to alert authorities in the event of an emergency.

Our CTN network implementation currently only provides node status updates from *Blue Bridges* to the CAAS when calls between clients are complete; when new clients join the CTN, or when Blue Bridges terminate communication sessions in the event of suspected packet loss. The disadvantage of status updates only in these instances is that client statuses on communicating *Blue Bridges* are updated, but the CAAS does not have the most recent client statuses (except where clients have not communicated since their last session). A possible extension could be to enable client status updates upon *Blue Bridges* querying routing information for destination clients from the CAAS.

VIII. Conclusion

This paper provided an overview of WMNs, CTNs and the Bluetooth protocol, as well as instances of how these technologies and systems are implemented in related work. This paper demonstrated a need for cost effective communication methods utilizing existing technologies and provided an architectural overview of our proposed CTN. This paper explained the benefits and potential constraints of the system, as well as possible solutions to these constraints. This paper identified the problems associated with voice communication in South Africa; provided an overview of existing systems and where they can be improved; and proposed a solution to these problems by means of bridging Bluetooth and IEEE 802.11 wireless connections on a series of Raspberry Pi computers (*Blue Bridge*). This paper also demonstrated how a CTN can be created through the inter-connection of these *Blue Bridges* by means of the proposed protocol - *Linkage*. Finally, this paper suggested possible extensions to the current infrastructure and how these extensions could be implemented.

Acknowledgment

We would like to thank our sponsors, the Telkom Centre of Excellence at Rhodes University, funded by Telkom SA, Business Connexion, Verso Technologies, THRIP, Stortech, Tellabs and the National Research Foundation.

References

[1] F. Ian Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks., 2005, vol. 47, no. 4, pp. 445-487.

[2] At&t., "Learn more about Push to Talk," 2012. Available at: http://www.wireless.att.com/learn/popups/push-talk-faq.jsp. [Accessed 04-10-2013].

[3] C. Bisdikian, "An overview of the Bluetooth wireless technology," Communications Magazine IEEE., 2001, vol. 39, no. 12, pp. 86-94.

[4] R. Bruno, M. Conti, and E. Gregori, "Bluetooth: Architecture, protocols and scheduling algorithms," Cluster Computing., 2002, vol. 5, no. 2, pp. 117-131.

[5] M.C. Castro, P. Dely, J. Karlson, and A. Kassler, "Capacity Increase for Voice over IP Traffic through Packet Aggregation in Wireless Multihop Mesh Networks," IEE Journal., 2007, vol. 2, pp. 350-355.

[6] S. Ganguly, V. Navda, K. Kim, A. Kashyap, D. Niculescu, R. Izmailov, S. Hong, and S.R. Das, "Performance Optimizations for delpoying VoIP Services in Mesh Networks," IEEE Journal, November 2006, vol. 24, no. 11, pp. 2147-2158.

[7] R. Huang, "Heavy-handed network throttling 'bad for business'," 2012. Available at: http://www.zdnet.com/heavy-

handed-network-throttling-bad-for-business-7000001953/. [Accessed 03-21-2013].

[8] J. Ishmael, S. Bury, D. Pezaros, and N.J.P Race, "Deploying rural community wireless mesh networks," IEEE Journal, 2008, vol. 12, no 4, pp. 22-29.

[9] P. Johansson, R. Kapoor, A. Kazantzidis, and M. Gerla, "Rendezvous scheduling in Bluetooth scatternets," IEEE International Conference., 2002, vol. 1, pp. 318-324.

[10] Push to Talk LTD., "Benefits of PTT," 2011. Available at: http://www.pushtotalkuk.com/push_to_talk_benefits.aspx. [Accessed 04-09-2013].

[11] Raspberry Pi., "An ARM GNU/Linux box for $25," 2012. Available at: http://www.raspberrypi.org. [Accessed 04-08-2013].

[12] B. Tubb, "Operators deny VOIP throttling," 2013. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=61979. [Accessed 03-21-2013].

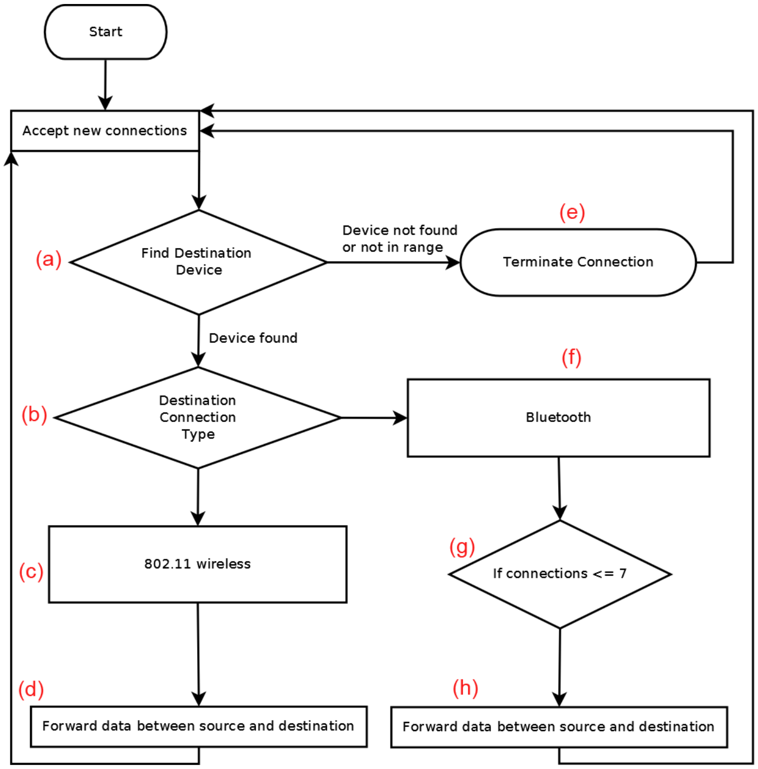


Figure 5. Process diagram for proposed CTN

ISBN: 978-1-61208-299-8

Addressing the Effects of Missing Receiver Problem in Access Networks

Mthulisi Velempini
Information Systems
North-West University
Mmabatho, South Africa
mvelempini@gmail.com

***Abstract*—The implementation of multi-channels at the MAC layer has created a new interference problem, the Missing Receiver Problem (MRP). The MRP is a multi-channel problem which relates to the use of multi-channels concurrently. As nodes communicate on different channels, they become unreachable and deaf. Bandwidth will be wasted when communication is initiated with deaf nodes. The paper evaluates the effects of MRP on network performance. The bandwidth of one control and two data channels is considered in relation to the size of control and data packets. Channel switching delay is also factored in the analysis. An analysis of channel bandwidth given the size of packets is presented. The proposed MRP solution is based on the cyclical scheduling algorithm, a proposed framework for solving multi-channel interference challenges. The framework is described at length and thereafter the analyses and the analytical results are discussed. The results show that the effects of the MRP can be reduced.**

Keywords-Channel Coordination; Channel Selection; Common Control Channel; Deafness; Missing Receiver Problem

I. INTRODUCTION

Wireless Mesh Networks (WMN) can be deployed effectively as a community wireless access network. However, the capacity of WMN falls short in meeting the requirements of time bounded data, largely due to interferences, such as the Hidden Terminals, the Exposed Terminals and the Terminal Deafness Problem. In general, the implementation of multi-channel systems has availed more capacity for wireless systems and improved their performance. Nevertheless, the above mentioned problems still require to be addressed for the increased network capacity to be realized.

WMN are widely touted as the possible future community access network offering high speed broadband connectivity offer last mile broadband wireless access. They overcome the shortcomings of ad hoc networks by overlaying or integrating mobile terminals with static nodes. The static nodes have high processing power, are more energy efficient and do act as a semblance of an infrastructure based network. However, more has to be done to position WMN as high speed last mile broadband wireless network solution.

One of the proposed directions of research aimed at increasing network capacity exploits the availability of the multi-channels at the physical layer prompting the need to redesign the Medium Access Control (MAC) protocols to handle multiple channels. In general, the results of the multi-channel schemes are encouraging [1] [2]. However, multi-channel interferences, such as the MRP still require attention.

This paper first presents in detail a proposed Cyclical Scheduling Algorithm (CSA), through which the multi-channel interferences such as the MRP can be addressed. The CSA is the multi-channel coordination, scheduling and channel selection scheme which transmit data in phases. The MAC schedules data transmissions in cycles. It then presents the assumptions underpinning the MRP solution. The MRP solution is premised on wasted bandwidth, given the ratio of control channel dwell on time to the data channel dwell on time, when an instance of the MRP is encountered.

The Missing Receiver Problem is caused by a would-be receiver, which is currently busy on a different channel either receiving or transmitting or just listening on it, while a sender is trying to send packets to it on a different channel. The sent packets fail to reach a receiver because the intended receiver would be tuned on a different channel. The MRP is caused by lack of synchronization between the sender and the receiver in multi-channel systems. The lack of synchronization of the sender and the receiver wastes bandwidth and network resources.

The need to reduce multi-channel interferences and for multi-channel approaches at the MAC layer is discussed in Section 2. Section 3 discusses related work. The proposed CSA model is presented in Section 4. The impact of the MRP on network performance and the analytical results are presented in Section 5. Section 6 and Section 7 summarize the future work and the proposed model, respectively.

II. MOTIVATION

Mesh networks combine the advantages of ad hoc networks and infrastructure based networks into one community based network. Different access networks can be deployed in a community forming an auto configuring, self healing and self organizing mesh network. The need and the requirements of quality of service and the time bounded data can be met by well designed multi-channel mesh networks.

Multi-channel techniques are robust, flexible and do increase network capacity. However, the coordination, selection and scheduling of multi-channels needs to be explored further.

The increase in network capacity in multi-channel systems comes at the expense of channel switching delay. The net effect of trading off channel switching cost with network capacity may improve the overall network performance.

The multiple channels are available at the physical layer; unfortunately the MAC layer is not designed for multi-channel systems; while the network layer is optimized for multi-channels and is designed to address the shortcomings of the MAC layer. The reconfiguration of the MAC will therefore, result in the realization of more capacity and flexibility. The channel selection, coordination and the terminal deafness challenges may be solved at the MAC layer for improved network performance.

We propose a multi-channel cyclical scheduling algorithm and present it as a framework for solving multi-channel interference problems. The MRP solution which is based on the proposed multi-channel framework is then presented and evaluated analytically.

III. RELATED WORK

Maheshwari et al. [1] reduces the effects of MRP by employing a receiver initiated solution. Unfortunately, it only alerts transmitters which are in their back off intervals. A new collision technique may be required to resolve contention of two or more invited transmitters which respond to the same invitation simultaneously. Furthermore, the user based quiescent channels may lead to network portioning.

Shi et al. [2] solve the multi-channel interference challenge through the synchronization of nodes on the control channel. However, synchronization is a challenge for mobile nodes.

Toham and Jan [3] employ a multi-interfaces approach and it solves MRP at high overhead cost of hello messages which degrade the network performance. It is also expensive in terms of hardware requirements. Mo et al. [4] proposed a similar multi-interfaces scheme. It also solves the deafness problem at high hardware cost.

Toham and Jan [3] argue that the use of a common control channel causes bottleneck. The implementation of a common control channel facilitates network connectivity and ensures that the network is not partitioned.

Seo and Ma [5] proposed a synchronous scheme using one transceiver. The system broadcast channel releases messages, and keeps both a neighbor status list and a channel status list. A significant percentage of bandwidth is lost in signaling and synchronization is a challenge. The proposed contention window may be too small in backlogged environments.

A CTS packet reserves a channel in [6] and fails to notify nodes in the neighborhood of the transmitter. However, the use of two transceivers minimizes the effects of missing receivers albeit at high cost of hardware.

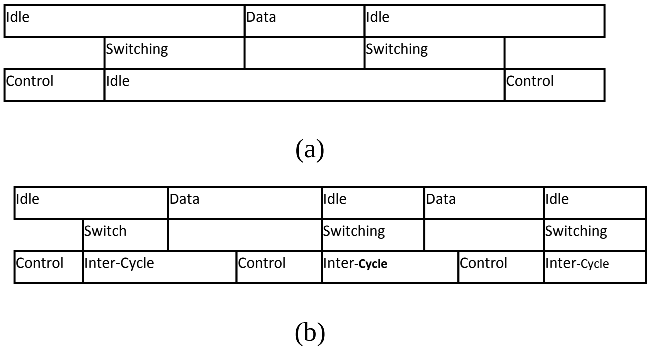
Incidents of the missing receiver problem increase due to lack of coordination in multi-channel systems. The pair of nodes may be on two different channels or one node may switch to a different channel thereby becoming unreachable. When one node is busy on one channel while a number of nodes (at least one) are trying to communicate with it on different channels, an unreachable terminal is said to be deaf [7].

IV. THE SYSTEM MODEL

The proposed CSA framework has four distinct components. The framework has the following techniques: the channel switching penalty, the Request To Send (RTS) based data channel reservation and access scheme, the inter-cycle, and the phasing of data transmission in cycles. We describe each of these four aspects separately and then show how they are integrated. The framework employs one dedicated control channel and N number of data channels. We then show how the envisaged framework reduces the effects of MRP.

The channel switching technique associates all the switching costs with the data channels. It considers two channel switching penalties. When a transceiver switches to and from a given data channel from the control channel it incurs two channel switching delays. When the transceiver switches to the data channel, it incurs a switching delay of 224μs (the maximum cost specified by the IEEE 802.11 standard) and the same duration is also incurred when it switches back onto the control channel. The effective channel switching delay is therefore set to 448μs to capture its double effect on data channels. The value of the switching delay is added to the data packet transmission duration.

Ideally, this will keep a data channel busy for a longer duration. However, it improves the performance of the control channel and it increases its capacity to drive more data channels before it saturates. In general, this approach is capable of improving the overall system performance.



(a)

(b)

Figure 1. The channel switching penalty model.

In Fig. 1a, we model the conventional approach where the next transmitter waits for the channel switching process to be performed first before contending for the control channel. All the terminals should be on the control channel before the next transmission is initiated. This approach wastes the capacity of the control channel and increases its saturation rate. The capacity of the control channel may be increased to improve the performance of the network. As shown in Fig. 1b, the capacity of the control channel has been improved. The control channel can now drive more data channels. In the proposed scheme, the data channel is reserved when it is about to finish the current transmission. As the current communicating pair switch back onto the control channel, the next pair switch onto the data channel. The terminals will cross each other as they switch to opposite directions. This equips the control channel with more capacity to support more data channels, which, in essence, increases its scheduling capacity and reduces its idleness. It should also be noted that there is no need in this case for nodes to perform a channel switching prior to control channel contention.

The RTS-based data channel reservation and access scheme limit channel contention to the control channel. Two terminals intending to exchange data will contend for and reserve the control channel. Thereafter, there will not exchange packets to negotiate which data channel to reserve. The reservation of the data channels will be linked to the reservation of the control channel. This is possible in the CSA framework given the fact that data transmission is scheduled in phases. The control channel is reserved during timeslots in which a given data channel is known to be idle. The main goal of this scheme is to reduce the contention and channel reservation duration and to avail more bandwidth for network performance improvement.

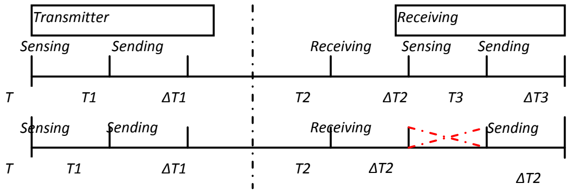


Figure 2. The RTS based channel reservation scheme.

In Fig. 2, the transmitter has to first identify idle data channels between time T and T1 and then sends the list to the receiver including its preferred data channel at T1. The receiver will also upon receiving the RTS packet at time T2, check whether the sender's preferred data channel is also free at its end. It may check other data channels in the list if the preferred data channel is not available. Thereafter, it will send either the confirming or the rejecting CTS back to the transmitter [2]. These processes are shown in the top block.

The bottom block shows the proposed approach where a sender does not have to first check whether the preferred data channel is indeed idle. The sender only includes one data channel in its RTS packet which is known to be idle and the receiver would be expected to accept it. The receiver will agree with the sender on the preferred data channel without having to first sense the medium. The sender chooses a preferred data channel without sensing the medium using virtual carrier sensing and network support scheme. The nodes are, therefore, able to determine when channels would be idle without relying on both the physical and the virtual carrier sensing mechanisms.

The implementation of the RTS-based data channel reservation assumes that the data channels would be available when the sender reserves the control channel. The receiver will therefore be expected to agree with the sender on the preferred data channel.

The inter-cycle scheme marks the beginning and the end of a given cycle. It defines the shortest duration a data channel will be busy before it is available for the next data transmission in the next cycle. It is the hold off duration which forces all terminals intending to use a given data channel to hold off their next transmissions long enough to allow data packets to be delivered successfully. In essence the inter-cycle is the time when the last control packet was received in the previous cycle to the time the next control packet is sent in the next cycle.

The inter-cycle duration is not fixed it varies with the number of data channels implemented. It is inversely related to the number of data channels. It has the longest duration when there are only two data channels and its length decreases as more data channels are added.

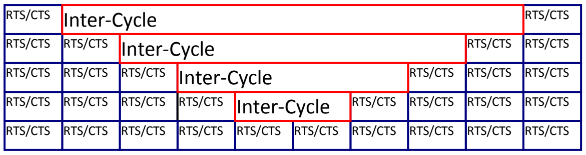

RTS/CTS Inter-Cycle RTS/CTS
RTS/CTS RTS/CTS Inter-Cycle RTS/CTS RTS/CTS
RTS/CTS RTS/CTS RTS/CTS Inter-Cycle RTS/CTS RTS/CTS RTS/CTS
RTS/CTS RTS/CTS RTS/CTS RTS/CTS Inter-Cycle RTS/CTS RTS/CTS RTS/CTS RTS/CTS
RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS RTS/CTS

Figure 3. The Inter-Cycle Scheme.

Fig. 3 shows the behavior of the inter-cycle duration as the number of data channels is increased. The inter-cycle duration decreases with the number of data channels. As it shrinks, the control channel becomes busier and its capacity improves. The control channel can schedule and drive more data channels.

The top row depicts a situation where there are two data channels. The control channel will lie idle after performing the first handshake of the two data channels until the current data transmissions are about to complete. Then the next handshake will be performed in the next cycle. The duration of the inter-cycle will reduce in the next row when two more data channels are added. This behavior will be exhibited by the inter-cycle for every additional data channels to been added. For the purposes of the analytical work, we assume that all the channels are orthogonal to each other.

Lastly, we describe briefly the cyclical nature of the algorithm. This attribute of the algorithm is related to the inter-cycle technique. All the available data channels will be accessed in phases through the control channel. When the last data channel in the current cycle finishes its transmission, the first channel, will be reserved for the first transmission in the next cycle. This attribute of the CSA is detailed in [8] [9] with accompanying diagrams.

The following pseudo-code gives an overall picture of the entire algorithm with its four components. The pseudo code gives the bird's view of the CSA. It explains the CSA in a very concise manner. The pseudo code also shows how the components of CSA are integrated to each other.

PSEUDO-CODE 1. CHANNEL SELECTION AND SCHEDULING

```
For (j && i = 0; j && i <= n-1; j++ &&i++)
1.  Begin channel access for terminal X+j
2.  defer for the inter-cycle duration for next cycle NC+i
3.  Contend for the control channel access C0
4.  RTS and CTS agree to reserve Data Channel DC, i+1
5.  Sender and receiver both Switch to DC, i+1
6.  Transmit on DC for DATA + 2 * switching delay( sw_p)
7.  Switch back to C0
8.  repeat 2 to 7 until DC, is equal  i + n - 1
9.  Reset counters and Begin next cycle, NC + i
```

We now discuss how the framework reduces the effects of the MRP. We assume that there are three channels, one control and two data channels. In each cycle, two data flows are scheduled. Given this assumption, we consider the number of terminals which are likely to be deaf and how terminals can be quickly synchronized to reduce the MRP.

In any given cycle there are two possible nodes which may be deaf. If other terminals try to send packets to them, bandwidth will be wasted. Furthermore, returning nodes will not have a complete picture of the network upon their return to the control channel. The status of some nodes is likely to change during their absence. Technically, two nodes may be unknown to any returning node when two data channels are implemented. This is possible because data channels are reserved whilst some nodes are still busy transmitting on data channels. As terminals in the current cycle are switching back to the control channel, the next set of terminals for the next cycle will be switching onto the data channels.

To reduce the effects of terminal deafness, returning terminals may be starved of their next transmission until they have knowledge of the network.

Deaf terminals are within the transmitter's communication range but are not able to overhear or receive packets from a transmitter because they are busy receiving or transmitting on a different channel. We therefore do not consider transmission ranges of terminals. We assume that all terminals are within the communication range of each other and can decode all received or overheard packets. The impact of MRP is modeled and analytically explored in the following section.

V. ANALYTICAL RESULTS

This section analyzes the effects of the missing receivers on network performance and analytical results are presented.

Throughput y, which is available to each node in the network, is given by dividing the capacity of the network by the number of nodes in the network [10]. Given this formula, the allotment of throughput to the nodes can be ascertained and predicted. The equation is given below: c is the capacity, while N the number of nodes.

$$y = {}^{c}/_{N} \qquad (1)$$

In the multi-channel environment, the capacity of the network increases with the number of channels implemented. It increases approximately at *N* times the channel capacity. *Nc* is therefore the total capacity of all the channels.

So and Vaidya [11] argues that a dedicated control channel in a three channel system constitutes a third of the total capacity. Generalizing the capacity of the control channel *Cc*, with *M*, the number of channels, the following formula is obtained:

$$C_c = \frac{N_c}{M} \quad , \qquad (2)$$

The instance of the MRP is equivalent to the control channel overhead as it wastes the same amount of bandwidth. Factoring the effects of the MRP in the allotment of bandwidth in (3) is obtained.

The network throughput in the presence of MRP, denoted by *YMRP* is expressed as follows:

$$Y_{MRP} = \frac{N_c\,(1-\frac{n}{M})}{N} \qquad (3)$$

Network capacity is denoted by *Nc*, the instance of the MRP by *n* and *N* denotes the number of nodes.

Given (3), the effects of the MRP can be modeled. If there are three channels, then one encounter of the missing receiver will result in one third degradation of the network throughput.

Two encounters of deafness in the proposed CSA will result in two-thirds throughput degradation. Fig. 4 depicts network throughput degradation under these assumptions, when the capacity is set to 12 Mbs and *M* to 3. *YMRP* denotes throughput in the presence of MRP.

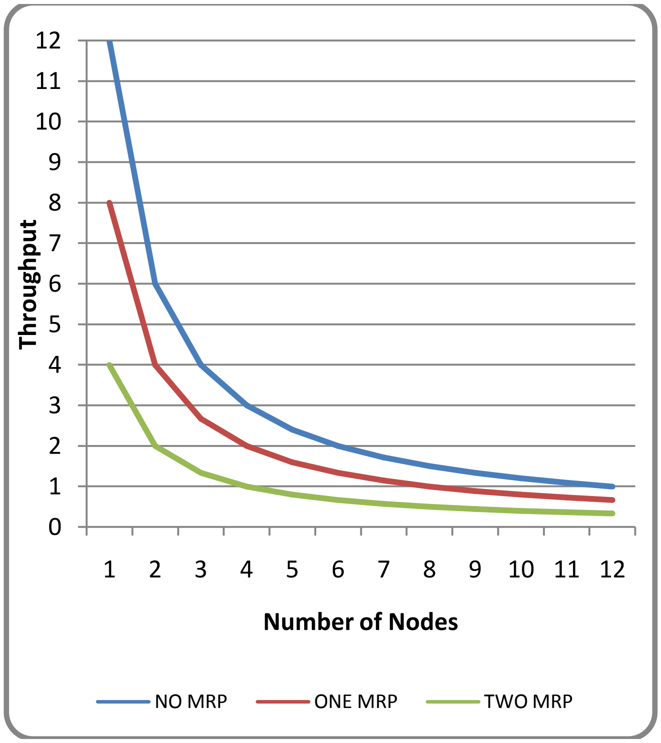


Figure 4. Effects of MRP on throughput

When the transmission durations of the control and the data channels are considered, it becomes apparent that the effects of MRP would be less severe. The transmission ratio of the control channel to the data channel is approximately *11 to 1* in terms of transmission durations taking into consideration the channel switching delay. The results of an *11 to 1* ratio are expected to differ significantly from the results in Fig. 4 which are based on a *2 to 1* ratio. The instance of a MRP will therefore cause a twelfth of network degradation.

Control channel overhead is represented by (1), when *M* is 12.

To calculate the network throughput after factoring the effects of the node deafness problem, equation (3) is employed. When an RTS is sent to a deaf node, a complete RTS/CTS handshake is recorded as a complete transmission amounting to a control channel overhead.

The amount of bandwidth utilized is therefore equal to the control channel overhead. The assumption that an instance of a MRP amounts to the control overhead is valid as the control channel would be unavailable for the entire duration of the RTS/CTS handshake.

The overhead caused by the instance of the MRP now translates to, $\frac{n}{12}$. Taking this fraction and factoring it into (3), we get the following equation.

$$Y_{MRP} = \frac{N_c\ (1-\frac{n}{M})}{N} \qquad (4)$$

Given equation (4) and that $N_\mathbf{c}$ is 12 Mbs and *M* is 12; the results in Fig. 5 are obtained.

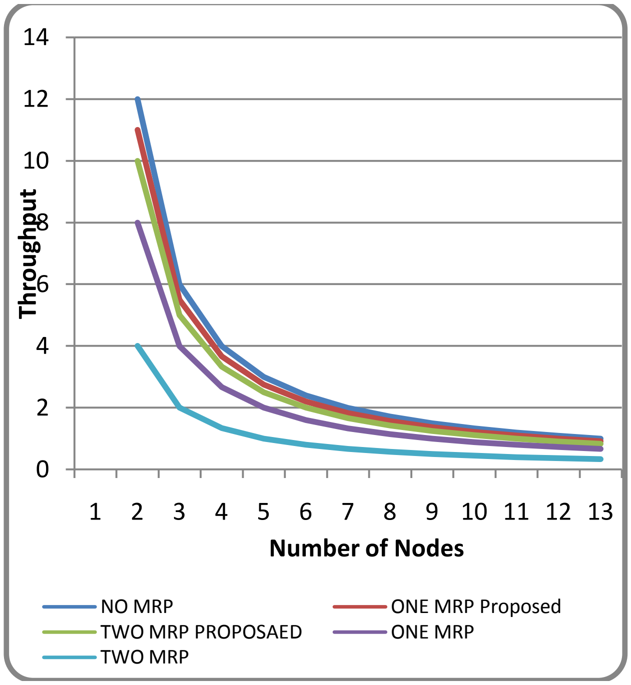


Figure 5. Effects of MRP on throughput in our proposed solution

Fig. 5 shows that the proposed approach is likely to perform better in the face of Missing Receivers and its performance would improve as more instances of MRP are encountered. For example, in Fig. 5 where two instances of node deafness are encountered, the proposed approach performed better that when only one instance was encountered. However, in any given cycle, at most two terminals may be deaf and unreachable, according to the CSA assumptions for a network with three channels.

The solution to MRP will improve the network throughput and reduce significantly the control channel overhead cost. Fig. 5 shows that the instances of missing receivers do increase the overhead of the control channel. It can also be seen in the same figure that the effects of node deafness in the proposed architecture will be less severe as compared to Fig. 4.

VI. Conclusion

Given the proposed underlying protocol the CSA, the MRP will be limited to the returning terminals. The returning nodes should be forced to delay their next transmissions until they have adequate information about the status of the network. This will reduce the effects of MRP. The waiting delay may be reconsidered where network support is implemented.

When the instance of the MRP is considered to be equal to the overhead of the control channel, and taking into consideration the actual packet lengths of both data and control packets, the effects of MRP will be reduced further. The phasing of data transmission enables terminals to have the correct information about the channels and to know when to contend for data channels when they become free.

The CSA also facilitates the implementation of the RTS-based data channel reservation and access scheme. Contention will be limited to control channel and there will be no need for the signaling packets to be employed in reserving and in agreeing on data channels to be used. The reservation of the data channels will be scheduled through the control channel when a given data channel is idle and available for the next data transmission.

The implementation of the CSA will make use of the virtual carrier sensing technique for data channel reservation. The physical carrier sensing, and the virtual carrier sensing, will be employed only for the control channel reservation.

The control channel facilitates network connectivity. Furthermore, there can be at most four channels available when non overlapping channels are considered [12]. We are experimenting on how network improves, assuming that all the channels are available and are orthogonal. Future work will look at how many possible channels can be utilized if the additional data channels do improve the performance of the network.

References

[1] Ritesh Maheshwari, Himanshu Gupta, and Samir R. Das, “Multichannel MAC protocols for wireless networks”, SECON 2006, Volume 2, 28 September 2006, Reston,VA, pp.393-401 [retrieved: May, 2013].

[2] Jingpu Shi, Theodoros Salonidis, and Edward W. Knightly (2006), "Starvation Mitigation Through Multi-Channel Coordination in CSMA Multi-hop Wireless Networks", MobiHoc'06, May 22–25, 2006, Florence, Italy, pp.214 - 225 [retrieved: June, 2013]

[3] Carine Toham, and François Jan (2006), "Multi-interfaces and Multi-channels Multihop Ad Hoc Networks: Overview and Challenges", Mobile Adhoc and Sensor Systems (MASS 2006), Vancouver, BC, **http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4053982 .** pp.696 -701[retrieved: May, 2013]

[4] Jeonghoon Mo, Hoi-Sheung Wilson So, and Jean Walrand (2005), "Comparison of Multi-Channel MAC Protocols", MSWiM 2005, 10 – 13 October, Montreal, Quebec, Canada. pp.209 – 218 [retrieved: June, 2013]

[5] Myunghwan Seo and Joongsoo Ma (2007), "Flexible Multi-channel Coordination MAC for Multi-hop Ad hoc Network", Technical Report, January 2007. [retrieved: July, 2011]

[6] Sudthida Wiwatthanasaranrom and Anan Phonphoem, "Multichannel MAC Protocol for Ad-Hoc Wireless Networks", Computer Engineering, Kasetsart University. pp.393-401 [retrieved: May, 2013]

[7] Pradeep Kyasanur Jungmin So, chandrakanth Chereddi, and Nitin H. Vaidya, "Multi-Channel Mesh Networks: Challenge and Protocols", University of Illinois. pp.30-36 [retrieved: July, 2013]

[8] Mthulisi Velempini and Mqhele E. Dlodlo (2008). Combating the effects of Hidden Terminals in Multi -channel MAC Protocols. SATNAC 2008, 7 – 10 September 2008. [retrieved: May, 2013]

[9] Mthulisi Velempini and Mqhele. E. Dlodlo (2009). Analyzing the effects of increasing data channels and the number of data flows on network performance. Wireless Vitae 2009, Aalborg, Denmark. pp.600 – 605 [retrieved: June, 2013]

[10] BelAir Networks (2006).Capacity of Wireless Mesh Networks. BelAir NetworksNorth America, Whitepaper. www.belairnetworks.com [retrieved: May, 2013].

[11] Jungmin So and Nitin Vaidya (2004), "Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using A Single Transceiver", *MobiHoc'04,* May 24–26, 2004, Roppongi, Japan. pp.222-233 [retrieved: July, 2013]

[12] Danilo Valerio, Fabio Ricciato, and Paul Fuxjaeger (2008). On the feasibility of IEEE 802.11 multi-channel multi-hop mesh networks. Computer Communications 31 (2008), www.elsevier.com/locate/comcom pp.1484 - 1496 [retrieved: June, 2013]

[13] Jeonghoon Mo, Hoi-Sheung Wilson So, and Jean Walrand, "McMAC: A Parallel Rendezvous Multi-Channel MAC Protocol", IEEE Wireless Communications and Networking Conference, 2007 www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 4224312 . pp. 334 – 339 [retrieved: June, 2013]

[14] Jenhui Chen and Shiann-Tsong Sheu (2004), "Distributed multichannel MAC protocol for IEEE 802.11 ad hoc wireless LANs", Computer Communications 28 (2005). pp.1000-1013 [retrieved: June, 2013]

[15] Wing-Chung Hung, K.L. Eddie Law, and A. Leon-Garcia (2002), "A Dynamic Multi-Channel MAC for Ad Hoc LAN", 21st Biennial Symposium on Communications, 5 April 2002. pp.1 -5 [retrieved: July, 2013]

[16] Balvinder Kaur Thind (2004), "A receiver-initiated mac protocol with enhancements for multi-hop wireless networks", Washington State University, master of science Thesis, May 2004. pp.1 – 122 [retrieved: June, 2013]

Vertical Handover in Wireless Mesh Networks and its Impact on Routing

Ferdawss Douma and Rafik Braham
PRINCE RG, ISITCOM - University of Sousse, Tunisia
E-mails :{ Ferdawss_douma@live.fr, rafik.braham@ensi.rnu.tn}

Abstract **—This paper proposes a new idea to improve routing in wireless mesh networks using IEEE 802.21's Media Independent Handover (MIH) functions. First, we evaluate the performance of a vertical handover using IEEE 802.21 protocol between WiFi and WiMax networks. Then, we present our proposal of using MIHF for optimizing the performance of IEEE 802.11s Wireless Mesh Networks (WMN) routing protocols, such as Hybrid Wireless Mesh Protocol (HWMP).**

Keywords-Wireless mesh networks; routing protocol; Handover; MIH; packets loss ratio; handover delay.

I. INTRODUCTION

In recent years, wireless communication technologies have evolved thanks to their utility and flexibility. This has led to the emergence of new wireless network solutions.

One such solution consists of Wireless Mesh Networks (WMN), which are gaining importance [1].

IEEE 802.11s Group [2] was established in January 2004 to provide mesh functions to IEEE 802.11 architectures and protocols.

Research in the field of WMNs [3] is broad and diverse. Indeed, substantial works are currently carried out by researchers on routing protocols and their performance indicators. In addition, many other works focus on higher-level protocols (Quality of Service (QoS), service discovery, etc.). Mobility is also a very active area of research.

Handover process causes a number of problems in routing, which degrades the service continuity. We have noticed, however, that works that connect routing and handover or use the characteristics of one to enhance the other are extremely rare. Our idea then is to link these two operations.

For this, we exploit the handover protocol described in IEEE's Media Independent Handover (MIH) [4] in order to improve routing between different network components and maintain service continuity.

This paper is organized as follows: Section II presents an overview of WMNs and popular routing protocols. Section III presents the MIH standard and Section IV describes related works found in the literature. Then, Section V describes simulation experiments. Different applications are used for this topic such as Constant Bit Rate (CBR) video and voice traffic.

Our approach to improve routing in WMNs using MIH is presented in Section VI. In Section VII, we discuss simulation results and present the advantages and disadvantages of our proposed idea. Finally, Section VIII provides a summary of this paper and some perspectives.

II. OVERVIEW OF IEEE 802.11S AND ROUTING PROTOCOLS

WMN technology is widely used in the world and its standardization becomes very necessary for large-scale applications. Currently, WMN standards are: IEEE 802.15.5, IEEE 802.16 and IEEE 802.11s.

IEEE 802.15.5 [5] is a standard which aims to introduce the MESH technology at the personal area networks level. This standard aims to identify and develop mechanisms that must be present at the physical and MAC layers in order to implement the MESH technology in WPANs. This standard provides personal area networks that offer higher rate and ensure transmissions over longer distances.

IEEE 802.16 standard group [6] introduces the Mesh structure in the IEEE 802.16 d/e standard. In IEEE 802.16 Mesh, any node in the network can form several links with its adjacent nodes and one of the links is selected to transmit the information from local node or other nodes.

IEEE 802.11s is a flexible and extensible standard for WMNs based on IEEE 802.11 family. One of the important functionalities of IEEE 802.11s is the wireless multi-hop routing, which sets up paths for wireless forwarding.

IEEE 802.11s mesh networks can be used in a wide range of application scenarios. These scenarios include residential for the digital home, companies and public places and temporary infrastructure in case of a disaster. Mesh networks are extensible to allow support for diverse applications and future innovation.

Routing, also called path selection, consists of finding the optimal route from source to destination. IEEE 802.11s routing protocols are particularly based on the work of the IETF MANET [7], but operate at layer 2 unlike MANET protocols, which operate at layer 3. The 11s group has as target configuration a network which contains 32 entities that participate in routing.

Two routing protocols are considered: Hybrid Wireless Mesh Protocol (HWMP) and Radio Aware Optimized Link State Routing Protocol (RA-OLSR) [8].

The HWMP is the default routing protocol for wireless mesh networks. It combines two approaches: reactive routing and proactive tree-based routing [9].

The main characteristic of reactive routing is that a path is computed only if one is needed for sending data between two mesh points.

Proactive routing is based on three routing bases:

- A distance vector routing tree is built and maintained if a root portal is present.
- Tree-based routing is efficient for hierarchical networks.
- Tree-based routing avoids unnecessary discovery flooding during discovery and recovery.

The RA-OLSR Protocol is an improvement of the Optimized Link State Routing Protocol OLSR [10]. The shortest path algorithm uses a radio-aware metric instead of the hop count metric. For that reason, a metric field is added to all topology information messages. RA-OLSR uses MAC addresses rather than IP addresses.

III. MEDIA INDEPENDENT HANDOVER (MIH)

The scope of the IEEE 802.21 MIH standard is to develop a standard that would provide generic link layer intelligence and other network related information to upper layers to optimize handovers between different heterogeneous media such as the 3rd Generation Partnership Project (3GPP), 3GPP2 and both wired and wireless media of the IEEE 802.21 family [11].

The main objective of MIH is to provide a framework that enables seamless handover between heterogeneous technologies. It uses a protocol stack implemented in all the devices involved in the handover which provides the necessary interactions among devices for optimizing handover decisions.

The standard allows providing information which could help at the phase of selection of the network and the activation of the interface. The execution and the decision of handover is not part of the standard.

In the mobility management protocol stack of both the MN and network element, the Media Independent Handover Function (MIHF) is logically defined as a sub-layer between L2 data link layer and L3 network layer. The upper layers are provided services by the MIH function through a unified interface.

The services exposed by the unified interface are independent of access technologies. This unified interface is known as Media Independent Handover Service Access Point (MIH_SAP). The lower layer protocols communicate with the MIHF via media dependent SAPs [11].

This standard defines services that comprise the MIHF services. These services which facilitate handovers between heterogeneous access links are:

- Media Independent Event Service (MIES) that provides event classification, event filtering and event reporting corresponding to dynamic changes in link characteristics, link status, and link quality.
- Media Independent Command Service (MICS) that enables MIH users to manage and control link behavior relevant to handovers and mobility,
- Media Independent Information Service (MIIS) that provides details on the characteristics and services provided by the serving and neighboring networks. The information enables effective system access and effective handover decisions.

MIHF provides asynchronous and synchronous services through SAPs for link layers and MIH users. In the case of a system with multiple network interfaces of arbitrary type, MIH users employ event service, command service, and information service provided by MIHF to manage, determine, and control the state of underlying interfaces.

These services provided by MIHF help the MIH users in maintaining service continuity, service adaptation to varying quality of service, battery life conservation, network discovery, and link selection.

The handover is considered as “hard” or “soft,” depending on whether the handover procedure is “break-before-make” or “make-before-break”.

IV. RELATED WORKS

Many papers associated with MIH have focused on improving handoff performances.

Several research studies have investigated the improvements that MIH could make to different mobility protocols at various levels.

At the network layer, Mussabbir and Yao [12] proposed using MIH services in order to optimize the procedure of handover for Mobile IPv6 Fast Handovers (FMIPv6).

Magagula [13] shows that Proxy Mobile IPv6 is a protocol for mobility management. It is effective in improving the performance indicators of the operation such as handover latency and packet loss in particular when used with the IEEE 802.21 protocol services MIH.

At the transport layer, Chen [14] proposed an interaction between SCTP and 802.21. This optimizes the handover mechanisms in networks within the campus for VoIP applications.

At the application layer, Choong [15] analyzes the improvements that can be gained by interaction between SIP and MIH.

Lee et al. [16] proposed a framework for the integration of IEEE 802.21 MIHF with OLSR to improve the performances of this ad-hoc routing protocol using the Hello interval.

Several research works evaluated routing protocols performances in mesh networks IEEE 802.11s. For example, N.R.Nomulwar et al. [17] presented performance analysis of routing protocol in Wireless Mesh Network such as HWMP, Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance-Vector (DSDV).

Baumann [18] introduced a notification protocol driven by the access points and independent of used routing protocol. When access points detect the clients’ macro mobility by the change of addresses, the MAPs send to source node a notification message which contains the new configuration parameters. The notification message will be sent periodically for each client, which may cause a heavy additional signaling overhead in Wireless Mesh Network.

A fast handoff management scheme in WMN have been developed by Kowalik et al. [19]. It is called MeshScan. It includes three main steps. First, a client device maintains a list of active Mesh Nodes (MNs) (SmartList). Then when it receives a disassociation message from the serving MN or when the measured signal strength from the serving MN exceeds the threshold, it performs the handoff. Finally, when handoff is required, a client transmits Authentication Request frames to all MNs on the list instead of broadcasting Probe Request frames as is usually the case in an active scan in order to discover available MNs.

The goal of our proposal is to achieve improvements in network performances for wireless mesh network environments through the integration of MIH with mesh routing protocols like HWMP.

V. SIMULATION MODEL BASED ON MIH PROTOCOL

The simulation scenario consists of one WLAN cell and a WiMAX cell. It is assumed that one MN, equipped with multiple interfaces, is connected to WiFi before it goes through the WiMAX coverage area.

The handover between the WLAN cell and WiMAX is performed when the MN leaves the coverage area of the WLAN AP.

Figure 1 shows four main elements:

- The WLAN AP
- WiMAX BS
- The router connected to CN (Correspondent Node)
- The multi-interface MN

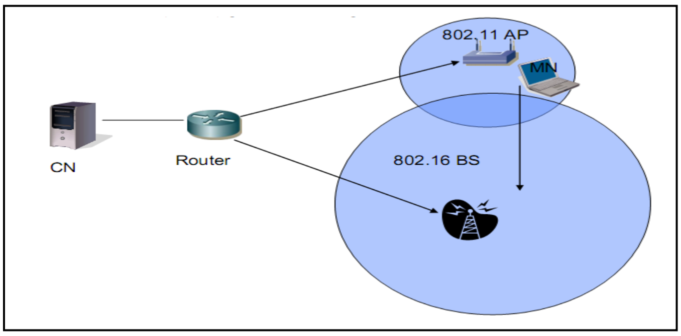


Figure 1. Simulation scenario

A. Simulation Parameters

Table I summarizes parameter values used in the simulations which illustrates the generic network topology used.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Network Topology	
WiMAX cell coverage	1000 m
WLAN cell coverage	20 m
Router Configuration	
MAX_RA_DELAY (s)	0.5
Router lifetime (s)Wlan	1800
Router lifetime (s)WiMax	20
802.11 MAC Layer Configuration	
WLAN beacon interval (s)	0.1
Default scanning mode	Passive
MinChannelTime (s)	0.02
MaxChannelTime	0.06
802.16 Configuration	
Dcd_interval	5
Ucd_interval	5
Client_timeout_	50
Default modulation (s)	OFDM_16_QAM
Application Traffic for Mobile Node	
Type	Depends on application
Packet size (bytes)	Depends on application
Packet inter-arrival time (s)	Depends on application

To evaluate handover performances, we have chosen to compare results between two applications. These are:

- CBR Video traffic (real-time data).
- CBR Voice traffic (real-time data).

We used a real-time traffic to study the effect of the handover on this type of application that requires a good Quality of Service (QoS).

The realization of our simulations is based on the NIST NS-2 implementation [20] of IEEE 802.21 for infrastructure-based network environments.

B. Performance criteria

The performance criteria adopted in our simulations to evaluate the vertical handover between WLAN and Wimax are Delay and Packets Loss Ratio. These parameters are the main criteria of QoS in the networks.

C. Simulation results:

1) Packet Loss Ratio

We calculate in this section the percentage of lost packets. Figure 2 demonstrates that the handover causes a jump in packet loss. Each curve contains a peak, which corresponds to the Packet Loss Ratio during roaming period. As expected, the handover process causes an increase in the number of dropped packets.

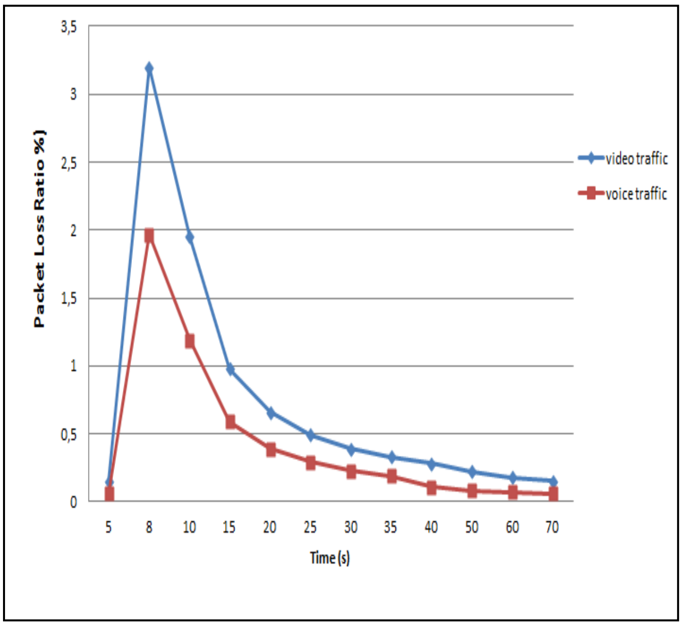


Figure 2. Packets Loss Ratio during simulation: voice and video traffic

For voice traffic, the packet size is 160 bytes, the CBR interval is 0.02 seconds and the mobile node velocity is 13 m/s. Figure 2 shows that the packet loss ratio increases suddenly at the beginning of handover to a value of 1.95%.

In the foreign network, the packet loss ratio for the mobile node degrades to achieve 0.06%.

For video traffic, we use a packets size of 1240 bytes, a CBR interval of 0.1 seconds and a velocity of 13 m/s.

We deduce that for low mobility handover performances are acceptable. Indeed, for a speed of 13 m/s the packet loss ratio is less than 3.2%. The higher value of loss appears during the execution of the handover (the peak of the curve), which reached 3.2% (see Figure 2).

When the mobile moves to the foreign network (WiMAX) the packet loss ratio decreases to a value below 0.5%.

The packets loss ratio for voice traffic during handover was 1.95%. Compared to the packets loss ratio of video type traffic (3.2%), it is much smaller. The result was as expected since the packet size will necessarily affect the packets loss ratio.

2) Delay

The delay is a very important parameter to evaluate the QoS for real time traffic. This is the time needed for a packet to be transmitted across a network from source to destination (end-to-end).

In this section, we discuss packet delays during the simulation time when applying the scenario of the handover from WLAN to WiMAX.

We present voice traffic results first. We notice the existence of a peak at the moment of the handover execution because the transfer time becomes quite important (between 0.76 and 1.18 s).

After executing the handover, the delay of packet transmission falls, it becomes almost constant and less than 0.2 seconds.

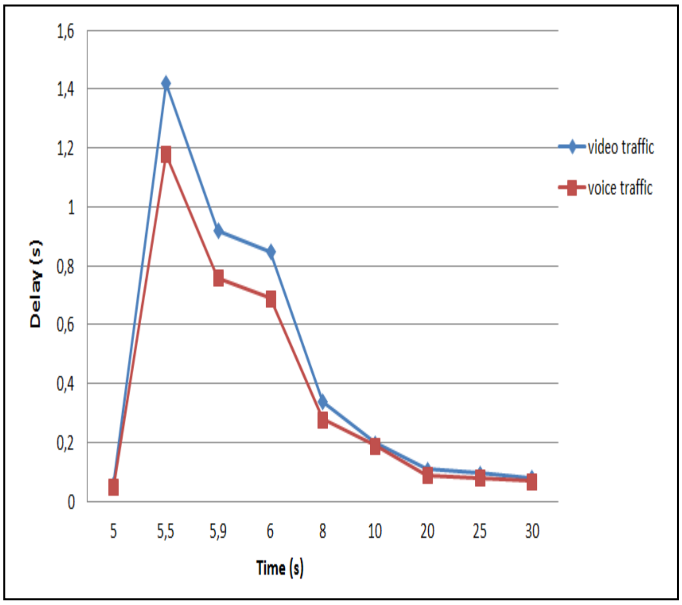


Figure 3. Delay during simulation: voice and video traffic.

For video traffic, we note that at the time of handover execution, the delay of packets transmission becomes important (between 0.8 and 1.43 s). The delay increases with the execution of the handover. This explains the occurrence of the peak at the starting moment of handover.

After executing the handover, the delay falls and becomes almost constant and less than 0.2 seconds.

VI. Proposed Approach to Improve Routing in WMN with MIH

A mobile node that implements MIH module includes two agents: MIH agent and routing agent. In wireless mesh networks, the routing agent used is HWMP or RA-OLSR. MIHF in the ad hoc node interacts with the MAC Layer and MIH users in higher layers.

Triggers for handoffs may be initiated from MAC, PHYSICAL or upper levels through the MAC SAP either at the Mobile node or at the BS [11]. The cause for these triggers can be either within the local stack or from the distant stack.

Layer 2 triggers are classified into two types, predictive and event triggers. Predictive triggers express a probability of a change in system properties in the future. Event triggers describe an exact event that has occurred. Link_Up is an example of an event trigger. Link-Going-Down is an example of a predictive trigger.

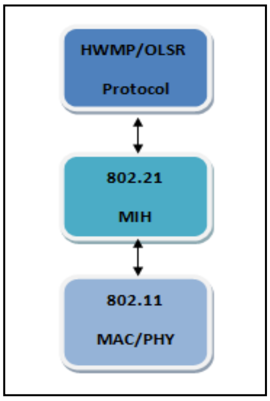


Figure 4. MIHF interaction to uper and lower layers.

The MAC layer receives measurement data of neighboring nodes and provides information to MIH. The MIH triggers the handover and HWMP/OLSR routing agent registers as a user and performs MIH stains triggered by the MIH agent.

For this, we propose to exploit the messages exchanged during the procedure of handover by the routing agent to detect the mobility of nodes faster and consequently routing can take place quickly.

We propose to use 2 messages to realize our approach:

- **MIH_Link_Down.indication** is sent to local MIHF users to notify them of a local event, or is the result of the receipt of a MIH_Link_Down indication message to indicate to the remote MIHF users who have subscribed to this remote event. Parameters used in this case are Type of link, MAC Address of mobile node, MAC Address of old Access Router and of course “Reason” for the link down.
- **MIH_Link_Up.indication** is sent to local MIHF users to notify them of a local event, or is the result of the receipt of a MIH_Link_Up indication message to notify remote MIHF users who have subscribed to this remote event. Parameters for this trigger are Type of link, MAC Address of mobile node, MAC Address of old Access Router, MAC Address of new Access Router, and Network Identifier for detecting possible change in subnet.

Figure 5 below illustrates the communication between the MIH agent and HWMP protocol.

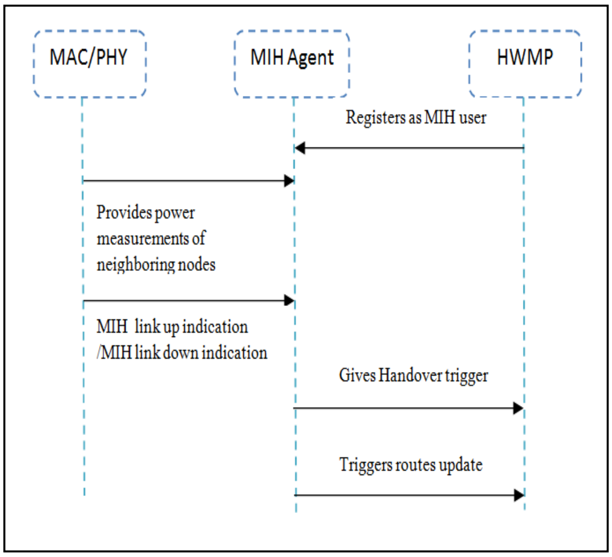

MAC/PHY
MIH Agent
HWMP
Registers as MIH user
Provides power measurements of neighboring nodes
MIH link up indication /MIH link down indication
Gives Handover trigger
Triggers routes update

Figure 5. Communication between HWMP and MIH agent.

At the beginning, we must register the routing protocol HWMP as an MIH user to receive messages issued by the MIHF. This can be implemented by providing an interface between the MIHF and HWMP agents in NS2 simulator, as in [16].

We will study two cases of mobility:

- A mobile node leaves a wireless mesh network to a foreign network.
- A new MN joins a wireless mesh network from another network.

We start by explaining the first case. As we have already indicated, when the received signal quality drops, the link layer of the terminal can anticipate the handover and triggers the event service Link_Going_Down on both MIH entities: MIHs terminal of the local mobile network and the MESH.

Then, the MIH agent informs the HWMP routing agent to update its routing table and remove the node corresponding to this link. A routing table’s update must be invoked at all nodes in the network. They must in turn remove the node associated with the message MIH_Link_Going_Down and do not wait for the periodic updating of routing tables. With this method, the node mobility is detected faster by all network users.

In the case when a mobile node tries to join a wireless mesh network while executing a handover and once all steps of link attachment are completed and the link is ready to send packets, a trigger event link-up indication may be sent to the MIH function on the local and remote link.

Once the MIH agent receives this message, it triggers the HWMP routing agent to update routes. The access point, then, triggers a links update throughout the network by broadcasting a PREQ message and putting the MN as destination. Thereafter, when an intermediary Mesh Point receives PREQ, it creates a path to the request source and forwards PREQ to the destination and so on until it reaches the mobile.

When the mobile node receives PREQ, it sends in unicast a PREP message to the source. When the source node receives the PREP message, it creates a path to the mobile node. This update will accelerate the detection of a new node that joins the network, which will therefore accelerate the data routing to that node.

VII. Discussion

Through the simulation of MIH protocol and according to our results, we note that the delay of a vertical handover can reach a maximum value of 1.43 s. To evaluate the performance of the this protocol, we can compare this value with that of a vertical handover without the MIH protocol like the case of [21], in which for streaming traffic between CDMA 2000 and IEEE 802.16e networks, handover delay can reach a value of 2 seconds. Concerning the packet loss ratio, in our scenario we have a maximum value of 3.2%. This value is lower than that of [21], which can reach 5%. We can conclude that the MIH provides a transaction from one network to another with a low delay and an acceptable packet loss ratio.

Our idea to accelerate routing data in WMN using messages exchanged during handover process may have positive and negative impacts.

When node movement is detected faster than before even by few seconds, it will accelerate data routing to the mobile node since the corresponding nodes will be informed of its new location and route data based on this new information. Consequently, Packets Loss Ratio will be reduced.

On another side, this route update needs a significant exchange of extra control messages, which can cause additional signaling overhead. It can also cause loss of energy of the mobile node.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we studied the mechanisms of vertical handover between WiMAX and WiFi networks by the implementation of protocols related to these mechanisms.

We defined a simulation scenario to implement this principle. Then we gave an analysis of vertical handover between WiFi and WiMAX and performance figures with the use of NS-2 simulator.

The objective of this work was to propose an approach that creates a link between the handover process and routing operation. Our main idea consists of using Media Independent Handover protocols in order to optimize routing in wireless mesh networks.

As a future work, we propose to simulate other scenarios. Indeed, we can illustrate the effect of the number of mobile nodes on the performance of vertical handover between WiMAX and WiFi. Other types of applications can also be simulated, such as a non-real time applications like FTP and best effort services (TELNET).

Another possible investigation may consist of evaluating the performance of MIH and other mobility protocols with other types of heterogeneous networks such as LTE, MPLS, etc.

Finally, it would also be interesting to run further simulations with our approach in order to further study its impact on routing in other mesh network scenarios.

References

[1] G. R. Hiertz, S. Max, E. WeiB, L. Berlemann, D. Denteneer, and S. Mangold, "Mesh Technology enabling Ubiquitous Wireless Networks," in Proceedings of the 2nd Annual International Wireless Internet Conference (WICON), Boston, USA, Aug. 2006, pp. 11-23.

[2] IEEE, “Draft amendment: ESS mesh networking”, IEEE P802.11s Draft1.00, November 2006.

[3] I.F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey”, Computer Networks, vol. 47, no. 4, Mar. 2005, pp. 445-487.

[4] IEEE 802.21, “IEEE 802.21 Media independent handover,” vol. 2006: IEEE 802.21 standards, http://ieee802.org/21/, 06.14.2013.

[5] M. Lee, R.Zhang, Ch.Zhu , and T.Park “Meshing wireless personal area networks: Introducing IEEE 802.15.5”, Communications Magazine, IEEE (Volume: 48, Issue: 1), January 2010, pp. 54–61.

[6] IEEE Std 802.16-2004, “IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Revision of 802.16-2001”, Oct 2004.

[7] “Mobile Ad-hoc Networks (MANET) Working Group,” Internet Engineering Task Force (IETF), http: //www.ietf.org/html.charters/manet-charter.html, 06.14.2013.

[8] M. Bahr, “Proposed Routing for IEEE 802.11s WLAN Mesh Networks”, The 2nd Annual International Wireless Internet Conference, Boston, ,2006, pp. 6-13.

[9] A. Amir Pirzada, M. Portmann, and J. Indulska. “Hybrid Mesh Ad-hoc On-demand Distance Vector Routing Protocol”, Proceeding ACSC '07 Proceedings of the thirtieth Australasian conference on Computer science-Volume 62, Australian Computer Society, Inc. Darlinghurst, Australia, 2007, pp. 49-58.

[10] P. Jacquet, P.Mühlethaler, A. Qayyum, A. Laouiti, T. Clausen, and L. Viennot, “Optimized Link State Routing Protocol”, IEEE INMIC Pakistan, Dec 2001, pp.62–68.

[11] Draft IEEE standards ,“IEEE802.21 Standard and Metropolitan Area Networks: Media Independent Handover Services”, Draft P802.21/D00.05, March 2006

[12] Q.B. Mussabbir, and W. Yao, “Optimized FMIPv6 handover using IEEE802.21 MIH Services”, Proc. of MobiArch 2006, ACM Press, New York , 2006, pp. 43–48.

[13] L Magagula, O.E. Falowo, and H.A. Cha. , “ PMIPv6 and MIH-enhanced PMIPv6 for mobility management in heterogeneous wireless networks.” Proceedings of Africon,Kenya, September 2009, pp. 23-25.

[14] Y.M. Chen, M.Y. Lai, S.C. Lin, S.C. Chang, and T.Y. Chung, “SCTP-based handoff based on MIH triggers information in campus networks”, The 8th International Conference of Advanced Communication Technology (ICACT’06), February 2006, pp. 1301-1305.

[15] K.N. Choong, V.S. Kesavan, S.L. Ng, F. de Carvalho, A.L.Y. Low and C. Maciocco, “SIP-based IEEE802.21 media independent handover - a BT Intel collaboration”, BT Technology Journal, vol. 25, no. 2, April 2007, pp. 219–230.

[16] J. Lee, A.McAuley and S.Das, “Framework for Integration of IEEE 802.21 MIH Function with Ad Hoc Routing Protocol”, Vehicular Technology Conference (VTC Spring) IEEE 73rd, Budapest-Hungary, 2011, pp. 1-6.

[17] N.R.Nomulwar, J. N. VarshaPriya, B. B. Meshram, and S. T. Shinghade, “Comparision of performance of routing protocol in Wireless Mesh Network”, The International Journal of Computer Science & Applications (TIJCSA), vol. 1, no. 3, May 2012, pp. 61-65.

[18] R. Baumann, O. Bondareva, S. Heimlicher, and M. May, “A Protocol for Macro Mobility and Multihoming Notification in Wireless Mesh Networks”, Advanced Information Networking and Applications Workshops (AINAW '07), 2007, pp. 34-37.

[19] Chen, Y., K. Kowalik, and M. Davis, “MeshScan: Fast and Efficient Handoff in IEEE802.11 Mesh Networks”, The 7th ACM International Symposium on Mobility Management and Wireless Access (MobiWAC 2009), Tenerife, Canary Islands, Spain, October 2009, pp. 105-108.

[20] The Network Simulator NS-2 NIST add-on IEEE 802.21 model, NIST January 2007.

[21] S. Park, S. Kim, J. Cho, I. Ryoo, D. Lee, J. Yu, J. Lim, and S. Oh, “A Performance Evaluation of Vertical Handoff Scheme between IEEE 802.16e and cdma2000 Networks”, Communications in Computing, Las Vegas, Nevada, USA, 2006, pp. 104-109.

Throughput Improvement of a Range-aware WiFi network by Minimizing Signal Interference

Jie Zhang HwaJong Kim GooYeon Lee Yong Lee
Dept. Computer Engineering
Kangwon National University,
ChunCheon, Korea
zarg_1982@hotmail.com hjkim3@gmail.com leegyeon@kangwon.ac.kr yleehyun@gmail.com

***Abstract*—In the smart-phone era, many WiFi devices around us need higher throughput and larger signal coverage which also generate unwanted signal interference among the devices. Signal interference is inevitable problem because of the broadcast nature of wireless transmissions. However, the interference could be minimized by reducing signal coverage of nearby wireless devices. But, smaller signal coverage means low transmission power and low data throughput. In the paper, we analyze the relationship among signal strength, coverage and interference of WiFi networks, and as a tradeoff between transmission power and data throughput, we propose a range-aware WiFi network scheme which controls transmission power according to locations and RSSI of WiFi devices. We analyze the efficiency of the proposed scheme by simulation.**

***Keywords-** signal interference; range-aware; data throughput; WiFi network,;signal coverage*

I. INTRODUCTION

Many WiFi networks have been introduced these days, and they usually need high power for larger transmit range and data throughput. However, with rapid increasing number of wireless devices such as smart phones, large signal coverage of WiFi causes high signal interference especially in densely populated area.

Signal interference is inevitable problem in wireless network, which may decrease throughput and cause security problems. The signal interference could be reduced by controlling network configuration. [1] and [2] suggested topology control method with changes transmission power in order to reduce signal interference in wireless ad-hoc network.

In WiFi networks, the interference can be managed by controlling the sender's transmission power. However, small signal power results in low throughput. There is a trade-off between signal interference and network throughput [5] [6]. In the paper, we analyze the relationship among signal transmission power, interference and network throughput. We propose a range-aware WiFi Network, which can adjust transmission power depending on the locations and Received Signal Strength Indication (RSSI) of the devices. We also showed the efficiency of the proposed scheme by simulations.

Section II is about interference problems in wireless network and related researches. In section III, we extract the relationship between signal strength, signal coverage and data throughput with experiments. Section IV proposes the Range-aware WiFi network and analyzes the efficiency with simulations. Conclusion followed.

II. RELATED WORK

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is IEEE 802.11 wireless protocol designed to avoid signal collision in local area network. CSMA/CA operates in the process:

1) Before sending data, listen the channel to be IDLE

2) When channel is IDLE, send a Request To Send (RTS) to the receiver, and wait for a Clear To Send (CTS). After receiving CTS, the sender starts transmission, and broadcast a NAV(Network Allocation Vector) message to its neighbors to announce the transmission activity.

3) After successful data receiving, the receiver sends an ACK (acknowledgement) to the sender.

Giuseppe Bianchi [3] analyzed the network performance of CSMA/CA, including network throughput with RTS/CTS handshake. Long distance communication with CSMA/CA suffers tough signal interference due to many interfering devices in between the sender and receiver.

Signal interference deteriorates network throughput and also wastes power. Reducing signal interference is widely researched in wireless ad-hoc network in order to minimize power consumption. Martin Burkhart et al. compared several topology control methods which claim to resolve interference, and proposed an interference-minimal method in wireless ad-hoc network with connectivity-preserving and spanner construction [1]. N. M. Karagiorgas introduced a multicost routing that constructs route with variable transmission power to reduce interference in ad-hoc network [2]. Sutep Tongngam [4] proposed a reducible transmission range approach for wireless network, which optimizes broadcasting latency. Ilenia Tinnirello and Giuseppe Bianchi analyzed the interference effects in WiFi networks [5].

Anand Kashyap et al. presented a passive monitoring of wireless traffic to estimate interference in WiFi networks [6].

Above researches show that in any of wireless network like ad-hoc network or broadcasting network, performance in data throughput takes high influence from signal interference. Wireless interference cannot be removed because of broadcasting properties but can be optimized by routing algorithms or topology control algorithms.

III. WIFI SIGNAL STRENGTH AND TRANSMISSION RATE

A. *Signal strength and data transmission rate*

The IEEE 802.11 WiFi network is composed of Basic Station Set (BSS), which contains an Access Point (AP) as a relay station to the Internet for the wireless local area network (see Figure 1).

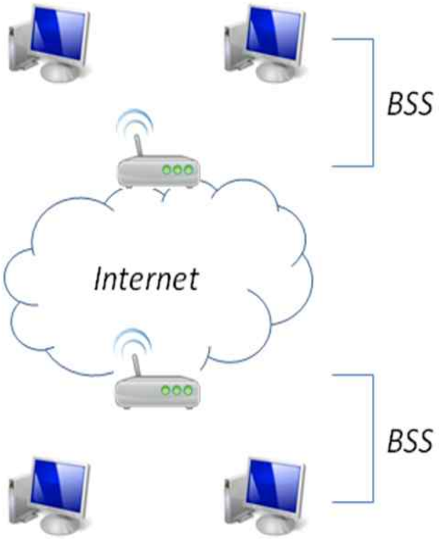


Figure 1. A WiFi network is composed of BSS (Basic Station Set), which contains AP(Access Point) and wireless devices

The most widely used scheme for a WiFi station to choose the appropriate AP is measuring the received signal strength from AP, known as RSSI. However, many researches showed that AP selection scheme based on the RSSI does not show good efficiency in optimizing throughput [7-9]. This is because the wireless communication quality depends on signal interference, fading and many other effect besides the signal strength itself. In the paper, we first simulate an interference-free environment and measure data throughput with different signal strength to find out the relationship between RSSI level and network throughput. Then, we extend the experiment with various signal interferences.

B. *Throughput under interference-free conditions*

Table 1 shows the specifications of the wireless device we used in the experiment to measure the RSSI and throughput under interference-free conditions.

TABLE I. EXPERIMENT DEVICE PARAMETERS USED TO MEASURE THE RSSI AND THROUGHPUT

Wireless protocol	802.11g
Transmission power(AP)	18dBm
Antenna gain(AP)	4dBi
Receive sensitivity	-74dBm
Maximum signal range	70m
Maximum throughput	54Mbps

We measured the upload and download throughput for every 5dBm of RSSI from -35dBm to -70dBm, and the result is shown in Figure 2.

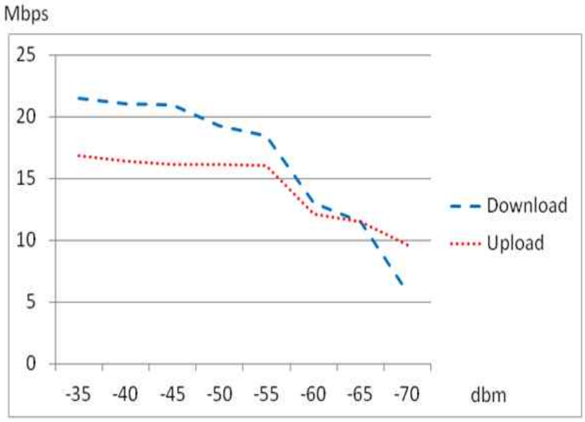


Figure 2. Throughput in a WiFi network without signal interference as a function of RSSI

Maximum bandwidth of the WiFi channel was 54Mbps, as a common throughput of WiFi network in 2.4GHz, however, the actual maximum throughput was 20Mbps because of the protocol overhead, such as control traffic and Ack frames etc.

C. *Signal transmission range and throughput*

In order to analyze interference effects in wireless network, we estimate the number of active WiFi networks in the signal range and evaluate the average throughput. Signal range is expressed by the path loss model as [10].

$$PL = PL_{1Meter} + 10\log(d^n) + s \quad (1)$$

$$RSSI = TxPower + AntennaGain - PL \quad (2)$$

Variables used in the formula are:

- PL: Total path loss experienced between the receiver and sender in dB
- PL_{1Meter}: Reference path loss in dB for the desired frequency when the receiver- to-transmitter distance is 1 meter
- d: Distance between the transmitter and receiver in meters
- n: Path loss exponent for the environment, 2 in free space, 3.5 – 4.5 in indoor environment

- s: Standard deviation associated with the degree of shadow fading in dB (3 ~ 7 dB)

From (1) and (2), signal distance between transmitter and receiver is given by

$$d = 10^{(TxPower + AntennaGain - RSSI - PL1Meter - s)/10n} \qquad (3)$$

Signal distance between AP and client devices obtained from the experiment of Section 3.2 and (3) is shown in Table 2. Distance and throughput is measured in each RSSI levels.

TABLE II. NETWORK THROUGHPUT AND SIGNAL TRANSMISSION DISTANCE FOR DIFFERENT RSSI VALUES

RSSI	Distance	Throughput (Downlink)
-35dB	1 m	21.49Mbps
-40dB	1.778279m	21.03Mbp
-45dB	3.162278m	20.94Mbp
-50dB	5.623413m	19.25Mbp
-55dB	10m	18.42Mbp
-60dB	17.78279m	13.04Mbp
-65dB	31.62278m	11.47Mbp
-70dB	56.23413m	5.79Mbp

In (1), PL_{1Meter} is set to be 54dB, path loss exponent n is 2 assuming free space, and shadow fading s is 3dB.

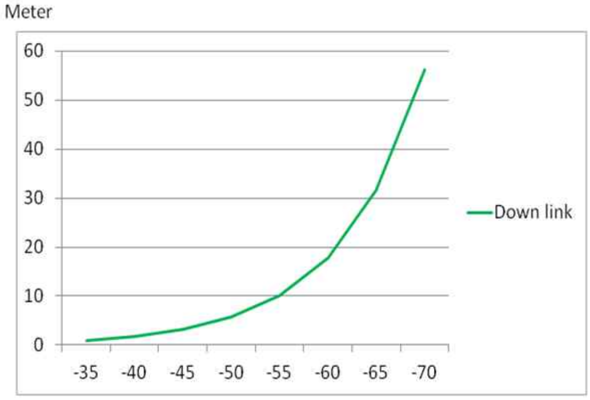


Figure 3. Signal transmission coverage for various RSSI values

Figure 3 shows the signal range variations for various RSSI levels, which may explain the relationship between distance of wireless nodes and related signal degrees.

IV. RANGE-AWARE WIRELESS WIFI NETWORK

High transmission power gives high signal interference. Low transmission power may increase throughput because of low interference, but small signal power would make shadow areas. We proposed a range-aware WiFi network in order to find optimum value of transmission power and signal interference. Figure 4 shows an instance of the proposed network scheme where APs have different signal coverage in order to minimize signal interference.

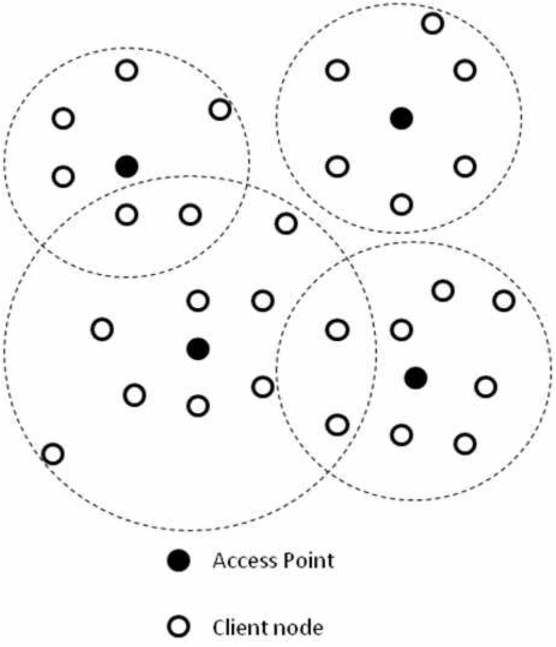


Figure 4. An example of range-aware wireless WiFi networks where APs have different signal coverage in order to minimize signal interference

The range-aware WiFi network can increase network efficiency by minimizing signal interference. The rationale of the range-aware wireless WiFi networks is controlling AP’s transmission power considering the locations of the wireless devices. There are three steps in configuring a range-aware WiFi Network.

1) Measuring clients’ RSSI periodically, calculate distances to the devices

2) Set AP's transmission power to reach the farthest client device

3) Announce the transmission power set at 2) to client devices

Clients’ transmission power control is set based on AP's transmission power. When client moves, the transmission power of AP and client are adjusted (see Figure 5).

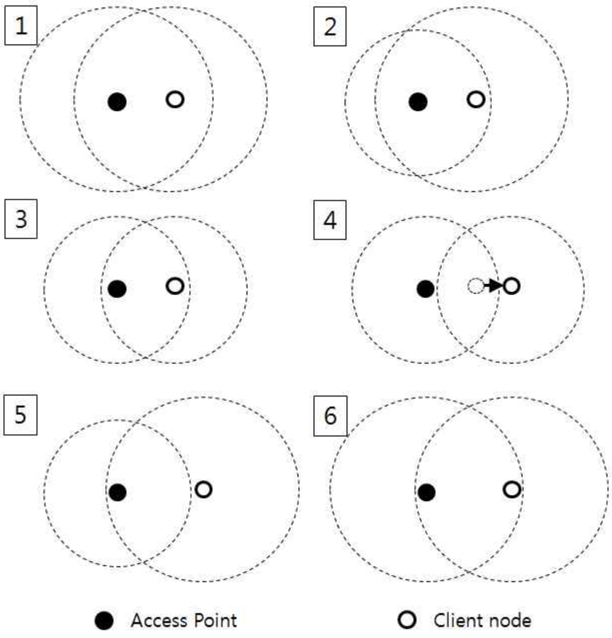


Figure 5. Transmission coverage changes as a client wireless device moves

The steps in Figure 5 are described as follows.

1) *Initial state of AP and client device*

2) *AP sets signal coverage considering clients' location, transmission power and announce it*

3) *Client device sets transmission power based on the announced AP's transmission power*

4) *The client device moves away from its AP*

5) *Client device uses default transmission power*

6) *AP recalculates distance between client and adjusts signal coverage*

We performed simulations to investigate the proposed method. Simulation topology is illustrated in Figure 6. A 120m x 120m area is divided into 9 cells, each cell contains one AP at the center and 6 randomly located devices. Network throughput for downlink (from AP to clients) is measured for different transmission powers of 18dBm, 13dBm and 8dBm. In the simulation, we assumed all clients use same channel and channel access time is equally shared by all client devices no matter how the actual throughput is. The simulation program is written by Java language, UDP unicast is used with maximum throughput of 54Mbps.

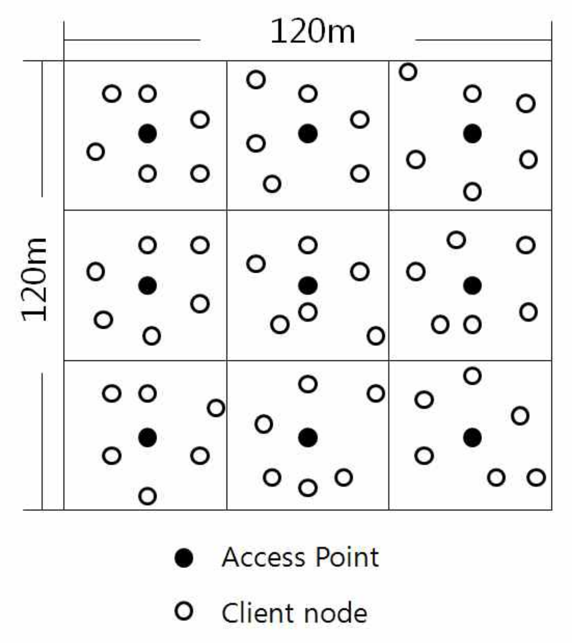


Figure 6. Simulation topology with 9 cells and 54 devices

First, we considered a conventional WiFi network without range-aware WiFi scheme. Figure 7 shows the simulation result with 18dBm (high) transmission power. All client devices show similar network throughput, however the throughput is quite low because of the high signal interference. Figure 8 shows the case with transmission power of 8dBm, where the network throughput is much higher than the case of Figure 7 (i.e., 18dBm) because of low signal interference. However, in this case, the AP's signal coverage is not long enough to cover all clients in the network that may cause shadow zone.

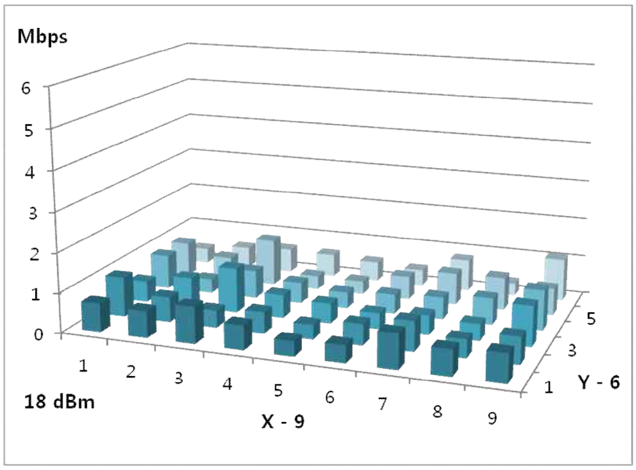


Figure 7. Throughputs at randomly located 54 clients with 18dBm transmission power

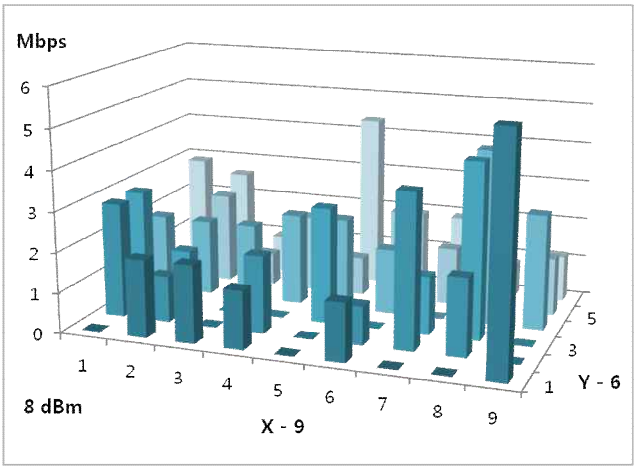


Figure 8. Throughputs at randomly located 54 clients with 8dBm transmission power

Figure 9 shows the simulation result of the proposed range-aware WiFi network. AP's transmission power is adjusted depending on the clients' location to be 18dBm, 13dBm and 8dBm, respectively. As shown in Figure 9, shadow zone does not exist and network throughput is much better than that of Figures 7 and 8. By choosing optimum transmission power associated with client's distance, we can minimize signal interference and maximize network throughput.

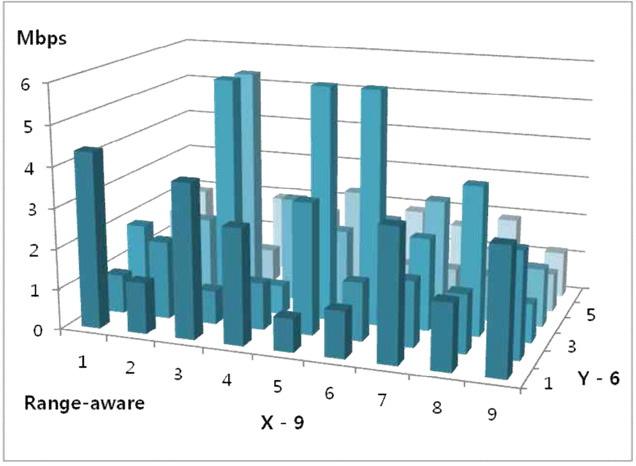


Figure 9. Throughputs at randomly located 54 clients with range-aware WiFi network scheme

Table III compares average network throughput of conventional WiFi network and range-aware WiFi network with transmission power 8dBm, 13dBm and 18dBm. It also compares the cases with 6 client devices in every cell (6x9 clients) and 9 client devices in every cell (9x9 clients).

TABLE III. AVERAGE THROUGHPUT(MBPS) COMPARISON OF A RANGE-WARE AND CONVENTIONAL WIFI NETWORK

	Range-Aware	8dBm	13dBm	18dBm
6 x 6	2.09	1.58	1.09	0.64
9 x 9	1.30	1.07	0.78	0.42

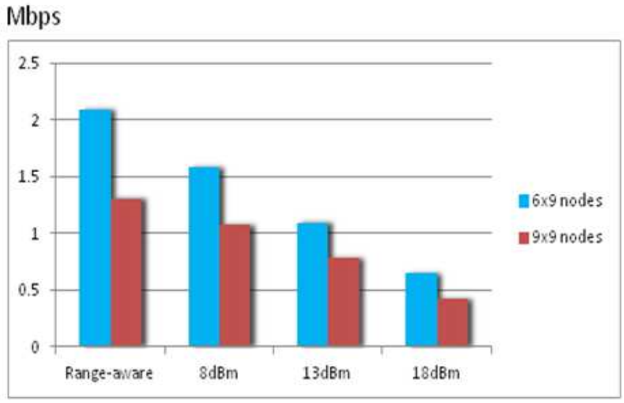


Figure 10. Average throughput comparison of a range-ware and conventional WiFi network (with different transmission powers)

Figure 10 shows that the proposed range-aware WiFi network gives much higher throughput from clients than conventional WiFi network. Throughput with the case of 9 client devices in each cell shows lower throughput than the case of 6 client devices in a cell, because 9 clients in a cell will use small amount of bandwidth than 6 clients in average.

In [7], Yutaka Fukuda et al. presented an AP selection scheme based on measurement of signal interference and showed a throughput improvement of 100% around. Controlling client to reach interference-minimum AP might improve certain node's throughput however should show few efficiency in improving whole network performance; the scheme should show similar result of Figure 9 with our simulation model. Today's WiFi environment has a very high density of wireless client due to rapid increase of WiFi devices, typically Smartphones. The most efficient way to optimize WiFi network should be controlling network topology, proposed Range-aware WiFi network presents one example.

V. CONCLUSION

Performance of a WiFi network does not only depend on signal strength but also on the interference from neighbor wireless devices. Higher transmission power from AP gives higher signal interference to other WiFi network. On other hand, if transmission power is too small it can reduce signal interference but may cause shadow zones where client devices could not connect to the network.

In the paper, we analyze the relationship between signal power, signal interference, and network throughput. We proposed a range-aware WiFi network that may increase network efficiency by minimizing signal interference with controlled transmission power. Simulation results show that the range-aware WiFi network gives higher network throughput than conventional WiFi network.

ACKNOWLEDGMENT

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the C-ITRC(Convergence Information Technology Research Center) support program (NIPA-2013-H0401-13-1002) supervised by the NIPA(National IT Industry Promotion Agency) and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(No. NRF-2011-0013951).

REFERENCES

[1] Martin Burkhart, Pascal von Rickenbach, Roger Wattenhofer, and Aaron Zollinger, “Does topology control reduce interference?”, Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing, 2004, pp.9-19

[2] Karagiorgas, N.M., Kokkinos, P.C., Papageorgiou, C.A., and Varvarigos, E.A, “Multicost Routing in Wireless AD-HOC Networks with Variable Transmission Power”, Personal, Indoor and Mobile Radio Communications, IEEE 18th International Symposium, 2007, pp. 1 – 5

[3] Giuseppe Bianchi, “Performance analysis of the IEEE 802.11 Distributed Coordination Function”, Selected Areas in Communications, Vol. 18, 2000, pp. 535 – 547

[4] Sutep Tongngam, “A Reducible Transmission Range Approach for Interference-Aware Broadcasting in Wireless Networks”, International Conference on Future Information Technology, 2011, pp. 144 – 148

[5] Tinnirello, I. and Bianchi, G., “Interference Estimation in IEEE 802.11 Networks”, Control Systems, vol. 30, 2010, pp. 30-43,

[6] Anand Kashyap, Utpal Paul, and Samir R. Das, “Deconstructing Interference Relations in WiFi Networks”, Sensor Mesh and Ad Hoc Communications and Networks, 7th Annual IEEE Communications Society Conference, 2010, pp. 1 – 9

[7] Yutaka Fukuda, Masanori Honjo, and Yuji Oie, “Development of Access Point Selection Architecture with Avoiding Interference For WLANs”, Personal, Indoor and Mobile Radio Communications, IEEE 17th International Symposium, 2006, pp.1-5

[8] Heeyoung Lee, Seongkwan Kim, Okhwan Lee, Sunghyun Choi, and Sung-Ju Lee, “Available Bandwidth-Based Association in IEEE 802.11 Wireless LANs”, Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems, 2008, pp.132-139

[9] Daniel Wu, Petar Djukic, and Prasant Mohapatra, “Determining 802.11 Link Quality with Passive Measurements”, Wireless Communication Systems, IEEE International Symposium, 2008, pp. 728 – 732

[10] Cisco, “WiFi Location-Based Services 4.1 Design Guide - Location Tracking Approaches”, 2008

XMPP Distributed Topology as a Potential Solution for Fog Computing

Jonathan Bar-Magen Numhauser, Jose Antonio Gutierrez de Mesa
Department of Computer Science
University of Alcala
Alcala de Henares, Spain
e-mail: {jonathan.bar-magen, jantonio.gutierrez}@uah.es

***Abstract*—Fog Computing is potentially harmful towards existing Cloud Computing systems as well as Big Data structures. Lack of privacy and potentially unauthorized content distribution are some of many issues to solve. As a possible solution, we propose in the following paper the definition of a new Network Topology as well as a working methodology to reduce its impact. It serves as an introduction to our investigation line and for future works that aim to solve the effect of the Fog Computing.**

Keywords-Fog Computing; topology; network; Big Data; XMPP.

I. INTRODUCTION

Our previous studies into Fog Computing [1][2] were basically introductory; being such an innovative subject devised by our research team, we defined its identity, and eventually obtained a structure that established what Fog Computing is, as well as its implications on Big Data structures. In this paper, we are following the established research steps, and present later the second part of the research process, which is equivalent to the first technical phase of the research guideline.

Fog Computing can be perceived both in large Cloud systems and Big Data structures, making reference to the growing difficulties in accessing objectively to information. These results in a lack of quality of the obtained content and, in some cases, even it's dumping. The effects of Fog Computing on Cloud Computing and Big Data systems may vary; yet, a common aspect that can be extracted are the limitations in accurate content distribution, an issue that for long has been tackled with the creation of metrics that attempt to improve such [9].

The influence of a variety of entities in the cloud/big data market impacts the magnitude of Fog Computing [6], as described by Agrawal et al. [4]. For this study, we supposed a network structure of Cloud or Big Data where we may find and advanced stage for Fog Computing. To bring a solution to such advanced stage, we are about to propose a number of methods, which were later tested. These results are examined for optimization and future research steps, as well as feedback for collaborative methodologies [1]. The first section of this paper will expose the necessary requirements needed for Fog Computing to appear in Cloud Computing and Big Data. It will be followed by a description of the evolution of Fog Computing in such structures. Once we establish the necessary requirements for a Big Data structure affected by Fog, this paper will explain the first steps taken to find a solution to such a situation, and show the development steps taken to find possible alternatives to solve the existence of Fog.

This paper will start by describing how Fog Computing manifests itself in Big Data structures; it will be followed by the analysis of algorithms to manage information systems. In the Methodology and Technological Background sections that follow, a study of the methods to use in the research work as well as the technological necessities will be treated. Once established the background variables, in the Investigation process section, the steps taken in the overall research work will be described to details.

After the research section, the Development section will establish the development process that took part in our work. Finally, the conclusion section will summarize all the work that took place in this project phase.

It is imperative to highlight that this is the first phase of a three-phase research process that will culminate in a complete empiric result analysis, which implies that in the early phases no more than topological and structural results will be exposed.

II. FOG COMPUTING IN BIG DATA

Big Data structures in the last few years have been acquiring a central role [5]. As the following evolution step of Cloud Computing, before entering into it, this evolution has to take place with a number of precautions to ensure that the Fog do not pass towards the Big Data structures [3].

Cloud Computing and Big Data function on the topology of third party storage information [4]. This structure advocates that each node of the network relies its information on a centralized data bank and allows the powerful core mainframes to process such information and obtain richer results. In case of Cloud Computing, the second part with regard to processing is not as evolved as in Big Data, in which the core calculations are a fundamental part of the system [5].

When creating these types of data structures, we have to consider the following issues: Relying the impact of size and memory in the mainframe, and Hardware costs that requires an effective and optimized algorithm to manage such information.

The research lines of semantic and indexation are having a major importance in many universities and laboratories,

ISBN: 978-1-61208-299-8

aiming at obtaining better search algorithms and reduce the impact of size and memory in the mainframe. This field of study is of such importance that most of the largest technological entities have independent research departments only to find new and improved search methods.

The need to find such solutions is intertwined with the constant change in the global network topology. The information-based structure is pushing towards studies to dedicate an increasing amount of time and energy in finding metrics and algorithms to improve search engines, and by default the management of information [7].

It is this increase of information structures that we consider is the trigger to the Fog Computing, and so the establishment of our research line [2]. Cloud Computing and Big Data implies a significant amount of information management, information that can be easily manipulated and filtered as it was proven in our previous introductory paper[2]. Fog Computing is the situation in which mass information structures loose control of the attempted impartial nature of information search. If we search for information of type “A”, a system affected by Fog Computing may intentionally or unintentionally filter the resulting information, which will have the effect of a limited visual spectrum for the user.

The causes of this manipulation can be either intentional or non intentional, as a result of the evolution of algorithms and their attempts to achieve perfection in result accuracy.

Fog Computing can be instigated by a number of external variables, those variable that covers numerous fields including security, commerce and politics, all of which have the same objective: the filtering or obscurity of information of type “A” behind information of type “B”.

These requirements can be found in most existing Cloud and Big Data networks, commercial and political in search engine information as seen in Bar-Magen [2]. From search engines, like Google Search, and Bing to profile-based networks, like Facebook or Twitter, Fog Computing can be found in each, represented by sponsored manipulated results, lack of user privacy and remote manipulation of sensitive data.

F Fog Computing has to be considered at the moment of designing a Big Data system; in the following sessions, we will expose a possible solution based in topological structure to reduce the impact of Fog in the network systems. It is important to state that Fog Computing cannot be totally solved, but we work to reduce its impact as much as possible.

III. Algorithms and Information Management

A. Algorithms for result optimization

Before heading on to the topology analysis and how to use it to solve Fog Computing, we would like to state a number of issues regarding the situation of present algorithms to manage information.

Algorithms to manage information are being devised constantly to improve the visualization of information. The evolution of these algorithms aims to optimize search results on regional and profile learning interests. These algorithms make use of a complex profile map, based on user interests, of the user who searches for such information [6]. The evolution of those algorithms aim to increase the search spectrum to use linked profiles of users related to the alpha user, which today attempts to use the power of profiled networks, like Facebook, and search engines, like Bing. The combination of these two tools attempt to keep optimizing the information management algorithms.

The overall objective of information management algorithms is to achieve a precise result and adapt it to the user’s instant necessities. By now, as a result of our previous studies, we obtained that such attempts to improve search algorithms result in the increment of Fog Computing in the information networks [2]. Many of the current top content management entities use such algorithms to stay at the highest position in search results success hits, pushing forward the algorithm evolution. Yet, this evolution ends up in the unconscious filtering of a larger amount of information, prioritizing one type of information over the other.

B. Information management and increase revenue

Information management had a main role in advanced civilizations and its motives are so vast that it merits a study of its own. In our case, the use of several algorithms in information management allows the benefit of several entities above others [8]. Those algorithms are mold to deal with the specific variables; the variables are, in general, established by entities that benefit from information management engines, which eventually render them partial and biased.

As a result of such partiality, we decided to approach the definition of a topological structure for network components, and once the structure is established define a new brand of algorithms that will manage the new network structure. Some of those resulting algorithms that will be exposed in the following sections are based on standardized XMPP/XEP XML protocols as well as localized environmental frameworks; for example, the iOS XMPPFramework created by Hanson [19].

The information management in a new topology will result in a different concept of data distribution and control. The most significant difference will be noticed in the content distribution and recollection, reducing the centralized management of such. This may be noticed in the choice of hardware for our project, being strongly based on mobile devices, and considering the dynamic characteristic of those devices, a swarm based structural functionality may be adopted imitating Swarm-Computing structures, which will imply the creation of a mobility-swarm based architecture [17]. We have chosen such distribution because it will allow us to establish a decentralized smart based peer to peer network in which each node will form part of a complete swarm structure. New content storage and distribution will allow an alternative option to achieve an impartial content exposure, and reduce substantially the Fog in many actual centralized network structures.

IV. Methodology Choice

The following step will be to establish the methodology to use in the following research work. To accurately predict the future steps of our work process, it is imperative that an appropriate methodology be chosen. Looking at our previous investigation into collaborative methodologies [1], that contemplated the creation of standardized rules for correct functionality in collaborative work, and alternatively analyze the results of our research in Native Based Development that included the definition of working steps to follow facing a project that spreads a large spectrum of technological environments, we concluded that a combined working technique of both fields is needed for our current project.

Collaborative Methodology requires the participation of a number of entities at the development phase of a project, and so we were able to obtain the collaboration of at least a couple of entities to work on this development. A second issue in Collaborative Methodology work is the dependency on collaborative tools, and the way to manage them in the course of the project development. The tools are related to the agile nature of this methodology, translated to the creation of a number of roles dedicated to the completion of certain objectives.

For this project, we adopted a Collaborative Methodology because we are also familiar with its workflow and phases allowing us to easily adapt the objectives of our software and hardware development.

As a result of the technical specification, it will be necessary to develop on each device, natively the intelligence necessary to manage the content transaction between each device. Combining it with Collaborative Methodology it will substantially reduce the work load, ensuring the coordination and synchronization of each member and each component being developed.

The resulting endeavor was influenced by the chosen methodology and allowed us to achieve a number of results that were not initially expected in the hypothesis.

V. Technological Background

Defining the correct background variables for our research process will help defining the basic development necessities to comply with our objectives. Peer-to-peer, Swarm Computing and privacy and security measures will be some of the issues that were studied as a background analysis.

A. Peer-to-Peer Concept

The studies on peer-to-peer have been numerous in the last years [14][15][16]. In our work we decided to make use of this network structure to attempt a possible by pass of centralized information flow, and so, create a new data structure for transactions that may permit the establishment of a standardized information distribution. This new data structure will be strongly based on peer-to-peer topological distribution used for our practice XMPP/Jabber system.

This new information distribution standard will be part of the main study to solve Fog. What we aim to describe in this section is that the concept of peer-to-peer information transaction has been adopted as an initial background requirement to solve the issue at hand.

Peer-to-peer network structures can be widely seen in a number of file transaction systems, as well as communication clients, in particular, based on either Adobe Cirrus multimedia server, or, in our case, the XMPP Jabber server [14].

XMPP server supports partial peer-to-peer connection in the messaging method, and full peer-to-peer transactions with the use of the Jingle extension [18]. With the available channels for distribution of information, we will be able to establish a main working method to follow in the research process.

B. Swarm Computing

As established in a number of places in the previous section, the adoption of Swarm Computing development rules will allow us to emulate a Swarm Computing behavior in the overall peer-to-peer system that will act as the solution to the Fog Computing issue.

Swarm Computing [17] refers to the technological field of independent processing modules coordinating to offer unified and larger information in a certain spectrum. Swarm Computing is strongly linked to the described in the previous point, for our research peer-to-peer and Swarm Computing refers to the same network structure. Depending on its use, the network structure can be more or less dependent on a centralized source.

In our study case, we opt to define the structure as mostly decentralized, offering the minimum required common points for successful communication establishment. An analysis of Swarm Computing on the propagation of Fog Computing and its synchronization with the rest of the background variables will follow.

C. Privacy and Security

Privacy and security of the shared data is a serious issue to be concerned with regarding Big Data structures. At the present, high security risks that can be found in common Big Data and Cloud Computing structures drive users to lower their trust levels in those systems, thus reducing the efficiency of Big Data systems.

Big Data thrives on the possible combination of information with the purpose of obtaining new and more optimal content. A great example is disease spreading, that with an efficient Big Data structure, can be better controlled and offer better solutions.

When we regard the issue of security and privacy in Big Data, we should always consider two main sources of difficulties, either the information exploits by the central system, which is the existence of an impartial and abusive central administration, or exploits driven by individual attackers, which can result in the trafficking of information by third parties.

Both issues form part of Fog Computing, and that is why we are driven in our research to find a trusted solution to these problems.

We believe that through the establishment of a new network structure, as well as the use of a number of studied technologies, we may be able to increase the security and privacy of members in a Big Data structure, and so reduce the impact of the Fog Computing in the system.

VI. Research Process

To initiate the first phase of our research, once defined the background variables, we proceeded with the establishment of the network structure that will form the new communication systems.

We seek to achieve a new method of communication and information distribution that may emulate a Big Data or Cloud Computing structure and offer a counter solution incase of a centralized structure affected by Fog Computing. Fogs in large information structures are the main issue to solve, and we started by defining a peer-to-peer based Swarm Computing topological system.

The system will require the functionality of XMPP/Jabber server to allow a centralized address access, serving as a directory for the members of the Big Data structure to communicate. To solve the massive information filtering systems, we studied the importance of background interaction of services with the technological environment. Each member of the swarm will be considered as a component from now on, with an associated entity id.

A. Component's background services

In our project we defined that each component of the swarm should contain a minimum number of services to function autonomously, considering it as part of its intelligence. This behavior will be achieved by using appropriate hardware and software characteristics. The basic hardware/software will be an operating system with I/O capabilities and network connection. In this specific test case we made use of an iOS device, and we categorized it as a component in the swarm.

Background services are what allowed components of the swarm to react to environmental changes, defining the importance of these services, that without them all the theory of our topological structure will fail. In the first phase, we opted to develop simple software to simulate the swarm activity in a component, and see the behavior of such component on a macro scale.

Those services will constantly communicate with other services in other components, and so complete the swarm behavior. It is through those services that we will achieve a complex Big Data counterpart to the traditional centralized structure.

B. Native-Based Development for Components

Even though we used for this sample case an iOS based environment, we should consider the importance of a native based development in our research process. Each component will be developed according to its environmental variables, on a software level. These native environments will cover iOS, Android, or AS3 in case of a PC device.

Their common denominator will be the communication protocol, which will be the Jingle XMPP protocol. Their communication will pass through a common server that will route the connection between two or more members of the swarm. That is why the use of a proper native development methodology is essential for a successful result.

C. Component's Characteristics.

If we consider each component to have enough autonomy to send and receive information, as well as to store it, we will notice the a creation of a peer-to-peer structure that at the same time also simulates a distributed network system and a Big Data structure.

By increasing the amount of sensors and interaction abilities of the components with its environment, we are successfully creating a richer swarm and an optimal information distribution algorithm. The importance of one type of information in regard to another will be defined not by centralized entities algorithms or interests, but by the same components that form the swarm.

The propagation of information in the swarm will exclusively depend on the components that form part of the swarm. If we compare it with the existing content distribution systems that make use of components as extremities instead of independent members of a swarm, we will notice that the need to route by content packages through a centralized device will result in a non arbitrary control of the obtained content, which will eventually increase the Fog in the system.

D. Lighthouse concept

In our new structure, we attempt to define each component in the swarm as independent enough to behave as a lighthouse in regard to information distribution. Components will store information, and propagate it as long as it will see fit, depending on the surrounding swarm members. Such is the dependency that eventually there may be a case in which information will not transcend more than one component or node.

This structure increases the efficiency of security and privacy of user information in the overall network, allowing him or her to freely hide and delete information from the general swarm. The lighthouse effect in the swarm structure will be the core solution for Fog Computing, allowing the component to decide either autonomously or by manual intervention what information should or should not be propagated.

This will instigate the need to establish new content treatment algorithms, and so we will introduce an initial phase for content manipulation in the swarm.

E. Content mangement in the swarm

Algorithms to manage content are vast in present systems, yet if we pretend to create a secure and private content control structure, as well as a trusted and optimized access to content, it is essential to establish a structure that will permit the evolution of content management and its algorithms.

Such changes should be open for either autonomous improvement as well as manual intervention. And it will have to contemplate the possible random improvement of information management algorithms. All this requisites will be treated towards the second phase of our study. Nonetheless we will establish a basic communication standard, on the foundation of XMPP XEP extensions, as well as the creation of new extensions [15]. The algorithms will be improved with time and increase in efficiency as the project advances. It will also contemplate the use of smart components as well as intermediate nodes that will allow a better flow of the content, but not its manipulation, so we can avoid a possible appearance of Fog in the system.

The increase in components complexity can either increase the efficiency of the structure or decrease it, depending on the algorithmic methods that are being followed.

F. *The Work Process*

Once we obtained all the pre requisites from our investigation into peer-to-peer, Swarm Computing, content management algorithms and XMPP servers, we proceeded with the creation of our first swarm based network, and analyze the possible existence of variables that may result in the appearance of Fog Computing.

VII. Development Process

At first we devised a network structure that will comply with the aspects described in the previous sections. The use of complex swarm components will suppose on one hand a higher cost in development, but on the other hand it may result in a greater source of information resulting from the created algorithms.

Initially we implemented a simple communication program that will use the network structure to simulate a peer-to-peer communication. The adaptation of XMPP libraries to the development environments was a costly process, but once it was completed, the propagation of the same enterprise to different native environments was successfully optimized.

The creation of custom extensions required a previous study of the limitation that XMPP structures have, in particular de XEP protocols, and how they restrict the exchange of content. The extensions required to be registered on a public domain. XMPP uses XML language structure, which also needed the preparation of modules to interpret those extensions in each network component or device.

Once established the peer-to-peer communication structure, we run some tests on the overall process of content transaction obtaining favorable results in regard to latency and bidirectional interaction. The bidirectional communication resulted in a fast and almost instantaneous interaction, having used in our case components existing in the Madrid surrounding area with a small component number of 20. Later on we passed the test components to a larger distance, from Latin America to Europe, resulting in favorable and low latency results. An average instantaneous message inside the Madrid area took 35ms to be received from source to destination. On the other hand, a message from Spain to Brazil took longer but not on a level out of our prediction: 125ms.

On pure peer-to-peer communication through Jingle node, latency was calculated using Wireshark package reader, receiving a number of interesting results. Latency inside the Madrid area was under 50ms, while latency between Madrid and Sao Paulo was around 230ms.

The following step was to improve the communication tools, and allow a higher quality of content exchange. Implementing a Jingle extension could do this. For this process we made use of a variety of sources, which in their core ended up resulting in the use of the Jingle Library supported by the Google Development Group.

This library created in C, is easily adapted to a variety of environments allowing a smoother process of integration in our swarm components. The result was favorable, and we were able to transmit audio content from one component to another using the peer-to-peer communication structure. Latency results on this case depended on a number of variables, including the unified size of the byte stream being sent, but in an overall analysis we obtained that the connection speed between the two nodes was favorable as well.

On regard to the internal behavior of the components, we established a number of methods to store relevant information. Initially we allowed the user to define if the swarm component will be a storage node and a propagator, or only a propagator. The difference will be noticed on the level of priority the component will have, where the storage nodes are of higher security priority. Storage nodes not only send their information, but also store the information for future distribution, and in case of deletion, if such information is not replicated in another storage node marked as origin, it will be completely removed from the system.

The available table management environment in the mobile devices, through the use of SQL structures, allowed the creation of an improved communication flow. By having a strong intelligence base, each node of the swarm can work as storage and propagator, as well as contain a variety of complex algorithms.

The final step of our first research phase was the creation of a unified extension to communicate between swarm components, and as a result analyze the frequency in which background services used to exploit these extensions. We noticed that some simple commands could be avoided from being used through Jingle extensions. Jingle uses an open socket channel between two nodes, and such channels may require a greater management level from the components software, which will result in higher complexity. Push commands could be passed by a normal extension and an IQ or Message type, which resulted in a cleaner and less dependent communication.

Information requests could also be executed through push requests instead of Jingle, but the greatest inconvenient will be in the limitation of content transaction and content size.

The background services that were implemented, in this case normal message reception as well as automatic light level management, worked according to our expectations. Later on we also incorporated the detection of the components movement based on the accelerometer. All those sensors sent information to the components that requested it, and even in some cases activated other components on the execution of a certain event, imitating the behavior of a smart swarm system.

The best example was the execution of an alert on the main control panel in the PC version of the program when the device fell from a high altitude. Thus it confirms the possible interaction of swarm elements, and the potential improvements for more complex content exchange algorithms.

VIII. Conclusion

For this research project we established a number of objectives to achieve. The first was to obtain the necessary requirements to identify a big data structure affected by Fog Computing. This was detailed in the first sections of this paper. The following goal was to obtain a study of the appropriate methodologies for the development of this project and the creation of this new content structure [2].

When we look into the topological study of a network structure, inflicted by Fog Computing, we have to consider privacy, security, and scalability and efficiency issues. These were our considerations when we approached the second step of our project. Basing on our experience from previous studies we concluded that opting to use a Collaborative Methodology, and a native based development workflow, would be the best choice confronting the existence of a swarm peer-to-peer network structure.

We should point that those methodologies will be composed of agile elements such as SCRUM amongst others. When we proceeded to the practical phase, we encountered the need to establish the technological pre requisites, as well as the overall structure that our network should be based on, as is shown by the compared network structures in Figure 1. From this study we devised the use of a swarm structure, and its combination with a decentralized peer-to-peer communication standard [16].

As part of our study we also decided to use XMPP protocol to achieve a true peer-to-peer communication structure, and also the use of smart components that will are parts of the swarm network [18].

The development ended up in the creation of a software, that can be run in a variety of components that allowed us to achieve substantial empiric results that are being studied to be exposed in the second phase of our research, and that in summary, show the possible peer-to-peer communication between components that are part of a decentralized swarm network, and even the possible incorporation of independent background services that will add complexity to the content manipulation.

Being this the first phase of a three-step project, we cannot yet inform on empiric results of the impact of this system on Fog Computing. What we can report is that a first phase of communication in a new swarm network structure was possible, and that the Fog Computing was reduced by allowing information to be stored in the components and so creating an alternative for improvements in privacy and security.

Future study will bring us more empiric results that may be compared to existing centralized structures, being one of them a Z Mainframe execution of such a network structure.

References

[1] J. Bar-Magen, A. Garcia-Cabot, E. Garcia, L. de-Marcos, and JA. Gutierrez de Mesa. “Collaborative Network Development for an Embedded Framework”. In: Uden L, Herrera F, Pérez JB, Corchado Rodríguez JM, editors. 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing: Springer Berlin Heidelberg; 2013. p. 443-453.

[2] J. Bar-Magen, “Fog Computing- Introduction to a new Cloud evolution”. In: Jose F. Fornies Casals, Paulina Numhauser, editor. Escrituras Silenciadas: El paisaje como Historiografia. 1st ed. Alcala de Henares, Madrid, Spain: UAH; 2013. p. 111-126.

[3] F. Frankel and R. Reid,Big data: “Distilling meaning from data.” Nature 2008 09/04;455(7209):30-30.

[4] D. Agrawal, S. Das, and A. El Abbadi. “Big data and cloud computing: current state and future opportunities.” In *Proceedings of the 14th International Conference on Extending Database Technology* (EDBT/ICDT '11), Anastasia Ailamaki, Sihem Amer-Yahia, Jignesh Pate, Tore Risch, Pierre Senellart, and Julia Stoyanovich (Eds.). ACM, New York, NY, USA, 2011, pp. 530-533.

[5] C. Lynch, “Big data: How do your data grow?” Nature 2008 09/04;455(7209): pp. 28-29.

[6] J. Brandon, “Living in the Cloud.” PC Magazine 2008;27(8): pp.19-20.

[7] D. Angeli, “A cost-effective cloud computing framework for accelerating multimedia communication simulations.” Journal of Parallel & Distributed Computing 2012;72(10): pp.1373-1385.

[8] MR. Nelson, “The Cloud, the Crowd, and Public Policy.” Issues in Science & Technology 2009;25(4): pp.71-76.

[9] S.J. Stolfo, M.B Salem., and A.D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on* , vol., no., pp.125,128, 24-25 May 2012

[10] A.S. Yüksel, M.E. Yuksel, and A.H. Zaim, "An Approach for Protecting Privacy on Social Networks," *Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on* , vol., no., pp.154,159, 22-27 Aug. 2010

[11] R. Buyya, J. Broberg, and A.M. Goscinski. 2011. “*Cloud Computing Principles and Paradigms*.” Wiley Publishing.

[12] K. McDonald, “Above the Clouds: Managing Risk in the World of Cloud Computing.” 2010.

[13] E. Boritz and W. Gyun No. 2009. “A Gap in Perceived Importance of Privacy Policies between Individuals and Companies.” In *Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business* (CONGRESS '09). IEEE Computer Society, Washington, DC, USA, 181-192

[14] DA Bryan, BB Lowekamp, and C. Jennings, “SOSIMPLE: A Serverless, Standards-based, P2P SIP Communication System.” Advanced Architectures and Algorithms for Internet Delivery and Applications, 2005 AAA-IDEA 2005 First International Workshop on 2005: pp. 42-49.

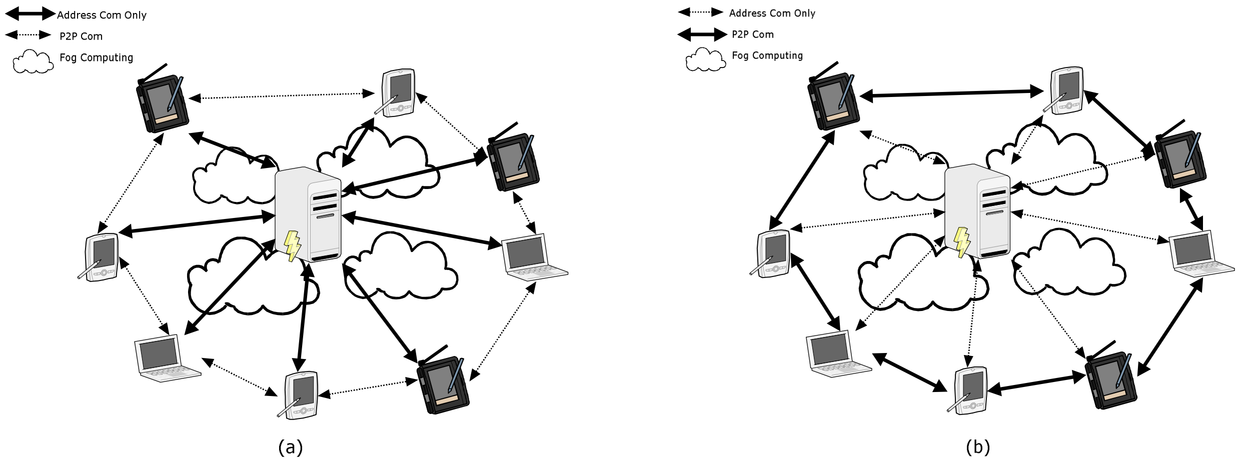
[15] C. dos Santos, S. Cechin, L. Granville, M. Almeida, and L. Tarouco, “On the performance of employing presence services in P2P-based network management systems.” In *Proceedings of the 2008 ACM symposium on Applied computing* (SAC '08). ACM, New York, NY, USA, 2090-2094..

[16] L. Stout, M. Murphy, and S. Goasguen,” ”Kestrel: an XMPP-based framework for many task computing applications.” In *Proceedings of the 2nd Workshop on Many-Task Computing on Grids and Supercomputers* (MTAGS '09). ACM, New York, NY, USA, , Article 11 , 6 pages.

[17] G. Beni, “From Swarm Intelligence to Swarm Robotics” Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, 1-9 pages.

[18] P. Saint-Andre, "Jingle: Jabber Does Multimedia," *MultiMedia, IEEE* , vol.14, no.1, pp.90,94, Jan.-March 2007.

[19] R. Hanson, XMPPFrameWork for iOS environments, https://github.com/robbiehanson/XMPPFramework/wiki/IntroToFramework



(a)

(b)

Figure 1. Network structures: (a) Centralized information network system, (b) XMPP P2P based information network system

Flow Classification in Delay-Aware NUM-Oriented Wireless Mesh Networks

Przemyslaw Walkowiak, Maciej Urbanski, Mateusz Poszwa, Radoslaw Szalski
Institute of Control and Information Engineering
Poznan University of Technology
Poznan, Poland
Email: {przemyslaw.walkowiak, maciej.urbanski, mateusz.poszwa, radoslaw.szalski}@put.poznan.pl

***Abstract*—The Network Utility Maximisation (NUM) framework is one of the most widely investigated approaches for designing the resource management system for wireless mesh networks. In order to perform the NUM-oriented per-flow network resource management, data flows have to be recognised and classified. Relevant solutions that are constituents of the state-of-the-art NUM frameworks are insufficient, since they are able to differentiate between various network flows only according to the transport layer protocol used. The paper describes improvements introduced to an existing DANUM System (DANUMS) implementation. They provide means for flexible flow classification enabling more accurate utility estimation for more diverse types of flows. The solution improves DANUMS' ability to assign appropriate utility functions suitable for different types of traffic. The experiments show that the enhanced framework enables improving the performance of the DANUMS.**

Keywords*-*DANUMS; wireless mesh networks; Network Utility Maximisation; traffic classification

I. Introduction

As the wireless network access is becoming more and more widespread, the needs of its users grow. When the demands exceed the network's capacity, not all flows can be served equally well. NUM [1] aims to manage network resources in an optimal way, which ensures maximal satisfaction of network users. DANUMS [2] provides NUM functionality by identifying and classifying flows, as well as by measuring and acting on changes of their utility. It is an application of and an enhancement to the NUM model providing delay awareness. The framework improves the fairness of the resource allocation among flows with different delay requirements. DANUMS has been designed to work in wireless mesh networks [2].

DANUMS is a part of the architecture developed within the *Carrier-grade delay-aware resource management for wireless multi-hop/mesh networks* (CARMNET) project [3] referred to as CARMNET architecture. This architecture consists of multiple components (see Figure 1): a routing component in the form of Optimised Link State Routing Protocol daemon (OLSRd), a custom SIP User Agent integrated with a Linux Loadable Kernel Module (LKM), a user interface (WebUI) and an IP Multimedia Subsystem (IMS) platform. SIP User Agent is responsible for asynchronous communication between LKM and the IMS. The user interface is a WWW application that allows users to bind utility functions to various types of traffic. The WebUI also provides insight into statistics about transmitted traffic and network usage cost.

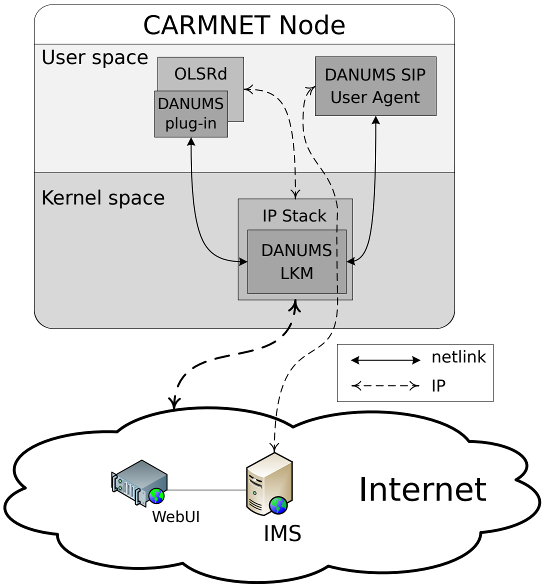


Figure 1. Architecture of the CARMNET network [3].

In NUM, network resource allocation is performed on per-flow basis. The flow classification is necessary for recognition of flow-to-application associations. Once the flow's category is identified, its utility can be computed according to its characteristics. Bidirectional flows, which can be referred to as request-response flows, also should be properly identified as their performance may affect each other's utility. TCP flows' rate and responsiveness depend on the timely delivery of ACK segments. Thus, it is desirable to prioritise request and response flows similarly in order to avoid unnecessary congestion window reductions due to excessive ACK segments queueing. Moreover, recognition of response flows is beneficial from the business perspective, which is important in the CARMNET architecture integrating Authentication, Authorisation and Accounting (AAA) and charging functionality [3]. Each node that generates traffic should have control over both request and response flows' *virtual prices* (see Section III).

The basic DANUMS implementation [2] differentiates flows according only to the transport layer protocol. While effective for basic scenarios, this solution is not versatile enough to control media streams with different needs. This paper describes a practical implementation of a more robust method for flow classification and recognition of response flows.

The paper structure is as follows. Related work is described in Section II. Section III introduces the Delay-aware Network Utility Maximisation (DANUM) model and provides its main purposes. Section IV discusses the problem of flow classification. Methods of recognition of response flows are described in Section V. Experiments and their results are described in Sections VI and VII, followed by conclusion in Section VIII.

II. Related work

Many NUM systems determine utility of flows according to the flows' throughput only [4]–[7]. Such an approach is not sufficient to effectively measure the utility of delay-sensitive flows. DANUMS, on the other hand, takes the delay into consideration as well [2].

The work [6] presents a policy ensuring constant worst-case delay, however, the utility function used in a maximisation scheme is based only on throughput. In [4], it is assumed that the mechanism based on providing inelastic flows with bandwidth exceeding their injection rate ensures satisfying their end-to-end delay requirements. The framework presented in [5] considers only TCP flows. Solutions presented in [7] require modification of a network card driver, which does not comply with the basic assumptions of CARMNET [3].

In order to estimate the flow's utility accurately, its type has to be determined. Advanced techniques, such as payload examination [8], machine learning algorithms [9], [10] or solutions based on neural networks [11], have been used for this purpose. However, DANUMS is also aimed at serving mobile nodes, which may be power-constrained. For this reason, classification methods for DANUMS should not be computationally complex.

III. DANUM System

The aim of the DANUM model is to provide an optimal packet scheduling policy regarding the maximisation of the network users' satisfaction. It targets the maximum of the network utility (a sum of utility of all flows within the network):

$$\max \sum_{r \in S} U_r(x_r, d_r), \tag{1}$$

where S denotes a set of flows within the network; x_r – rate of flow r; d_r – delay of flow r; U_r – the utility function of flow r. In other words, DANUMS aims at solving the NUM problem in a delay-aware way.

The relation between measurable flow transmission quality parameters and its utility is modelled by means of a utility function. Each function corresponds to flows of a given type or, more precisely, to flows with specific network requirements. In DANUMS the utility is determined not only according to the flow's throughput, but also to its end-to-end delay. Each flow may have a distinct utility function since it may prioritise different network performance parameters. Assigning utility functions to flows is a task of the Flow Classifier described in Section IV.

It has been proven that the Max-Weight Scheduling (MWS) algorithm is a solution to the standard throughput-oriented NUM problem formulation [12]. The DANUMS applies the MWS algorithm to virtual queue levels in order to determine the next flow queue to transmit a packet from.

A virtual queue is defined as a product of flow's packet backlog level and a *virtual price* of a single packet. Packet's virtual price is a value of the derivative of a utility function assigned to the flow. In other words, the more utility a flow would gain from improving its network performance parameters (e.g., by lowering its delay), the higher is the virtual price. The virtual price plays an important role in packet scheduling as well as influences the cost of CARMNET network usage.

DANUMS LKM is responsible for packet queueing, measuring flows' characteristics, as well as applying utility functions and the backpressure scheduling algorithm. Packets scheduled by DANUMS are relayed to the network interface output buffer, the level of which is kept low as a result of using Layer-2 Queue level Estimation [13]. Possible routes acquisition and explicit signalling of virtual queues is done through modified OLSRd. The details concerning the DANUM and its implementation can be found in [2], [13]–[15].

IV. Flow Classification Framework for DANUMS

Flows can be divided into two general groups: throughput-demanding and delay-sensitive. They roughly correspond to the TCP- and UDP-based traffic, respectively. Such a division was used in DANUMS prior to implementation of the Flow Classifier presented in this section. However, for some scenarios, this simple classification is insufficient. The application of the classification subsystem in DANUMS allows a more fine-grained flow classification. The more traffic classes a given NUM system is able to recognise, the more accurately the utility functions may reflect the requirements of different types of traffic.

Flow Classifier used in DANUMS is a cascade of simple filters (see Figure 2). Flow's properties are checked against rules defined for each of the filters. Each rule is a pair composed of filter-specific constraints and a flow type. If any of the rules matches the flow, i.e., the flow's properties meet the rule's constraints, the classification yields a flow type assigned to the matching rule as a result. An unspecialised utility function is assigned if all the filters fail to classify the flow. Using this utility function is equivalent to setting a constant virtual price for each packet, i.e., excluding the flow from the evaluation of NUM.

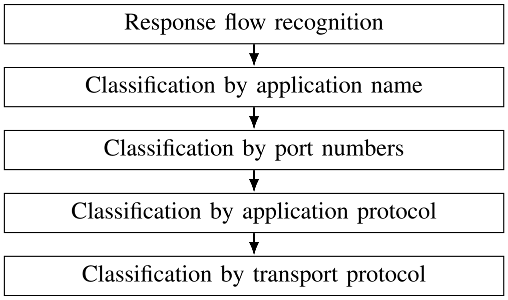

Response flow recognition
Classification by application name
Classification by port numbers
Classification by application protocol
Classification by transport protocol

Figure 2. Overview of the Flow Classification Framework for DANUMS. Arrows denote the order of applying the filters.

A. Classification by a transport layer protocol

Classification by the transport layer protocol is the simplest solution, nevertheless, it lacks the ability to differentiate specific uses of each of the protocols. An example of different TCP protocol applications can be provided: the comfort of Web navigation depends on low delay, whereas comfort of sending an e-mail does not.

B. Classification by source and destination port numbers

A common way to determine flow's type is to assume that the traffic of a certain service or an application is bound to a predefined port. The advantage of this approach is that the port numbers are already known to the classifier, so no additional processing is needed to determine them. However, this assumption usually holds true only for services using the *well-known ports* provided they were not configured to use non-standard ports. Moreover, some application layer protocols can be used with random ports, or even different transport protocols. For the given reasons, the method assuming that the traffic of a certain service or an application is bound to a predefined port would require constant reconfigurations to ensure an optimal classification of flows.

C. Classification by an application layer protocol

In order to address the limitations of the above-described approaches, classification by the application layer protocol has been considered. The transport layer and network layer protocols' headers do not provide any indication of the application layer protocol used. Therefore, it has to be determined by a direct analysis of the payload data, which is a complex task and should be delegated to an external program such as l7-filter [8]. However, its kernel-space implementation is known to cause problems on SMP-enabled processors [16], and the use of the user-space implementation in critical systems is discouraged by its authors [16]. Due to these disadvantages as well as lack of well tested alternatives, this classification method was not yet implemented.

Even if it was possible to use some version of the l7-filter to classify flows, some of its patterns return false results [17] and the cost of this method is considerably higher than the cost of other methods discussed here. This may have an influence both on performance and energy consumption. The latter aspect is of great importance for the use of mobile nodes, which DANUMS is designed for [2].

D. Classification by filename of sending application

It is possible to use locally available information to automatically determine the filename of the application sending the flow. Moreover, it is much more probable that the node's user is able to state the name of the application she uses, than that she is able to determine the port numbers bound to flows sent by the application. Thus, this method supports associating flows with desired utility functions chosen by the user through the WebUI.

On the other hand, some applications send many types of flows simultaneously. A VoIP client, for example, is responsible for setting up sessions, sending multimedia streams and reporting statistics by means of SIP, RTP and RTCP protocols respectively. It is essential to choose a utility function meant for the protocol whose transmission quality impacts the application usability the most (in this case – RTP). In this approach, heterogeneous flows sent by a single application are assigned the same utility function, which is, obviously, not the optimal assignment.

E. Combining the classification methods

Each of the aforementioned methods has disadvantages, which render each of them insufficient when used separately. Some of the disadvantages may be avoided or minimised by combining several classification methods.

Response flows are already classified by their destination nodes (referred to as "owners"). They are treated specially and should be filtered out first.

The most desired classification criterion is the application layer protocol used for the flow payload. Unfortunately, as discussed above, it is computationally expensive to determine. For this reason, classification based on regular expressions should be preceded by less complex methods. Classification by the sending application filename is unreliable in case of applications that send multiple flows of various types. Nevertheless, it reflects the end user's needs most strictly, so it should be the first filter for request flows. Classification by the transport layer protocol can serve as a fallback mechanism for flows which fail to be classified by any other criteria. The final order of filters is illustrated in Figure 2.

V. Recognition of request and response flows

A request flow originating from one node and addressed to the other is usually accompanied by a response flow transmitted in the opposite direction. These two flows provide a duplex point-to-point connection between two nodes.

However, as far as DANUMS is concerned, a node which initiates a request flow should also be charged for the response flow. Such a node is marked as the "owner" of both flows. Information about flow "ownership" is propagated by OLSRd along the flow's path and allows the flow classifier to differentiate request and response flows.

If the flows were considered separately, a utility function would be assigned to each of them by the source node. Such a scheme would have undesirable consequences. Let us consider a scenario in which the requesting node assigns a utility function demanding a very low delay to a certain type of flow, but the responding node user does not require such low delay for that type of flow. Even though the requests could be sent quickly, thanks to the assigned utility function, the perceived utility of network may not be satisfying for requesting node's user, as the response flow may fail to be prioritised by the replying node.

Another example of undesirable consequence of mismatching utility functions is related to the CARMNET business model [3]. When the source node is outside the CARMNET network, the destination node is charged for the transmission of the flow. Were the flows considered separately, their utility would be decided by the node at the border of the CARMNET network (an Internet-sharing node), which forwards the flow to the destination node inside the CARMNET network. Since the utility of a flow is closely related to its virtual price, it should not be set by a node other than the one which is charged for transmitting the flow.

For the aforementioned reasons, a mechanism for recognising response flows has been implemented that enables two methods for response flows' virtual price adjustment. Their performance has been evaluated in Section VI.

1) Copying the request flow's virtual price: The information about the virtual price of each flow, encapsulated in the Queue Report Message (QRM) packets [15], is propagated through the network along the flow's path. Therefore, it is available for the replying node and can be applied to the response flow. This simple method does not require the replying node to analyse the flow to which virtual price is applied or to fetch requesting node's profile. However, the potential issues this method introduces need to be considered.

In DANUMS, characteristics of a certain path are measured on per-flow basis. When the network is congested, throughput and delay measured at both endpoints of a flow may differ significantly. Undesired consequences of using this method may also arise when request and response flows' requirements differ. Such situation is illustrated by the first experiment described in Section VI-B1.

2) Calculating the request flow's new virtual price by applying a utility function at the replying node: The other method of controlling the virtual price of a response flow is to assign a utility function chosen by the requesting node. This information can be retrieved from IMS by sending the *Get Profile* message [3]. While flows' *owner* node can assign the same utility function to both request and response flows, its parameters will differ from those measured on each endpoint of respective flows. Network characteristics perceived at both nodes may be influenced by factors such as congestion, asymmetry of links or choice of routes. Therefore, it is more accurate to calculate the flow's virtual price at the transmitting node, whether or not it is the flow's "owner".

VI. Experiments

A. Testbed

Experiments have been performed in a wireless network testbed called wnPUT [18]. The wnPUT testbed deployment approach has been influenced by the Distributed Embedded System Testbed (DES-Testbed) [19] architecture. Currently our testbed consists of about 20 PC-class machines, each equipped with two network interfaces, wired and wireless. The wired network is used for out-of-band management. The wireless connections are used for experimentation purposes only. Each testbed node runs a Debian GNU/Linux distribution.

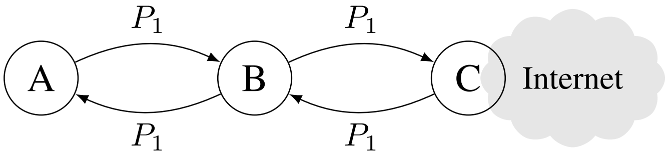


Figure 3. Copying the flow's virtual price. **A** – CARMNET node, **B** – CARMNET Relaying node, **C** – CARMNET Internet Sharing node, $\mathbf{P_1}$ – Virtual price calculated at Node A

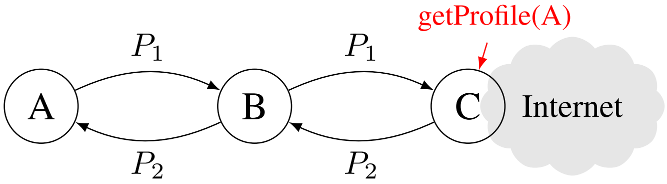


Figure 4. Applying utility function at replying node. **A** – CARMNET node, **B** – CARMNET Relaying node, **C** – CARMNET Internet Sharing node, $\mathbf{P_1}$ – Virtual price calculated at Node A, $\mathbf{P_2}$ – Virtual price calculated at Node C

The testbed allows for an easy and automated experiment execution. It handles parsing of the experiment description files, setting up wireless network, configuring topology, executing specified commands and, finally, gathering results. Experiments are described using the scenario files written in XML. The syntax of those files is an extension of the DES-CRIPT [20] language used in DES-Testbed [19]. The unified format of experiment description files has many benefits such as portability and expressiveness, as well as allowing the experiments to be performed on different testbeds. Although the testbed framework was heavily modified, the phases of experimentation remain as defined in the previous work [18], [19]. Status of performed commands and the DANUMS LKM is acquired in real-time by means of `rsyslogd` and visualised by a monitoring system in order to make the analysis easier.

Due to space constraints, currently all nodes are directly connected to each other in a wireless mesh network sharing the same collision domain. Taking the wireless networks characteristic into account, in which even nodes separated by 2 hops might interfere with each other, it has been assumed that 2-hop topology can be simulated by blocking traffic on software level. Thus, the wnPUT testbed framework allows user to specify desired topology, which is attained with `iptables` rules generated automatically during experiment initialisation.

B. Experiment scenarios

In order to illustrate the benefits of recognising response flows, two experiment scenarios were prepared. Their purpose is to show possible undesirable outcome of miscalculating flows' virtual price, which may result from taking wrong measurements under consideration. For both scenarios, the linear topology consisting of three nodes was used (see Figure 3).

In both experiments, Node A initiates communication by sending data to Node C. Since Nodes A and C are not directly connected, Node B forwards the flow in order to provide connection between them. Node C responds with a reverse flow addressed to Node A.

In the first experiment, Node C marks the destination of the response flow (Node A) as its owner in order to inform relaying nodes (Node B) that the flow's virtual price has to be copied from Queue Information Block (QIB) blocks corresponding to the request flow. In the second experiment, Node C fetches the profile of Node A and applies the utility function corresponding to the served flow in order to determine response flow's virtual price. These two experiments correspond to the methods of adjusting the virtual price described in Section V.

1) Experiment 1: The first experiment illustrates a possible undesired consequence of using the method based on virtual price copying described in Section V-1. This scenario models a VoIP call (labelled as "RTP C→A" in Figure 5 and Figure 6) made during a HTTP file transfer (labelled as "HTTP C→A"). The experiment starts with a HTTP request (labelled as "HTTP A→C") sent from Node A to Node C. Its size was artificially enlarged to 5MB for experiment clarity purposes. Node C responds to the requester with a 25MB HTTP response, one second after receiving the request. While the response is being transmitted, Node C initiates a 35-second long RTP flow at constant rate of 2.5Mbit/s addressed to Node A. The experiment ends when both flows originating from Node C are terminated.

2) Experiment 2: In the second experiment, timing and characteristics of flows are the same as in Experiment 1. The only difference is the virtual price of the response flow, which is now calculated at Node C according to the method described in Section V-2.

C. *Utility functions assignment*

For RTP flows, the following utility function was used [15]:

$$U_U(x,d) = \frac{w_u}{\left(1+e^{a(x_t-x)}\right)\left(1+e^{b(d-d_t)}\right)} \tag{2}$$

where $w_u = 10^6$ is an aggressiveness parameter; $x_t = 2.5 \cdot 10^6$ and $d_t = 300$ denote desired bitrate and delay respectively; $a = b = 0.01$ are parameters controlling the slope of utility function; The utility function assigned to RTP flows aims to maintain their delay below 300ms, i.e., the flow's virtual price peaks when its delay equals 300ms.

Utility function used for HTTP flows is as follows:

$$U_T(x,d) = w_t log(x) \tag{3}$$

To ensure desired assignment of the utility functions, appropriate classification rules have been configured. They were based on the application filename criterion (discussed in Section IV-D).

VII. Results

Virtual price values in both experiments indicate that the flow classifier was able to differentiate flows correctly. Delay-sensitive utility function has been assigned to the RTP flow (which may be observed in Figure 5 near $t = 55$s, when the flow's virtual price drops due to high delay) and throughput-oriented utility function has been assigned to HTTP flows (whose virtual price rises when its rate drops considerably).

The virtual price values also show that the response flows have been properly recognised by the classifier. Therefore, methods for response flows' virtual price adjusting described in Section V could be applied and evaluated.

In Experiment 1, the transmission of the RTP flow ended prematurely, because the HTTP response flow had its virtual price set inappropriately high. The virtual price was calculated at Node A for a low-throughput sequence of TCP acknowledgements and was not meant to be used with high-throughput TCP flows. The HTTP response flow overwhelmed the RTP flow despite having lower product of utility derivative and packet queue level, causing the RTP flow's delay to rise beyond the d_t threshold value, which led to lowering the RTP flow's virtual price. Such a behaviour is an undesirable outcome of copying the virtual price calculated for accompanying request flow when its characteristics differ considerably.

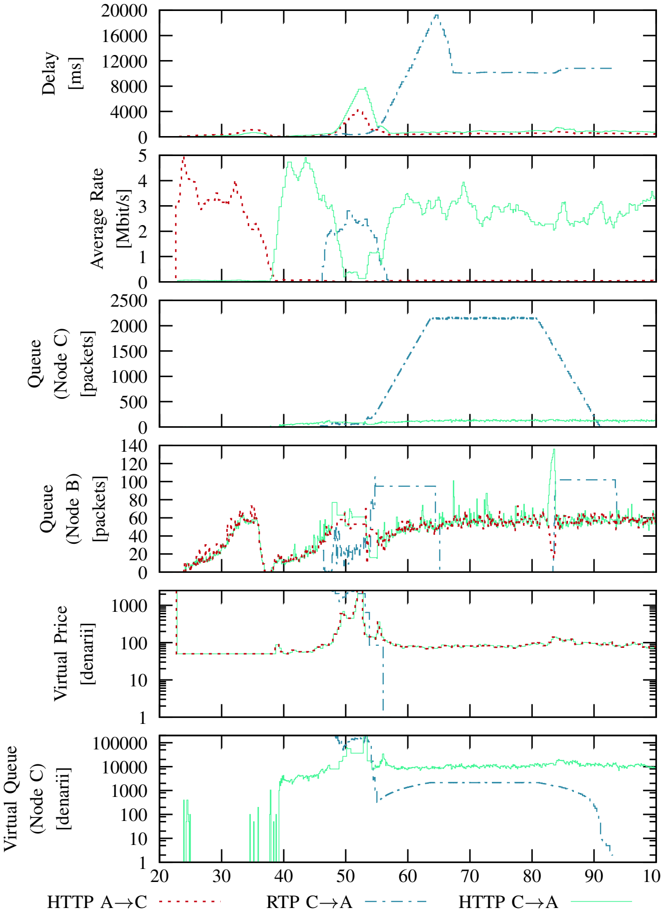


Figure 5. Results of Experiment 1.

In Experiment 2, the virtual price of HTTP response flow was calculated locally on Node C, resulting in much lower virtual price of the response flow since the derivative of HTTP flows' utility declines with the growth of throughput. As a result, the virtual queue level of the RTP flow was high enough to successfully compete with HTTP flows while maintaining a satisfiable delay.

VIII. Conclusion and Future Work

Two ways of dealing with request/response flows were presented. The first one is based on copying the flow's virtual price between requesting and replying nodes, the second forces utility recalculation on both nodes. The copying-based approach is a less demanding solution since it involves sending the virtual price using CARMNET-specific protocol. However, as the experiments showed, applying this simplification may destabilise DANUMS. On the other hand, the virtual price recalculation using actual parameters at the replying node, results in a better stability of the system. Nonetheless, the local resource requirements are higher, as this method requires

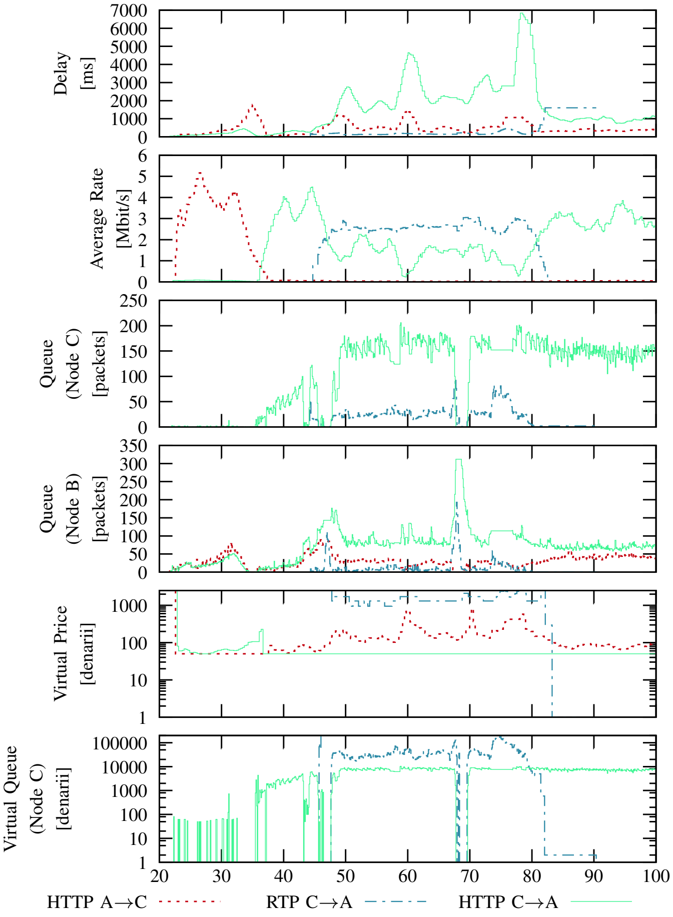


Figure 6. Results of Experiment 2.

nodes to acquire and store users' profiles, as well as to perform additional calculations. Most importantly, after all, this approach achieves the highest stability.

The implementation of the flow classifier improved flexibility of DANUMS by enabling the use of utility functions adapted to specific applications' requirements. However, the classification could likely be enhanced even further by introducing more reliable or more fine-grained, but still power-efficient (in terms of the battery power consumption caused by necessary computations) filters. Adding the possibility of combining multiple criteria into a single rule may also be beneficial to the quality of flow classification.

Acknowledgement

Supported by a grant from Switzerland through the Swiss Contribution to the enlarged European Union (PSPB-146/2010, CARMNET).

References

[1] F. Kelly, "Charging and rate control for elastic traffic," European Transactions on Telecommunications, vol. 8, no. 1, Jan. 1997, pp. 33–37. [Online]. Available: http://doi.wiley.com/10.1002/ett.4460080106

[2] A. Szwabe, P. Misiorek, and P. Walkowiak, "Delay-Aware NUM system for wireless multi-hop networks," in European Wireless 2011 (EW2011), Vienna, Austria, Apr. 2011, pp. 530–537.

[3] M. Glabowski and A. Szwabe, "Carrier-Grade Internet Access Sharing in Wireless Mesh Networks: the Vision of the CARMNET Project," The Ninth Advanced International Conference on Telecommunications, Jun. 2013, in print.

[4] U. Akyol, M. Andrews, P. Gupta, J. D. Hobby, I. Saniee, and A. Stolyar, "Joint scheduling and congestion control in mobile ad-hoc networks," in The 27th IEEE International Conference on Computer Communications (INFOCOM 2008), Apr 2008, pp. 619–627.

[5] B. Radunović, C. Gkantsidis, D. Gunawardena, and P. Key, "Horizon: Balancing TCP over multiple paths in wireless mesh network," in Proceedings of the 14th ACM international conference on Mobile computing and networking, MobiCom 2008, 2008, pp. 247–258.

[6] M. Neely, "Delay-based network utility maximization," In Proc. IEEE INFOCOM 2010, 2010, pp. 1–9.

[7] A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practical differential backlog congestion control for wireless networks," in The 28th IEEE International Conference on Computer Communications (INFOCOM 2009), Apr. 2009, pp. 262–270.

[8] Application Layer Packet Classifier for Linux. [Online]. Available: http://l7-filter.clearfoundation.com [retrieved: Jun., 2013]

[9] N. Williams, S. Zander, and G. Armitage, "A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification," ACM SIGCOMM Computer Communication Review, vol. 36, no. 5, Oct. 2006, pp. 5–16. [Online]. Available: http://dl.acm.org/citation.cfm?doid=1163593.1163596

[10] I. Anantavrasilp and T. Schöler, "Automatic flow classification using machine learning," in Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. 15th International Conference on. IEEE, 2007, pp. 1–6.

[11] M. Ilvesmäki, M. Luoma, and R. Kantola, "Flow classification schemes in traffic-based multilayer IP switching–comparison between conventional and neural approach," Computer Communications, vol. 21, no. 13, Sep. 1998, pp. 1184–1194. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366498001637

[12] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling for maximum throughput in multihop radio networks," IEEE Transactions on Automatic Control, vol. 37, no. 12, Dec. 1992, pp. 1936–1949.

[13] A. Szwabe, P. Misiorek, and P. Walkowiak, "Protocol Architecture for DANUM Systems," Poznan University of Technology, Institute of Control and Information Engineering, Tech. Rep. IAII-595, Apr. 2010.

[14] A. Szwabe, "DANUMS: The First Delay-Aware Utility Maximization System for Wireless Networks," in Proc. of NEM Summit - Towards Future Media Internet. NEMS 2009, Sep. 2009, pp. 59–64.

[15] A. Szwabe, P. Misiorek, and P. Walkowiak, "DANUM System for Single-hop Wireless Mesh Networks," In Proceedings of 2010 International Conference on Future Information Technology (ICFIT 2010), volume 1, Changsha, China, IEEE Press, Dec. 2010, pp. 365–369.

[16] Application Layer Packet Classifier for Linux – Getting started. [Online]. Available: http://l7-filter.clearfoundation.com/docs/readme#getting_started [retrieved: Jun., 2013]

[17] L7-filter supported protocols. [Online]. Available: http://l7-filter.sourceforge.net/protocols [retrieved: Jun., 2013]

[18] A. Nowak, P. Walkowiak, A. Szwabe, and P. Misiorek, "wnPUT Testbed Experimentation Framework," in Distributed Computing and Networking, ser. Lecture Notes in Computer Science, L. Bononi, A. Datta, S. Devismes, and A. Misra, Eds. Springer Berlin Heidelberg, 2012, vol. 7129, pp. 367–381. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25959-3_27

[19] The Distributed Embedded Systems Testbed (DES-Testbed) Webpage. [Online]. Available: http://www.des-testbed.net [retrieved: Jun., 2013]

[20] M. Güneş, F. Juraschek, B. Blywis, and O. Watteroth, "DES-CRIPT - A Domain Specific Language for Network Experiment Descriptions," in Next Generation Wireless Systems 2009 – Proceedings, N. Chilamkurti, Ed., Mar. 2010.