MESH 2011

The Fourth International Conference on Advances in Mesh Networks

ISBN: 978-1-61208-147-2

August 21-27, 2011

Nice/Saint Laurent du Var, France

MESH 2011 Editors

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

Bernard Tourancheau, INRIA, France

MESH 2011

Foreword

The Fourth International Conference on Advances in Mesh Networks (MESH 2011), held between August 21-27, 2011 in Nice/Saint Laurent du Var, France, 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 multihop 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 2011 technical program committee as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the MESH 2011. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the MESH 2011 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success.

We hope the MESH 2011 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the field of mesh networks.

We hope Côte d'Azur provided a pleasant environment during the conference and everyone saved some time for exploring the Mediterranean Coast.

MESH 2011 Chairs

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
Bernard Tourancheau, INRIA, France

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

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

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 2011

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
Bernard Tourancheau, INRIA, France

MESH 2011 Industry Liaison Chairs

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

MESH 2011 Research/Industry Chairs

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

MESH 2011 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 2011 Technical Program Committee

Khodor Abboud, Ecole centrale de Lille, LAGIS/CNRS - Villeneuve d'ASCQ, France
Wessam Ajib, Université de Québec à Montréal (UQAM) , Canada
Gleicy Aparecida Cabral, Federal University of Minas Gerais, Brazil
Michael Bahr, Siemens AG - München, Germany
Mostafa Bassiouni, University of Central Florida - Orlando, USA
Lofti Ben Othmane, Kalamazoo College, USA
Jalel Ben-Othman, Université de Versailles, France
Roberto Beraldi, University of Rome "La Sapienza", Italy
Mats Björkman, Mälardalen University, Sweden
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania

Stefan Bouckaert, Ghent University - IBBT, Belgium
Glenn Colby, US Navy, USA
Antonio de la Oliva, University Carlos III of Madrid, Spain
Tullio Facchinetti, University of Pavia, Italy
Karoly Farkas, University of West Hungary / Budapest University of Technology and Economics, Hungary
Gianluigi Ferrari, University of Parma, Italy
Nuno M. Garcia, Universidade Lusófona de Humanidades e Tecnologias - Lisbon, Portugal
Dan Harkins, Aruba Networks, USA
Li-Ling Hung, Aletheia University, Taiwan
Francisco Jose Bellido Outeiriño, University of Cordoba, Spain
Andreas J. Kassler, Karlstad University, Sweden
Jarkko Kneckt, Nokia Research Center, Finland
Vinay Kolar, Carnegie Mellon University - Doha, Qatar, USA
Volker Köster, TU Dortmund, Germany
Andrey Larionov, RDC / Institute of Russian Academy of Sciences - Moscow, Russia
Ha Cheol Lee, Yuhan University - Bucheon City, Korea
Yao-Nan Lien, National Chengchi University - Taipei, Taiwan, R.O.C.
Sebastian Max, Riedel Communications - Wuppertal, Germany
Hamid Menouar, QU Wireless Innovations Center - Doha, Qatar
Jens Myrup Pedersen, Aalborg University - AalborgØst, Denmark
João Paulo Barraca, University of Aveiro, Portugal
Saquib Razak, Carnegie Mellon University - Doha, Qatar
Susana Sargento, University of Aveiro, Institute of Telecommunications - Pole of Aveiro, Portugal
Dirk Staehle, University of Würzburg, Germany
Young-Joo Suh, Pohang University of Science and Technology - Pohang, Korea
David R. Surma, Indiana University South Bend, USA
Abd-Elhamid M. Taha, Queen's University Kingston, Canada
Bernard Tourancheau, INRIA, France
Goce Trajcevski, Northwestern University - Evanston, USA
Tzu-Chieh Tsai, National Chengchi University, Taiwan
Mthulisi Velempini, University of Cape Town, South Africa
Christian Wietfeld, TU Dortmund University, Germany
Sherali Zeadally, University of the District of Columbia, USA

Copyright Information

Table of Contents

A Density Based Clustering Algorithm for Efficient Channel Allocation in Multi-radio Multi-channel Wireless Mesh Networks

Sana Ghannay, Sonia Mettali Gammar
National School of Computer Sciences
CRISTAL Laboratory, Tunisia
Email: sana.ghannay@cristal.rnu.tn, sonia.gammar@ensi.rnu.tn

Fethi Filali
QU Wireless Innovations Center
Doha, Qatar
Email: filali@quwic.com

***Abstract*—Efficient channel selection is essential in 802.11 mesh deployments, for minimizing contention and interference among co-channel devices. The IEEE 802.11 standard provides at least three non-overlapping channels and thus its possible for a node equipped with more than one network interface card (NIC) to operate on different channels simultaneously. This may increase the aggregate bandwidth available. In this work, we propose a density based clustering algorithm for channel allocation (DCCA) for multi-radio multi-channel mesh networks. DCCA manages the network topology by partitioning the mesh network into balanced cluster and affects a fixed and static channel to each cluster to be used mainly for control traffic. DCCA reduces intra- and inter-clusters interference and can be used in conjunction with a dynamic channel assignment strategy. Simulation results show that our solution gives balanced clusters and reduces broadcast time.**

Keywords-mesh networks; multi-channel; multi-rate; clustering; DCCA.

I. Introduction

Wireless Mesh Networks (WMNs) [1] have recently gained increasing attention and have emerged as a technology with great potential for a wide range of applications. WMN are composed of static wireless node which form the backbone. One or several nodes which belong to the mesh infrastructure can be configured as gateway to allow access to external network such as Internet. Moreover, some of mesh nodes can play the role of access point to allow mesh network access to client station. In mesh network, nodes are either stationary or minimally mobile and have ample energy supply. For wireless local area networks, an extension named IEEE 802.11s is being standardized. The essential motivation for the 802.11s standard is to provide a means by which a wireless backbone can be realised with minimal configuration effort useful in scenarios such as office buildings, home networking, and apartment blocks. The IEEE 802.11s working group specifies a new architecture defining three network components: Mesh Point (MP), Mesh Portal Point (MPP) and Mesh Access Point (MAP) [2]. The MP determines how to route packets through the mesh. The MPP is a particular MP connected to a wired gateway and it allows MP to access external network such as Internet. The MAP is a particular MP that allows client stations to access to the mesh network.

Each node in WMN can be equipped with multiple radios and each node interface can be configured to a different channel. Allowing multiple channels use in the same network is often presented as a possible way to improve the network capacity. In fact, with proper design, leveraging multiple channels available today has several benefits, including increasing system throughput, decreasing end-to-end delay, and achieving better load balancing.

Several multi-channel researchers [3] use a dedicated control channel and one interface is statically tuned to the control channels. This interface will be used to ensure connectivity and to send broadcast and control messages. In these solutions, control channel can become a bottleneck under heavy loads. In addition, in IEEE 802.11, there are only three orthogonal channels. Thus, 33% of the channel resource is consumed exclusively for control purposes.

In this work, we propose a clustering algorithm based on a density metric to manage the mesh network topology. Our algorithm is called DCCA for Density based Clustering algorithm for Channel Allocation. DCCA constructs balanced clusters, ensures that neighbor clusters doesn't interfere with each other and provides connectivity between nodes. In fact, the intra-cluster connectivity is guaranteed by affecting a fixed channel FC to each cluster according to a coloration algorithm. In addition, the inter-cluster connectivity is ensured by an efficient inter-cluster channel assignment. DCCA allows configuring one interface on FC used to exchange control and data traffic and it can be used in conjunction with a dynamic channel assignment solution to assign channels to pending radio interfaces.

The remainder of the paper is structured as follows: in Section 2, we present multi-channel related works and challenges. Section 3 reviews and compares load balancing clustering algorithm. In Section 4, we detail our clustering algorithm and inter and intra-cluster channel assignment. A Simulation-based performance study is presented in Section 5. Section 6 concludes this paper.

ISBN: 978-1-61208-147-2

II. Multi-channel in WMN

The main goal of channel assignment approaches is to allocate the available channels to network interfaces of nodes in a way that minimizes interference and maximizes the average throughput [3]. Severals works was proposed in litterature to achieve this goal. Before developping these works, we first present multichannel challenges.

A. Multichannel Challenges in WMN

1) Ensure connectivity: The wireless mesh network may be split due to channel assignment. This can happen if a node doesn't share a common channel with any of its neighbor. In this context, channel assignment must guarantee connectivity between nodes in wireless network.

2) Support of broadcast: There are two methods to broadcast messages in multichannel mesh network. The first one is the use of a dedicated control interface tuned statically to a fixed control channel to isolate control packets from data packets. The second method is to use different channels and broadcasted messages will be sent over all radio interfaces. Both of methods have drawbacks. In fact, in the first method the dedicated interface can be overloaded, whereas in the second method, a huge number of control messages is observed in the network.

3) Balance load: Utilizing multiple channels allows parallel transmissions on non-overlapping channels. However, without accounting for the channel load in terms of the contention group size (the number of nodes using the same channel in the vicinity) some channels may become overloaded which increases interference and degrades network capacity

4) Minimize the overall interferences: The interference generated by neighboring nodes to send control traffic should be minimized to decrease the packet loss probability and improve thereby the overall performance of the network. To reduce interference a node should minimize the number of neighbors who use with him a common channel.

B. Related work

Several researchers proposed to manage the network topology by using clustering in dynamic multi-channel solutions such as [4] and [5] or tree architecture such as [7]. Nevertheless, clustering algorithms used by these solutions are not adapted for multichannel. For example, Liu *et al*. [4] uses Max-Min D-cluster algorithm which clustering result depends mainly on the distribution of nodes identifiant in the network. Max-Min D-cluster may lead to some small clusters (clusters with radius equal to one or clusters with small number of members). Small cluster may cause inter cluster interference. Thus, the clustering algorithm must be topology based. Makram *et al*. [5] requires a clustering at the beginning, wherein the MPs nodes are grouped into subsets of nearby nodes. It deploys the Highest Connectivity Cluster (HCC) [6] algorithm, where a node is elected as a clusterhead if it is the most highly connected node (having the highest number of neighbor nodes). The HCC can construct unbalanced one hop clusters. Raniwala *et al*. [7] defines a multi-channel WMN tree architecture based. Each MPP is the root of a spanning tree and each node attempts to participate in one or multiple such spanning tree. The solution of Raniwala *et al*. [7] has a drawback of providing path to wired network only. Besides, it uses a dedicated control interface to broadcast control messages. This interface can become overloaded which increases collisions and interference.

III. Clustering algorithms for load balancing

Our first objective when forming clusters is to limit the number of mobile nodes in each cluster to reduce intra- and inter-cluster interference. As regard clustering schemes, they can be classified according to their objectives into six categories [8]. Dominating-Set based clustering, low-maintenance clustering schemes, mobility-aware clustering, energy-efficient clustering, load balancing clustering schemes and combined-metrics based clustering. In our work, we opted for load balancing clustering. In fact, this category attempts to limit the number of mobile nodes in each cluster to a specified range so clusters are of similar size. Obtained cluster sizes have significant importance. Indeed, a too-large cluster may has several nodes using the same FC channel causing to heavy of interference in intra-cluster and reducing system throughput. A too-small cluster however may produce a large number of clusters and thus increases the inter-cluster interference.

A. Load-balancing clustering schemes

1) AMC (Adaptive Multi-hop Clustering): AMC [9] maintains a multihop cluster structure based on load-balancing clustering. For cluster maintenance each mobile node periodically broadcasts its information, including its ID, CID (Clusterhead ID), and status (clusterhead/member/gateway) to others within the same cluster. By such message exchange, each mobile node obtains the topology information of its cluster. Each gateway also periodically exchanges information with neighboring gateways in different clusters and reports to its clusterhead. Thus, a clusterhead can recognize the number of mobile nodes of each neighboring cluster. AMC sets upper and lower bounds (U and L) on the number of cluster members that a clusterhead can handle. When the number of cluster members in a cluster is less than the lower bound, the cluster needs to merge with one of the neighboring clusters. On the contrary, if the number of cluster members in a cluster is greater than the upper bound, the cluster is divided into two clusters.

2) DLBC (Degree-Load-Balancing Clustering): Periodically, DLBC [10] runs the clustering scheme in order to keep the number of mobile nodes in each cluster around

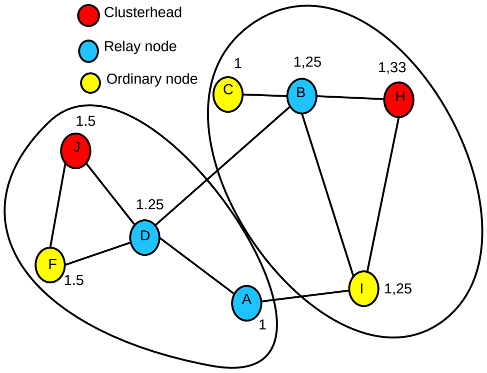


Figure 1. An example of DBC algorithm

a system parameter, ED (Eledted Degre), which indicates the optimum number of mobile nodes that a clusterhead can handle. A clusterhead degrades to an ordinary member node if the difference between ED and the number of mobile nodes that it currently serves exceeds some value, MaxDelta.

3) ACLB (Adaptive Cluster Load Balance method): A new approach in [11] is given. In hello message format, an ”Option” item exists. If a sender node is a clusterhead, it will set the number of its dominated member nodes as ”Option” value. When a sender node is not a clusterhead or it is undecided (H or non-CH), ”Option” item will be reset to 0. When a clusterhead’s Hello message shows its dominated nodes’ number exceeds a threshold (the maximum number one clusterhead can manage), no new node will participate in this cluster.

4) DBC (Density Based Clustering): DBC [12] adopts an approach based on a density metric to build clusters and to elect clusterhead. The density aims to characterize the node’s importance inside the wireless network and in its neighborhood. The metric of density is the ratio between the number of edges between a node U and its neighbors, the number of edges between U’s neighbors and the number of nodes inside U’s neighborhood. Each node broadcast its density and the clusterhead will be the node having the highest density value. To elect a clusterhead, each node computes its density value and broadcasts it locally to all its neighbors. By receiving this value, each node is able to know which node will be the clusterhead. Once a cluster head is elected, the cluster head MAC Address and its density are locally broadcast by all nodes that decided to join that cluster. A cluster can then extend itself until it reaches a cluster frontier of another clusterhead. Let ’s consider an example of DBC algorithm in Fig. 1. Before partitioning the network, it is necessary to evaluate the density for each node. The density of node H is 1.33 ($1.33 = (2 + 1)/2$) because H has 2 edges with its neighbors (links (H, B) and (H, I)), 1 egde between its neighbors (link (B, I) and 2 neighbors (B and I).

B. Comparison of Load-balancing Clustering

Table I
COMPARISON OF LOAD BALANCING CLUSTERING ALGORITHMS

	AMC	DLBC	ACLB	DBC
Clustering Multi-hops	2-hop	2-hop	1-hop	2-hop
Metric	NA	Degree	Degree	Density
Nono-verlapping Clusters	Yes	No	No	Yes
Balanced Clusters	Depend on U and L	Yes	Yes	In dense Network
Clusterhead in the middle	No	Yes	Yes	Yes
Distance between Clusterheads	More then three hops	More then three hops	Less then three hops	More then three hops
Direct connectivity to clusterhead	No	Yes	Yes	Yes

Table. I presents a summary of the load-balancing clustering schemes addressed before. We have fixed criterions related to multichannel to compare these clustering algorithms. The aim of this comparison is the selection of the most suitable clustering algorithm to manage network topology. The first criterion that we have considered is clustering multi-hop. In fact, multi-hop clustering is preferred than one-hop clustering and especially 2-hop clustering. In fact, if the radius of clusters is set to 1 then two non neighbor clusters may still interfere with each other. In contrast, if the radius of the clusters is 2 then non-neighbor cluster interference can only occur when the intermediate cluster is small enough, which reduces the possibility of non-neighbor cluster interference to a very small extent. If the radius of clusters is larger than 2, the efficiency of clustering algorithm will be reduced sharply and the intra-cluster interference on the Fc channel will increase. AMC, DLBC and DBC keep a multi-hop cluster structure while ACLB is 1-hop clustering algorithm. To have balanced clusters, a metric that consider topology is required. DLBC and ACLB use the metric of degree while DBC uses the metric of density. The density metric permits to obtain balanced clusters as it consider neighbor and links between neighbors. To reduce interference, clusters must be non-overlapping. AMC and DBC gives nonoverlapping clusters. The third criterion is the size of obtained clusters. In fact, The resulting clusters obtained from AMC are balanced if U (Upper bound) is closer to L (Lower bound). DLBC and ACLB give balanced cluster and DBC gives balanced cluster in dense network. The next criterion is the position of the clusterhead in the cluster. The ideal position is in the middle of the cluster to have a direct connectivity with major node members to minimize the number of exchanged message. In DLCB, ACLB and DBC clusterheads are in the middle while in AMC, clusterheads can be in the periphery of clusters. Finally, the last criterion is the distance between clusterheads. A distance of 3 hops and more is suitable. In fact, clusterheads will disseminate information on channel FC. Therefore, clusterheads must be distant to avoid interference between their transmissions. DLBC, ACLB and DBC require that neighboring clusterheads should be at least three hops away.

IV. DCCA: Density based Clustering algorithm for Channel Allocation

We present environment features and constraints before decribing our solution DCCA.

A. Assumptions

1) Initially, every node set one of its interfaces to a Default Channel.
2) The available non-overlapping channels are limited (3 at least for IEEE 802.11 standard).
3) Every node has at least two network interfaces but we don't require the same number of interfaces by node.
4) We consider that the mesh network is composed of static MP.
5) We assume that our network includes one MPP. However, if multiple MPP exist only one of them will be designated to unroll DCCA protocol. This MPP could be chosen based on the MAC address.

From Table I, we observe that the density algorithm is the more appropriate clustering algorithm to manage the network topology in a multichannel solution. We opted for DBC because it provides balancing and non-overlapping clusters and each cluster has at least a diameter of 2 which reduces the possibility of non-neighbor clusters interference. Moreover, the distance between neighboring clusterheads in DBC is 3 hops to avoid contention between clusterheads transmissions. Finally, clusterhead are closer to the middle of the cluster which implies less control exchanges into a cluster. However, DBC may construct unbalanced clusters in low density networks [12]. For this reason, we propose an improvement of DBC named DCCA (Density based Clustering algorithm for Channel Allocation) in order to obtain balanced clusters.

B. Clustering mechanism

DCCA is based on DBC. DBC computed the density of each node then it partitions network topology into clusters (see Sec. III-A4). In order to balance clusters sizes, each clusterhead in DCCA broadcast its MAC address and its cluster size. A relay node which is the node on the periphery of cluster such as node A receives messages from adjacent clusterheads and then knows the total number of nodes in each cluster. If this node finds that there is unbalance between the size of its cluster and one of its neighbor clusters (difference between node numbers in each cluster greater than 2), and if this node is 2 hops away from its clusterhead, it tries to migrate. Therefore, it sends an ATTACH message to the neighbor clusterhead (J) and DETACH to its appropriate clusterhead (H). The ATTACH message contains the relay MAC address, the neighbor clusterhead MAC address and the number of nodes in its cluster. The DETACH message contains the relay MAC address, its clusterhead MAC address and the neighbor cluster size. J accepts this migration only if the number of nodes in the ATTACH request is greater than the number of J's cluster. In this case, it sends an ACCEPT message. Moreover, H accepts this migration only if the number of nodes in the DETACH request is lower than the number of H's cluster. In this case, it also sends an ACCEPT message. If the relay node receives ACCEPT messages from J and H, it sends a CONFIRM message to H and J. Finally, this relay node will update its information about its new clusterhead. As a result of DCCA, the obtained clusters have approximately the same size (4 in this example).

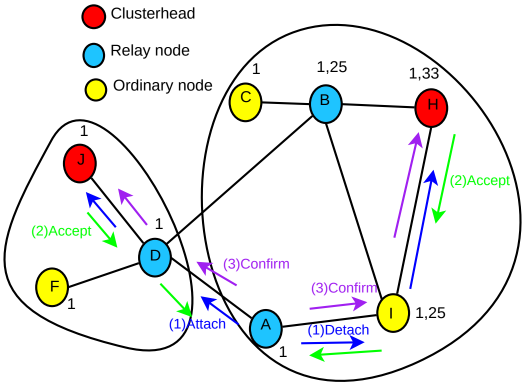


Figure 2. DCCA Algorithm

C. Inter- and intra-cluster channel assignment

The purpose of the inter-cluster channel assignment is to distribute the available channels between clusters in a way that two neighboring clusters get different channels. In order to reach this objective, a modified DSATUR coloration algorithm [13] is deployed. In modified DSATUR, the MPP sends a declaration message PDEC (Portal DEClaration) in the mesh network (we can use the PANN (Portal ANNouncement) message defined in IEEE 802.11s draft [2]). Upon reception of PDEC, each clusterhead sends a unicast PREG (Portal REGistration) to the MPP via the MP from which it received the PDEC. The registration message contains several information such as neighbor clusterhead addresses and a hop count field which calculate the number of hops between the MPP and the clusterhead. The MPP establishes a clusterheads table and a cluster connectivity matrix. The Clusterheads Table gives the level of each clusterhead which is obtained by dividing the distance between the clusterhead and the MPP by 3 (3 is the minimum distance between clusterheads)(example in (Fig. 3) the Clusterheads Table is given by Table. IV-C).

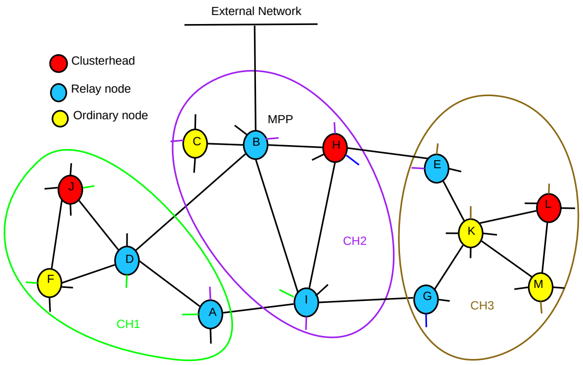


Figure 3. Inter-cluster channel assignement

In addition, the Connectivity Matrix permits to obtain the degree of a clusterhead which is the number of neighbor clusters (example in (Fig. 3) the Connectivity Matrix is given by (Table. IV-C)). For example in Fig. 3, the degree of clusterhead H is 2 as its cluster has two neighbor clusters.

Table II
CLUSTERHEADS TABLE

Id Clusterhead	Level
H	0
J	0
L	1

Table III
CONNECTIVITY MATRIX

	H	J	L
H	0	1	1
J	1	0	0
L	1	0	0

After a fixed timer (the necessary delay to receive all PREG messages from clusterheads), the MPP node affects to each clusterhead a fixed channel FC according to a modified DSATUR coloration algorithm. Indeed, this problem can be considered as a classical graph k-coloring problem: each clusterhead is a vertex in the graph. Two clusterheads are neighbor means that there are relay nodes between the two clusters. The Inter-cluster channel assignment algorithm (Algorithm 2) colors all vertices with k colors (k is the number of channels) so that neighbor vertices have different colors or the number of conflicts is as small as possible.

The MPP broadcasts a channel list message containing all clusters and affected fixed channels. Each node that receives this message configures one of its interfaces on the corresponding FC. A relay node has already an interface on FC of its cluster and affects its pending interfaces according to the algorithm (Algorithm 3).

Algorithm 1 DSAT

```
1: if If no neighbor of v is colored Then then
2:     DSAT (v) = degree (v)
3: else
4:     DSAT (v) = the number of different colors used in
       the first neighborhood of v
5: end if
```

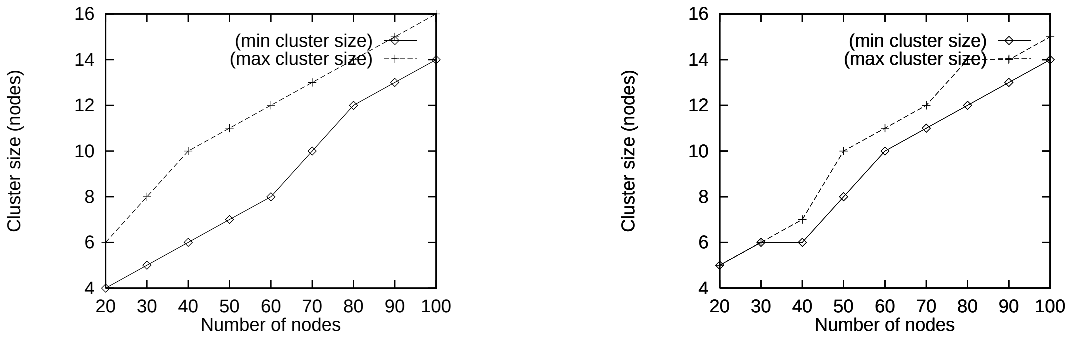
Algorithm 2 Inter-cluster Channel Assignement

```
1: Order the vertices in descending order of degree
2: Color the vertex having the maximum degree with color
   1
3: Choose an uncolored vertex x having the maximum
   value of DSAT (Algo. 1)
4: if conflict then
5:     Choose the vertex with the minimum level
       // vertices having same DSAT
6: else
7:     if conflict then
8:         Choose the vertex with the minimum ID
           // vertices having same Levels
9:     end if
10: end if
11: Let FREE(x) a set of colors unused by the neighbors of
    x
12: if FREE(x) $\subset \{1, 2, ..., k\}$ is not empty then
13:     Color the vertex x with the smallest color in FREE(x)
14: else
15:     Choose a color unused by the cluster of the MPP
        among the least used colors
16: end if
17: if all vertices are colored then
18:     Stop
19: else
20:     Go to 3
21: end if
```

In this way, intra- and inter-cluster connectivity are assured. Moreover, broadcast can be done efficiently. In fact, relay nodes dessiminate messages on all interfaces whereas other nodes dessiminate messages on the interface configured on FC. Therefore, our proposal reduces interference involved by broadcast messages.

V. PERFORMANCE EVALUATION

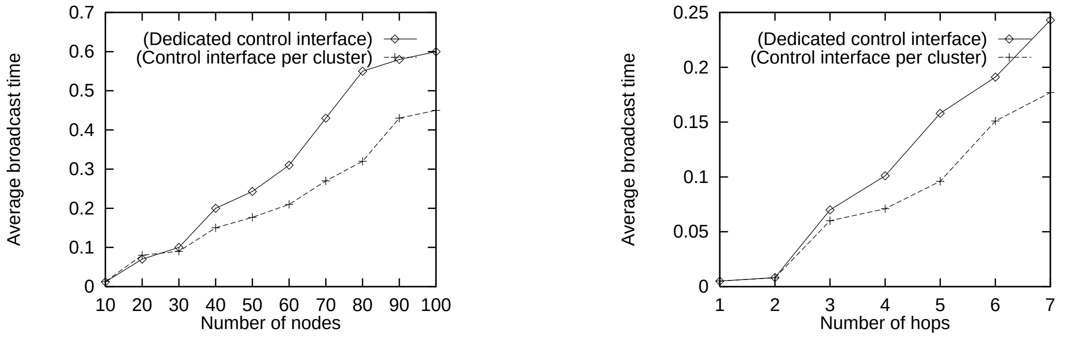
We studied the performance gains of the proposed multichannel WMN architecture based on clustering through extensive Qualnet simulations. The following are the default settings for the simulations. We consider only the mesh network infrastructure. Nodes are uniformly distributed in $1500m * 1500m$ simulation network. Each node is equipped with 2 NICs and the number of channels is set to 3. The ratio between the communication range and the interference range is set to 2. One of nodes is designated as the MPP node and is connected to the wired network. A random



(a) DBC

(b) DCCA

Figure 4. Obtained clusters size with: (a) DBC algorithm, (b) DCCA algorithm



(a) Number of nodes

(b) Number of hops

Figure 5. Average broadcast time as a fuction of: (a) the number of nodes, (b) the number of n hops

Algorithm 3 Relay Interfaces Configuration

```
if it is a relay to a single cluster (case of node $B$) then
    It sets up one of its interfaces on the channel of the FC of the neighbor cluster
else
    if the number of neighbor clusters exceeds the number of its interfaces then
        It lefts one of its interfaces on the Default Channel.
    else
        It configures its interfaces on the channels of neighboring clusters
    end if
end if
```

selected node sends a broadcast message on n hops away (n is a simulation parameter). Figures 4(a) and 4(b) show the maximum and minimum cluster sizes in terms of node members using the DBC and DCCA clustering algorithms respectively. DCCA gives more balanced clusters than DBC thanks to relay nodes migration if there is an unbalance between neighbor cluster sizes. That's way the difference between the maximum and minimum cluster sizes given by DCCA is smaller than the difference expressed by DBC. In dense network (about 100 nodes), there is a constant and low difference between obtained cluster sizes using DCCA and DBC.

Figures 5(a) and 5(b) show the average broadcast time using a dedicated control interface and a control interface per cluster by varying the number of nodes and the number of broadcast hops (n). We observe that DCCA minimize the average broadcast time. In fact, DCCA uses different channels for neighbor clusters. Therefore, nodes broadcast messages using non overlapping channels which minimize interference and collision. The channel used by the dedicated control interface becomes overloaded which induces more time to propagate the broadcast message.

VI. Conclusion and future works

In this paper, we proposed a Density based Clustering algorithm for Channel Allocation (DCCA) in multi-radio and multi-channel wireless mesh network. DCCA uses a density metric and partitions the mesh network infrastructure into balanced clusters. Each cluster is affected a fixed channel FC using a coloration algorithm executed by the MPP. Obtained clusters have different fixed channels to minimize intra- and inter-cluster interference. Performance evaluation has shown that our proposal gives balanced clusters. DCCA also minimize the average time of broadcast messages.

DCCA can be considered as a first step in a dynamic load aware channel assignment mechanism as it assigns a fixed channel per cluster; nodes can configure their pending interfaces according to a dynamic channel allocation. In future, we will use the obtained network topology from DCCA in a joint routing and channel allocation protocol.

VII. Acknowledgments

The work presented in this paper has been partially funded by Qatar Telecom (Qtel).

References

[1] I.F. Akyildiz, X. Wang, and W. Wang, *Wireless mesh networks: a survey*, Computer Networks, Vol. 47, Iss. 4, pp. 445-487, March 2005.

[2] IEEE P802.11s/D8.0, *Draft STANDARD*, March 2009.

[3] J. Crichigno, M.Y. Wub, and W. Shu, *Protocols and architectures for channel assignment in wireless mesh networks, Ad hoc Networks*, Vol. 6, pp. 1051-1077, September 2008.

[4] C. Liu, Z. Liu, Y. Liu, H. Zhao, T. Zhao, and Wei Yan, *A Clustering Based Channel Assignment Algorithm and Routing Metric for Multichannel Wireless Mesh Networks*, In Proc of ISPA, pp. 832-843, August 2007.

[5] S. A. Makram, M. Gunes A. Kchiche, and M. Krebs, *Dynamic Channel Assignment for Wireless Mesh Networks using Clustering*, In Proc of ICN, pp. 539-544, April 2008.

[6] M. Gerla and J.T.C. Tsai, *Multicluster, mobile, multimedia radio network*. Wireless Networks, Vol. 1, N. 3, pp. 255-265, 1995.

[7] A. Raniwala and P. Chiueh, *Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network*, in Proc of IEEE Infcom, pp. 2223-2234, March 2005.

[8] Y. Jane and P. Chong, *A survey of clustering schemes for mobile ad hoc networks*, IEEE Communications Surveys, Vol. 7, pp. 32-48, 2005.

[9] T. Ohta, S. Inoue, and Y. Kakuda, *An Adaptive Multihop Clustering Scheme for Highly Mobile Ad Hoc Networks*, in Proc ISADS, pp. 293-300, April, 2003.

[10] A. D. Amis and R. Prakash, *Load-Balancing Clusters in Wireless Ad Hoc Networks*, in Proc of IEEE ASSET, pp. 25–32, March 2000.

[11] F. Li, S. Zhang, X. Wang, X. Xue, and H. Shen, *Vote-Based Clustering Algorithm in Mobile Ad Hoc Networks*, In Proc of ICNIT, pp. 13-23, February 2004.

[12] N. Mitton and E. Fleury. *Self-organization in multi-hop wireless networks*, In Proc of MedHocNet, June 2004.

[13] M. Kubale, *Graph Colorings*, American Mathematical Society, 2004.

ISBN: 978-1-61208-147-2

Performance Analysis of Pilot Aided OFDMA Systems for Mesh Networks

Jung-Hyun Kim, Jihyung Kim, Kwang Jae Lim, and Dong Seung Kwon
Wireless System Research Department, Internet Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, Korea
{jh.kim06, savant21, kjlim, dskwon}@etri.re.kr

***Abstract*—This paper presents a systematic approach for analyzing the bit error probability of pilot aided orthogonal frequency-division multiple access (OFDMA) systems. A comparative analysis with the conventional pilot pattern schemes, overlapped pilot scheme and interlaced pilot scheme, is developed. The results obtained here can be directly applied to evaluate the performance of OFDMA systems in mesh networks as well.**

***Keywords*-mesh networks; channel estimation; OFDMA;**

I. Introduction

In recent years, orthogonal frequency division multiple access (OFDMA) has been widely adopted for many contemporary wireless systems such as wireless LANs, digital video broadcasting for handheld terminals (DVB-H) [1], Worldwide Interoperability for Microwave Access (WiMAX) [2], and second generation terrestrial digital video broadcasting (DVB-T2) [3] due to its flexibility on resource allocation and robustness to multipath fading channel.

Channel estimation plays an important part in an OFDMA system because it is used to coherently decode the transmission signal and to combine the diversity. The effect of channel estimation for OFDM systems is considered recently for examples in [4], [5], and [6]. For the channel estimation, a known signal so-called pilot is usually employed. The pilot symbols are uniformly inserted into the transmission data stream. These pilot symbols are transmitted through the channel to convey the channel information. Channel estimator at the receiver obtains the channel information from these corrupted pilot symbols and determines the channel response of data symbol region by interpolating the channel response between samples obtained using pilot symbols.

For a single user case, it is obvious that more pilot symbols lead to better performance but with sacrificing in the symbol rate. Therefore the number of pilot symbols is a trade-off between channel estimation accuracy and bandwidth efficiency. However, for multi-user case, it is not obvious that more pilot symbols outperform less pilot symbols due to interference between users. If pilot symbols are corrupted, data fail to be demodulated irrespective of correcting processes such as despreading and decoding. Pilot power boost-up does not help in this case because signal to interference ratio remains the same. The solution is to make the pilot symbols from different users not to collide each other because pilot symbols are relatively stronger than spread data symbols. The channel estimation performance is improved by reducing the number of pilot symbol collisions. However better channel estimation performance dose not always guarantee better data detection performance. The interference of pilot symbol region and the interference of data symbol region are trade-off each other. With this point, we focus on how to design pilot pattern for mesh networks where serious interference exists.

In this paper, our objective is to present an initial approach to design pilot patterns for mesh networks by analyzing the performance of OFDMA system using traditional pilot schemes, overlapped pilot scheme and interlaced pilot scheme, for multi-user channel. The analysis and results can be directly extended to the design of pilot patterns for mesh networks.

The rest of the paper has been organized as follows. Section II contains the system model and pilot aided channel estimation for OFDMA system. Section III provides bit error probability (BEP) analysis for uncoded OFDMA and coded OFDMA systems. Simulation results are in Section IV. Finally, Section V summarizes our main results.

II. System Model

A typical OFDM system is reviewed as follows. In the discrete time domain, the transmitted lth OFDM signal is expressed by

$$x_l[n] = \sum_{k=0}^{N-1} X_l[k] e^{j2\pi kn/N} \tag{1}$$

where $X_l[k]$ is a data signal and n is the time index and k and N are subcarrier index and total number of subcarriers respectively.

The received OFDM signal can be written as

$$\begin{aligned} Y_l[k] &= \sum_{n=0}^{N-1} \left\{ h_l[n] \circledast x_l[n] + z_l[n] \right\} e^{-j2\pi kn/N} \\ &= \sum_{n=0}^{N-1} \left\{ \sum_{m=0}^{\infty} h_l[m] x_l[n-m] + z_l[n] \right\} e^{-j2\pi kn/N} \end{aligned}$$

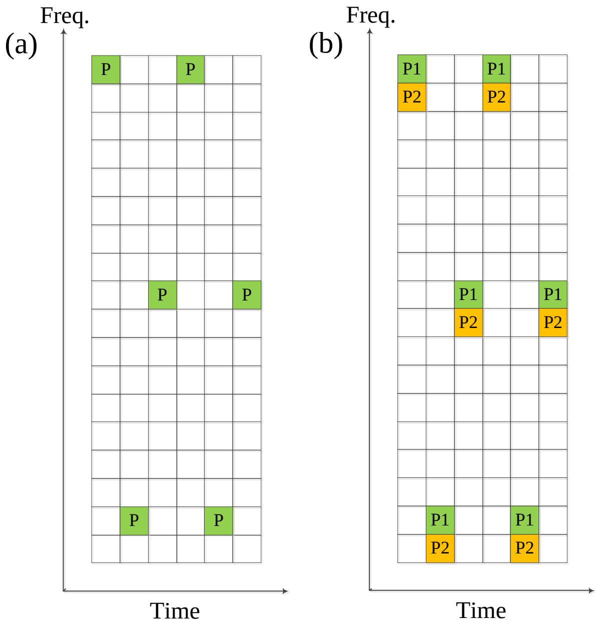


Figure 1. Pilot Patterns for OFDMA systems: (a) Overlapped pilot scheme, (b) Interlaced pilot scheme.

$$= \sum_{n=0}^{K-1} \left\{ \sum_{m=0}^{\infty} h_l[m] \left\{ \frac{1}{N} \sum_{i=0}^{N-1} X_l[i] e^{j2\pi i(n-m)/N} \right\} \right\}$$

$$\cdot\, e^{-j2\pi kn/N} + Z_l[k]$$

$$= H_l[k] \cdot X_l[k] + Z_l[k]. \tag{2}$$

where $\circledast$ is the convolution function, $H_l[k]$ is the channel response of the kth signal and lth OFDM symbol and $Z_l[k]$ is interference and Gaussian noise term.

Based on equation (2), if $H_l[k]$ is known perfectly at the receiver, the maximum-likelihood (ML) receiver would decode the symbol as follows:

$$\hat{X}_l[k] = \frac{Y_l[k]}{H_l[k]} \tag{3}$$

However, in various OFDMA systems (just as many other systems), the channel is not perfectly known. Thus, the channel estimation is necessary and pilot symbols are usually used for the channel estimation.

A. Pilot Aided Channel Estimation

For the channel estimation, a known symbol so-called pilot signal is usually employed. Before the transmission, pilot signals are uniformly inserted into the data stream. Upon receiving the corrupted pilot signals at the receiver, the channel impulse response at pilot locations is estimated. The channel impulse response at data locations can then be obtained through interpolation with the channel impulse response estimated at pilot locations.

We consider the least-squares (LS) estimate for the channel estimation. The lth estimated channel response can be obtained as follows:

$$\hat{H}_l[p] = \frac{Y_l[p]}{X_l[p]} = H_l[p] + \frac{Z_l[p]}{X_l[p]} = H_l[p] + V_l[p] \tag{4}$$

where the subscript p denotes the index of pilot subcarrier, $X_l[p]$ is the pth pilot signal at the lth OFDM symbol and $Y_l[p]$ is the received symbol corresponding to pilot signal $X_l[p]$ and $V_l[p]$ is the channel estimation error term.

For the data location, the channel response can be estimated by taking interpolation between the pilot's channel estimate. There are several forms to interpolate: uniform, spline interpolation, and 2D Wiener interpolation etc. Here, the linear interpolation is used. In the linear interpolation, the data channel estimate is given by

$$\hat{H}_l[d] = \left(1 - \frac{s}{S}\right) \hat{H}_l[p] + \frac{s}{S} \hat{H}_l[p+1] \tag{5}$$

where d denotes the index of data subcarrier, S is the interval between pilot subcarriers and s is the distance between the pth pilot subcarrier and the dth data subcarrier.

Thus, the transmitted data signal at the dth data subcarrier and the lth OFDM symbol can be estimated by

$$\hat{X}_l[d] = \frac{Y_l[d]}{\hat{H}_l[d]}. \tag{6}$$

For two schemes, overlapped pilot scheme and interlaced pilot scheme, the above formula can be re-written as follows:

Overlapped pilot scheme:

$$\hat{X}_l[d] = \frac{Y_l[d]}{\hat{H}_l[d]} = X_l[d] + \frac{Z_l[d]}{\hat{H}_l[d]} - \frac{V_l[d] X_l[d]}{\hat{H}_l[d]} \tag{7}$$

$$\hat{Z}_l[d] = I_l[d] + N_l[d] \tag{8}$$

$$I_l[d] = \sum_{i \in \kappa} H_l^{(i)}[d] X_l^{(i)}[d] \tag{9}$$

where $I_l[d]$ is the interference of dth data signal and lth OFDM symbol, $H_l^{(i)}[d]$ and $X_l^{(i)}[d]$ are the channel response and the data signal of ith user respectively and κ is the set of neighbor users.

Interlaced pilot scheme:

$$\hat{X}_l[d_1] = \frac{Y_l[d_1]}{\hat{H}_l[d_1]} = X_l[d_1] + \frac{Z_l[d_1]}{\hat{H}_l[d_1]} - \frac{V_l[d_1] X_l[d_1]}{\hat{H}_l[d_1]} \tag{10}$$

$$\hat{Z}_l[d_1] = I_l[d_1] + N_l[d_1] \tag{11}$$

$$I_l[d_1] = \sum_{i \in \kappa, i \neq j} H_l^{(i)}[d_1] X_l^{(i)}[d_1] + H_l^{(j)}[p] X_l^{(j)}[p] \tag{12}$$

$$\hat{X}_l[d_2] = \frac{Y_l[d_2]}{\hat{H}_l[d_2]} = X_l[d_2] + \frac{Z_l[d_2]}{\hat{H}_l[d_2]} - \frac{V_l[d_2] X_l[d_2]}{\hat{H}_l[d_2]} \tag{13}$$

$$\hat{Z}_l[d_2] = I_l[d_2] + N_l[d_2] \tag{14}$$

$$I_l[d_2] = \sum_{i \in \kappa} H_l^{(i)}[d_2] X_l^{(i)}[d_2] \tag{15}$$

ISBN: 978-1-61208-147-2

where j is the user index that jth user's pilot signal is interfering.

For the interlaced pilot scheme, we can divide the data signals into two parts. The first part is the region that one of neighbor user's pilot signal and another neighbor users' data signals are interfering. The second part is the region that all of neighbor users' data signals are interfering. The first part gets more interference than second part because the pilot power is boosted for accurate channel estimation. At the above equations, we denote d_1 as the data subcarrier index in the first part and d_2 as the data subcarrier index in the second part.

III. PERFORMANCE ANALYSIS OF OFDMA SYSTEM

A. Uncoded OFDMA System

In this paper, we show the BEP performance analysis of the QPSK because the performance of other constellations, 16-QAM and 64-QAM, can be derived in a similar manner. A QPSK symbol can be written as $X = X_I + iX_Q = |X|e^{i\theta}$, where $X_I,\ X_Q \in \{1, -1\}$.

$$\begin{aligned}
\hat{X} &= \frac{HX + Z}{\hat{H}} \\
&= \frac{1}{|\hat{H}|}\left(|H|e^{i(\angle H - \angle \hat{H})}X + |Z|e^{i(\angle H - \angle \hat{H})}\right) \\
&= \frac{1}{|\hat{H}|}\left(|H|e^{i\psi}X + Z'\right) \\
&= \frac{1}{r_2}\left(r_1 X e^{i\psi} + Z'\right) = \frac{1}{r_2}\left(r_1|X|e^{i(\theta+\psi)} + Z'\right) \\
&= \frac{r_1|X|cos(\theta+\psi) + Z'_I}{r_2} + i\frac{r_1|X|sin(\theta+\psi) + Z'_Q}{r_2} \\
&= \hat{X}_I + i\hat{X}_Q \qquad (16)
\end{aligned}$$

where $r_1 = |H|$, $r_2 = |\hat{H}|$, and $Z' (= Z'_I + iZ'_Q)$ is a zero-mean complex Gaussian random variable with the variance equal to that of Z. If the transmitted data signal is $X = -1 + 1i$, the conditional BEPs are given by

$$\begin{aligned}
&P_b(E|r_1, r_2, \psi, X = -1 + 1i) \\
&= \frac{1}{2}P_{b,I}(E|r_1, r_2, \psi, X = -1 + 1i) \\
&+ \frac{1}{2}P_{b,Q}(E|r_1, r_2, \psi, X = -1 + 1i) \\
&= \frac{1}{2}Pr(\hat{X}_I > 0|X_I = -1) \\
&+ \frac{1}{2}Pr(\hat{X}_Q < 0|X_Q = +1)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{4}Pr(N_I > r_1|X|cos(\psi+\theta)) \\
&+ \frac{1}{4}Pr(-N_Q > r_1|X|sin(\psi+\theta)). \qquad (17)
\end{aligned}$$

For the above equation, each term on the last line is either of the form

$$\begin{aligned}
&Pr[\pm N_I > a|X|r_1 cos(\psi+\theta)] \\
&\qquad = Q\left(\frac{a|X|r_1 cos(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_I^2}}\right) \qquad (18) \\
&Pr[\pm N_Q > a|X|r_1 sin(\psi+\theta)] \\
&\qquad = Q\left(\frac{a|X|r_1 sin(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_I^2}}\right) \qquad (19)
\end{aligned}$$

where $Q(x) \triangleq 1/\sqrt{2\pi}\int_x^\infty e^{-t^2/2}dt$, $a = \pm 1$, $|X| = \sqrt{X_I^2 + X_Q^2} = \sqrt{2}$, $\sigma_N^2 = var(N_I) = var(N_Q) = (N_0/2)$ is the noise variance and σ_I^2 is the interference variance.

We can obtain the overall conditional BEP is

$$\begin{aligned}
P_b(E|r_1, r_2, \psi) &= \sum_{X\in\chi}\frac{1}{4}P_b(E|r_1, r_2, \psi, X) \\
&= \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 cos(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_I^2}}\right) \\
&+ \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 sin(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_I^2}}\right) \qquad (20)
\end{aligned}$$

where χ is the set of QPSK constellations.

Similarly with [4], the joint probability density function (pdf) of (r_1, r_2, ψ) is

$$\begin{aligned}
&p(r_1, r_2, \psi) = \frac{r_1 r_2}{2\pi\sigma_1^2\sigma_2^2(1-\rho^2)}\cdot \\
&exp\left\{-\frac{1}{2(1-\rho^2)}\left[\frac{r_1^2}{\sigma_1^2} + \frac{r_2^2}{\sigma_2^2} - 2\frac{r_1 r_2}{\sigma_1\sigma_2}(\rho_1 cos\psi - \rho_2 sin\psi)\right]\right\} \\
&\qquad (21)
\end{aligned}$$

where $\sigma_1^2 \triangleq \frac{1}{2}E[|H|^2]$, $\sigma_2^2 \triangleq \frac{1}{2}E[|\hat{H}|^2]$, $\rho \triangleq \sqrt{\rho_1^2 + \rho_2^2}$, $\rho_1 \triangleq \frac{\mu_1}{\sigma_1\sigma_2}$, and $\rho_2 \triangleq \frac{\mu_2}{\sigma_1\sigma_2}$ with $\mu_1 = \frac{1}{2}Re\left\{E[\hat{H}H^*]\right\}$ and $\mu_2 = \frac{1}{2}Im\left\{E[\hat{H}H^*]\right\}$.

The BEP is given by

$$\begin{aligned}
P_b(E) = \int_0^\infty\int_0^\infty\int_{-\pi}^{\pi} &P_b(E|r_1, r_2, \psi) \\
&\cdot p(r_1, r_2, \psi)d\psi dr_1 dr_2. \qquad (22)
\end{aligned}$$

Substituting (20) and (21) into (22), we obtain (23).

Assuming that the channel response is stationary during one packet duration and transmitted symbols are mutually uncorrelated, the instantaneous effective signal to interference and noise ratio (SINR) per bit of kth subcarrier is

$$P_b(E) = \frac{1}{2}\left[1 - \frac{1}{2}\frac{\frac{(\rho_1+\rho_2)}{\sqrt{2}}}{\sqrt{1+\frac{1}{2\overline{\gamma}_b}-\frac{(\rho_1-\rho_2)^2}{2}}} - \frac{1}{2}\frac{\frac{(\rho_1-\rho_2)}{\sqrt{2}}}{\sqrt{1+\frac{1}{2\overline{\gamma}_b}-\frac{(\rho_1+\rho_2)^2}{2}}}\right] \quad (23)$$

obtained as

$$\overline{\gamma}_b[k] = \frac{E[|H[k]X[k]|^2]}{(E[|Z[k]|^2 + |V[k]|^2|X[k]|^2])} \quad (24)$$

where $V[k](=\ H\hat{[k]} - H[k])$ is the channel estimation error at kth subcarrier and K denotes the number of bits represented by one symbol. For example, $K = 1$ for BPSK and $K = 2$ for QPSK.

For a reasonably good estimate, $\hat{H} \approx H$ then the average SINR per bit is approximated by

$$\overline{\gamma}_b \approx \frac{E[|HX|^2]}{K(E[|Z|^2])}. \quad (25)$$

From the above equation 25, the average SINR per bit of QPSK is expressed as

$$\overline{\gamma}_b = \frac{2\sigma_1^2}{2(\sigma_N^2 + \sigma_I^2)} \quad (26)$$

where $\sigma_1^2 = \frac{1}{2}E[|H|^2]$, σ_N^2 is the variance of noise and σ_I^2 is the variance of interference.

For two cases, the overlapped pilot case and the interlaced pilot case, above equation (20) and (22) can be re-written as follows:

Overlapped pilot scheme:

$$\begin{aligned} &P_b(E|r_1, r_2, \psi) \\ &= \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 cos(\psi+\theta)}{\sqrt{\sigma_N^2 + \sum_{u\in\kappa}\sigma_{D,u}^2}}\right) \\ &+ \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 sin(\psi+\theta)}{\sqrt{\sigma_N^2 + \sum_{u\in\kappa}\sigma_{D,u}^2}}\right) \quad (27) \end{aligned}$$

$$P_b(E) = \int_0^\infty \int_0^\infty \int_{-\pi}^{\pi} P_b(E|r_1, r_2, \psi) \cdot p(r_1, r_2, \psi)d\psi dr_1 dr_2 \quad (28)$$

where κ is the set of neighbor users and $\sigma_{D,u}^2$ is the variance of interference by uth neighbor user data signal.

Interlaced pilot scheme:

$$\begin{aligned} &P_{b,1}(E|r_1, r_2, \psi) \\ &= \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 cos(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_{P,j}^2 + \sum_{u\in\kappa,u\neq j}\sigma_{D,u}^2}}\right) \\ &+ \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 sin(\psi+\theta)}{\sqrt{\sigma_N^2 + \sigma_{P,j}^2 + \sum_{u\in\kappa,u\neq j}\sigma_{D,u}^2}}\right) \quad (29) \end{aligned}$$

$$P_{b,1}(E) = \int_0^\infty \int_0^\infty \int_{-\pi}^{\pi} P_{b,1}(E|r_1, r_2, \psi) \cdot p(r_1, r_2, \psi)d\psi dr_1 dr_2 \quad (30)$$

$$\begin{aligned} &P_{b,2}(E|r_1, r_2, \psi) \\ &= \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 cos(\psi+\theta)}{\sqrt{\sigma_N^2 + \sum_{u\in\kappa}\sigma_{D,u}^2}}\right) \\ &+ \sum_{X\in\chi}\frac{1}{4}Q\left(\frac{a|X|r_1 sin(\psi+\theta)}{\sqrt{\sigma_N^2 + \sum_{u\in\kappa}\sigma_{D,u}^2}}\right) \quad (31) \end{aligned}$$

$$P_{b,2}(E) = \int_0^\infty \int_0^\infty \int_{-\pi}^{\pi} P_{b,2}(E|r_1, r_2, \psi) \cdot p(r_1, r_2, \psi)d\psi dr_1 dr_2 \quad (32)$$

$$P_b(E) = \frac{P_{b,1}(E) + \epsilon P_{b,2}(E)}{1+\epsilon} \quad (33)$$

where the subscript j is the user index that jth user's pilot is interference and $\sigma_{P,j}^2$ is the variance of interference by jth neighbor user pilot signal, $\epsilon = \epsilon_D/\epsilon_P$, $\epsilon_D(\epsilon_P)$ is the number of signals affected by data(pilot) signals of another users as interference.

B. Coded OFDMA System

Error correcting coding is an essential part of OFDMA systems for wireless communications. OFDMA in a fading environment is almost always used with coding to improve its performance and as such is often referred to as Coded OFDMA or COFDMA. Just as we can introduce time diversity through coding and interleaving in a flat-fading single-carrier system, we can introduce frequency diversity through coding and interleaving across subcarriers in an OFDMA system. With coding and interleaving across subcarriers, the strong subcarriers help the weak ones. Thus overall data detection performance is dependent on the ratio of strong part and weak part.

To compare the performance of COFDMA systems using overlapped pilot scheme and interlaced pilot scheme, we consider the union bound derived in [7], [8]. We use turbo code and BPSK signaling on the Rayleigh fading channel. Then the union bound on the bit-error rate is given by

$$P_b(E) \le \sum_{i=1}^{k} \frac{i}{k} \binom{k}{i} P(i + 2\mu_i) \tag{34}$$

and the probability of an error by maximum likelihood decoding with codeword Hamming weight ω is expressed by

$$P(\omega) \le \frac{1}{2}\left(1 - \sqrt{\frac{R\overline{\gamma}_b}{1 + R\overline{\gamma}_b}}\right) \cdot \left(\frac{1}{1 + R\overline{\gamma}_b}\right)^{\omega - 1} \tag{35}$$

and $\mu_i = r\rho_i$ with

$$\rho_i = \frac{1}{2}\left[1 - \frac{1 - 2i/k}{k} \cdot \frac{1 - (1 - 2i/k)^{k\eta/R}}{1 - (1 - 2i/k)^{\eta/R}}\right] \tag{36}$$

or for large $k (k \to \infty)$:

$$\rho_i = \frac{1}{2}\left[1 - \frac{1 - exp(-2i\eta/R)}{2i\eta/R}\right] \tag{37}$$

where R is the code rate, k is the number of information bits, r is the number of redundant bits of component codes, and η is the *time varying* factor defined in [7].

For the overlapped and interlaced pilot schemes, the average SINR per bit defined by (24) becomes

Overlapped pilot scheme:

$$\overline{\gamma}_b = \frac{2\sigma_1^2}{2\left(\sigma_N^2 + \sum_{u \in \kappa} \sigma_{D,u}^2 + \sigma_V^2 \sigma_{D,i}^2\right)} \tag{38}$$

where σ_V^2 is the variance of channel estimation error term and $\sigma_{D,i}^2$ is the variance of own data signal, κ is the set of neighbor users and $\sigma_{D,u}^2$ is the variance of interference by uth neighbor user data signal.

Interlaced pilot scheme:

$$\overline{\gamma}_{b,1} = \frac{2\sigma_1^2}{2\left(\sigma_N^2 + \sigma_{P,j}^2 + \sum_{u \in \kappa, u \ne j} \sigma_{D,u}^2 + \sigma_V^2 \sigma_{D,i}^2\right)} \tag{39}$$

$$\overline{\gamma}_{b,2} = \frac{2\sigma_1^2}{2\left(\sigma_N^2 + \sum_{u \in \kappa} \sigma_{D,u}^2 + \sigma_V^2 \sigma_{D,i}^2\right)} \tag{40}$$

$$P_b(E) = \frac{P_{b,1}(E) + \epsilon P_{b,2}(E)}{1 + \epsilon} \tag{41}$$

where $\sigma_{P,j}^2$ is the variance of interference by jth neighbor user pilot signal, and $\epsilon = \epsilon_D / \epsilon_P$, $\epsilon_D(\epsilon_P)$ is the number of symbols that affected by data(pilot) symbols of another users as an interference.

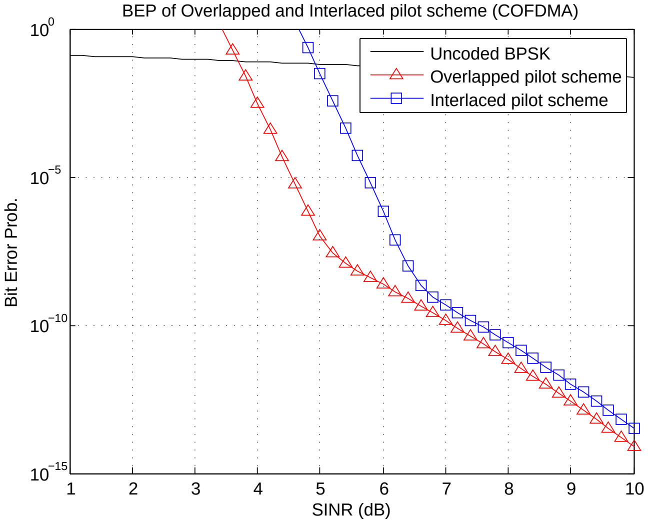


Figure 2. Bit error probability of uncoded BPSK, overlapped pilot scheme, and interlaced pilot scheme for 2 Users, pilot boosting 3dB, pilot space 16 at SNR 15dB.

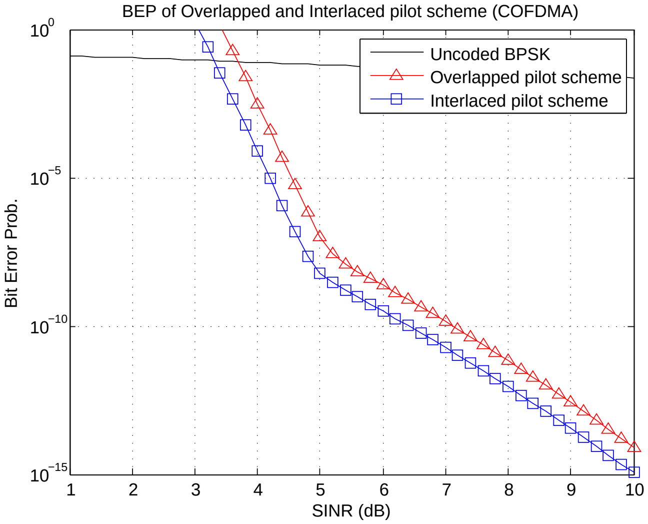


Figure 3. Bit error probability of uncoded BPSK, overlapped pilot scheme, and interlaced pilot scheme for 4 Users, pilot boosting 3dB, pilot space 16 at SNR 15dB.

IV. Simulation Results

For the simulation, we used turbo code of Fig. 2 in [9] and punctured with code rate $1/2$. The LS channel estimation method is used on the Rayleigh fading channel. All simulations are performed in MATLAB program.

Figs. 2 and 3 show the BEP performance of overlapped pilot scheme and interlaced pilot scheme, and uncoded BPSK in [10]. These figures indicate that interlaced pilot scheme outperforms overlapped with some serious interference environments (not always). We can recheck this from Fig. 4.

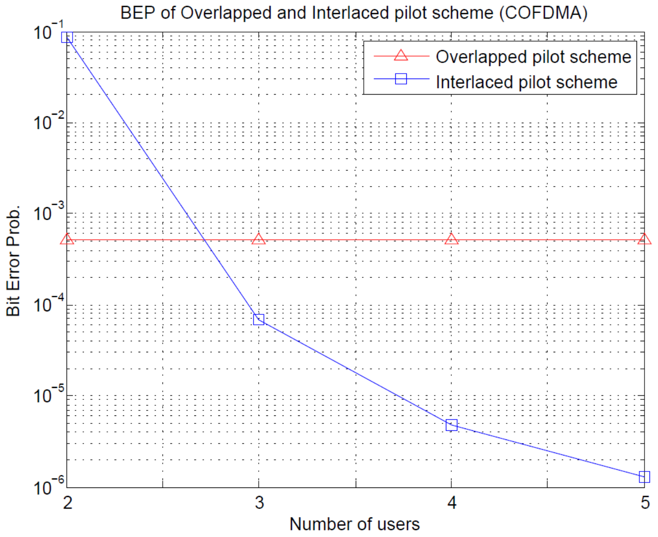


Figure 4. Bit error probability of overlapped pilot scheme and interlaced pilot scheme for various users, pilot boosting 3dB, pilot space 16 at SINR 4dB and SNR 10dB.

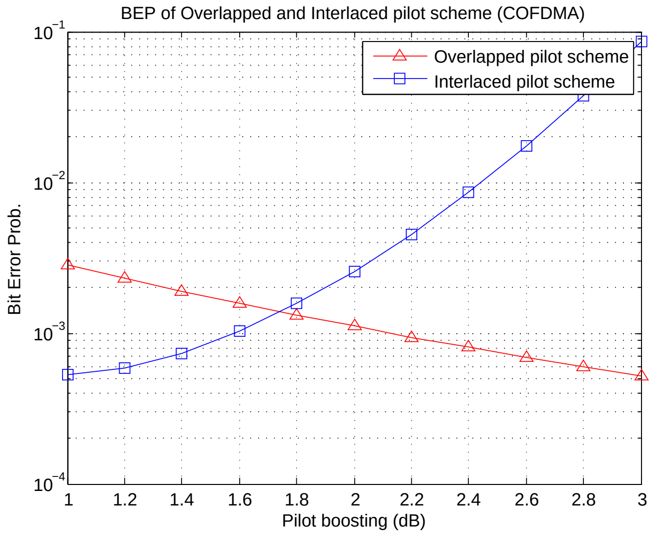


Figure 5. Bit error probability of overlapped pilot scheme and interlaced pilot scheme for 2 Users, various pilot boosting, pilot space 16 at SINR 4dB and SNR 10dB.

The effect of pilot power boosting can be observed from Fig. 5. When the pilot power boosting increases, the BEP performance of interlaced pilot scheme becomes worse. The reason for this is that the pilot power of interference are also increased. For overlapped pilot scheme, the BEP performance is improved as pilot power increase because channel estimation error is decreased with fixed SINR simulation environment.

V. Conclusion and Future Work

In this paper, we analyze the performance of overlapped pilot scheme and interlaced pilot scheme for channel estimation. This comparison is of special interest since the pilot pattern affects the performance of OFDMA systems. Simulation results in terms of BEP corroborate our theoretical analysis.

We notice that interlaced pilot pattern is more suitable for the multi-user networks like mesh network in which serious interference exists. Various pilot design is possible for mesh networks and we expect that our systematic approach and simulation results obtained here can be directly applied to evaluate the performance of pilot aided OFDMA systems for mesh networks.

Acknowledgment

This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)(KCA-2011-10913-04003).

References

[1] ETSI, ”digital video broadcasting (DVB); DVB-H Implementation Guidelines,” TR 102 377 v1.3.1, Mat 2007.

[2] IEEE, ”Air Interface for Fixed and Mobile Broadband Wireless Access Systems,” *IEEE Standard*, P802.16e/D12, February 2005.

[3] ETSI, ”Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2),” *European telecommunication Standard*, EN 302 755 V1.1.1, September 2009.

[4] X. Tang, M.-S. Alouini, and A. J. Goldsmith, ”Effect of channel estimation error on M-QAM BER performance in Rayleigh fading”, *IEEE Trans. Commun.*, vol. 47, No. 12, pp. 1856-1864, December 1999.

[5] H. Cheon and D. Hong, ”Effect of channel estimation error in OFDM-based WLAN”, *IEEE Commun. Lett.*, vol. 6, no. 5, pp. 190-192, May 2002.

[6] T. Hurnanen and J. Poikonen ”Analysis of channel estimation error for OFDM reception over severely time-dispersive channels”, *Proc. IEEE MELECON 2010*, pp. 1315-1319, April 2010.

[7] Y.V. Svirid, ”Weight distributions and bounds for turbo codes,” *European Trans. on Telecommunications*, Vol. 6, No. 5, pp. 543-555, September-October 1995.

[8] E. K. Hall and S. G. Wilson, ”Design and analysis of turbo codes on Rayleigh fading channels,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 160-174, Feb. 1998.

[9] C. Berrou, A. Glavieux, and P. Thitimajshima, ”Near Shannon limit error-correcting coding and decoding: Turbo codes,” *Proc. IEEE Int. Conf. Commun.*, pp. 1064-1070, May 1993.

[10] J. G. Proakis, *Digital Communications* 3rd ed., Englewood Ciffs, NJ: Prentice-Hall, 1995.

A MAC Throughput over Rayleigh Fading Channel in The 802.11a/g/n-based Mobile LAN

Ha Cheol Lee
Dept. of Information and Telecom. Eng.
Yuhan University
Bucheon City, Korea
e-mail: hclee@yuhan.ac.kr

***Abstract* – This paper explores a MAC (Medium Access Control) layer throughput with DCF (Distributed Coordination Function) protocol in the IEEE 802.11a/g/n-based mobile LAN. It is evaluated in Rayleigh fading wireless channel, using theoretical analysis method. The DCF throughput performance is analyzed by using the number of stations with both variable payload size and mobile speed on the condition that fading margin and transmission probability are fixed. In the IEEE 802.11n, A-MSDU (MAC Service Data Unit Aggregation) scheme is considered and number of subframe is used as the variable parameter. It is identified that MAC efficiency of IEEE 802.11n is the best out of four schemes.**

***Keywords* - Mobile LAN, MAC, Throughput, CSMA/CA, DCF, IEEE 802.11a/g/n.**

I. INTRODUCTION

Over the past few years, mobile networks have emerged as a promising approach for future mobile IP applications. With limited frequency resources, designing an effective MAC protocol is a hot challenge. IEEE 802.11b/g/a/n networks are currently the most popular wireless LAN products on the market [1]. The conventional IEEE 802.11b and 802.11g/a specification provide up to 11 and 54 Mbps data rates, respectively. However, the MAC protocol that they are based upon is the same and employs a CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) protocol with binary exponential back-off. IEEE 802.11 DCF is the de facto MAC protocol for wireless LAN because of its simplicity and robustness [2]. Therefore, considerable research efforts have been put on the investigation of the DCF performance over wireless LAN [2][3][4]. With the successful deployment of IEEE 802.11a/b/g wireless LAN and the increasing demand for real-time applications over wireless, the IEEE 802.11n Working Group standardized a new MAC and Physical Layer (PHY) specification to increase the bit rate to be up to 600 Mbps [5]. The throughput performance at the MAC layer can be improved by aggregating several frames before transmission [6]. Frame aggregation not only reduces the transmission time for preamble and frame headers, but also reduces the waiting time during CSMA/CA random backoff period for successive frame transmissions. The frame aggregation can be performed within different sub-layers. In 802.11n, frame aggregation can be performed either by MAC Protocol Data Unit Aggregation (A-MPDU) or MAC Service Data Unit Aggregation (A-MSDU). Although frame aggregation can increase the throughput at the MAC layer under ideal channel conditions, a larger aggregated frame will cause each station to wait longer before its next chance for channel access. Under error-prone channels, corrupting a large aggregated frame may waste a long period of channel time and lead to a lower MAC efficiency [6]. On the other hand, wireless LAN mobile stations that are defined as the stations that access the LAN while in motion are considered in this paper [4]. The previous paper analyzed the IEEE 802.11b/g/n MAC performance for wireless LAN with fixed stations, not for wireless LAN with mobile stations [2][3][7][8]. On the contrary, Xi Yong [4] and Ha Cheol Lee [9] analyzed the MAC performance for IEEE 802.11 wireless LAN with mobile stations, but considered only IEEE 802.11 and 802.11g/a wireless LAN specification. So, this paper extends the previous researches and analyzes the IEEE 802.11n MAC performance for wireless LAN with mobile stations. In other words, we will present the analytical evaluation of saturation throughput with bit errors appearing in the transmitting channel. IEEE 802.11g/a/n PHY and MAC layer focused in this paper are reviewed and frame error rate of mobile wireless channel is derived in Section 2. The DCF saturation throughput is theoretically derived in Section 3 and numerical results are analyzed in Section 4. Finally, it is concluded with Section 5.

II. WIRELESS ACCESS ARCHITECTURE

Fig. 1 shows ad hoc mode operation of wireless access architecture in the 802.11a/g/n-based mobile LAN. The protocols of the various layers are called the protocol stack. The TCP/IP protocol stack consists of five layers: the physical, data link, network, transport and application layers. 802.11 of Fig. 1 means physical layer and data link layer which consists of MAC and LLC (Logical Link Control) sub-layers. And this paper is focused on physical layer and MAC sublayer. An ad hoc network might be formed when people with laptops get together and want to exchange data in the absence of a centralized AP (Access Point).

ISBN: 978-1-61208-147-2

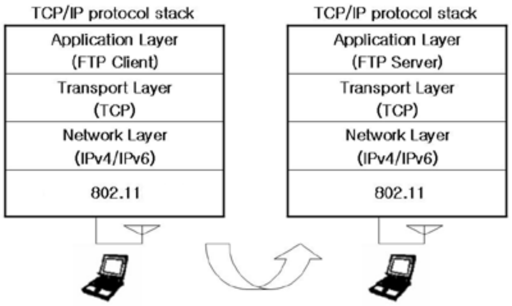
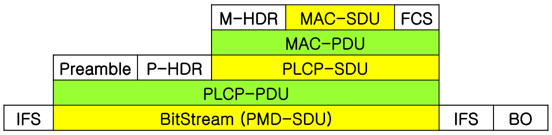


Figure 1. Ad hoc mode operation in the mobile LAN

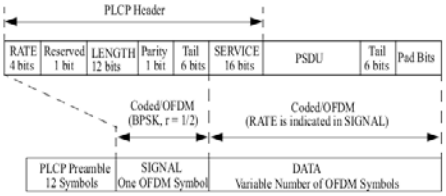
A. 802.11a/g PHY/MAC layer

Fig. 2 shows the 802.11a/g-based physical and MAC layer protocol stack and typical frame structure focused in this paper. When a higher layer pushes a user packet down to the MAC layer as a MAC-SDU (MSDU), the MAC layer header (M-HDR) and trailer (FCS) are added before and after the MSDU, respectively and form a MAC-PDU (MPDU). The PHY (Physical) layer is again divided into a PLCP (Physical Layer Convergence Protocol) sub-layer and a PMD (Physical Medium Dependent) sub-layer. Similarly the PLCP preamble and PLCP header (P-HDR) are attached to the MPDU at the PLCP sub-layer. Different IFS (Inter Frame Space)s are added depending on the type of MPDU.

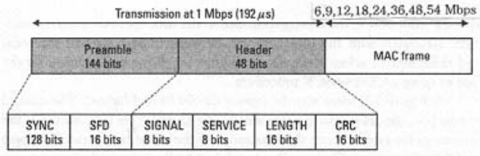
IEEE 802.11a operates in the 5 GHz band and uses OFDM (Multiple-Input Multiple-Output). The achievable data rates are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. 802.11g uses DSSS, OFDM, or both at the 2.4 GHz ISM band to provide high data rates of up to 54 Mbps. 802.11g device can operate with an 802.11b device. Combined use of both DSSS and OFDM is achieved through the provision of four different physical layers. The four different physical layers defined in the 802.11g standards are ERP-DSSS/CCK, ERP-OFDM, ERP-DSSS/PBCC and DSSS-OFDM. The standards that support the highest data rate of 54 Mbps are ERP-OFDM and DSSS-OFDM. ERP-OFDM is a new physical layer in IEEE 802.11g and OFDM is used to provide IEEE 802.11a data rates at the 2.4 GHz band. DSSS-OFDM is a new physical layer that uses a hybrid combination of DSSS and OFDM. The packet physical header is transmitted using DSSS, while the packet payload is transmitted using OFDM. Fig. 3 shows basic access scheme of CSMA/CA mechanism. The SIFS (Short Inter-Frame Space) and the slot time are determined by the physical layer. DIFS (Distributed Inter-Frame Space) is defined based on the above two intervals.



(a) Protocol stack of physical and MAC layer

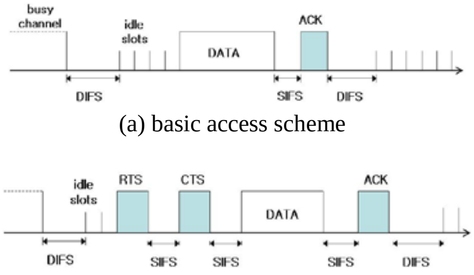


(b) 802.11a and 802.11g ERP-OFDM frame



(c) 802.11g DSSS-OFDM frame

Figure 2. Protocol stack and frame structure of IEEE 802.11a/g/n-based mobile LAN



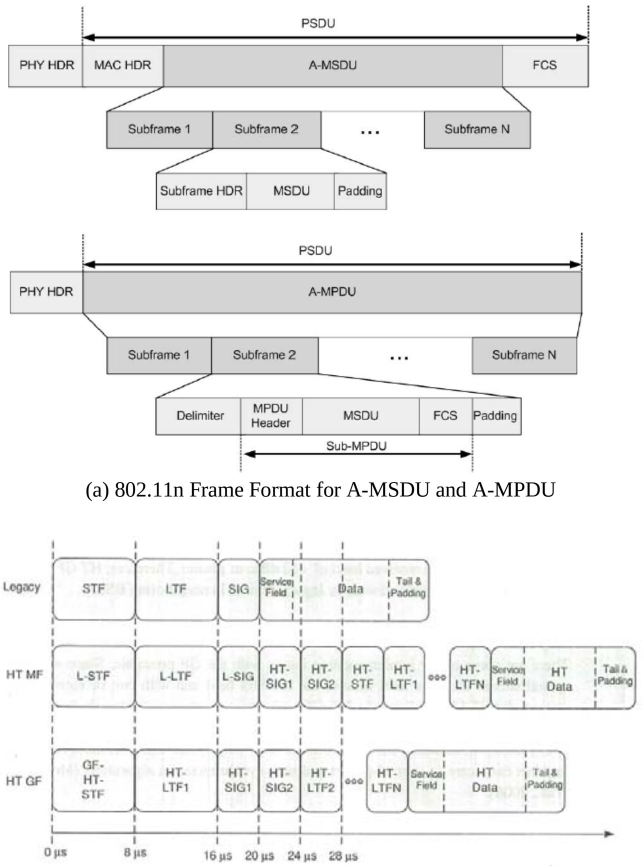
(a) basic access scheme

(b) RTS/CTS scheme

Figure 3. IEEE 802.11g/a DCF channel access mechanism

B. 802.11n PHY/MAC layer

At the MAC layer, 802.11n use several new MAC, including the frame aggregation, block acknowledgement, and bi-directional data transmission. There are two ways to perform frame aggregation at the MAC layer as shown in Fig. 4. The first technique is by concatenating several MAC Service Data Units (MSDUs) to form the data payload of a large MAC Protocol Data Unit (MPDU). The PHY header and MAC header, along with the frame check sequence (FCS), are then appended to form the Physical Service Data Unit (PSDU). This technique is known as A-MSDU. The second technique is called A-MPDU. It begins with each MSDU appending with its own MAC header and FCS to form a sub-MPDU. An MPDU delimiter is then inserted before each sub-MPDU. Padding bits are also inserted so that each sub-MPDU is a multiple of 4 bytes in length, which can facilitate subframe delineation at the receiver. Then, all the sub-MPDUs are concatenated to form a large PSDU. Figure 4 also shows timing of the preamble fields in legacy, MF(Mixed Format) and GF (Green Field). At the PHY layer, 802.11n will use MIMO and OFDM (Orthogonal Frequency Division Multiplexing). It supports up to a transmission rate of 600 Mbps and is backward compatible with 802.11a/b/g. 802.11n provides support for both 2.4 GHz and 5 GHz frequency bands at the same time. 802.11n defines implicit and explicit transmit beamforming (TxBF) methods and space-time block coding (STBC),



(a) 802.11n Frame Format for A-MSDU and A-MPDU

(b) Timing of the preamble fields in legacy, MF and GF

Figure 4. Frame structure of IEEE 802.11n-based mobile LAN

which improves link performance over MIMO with basic spatial-division multiplexing (SDM). It also defines a new optional low density parity check (LDPC) encoding scheme, which provides better coding performance over the basic convolutional code. The possible timing sequences for A-MPDU and A-MSDU in the uni-directional transfer case are shown in Figure 5. If RTS/CTS (Request To Send/Clear To Send) is used, the current transmission sequence of RTS–DATA (Data frame)–ACK (Acknowledgement) only allows the sender to transmit a single data frame. The DATA frame represents either an A-MPDU or an A-MSDU frame. The system time can be broken down into virtual time slots where each slot is the time interval between two consecutive countdown of backoff timers by non-transmitting stations. The 802.11n also specifies a bi-directional data transfer method. In the bi-directional data transfer method, the receiver may request a *reverse* data transmission in the CTS control frame. The sender can then grant a certain medium time for the receiver on the reverse link. The transmission sequence will then become RTS-CTS-DATAf-DATAr-ACK. This facilitates the transmission of some small feedback packets from the receiver and may also enhance the performance of TCP which requires the transmission of TCP ACK segments. Block Acknowledgement (BACK) can be used to replace the previous ACK frame. The BACK can use a bit map to efficiently acknowledge each individual sub-frame within the aggregated frame.

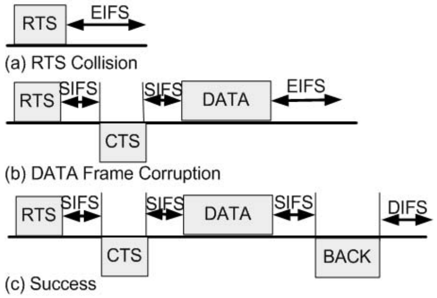


Figure 5. IEEE 802.11n Uni-directional RTS/CTS Access Scheme

C. Frame error rate

Mobile wireless channel is assumed to be flat fading Rayleigh channel with Jake spectrum. The channel is in fading states or inter-fading states by evaluating a certain threshold value of received signal power level. If and only if the whole frame is in inter-fading state, there is the successful frame transmission. If any part of frame is in fading duration, the frame is received in error. In the fading channel fading margin is considered and defined as $\rho = R_{req}/R_{rms}$, Where R_{req} is the required received power level and R_{rms} is the mean received power. Generally, the fading duration and inter-fading duration can be taken to be exponentially distributed for ρ<-10dB. With the above assumptions, let Tpi be the frame duration, then the frame error rate is given by (1) [4].

$$FER = 1 - \frac{Ti}{Ti + T_f} P(t_i > Tpi) \qquad (1)$$

Where, t_i is inter-fading duration and t_f is fading duration. Ti is the mean value of the random variable t_i and T_f is the mean value of the random variable t_f . $P(ti > Tpi)$ is the probability that inter-fading duration lasts longer than Tpi . Since exponential distribution is assumed for t_i , $P(t_i > Tpi) = \exp(-\frac{Tpi}{Ti})$. For Rayleigh fading channel, the average fading duration is given by (2).

$$Ti = \frac{\exp(\rho) - 1}{fd\sqrt{2\pi\rho}} \qquad (2)$$

$T_i + T_f$ is $\frac{1}{N_f}$, where N_f is the level crossing rate, which is given by $fd\sqrt{2\pi\rho}\exp(-\rho)$. f_d is the maximum Doppler frequency and evaluated as $\frac{v}{\lambda}$. v is the mobile speed and λ is wavelength. Frame error rate can be expressed by (3).

$$FER = 1 - \exp(-\rho - f_d \sqrt{2\pi\rho} Tpi) \qquad (3)$$

Equation (3) shows that frame error rate is determined by fading margin, maximum Doppler frequency and frame duration. Since fading margin and maximum Doppler frequency are hard to dynamically control, the only controllable parameter is frame duration to get required frame error rate. For the RTS/CTS access mode, the frame duration T_{pi} is $T_H + T_{RTS} + T_{CTS} + T_{DATA} + T_{ACK}$. T_H is preamble transmission time + PLCP header transmission time + MAC header transmission time. T_{DATA} is MSDU transmission time and T_{ACK} is ACK frame transmission time. T_{RTS} is RTS frame transmission time and T_{CTS} is CTS frame transmission time.

III. DCF THROUGHPUT ANALYSIS

The back-off procedure of the DCF protocol is modeled as a discrete-time, two-dimensional Markov chain. Fig. 4 shows the Bianchi's Markov chain model for the back-off window size [7]. We define $W = CW_{\min}$. Let m, the maximum back-off stage, be such value that $CW_{\max} = 2^m W$. We also define $W_i = 2^i W$, where $i \in (0, m)$ is called the back-off stage. Let $s(t)$ be the stochastic process representing the back-off stage $(0,...,m)$ of the station at time t. p is the probability that a transmission is collided or unsuccessfully executed.

We will present the analytical evaluation of saturation throughput with bit errors appearing in the transmitting channel. The number of stations n is assumed to be fixed and each station always has packets for transmission. In other words, we operate in saturation conditions, the transmission queue of each station is assumed to be always nonempty.

Let S be the normalized system throughput, defined as the fraction of time in which the channel is used to successfully transmit payload bits. P_{tr} is the probability that there is at least one transmission in the considered slot time.

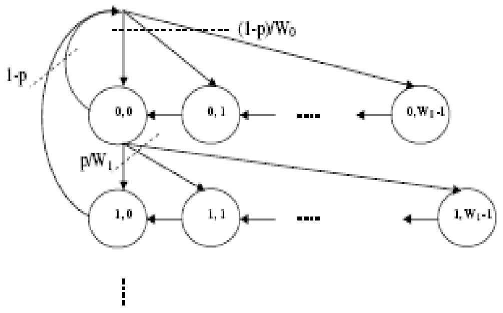


Figure 6. Markov chain model for the backoff window size

Since n stations contend on the channel and each transmits with probability τ, we get

$$P_{tr} = 1 - (1-\tau)^n \qquad (4)$$

Table 1 shows physical and MAC layer parameters of IEEE 802.11a/g/n–based mobile LAN.

TABLE I
IEEE 802.11a/g PARAMETERS

Parameter	Explanation
FER	Frame error rate
τ	Packet transmission probability
N	Number of stations
P	Payload size
T_{RTS}	RTS frame transmission time
T_{CTS}	CTS frame transmission time
T_H	PLCP preamble transmission time + PLCP header transmission time + MAC header transmission time
T_{DATA}	Payload transmission time
T_{ACK}	ACK frame transmission time
T_{BACK}	Block ACK frame transmission time
σ	Slot time
T_{SIFS}	SIFS time
T_{DIFS}	DIFS time
T_{EIFS}	EIFS time
$CW_{\min}$	Minimum backoff window size
$CW_{\max}$	Maximum backoff window size

A. 802.11a/g DCF throughput

Saturation throughput is represented as shown in (5) [9].

$$S = \frac{P_s P_{tr} P}{(1-P_{tr})\sigma + P_{tr} P_s T_s + P_{tr}(1-P_s) T_c} =$$

$$\frac{n\tau(1-\tau)^{n-1}(1-FER)P}{(1-\tau)^n \sigma + n\tau(1-\tau)^{n-1}(1-FER)T_S + [1-(1-\tau)^n]T_C - n\tau(1-\tau)^{n-1}(1-FER)T_C} \qquad (5)$$

P_s is the probability that a transmission successfully occurs on the channel and is given by the probability that exactly one station transmits on the channel, conditioned on the fact that at least one station transmits.

$$P_s = \frac{n\tau(1-\tau)^{n-1}(1-FER)}{P_{tr}} \qquad (6)$$

The average amount of payload information successfully transmitted in a slot time is $P_{tr} P_s P$, since a successful transmission occurs in a slot time with probability $P_{tr} P_s$. The average length of a slot time is readily obtained considering that, with probability $1 - P_{tr}$, the channel is empty, with probability $P_{tr} P_s$ it contains a successful

Copyright (c) IARIA, 2011. ISBN: 978-1-61208-147-2

transmission, and with probability $P_{tr}(1-P_S)$ it contains a collision. Where T_S is the average time the channel is sensed busy because of a successful transmission, and T_C is the average time the channel is sensed busy by each station during a collision or error. σ is the duration of an empty slot time. In the RTS/CTS access scheme, we obtain,

$$T_S = T_{RTS} + T_{CTS} + T_{DATA} + T_{ACK} + T_{DIFS} + 3T_{SIFS} \tag{7}$$

$$T_C = T_{RTS} + T_{EIFS} = T_{RTS} + T_{SIFS} + T_{ACK} + T_{DIFS}$$

B. 802.11n DCF throughput

In the uni-directional case shown in Fig. 5, the saturation throughput can be calculated as follows [8].

$$S = \frac{E_p}{E_t} = \frac{L_p P_{tr} P_s (1-P_e)}{T_{idle}P_{idle} + T_c P_{tr}(1-P_s) + T_e P_{err} + T_{succ}P_{succ}}$$

$$\frac{L_p n\tau(1-\tau)^{n-1}(1-P_e)}{(1-\tau)^n\sigma + n\tau(1-\tau)^{n-1}(1-P_e)T_{succ} + [1-(1-\tau)^n - n\tau(1-\tau)^{n-1}]T_c + n\tau(1-\tau)^{n-1}P_eT_e} \tag{8}$$

where E_p is the number of payload information bits successfully transmitted in a virtual time slot, and E_t is the expected length of a virtual time slot. P_e is the error probability on condition that there is a successful RTS/CTS transmission in the time slot. P_{idle} is the probability of an idle slot. P_s is the probability for a non-collided transmission. P_{err} is the transmission failure probability due to error (no collisions but having transmission errors). P_{succ} is the probability for a successful transmission without collisions and transmission errors. T_{idle} , T_c and T_{succ} are the idle, collision and successful virtual time slot's length. T_e is the virtual time slot length for an error transmission sequence. L_p is the aggregated frame's payload length. In the RTS/CTS scheme, we obtain,

$$T_C = T_{RTS} + T_{EIFS} \tag{9}$$

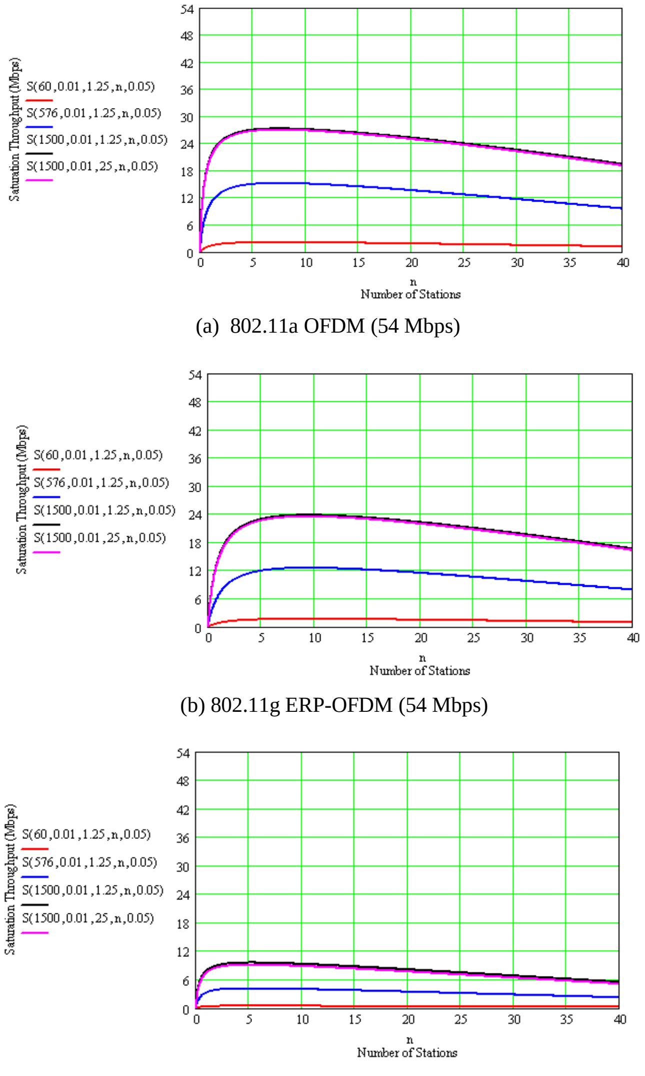
$$T_{succ} = T_{RTS} + T_{CTS} + T_{DATA} + T_{BACK} + 3T_{SIFS} + T_{DIFS}$$

$$T_e = T_{RTS} + T_{CTS} + T_{DATA} + T_{EIFS} + 2T_{SIFS}$$

IV. NUMERICAL RESULTS

This section evaluated DCF throughput of the IEEE 802.11a/g-based mobile LAN. The maximum physical transmission rate of IEEE 802.11a/g is 54 Mbps and that of IEEE 802.11n-based mobile LAN is 600 Mbps. In this paper, bandwidth of 20 MHz, long guard interval and MCS (modulation and coding scheme) index of 15 for two spatial streams are used in Fig. 7. MCS index 15 uses 64-QAM modulation scheme and coding rate of 5/6. So, the physical transmission rate of 130 Mbps is assumed. Also, both ERP-OFDM and DSSS-OFDM standard are only used in this evaluation for the IEEE 802.11g standard because of considering their maximum transmission rate of 54 Mbps [14]. Generally, the three common packets passed down to the MAC layer are 60 bytes (TCP ACK), 576 bytes (typical size for web browsing) and 1,500 bytes (the maximum size for Ethernet) in length. In the IEEE 802.11n-based mobile LAN, the two common packets are only considered and the number of packets aggregated in one MAC frame varies from 1 to 80, which leads to an aggregated frame's payload length (L_p) from 576 and 1,500 bytes to 46.08 and 120 Kbytes. In the Fig. 7(a) ~ Fig. 7(c), the symbol S (P , ρ, ν , n , τ) shows the saturation throughput over error-prone channel according to the number of stations (n) for common packet sizes (P) on the condition that packet transmission probability (τ), mobile velocity (ν) and fading margin (ρ) are fixed. In the Fig. 8(a) and Fig. 8(b), the symbol S (n_s , P, ρ, ν , n , τ) and S (P, n_s , ρ, ν , n , τ) respectively shows the saturation throughput over error-prone channel according to the number of stations (n) and the typical number of packets aggregated in one MAC frame (n_s) for two subframe length on the condition that packet transmission probability (τ), mobile velocity (ν) and fading margin (ρ) are fixed. For example, in the Fig. 7(a), if the number of stations is 7, packet transmission probability is 0.05, packet length is 1,500 and fading margin is 0.01, mobile station with the speed of 1.25 m/s can get the throughput of 27.238 Mbps, whereas mobile station with the speed of 25 m/s can get the throughput of 26.968 Mbps. In the Fig. 8(a), if the number of subframe is 30 and the same conditions mentioned above are applied, mobile station with the speed of 1.25 m/s can get the throughput of 113.511 Mbps with six stations, whereas mobile station with the speed of 25 m/s can get the throughput of 84.607 Mbps. Also, Fig. 7(a~c) and Fig. 8(a) show that the longer frame (or subframe) length is, the higher throughput is. And, for the same frame (or subframe) length, the higher speed is, the lower throughput is. As the results of evaluation, we also know that there is optimum number of stations to maximize saturation throughput under the error-prone channel. Specially, in Fig. 8(b), the number of subframes is considered and it is identified that there is optimum number of subframes to maximize saturation throughput under the error-prone channel. In conclusion, we obtained the fact that there exist an optimal number of stations (or subframes) to maximize the saturation throughput under the error-prone channel. Also, we can identify that the larger payload (or subpayload) size be, the higher saturation throughput be. And if a mobile velocity of station is increased, the throughput is decreased a little. Out of the three different physical layers defined in this analysis with the maximum transmission rate of 54 Mbps, which are 802.11g ERP-OFDM, 802.11g DSSS-OFDM and 802.11a OFDM, the DCF saturation throughput of 802.11a OFDM is the highest.

In the case of 802.11n, because A-MSDU (MAC Service Data Unit Aggregation) scheme is applied, it is identified that MAC efficiency of IEEE 802.11n is better than any other mobile LAN specifications.

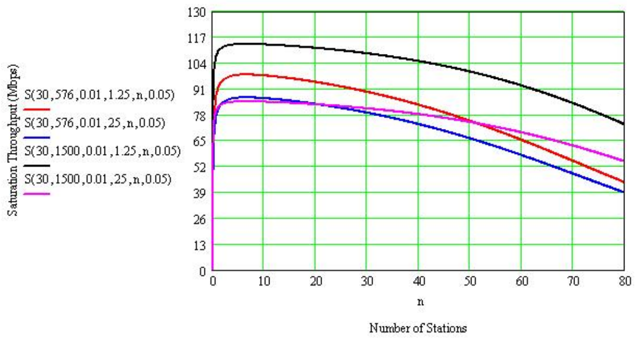


(a) 802.11a OFDM (54 Mbps)

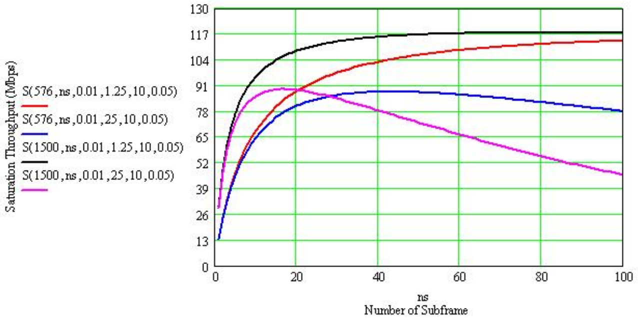
(b) 802.11g ERP-OFDM (54 Mbps)

(c) 802.11g DSSS-OFDM (54 Mbps)

Figure 7. DCF throughput of IEEE 802.11a/g mobile LAN



(a) 802.11n OFDM (130 Mbps, number of stations)



(b) 802.11n OFDM (130 Mbps, number of subframe)

Figure 8. DCF throughput of IEEE 802.11n mobile LAN

V. CONCLUSIONS

This paper explored the saturation throughput performance of DCF protocol in the IEEE 802.11a/g/n-based mobile LAN under the error-prone channel. IEEE 802.11a and IEEE 802.11g have the same maximum transmission rate of 54 Mbps, but the DCF saturation throughput of 802.11a is higher than that of 802.11g. Of the two 802.11g standards, DCF saturation throughput of 802.11g ERP-OFDM is higher than that of 802.11g DSSS-OFDM. We are recognizing that a 802.11n-based device can operate with a 802.11 legacy devices, but 802.11a-based device does not operate with a 802.11b/g-based device. So either constructing 802.11a/n-based mobile LAN or constructing 802.11g/n-based mobile LAN have to be considered for interoperability.

REFERENCES

[1] Upkar Varshney, "The Status and Future of 802.11-based Wireless LANs," IEEE Computer, Jun. 2003, pp. 102-105.

[2] Zuoyin Tang, Zongkai Yang, Jianhua He, and Yanwei Liu, “Impact of Bit Errors on the Performance of DCF for Wireless LAN,” *IEEE*, 2002, pp. 529-533.

[3] Dimitris Vassis, George Kormentzas, Angelos Rouskas, and llias Maglogiannis, “The IEEE 802.11g Standard for High data rate WLANs,” *IEEE Network*, May/Jun. 2005, pp. 21-26.

[4] Xi Yong, Wei Ji Bo, and Zhuang Zhao Wen, “Throughput Analysis of IEEE 802.11 DCF over Correlated Fading Channel in MANET,” IEEE, 2005, pp. 694-697.

[5] IEEE Std 802.11n 2009 “ Part11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput,” Oct. 2009.

[6] D.Skordoulis, Q.Ni, H.Chen,A.P.Stephens, C.Liu, and A.Jamalipour, “IEEE 802.11n MAC Frame Aggregation Mechanisms for Next-Generation High-Throughput WLANs,” *IEEE Wireless Communications*, vol.15, Feb. 2008, pp. 40-47.

[7] Giuseppe Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function,” *IEEE Journal on Selected Areas in Communications*, Vol. 18, No.3, pp. 535-547, Mar. 2000.

[8] Y. Lin and V. W. S. Wong, “Frame Aggregation and Optimal Frame Size Adaptation for IEEE 802.11n WLANs,” in *Proc. IEEE GLOBECOM*, San Francisco, CA, Nov. 2006, pp. 1–6.

[9] Ha Cheol Lee, "A MAC Layer Throughput over Error-Free and Error-Prone Channel in The 802.11a/g-based Mobile LAN," MICC 2009, Dec. 2009

Performance Evaluation of Handover Policies in Mobile Heterogenous Networks

Mircea Axente-Stan
Telecommunication Department
Universitatea Politehnica Bucuresti (UPB)
Bucharest, Romania
mastan@elcom.pub.ro

Eugen Bocorci
Telecommunication Department
Universitatea Politehnica Bucuresti (UPB)
Bucharest, Romania
eugen.borcoci@elcom.pub.ro

Abstract— **The increasingly ubiquitous deployment of wireless networks together with efforts to complete the standardization of Media Independent Handover (MIH) will support the 4G (Fourth Generation) vision in offering seamless access and an integrated network-of-networks (i.e. all IP network). In the same time, the handover process complexity will increase in next generations of wireless networks, creating the need for augmented knowledge about context, as well as more flexibility in managing the resources. The last two objectives cannot be addressed using the current static (hardcoded) mechanisms for handover initialization, decision and execution; therefore, a new policy-based architecture is proposed to assure the required level of adaptability and flexibility and to respond to user and network dynamics.**

Keywords-mobile heterogenous networks, vertical handover, MIH, context aware, policy-based management.

I. INTRODUCTION

Next generation of mobile wireless technologies, defined in cellular terminology as *fourth generation* (*4G*), must support targets peak data rates of about 100 Mb/s for highly mobile access (at speeds of up to 250 km/h), and 1 Gb/s for low mobility (pedestrian speeds or fixed) access.

Besides meeting the above date rates, the 4G networks will consist of heterogeneous access networks providing a broad range of services to subscribers. In such an environment, vertical handover between various access technologies will be a common operation; therefore finding ways to handle optimally the network dynamics and complexity will be a challenging task requiring a great level of flexibility, scalability and adaptability.

Currently, there are many efforts devoted to interworking, seamless mobility techniques on integrated all-IP network and on self-managing virtual resource overlay that can span across heterogeneous networks, support service mobility, quality of service and reliability. In Europe, as part of ICT FP7 (Information & Communication Technologies Seventh Framework Programme), the relevant studies have been carried out in several projects such as WINNER (Wireless World Initiative New Radio) [12], HURRICANE (Handovers for ubiquitous and optimal broadband connectivity among Cooperative networking environments) [11] and AUTOI (Autonomic Internet) [10].

Moreover, System Architecture Evolution (SAE) in 3rd Generation Partnership Project (3GPP) [1] dedicates itself to cope with interworking and handover signalling, which aim at solving seamless mobility between different packet switched domains belonging to existing and evolving 3GPP access networks and non-3GPP access networks.

One-step in offering seamless handover is made by the standardization of Media Independent Handover Services (MIH) [13]. This standard tries to provide link layer intelligence and other related information to upper layers to optimize the handovers between heterogeneous media. The standard focuses primarily on the decision (or pre-execution) phase of handovers, but only reducing the handover latency is aiming to have little or no perceptible disruption of the users' applications, is not enough. However, there still exist several limitations in MIH architecture as follows:

- In MIH, the handover process typically based on measurements and triggers supplied from link layers, which disregards the influence of the application and user context information on mobility management.
- The network information provided by MIH lacks of flexibility since only less dynamic and static information derived.

To cope with network complexity and to be able to offer service continuity (e.g., context transfer, resource reservation), only using the facilities offer by MIH is not enough, therefore an aggregated view of user, network, mobility and service context should be taking in account during handover process. This augmented knowledge about context, as well as flexibility in managing the resources cannot be achieved without a certain level of automation and abstraction. To achieve above-mentioned requirements the solution proposed in this paper combines the use of policy-based management framework and context aware information to manage the handover process.

The reminder of this paper is organized as follows. Section II gives an overview of policy-based handover systems and shows possible network architectures. Section III gives a brief description of the proposed policy-based management architecture. Section IV describe the primary scenarios, validate the policies and evaluate the solution through simulation. Finally, in Section V we conclude our work and discuss possible directions of future work.

II. BACKGROUND AND RELATED WORK

The idea of handover control, which is not based only on the received signal strength (RSS), has been heavily studied in the past years. Most of the papers propose either a

Copyright (c) IARIA, 2011. ISBN: 978-1-61208-147-2

framework or taxonomy, but they are lack on implementing the framework in a simulation or testbed environment.

Paper written by Kassar et al. [16] make a summary of the policy-based handover solutions as follows:

- Decision function-based strategies (DF) [7, 8];
- User-centric strategies (UC) [2, 20];
- Multiple attributes decision strategies (MAD) [6]
- Fuzzy logic and neural networks based strategies (FL/NN) [21]
- Context-aware strategies (CA) [17, 22].

The solutions using DF strategies seem to be more flexible for the use of vertical handover policies but less efficient on this aspect for real-time applications. The use of FL and MAD algorithms gives the best and accurate solution with regrouping all the decision factors, but they are weak in flexibility. CA strategies try to ensure a high flexibility as important as a high efficiency facing a heterogeneous environment, but this comes with a drawback related to reactivity in case of real time applications.

To overcome the limitations of the above-mentioned solutions and to be able to validate the results in a simulation environment, we define a new policy-based architecture to assure the required level of adaptability and flexibility and to respond to user and network dynamics. Our solution combines the context-aware (CA) and multiple attribute decision strategies (MAD) using the MIH protocol to convey the policies and context information.

III. CONTEX-AWARE HANDOVER MANAGEMENT

In this section, we describe the proposed high-level architecture to manage handover process using policy-based management framework and context aware information.

Policy-based management defines high-level objectives of network, and system management based on a set of policies that can be enforced in the network. The policies are a set of pre-defined rules (when a set of conditions are fulfilled then some defined actions will be triggered) that determine allocation and control of network resources. These conditions and actions can be established by the network administration with parameters that determine when the policies are to be implemented in the network.

Policy-based management provides a high-abstraction view of a network to its operator, as it does not need to consider details concerning the size or complexity of the network [18].

The architecture combines the design principles of MIH and PBM (Policy-Based Management) frameworks. On one hand, it uses the services of MIH to exchange the policy information and to facilitate a distributed way of taking the handover decision and on other hand makes use of PCIM framework [3] to offer a high level of flexibility and adaptability of the system.

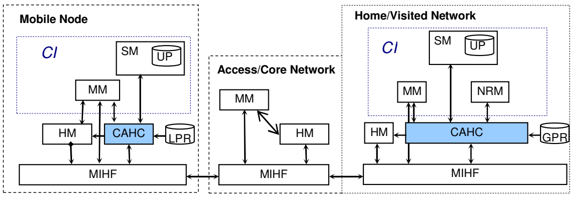


Figure 1. System architecture

As seen in fig. 1 the main functional entities of handover management architecture are Context Aware Handover Controller (CAHC) and Handover Manager (HM). These two functional entities are either assisted or makes use of the services offered by mobility management protocols (L3MP – e.g. MIP or SIP), context information (CI) triggers and policies stored in policy repository (PR) which are either local (MN side) or global (network side).

A. *Context Aware Handover Controller*

Context Aware Handover Controller (CAHC) plays the role of Policy Decision Point (PDP) in policy-based management framework and MIH User (MIHU) in MIH framework. It uses the rules stored in Policy Repository (PR) to take decisions and to enforce the required actions further to HM. Policy Repository can be located at MN level using local rules stored in Local Policy Repository (LPR) or at network level and in that case the repository store the global rules, therefore is called Global Policy Repository (GPR).

CAHC it is able to extract relevant information from received triggers and if need, to query for additional information from external entities, aggregate the information and then take decision. In order to receive triggers the CAHC must first register to external entities specifying the type and number of events that should be received. The context information (CI) can convey user, service, and network or mobility information.

In this paper, we will not develop further the protocol used to convey the context information or the message exchange between CAHC and external functional entities. We will try to summarize the requirements for such kind of protocol. First, the protocol must support a registering mechanism, which will allow specifying types and numbers of the events that CAHC it is willing to receive later. Secondly, the protocol must support on-demand query for context information without prior registration. This will facilitate a better usage of the network resources and will increase the scalability of the solution. Last but not least the protocol should convey context information to/from remote entities (e.g. terminal to network) in order to allow distributed decision (e.g. network controlled and terminal assisted).

For an integrated approach and to achieve the above-mentioned requirements the MIH protocol can be re-used, extending the Media Independent Event Service (MIES) and Media Independent Information Service (MIIS).

B. Handover Manager

Handover Manager (HM) identifies the Policy Enforcement Point (PEP) in policy-based management framework and MIHU in MIH framework. HM implements decisions coming for CAHC execute the proper handover procedure and release the right resources.

C. Policy information exchange

In general, the policy information exchange is decoupled from the handover management process. As presented in the fig. 2, depending on capabilities of the CAHC, policy information can be pulled by the MN or can be pushed by the CAHC from the network side. In the second case prior to any interrogation, the MN must first register to CAHC.

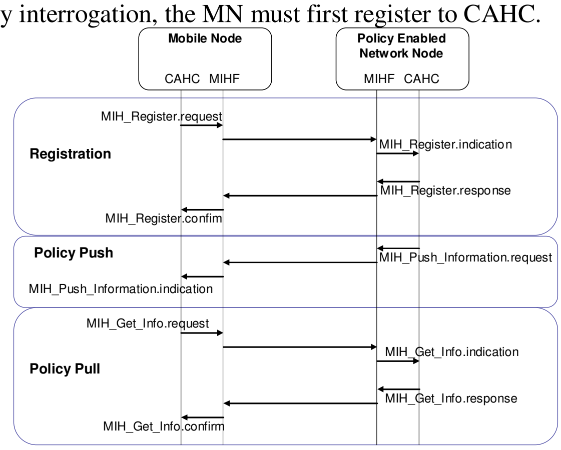


Figure 2. Registration process

From the architecture point of view, it is possible to coordinate the decision-making on network side or on the terminal side, but the later one can lead to scalability issues [9].

In this section we will present the main steps encountered during handover process from initialization to execution in case of network controlled handover.

The handover process may be conditioned by the measurements and triggers offered by different sources, such as the link layer or application layer, or network context from network side. There are two methods to obtain the required trigger events and the related information for MIH users (CAHC or upper layers).

The first method is registration mechanism. The registration mechanism enables an endpoint to register its interest in particular event type. After registration, the MIH users may specify a list of events for which they wish to receive notifications from the MIH Function. MIH users may specify additional parameters during the registration process in order to control the behaviour of the Event Service.

The second method is query/response mechanism. The query/response mechanism is to retrieve the available information. CAHC may send a request to Mobility Manager (MM), Service Manager (SM), Network Resource Manager (NRM) or User Profile (UP) server with additional parameters. In this case, the prior registration is unnecessary. The corresponding response includes either application/user information in client side or the static or dynamic information in network side.

There are four categories of context information (CI) that can be received or queried:

- User Context (UC) – user context information identify, either static user information (billing preferences, energy, security level) or dynamic user information (location). User Context (UC) information can be triggered or queried from User Profile server (UP) placed on network side or can be stored at MN level.
- Service Context (SC) – service context information can be triggered or queried from Service Manager (SM), see the Fig. 1. The SM controls and authorizes the requests coming from local applications in case of SM placed on Mobile Node (MN) or globally for application requests managed at the network level. When a new service request is received by the SM, or there is a change of an already establish service, the SM can generate a trigger to notify the CAHC with regard service characteristics (QoS parameters, service type). The SM performs service level management: planning, provisioning, offering and fulfilment of the services required for end-to-end QoS-enabled content deliver.
- Network Context (NC) – network context information is provided by Network Resource Manager (NRM) and can specify static (cost, throughput, network type, power consumption, topology information) or dynamic (network load, latency, packet loss, jitter, and congestion level) network related information. The NRM it is a functional entity placed on the network side, which is responsible for managing the resources at network level (see the Fig. 1).
- Mobility Context (MC) – mobility context information is provided by Mobility Manager (MM), see the Fig. 1. Mobility Manager stores the current status provided by MIH protocol and higher-level mobility protocols (L3MP), such as MIP (Mobile IP) [4, 5] or SIP (Session Initiation Protocol) [15, 16].

The vertical handover can be divided in three steps: handover *initiation*, *decision* and *execution*. During the handover initiation step, the mobile nodes equipped with multiple interfaces have to determine which networks can be used and the services available in each network. In the handover decision step, the mobile node determines which network it should connect. The decision may depend on various parameters, which define the aggregated user context. Finally, during the handover execution step, the connections need to be re-routed from the existing network to the new network in a seamless manner. This step also includes the authentication and authorization, and the transfer of user’s context information.

D. Handover Initialisation

In this phase, the CAHC is starting to gather more information about the current context:

- query MM for available networks and mobility protocols supported;
- query user profile server (UP) for user preferences (cost, network type) and user location;
- query the NRM about network load, type, throughput and other useful information;

When all the information, which defines the user context, is present, the aggregate information is used to match policies stored in policy repository (PR).

The process can be further optimized with a caching mechanism at CAHC level, which can be combined with registering mechanism or with query/response interrogation. Each context information will have associated a specific lifetime depending on category of information cached (e.g. topology vs. network load).

E. Handover Decision

In this phase, the aggregated information will match a policy from the PR list and based on the user context. The aim is to find an appropriate network. The reference network and other candidate access networks will be ranked according to certain policy. Finally, the one before the reference network is selected as the target network. Therefore, both user experiences and resource efficiency could be guaranteed in this mechanism.

Then current network sends handover preparation request to target network, with the information of MN capability and context. The target network will reserve the resources for MN in order to reduce interruption time and to preserve service continuity.

F. Handover Execution

After link layer handover is finished, higher layer mobility protocol (MIP or SIP) signalling is exchanged over the radio network. When the handover execution is complete, the resources from previous network are released.

IV. Evaluation of Policy Handover Strategies

Architecture validation is done implementing the complete framework of the ns-2 [19] simulation environment for both vertical handover (Wi-Fi to Wimax) and horizontal handover (Wimax to Wimax). The energy model is part of core functionalities of ns-2 and the 802.21 functionality is incorporated in ns-2 as add-on modules developed by the National Institute of Standards and Technology (NIST) based on 802.21 (draft 3)[23]. Starting from the basic handover types, we define a set of six primary scenarios used to handle mobility (MIP or MIP+MIH). Finally, the primary scenarios are validated for different simulation parameters (speed, signal strength, advertising interval).

A. Scenarios

In defining the scenarios we took into account the *mobility type* – horizontal (between different cells of the same technology - HHO) and vertical (between different types of technologies - VHO), *protocol(s)* used for mobility management – MIP or MIP with MIH support and the usage of the *multiple interfaces* in case of vertical handover.

We evaluate the scenarios using user velocity, RSS threshold and routing advertising interval:

1) HHO-MIP

In this scenario, the user is performing a horizontal handover and the decision is based on signal strength and mechanism offered by the MIP for move detection.

2) HHO-MIP-MIH

In this scenario, the user is performing a horizontal handover and the decision based on triggers offered by MIH (link down or link going down) and mechanism offered by the MIP for move detection.

3) VHO-MIP-single interface

In this scenario, the user is performing a vertical handover, the decision based on signal strength and mechanisms offered by the MIP for move detection and use one interface at a certain time.

4) VHO-MIP-multiple interfaces

In this scenario, the user is performing a vertical handover, the decision is based on signal strength and mechanism offered by the MIP for move detection, but during handover preparation and execution uses both interfaces (e.g. Wi-Fi and Wimax).

5) VHO-MIP-MIH-single interface

In this scenario the user is performing an vertical handover and the decision is based on triggers offered by MIH (link down or link going down) and mechanism offered by the MIP for move detection and use one interface at a certain time (either Wi-Fi or Wimax).

6) VHO-MIP-MIH-multiple interfeces

In this scenario the user is performing an vertical handover and the decision is based on triggers offered by MIH (link down or link going down) and mechanism offered by the MIP for move detection, but during handover preparation and execution use both interfaces (e.g. Wi-Fi and Wimax).

B. Simulation results

In this section, we present the results obtained by simulating the primary scenarios. For each scenario, we measure (i) system packet loss, (ii) handover time (latency), (iii) bandwidth efficiency and (iv) energy consumption.

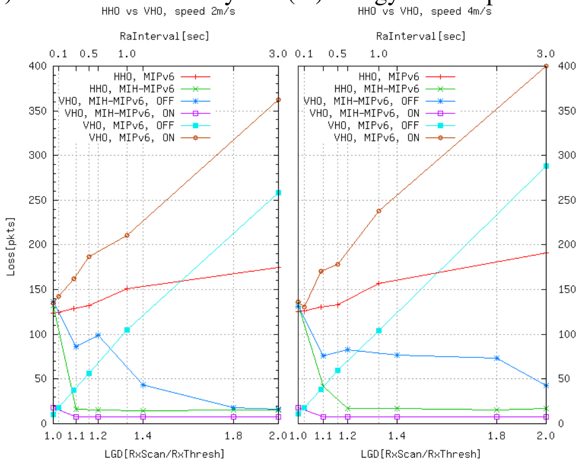


Figure 3. Packet loss

Fig. 3 shows the packet loss in the system. The packet loss in the system is the difference between the total number of packets sent by the CN and the number of the packets received by MN (including both Wimax and Wi-Fi interfaces).

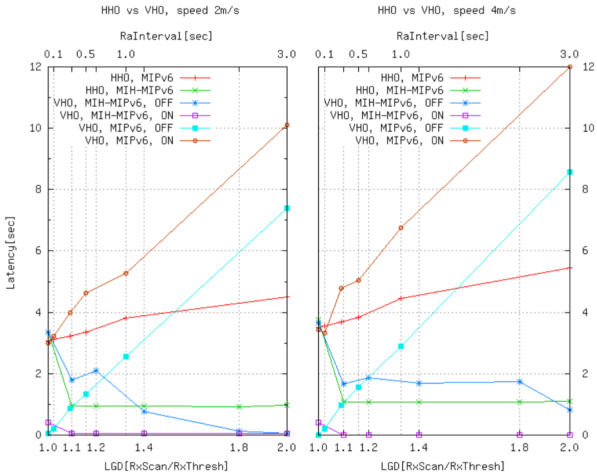


Figure 4. Handover time (latency)

Fig. 4 shows the evolution of HO time from old to new access network. The HO time is the amount of time that elapses between an interface is becoming *DOWN*, it is sending a MIPv6 *Redirect Request* to the CN and is receiving the correspondent *Redirect Ack* from the CN.

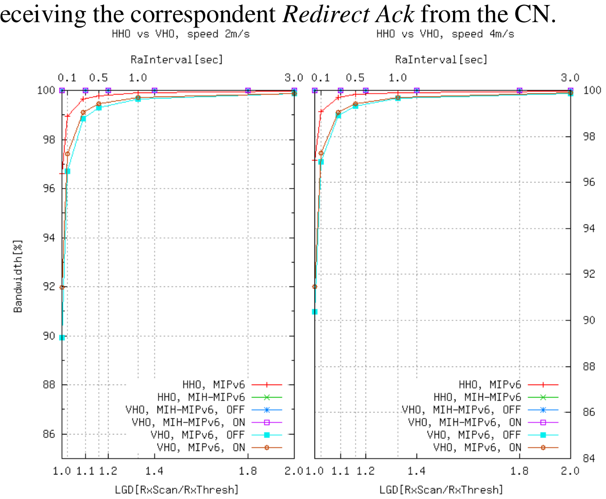


Figure 5. Bandwidth efficiency

Fig. 5 presents the efficiency in utilizing the bandwidth available in the system. The bandwidth efficiency measure the ratio of bandwidth used for application traffic and total bandwidth (application and signalling). The application traffic represented by video stream of UDP packets sent at a constant bit rate (CBR) of 409.6 kbps. The data is used o exchange control information in between functional elements (MIH message and/or ND messages).

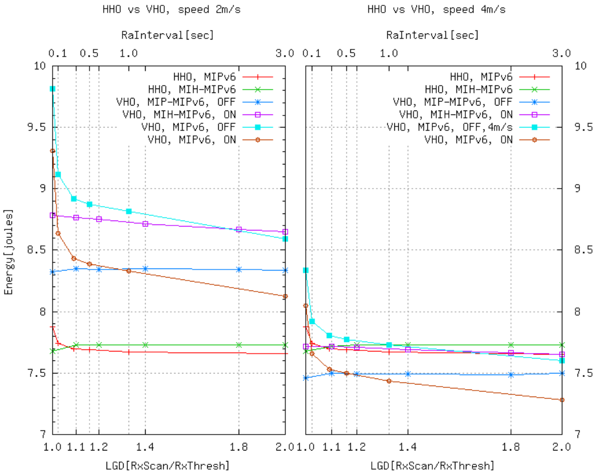


Figure 6. Energy consumption

Fig. 6 shows the energy consumption variation. The energy consumption it is another way of expressing the battery lifetime of the mobile node and it measure the amount of energy consumed during simulation time.

C. *Policy enforcement*

In order, validate the architecture we define two simple policies. First policy (Policy 1) specifies that during the handover the number of packet loss is lower or equal to 20 packets. Second policy (Policy 2) is defined based on energy consumption and it requires that energy consumed during 100 sec (simulation time) to be lower or equal with 8 joules.

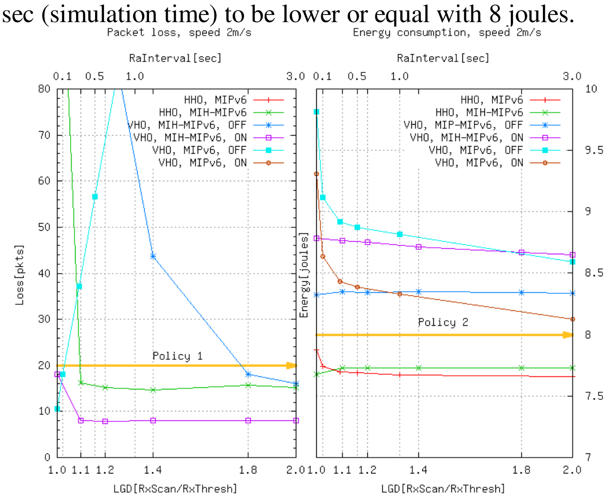


Figure 7. Policies enforcement for the same user context

When we apply the two policies for the same user context (e.g. same user velocity), the solution space will be different in terms of possible handover types, mobility protocols, usage of multiple interfaces or signal strengths (see Fig. 7).

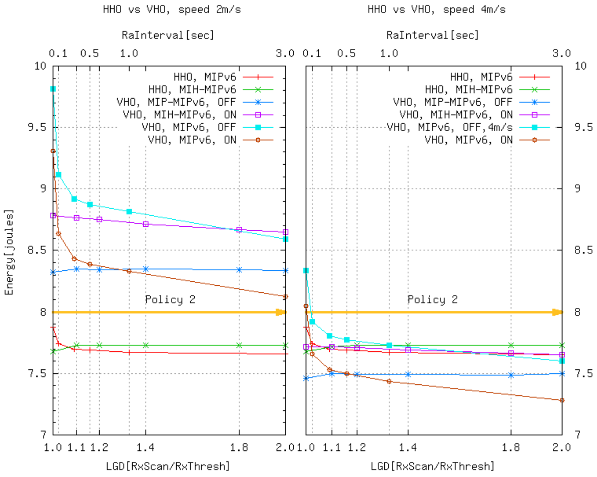


Figure 8. The same policy in two user's contexts

Similarly, if we apply the same policy in different user contexts (see Fig. 8) the solution space will depend on the same parameters, but with other results.

Combining more than one metrics in one policy (e.g. Policy 3 = (Policy 1 && Policy 2)) will narrow the solution space for a specific user context.

The use MAD strategies gives the best and accurate solution by regrouping all the decision factors (e.g. solution space), but they are weak in flexibility. Combining the decision factors with CA strategies will ensure a high flexibility and a high efficiency facing a heterogeneous environment.

V. CONCLUSON AND FUTURED WORK

In this paper, we provided an integrated architecture for handling the handover process in next generation of wireless networks using policy-based management and aggregated context information.

Handover process complexity will require an augmented knowledge about context, as well as more flexibility in managing the resources. Previous objectives cannot addressed using the current static (hardcoded) mechanisms for handover initialization, decision and execution, therefore a policy-based architecture is proposed to assure the required level of adaptability and flexibility and to respond to user and network dynamics.

Integrating the proposed architecture in a policy based management framework together with MIH services can further add flexibility to the network management and allow operators to make abstraction of the concrete wireless technology existent in the access network.

The details of the protocol messages used convey policy information and its behaviour are under investigation. In addition, the design considerations related to coordinated decision on network and terminal side, caching mechanism and context information lifetime are open to further research, pending for a formal validation based on a prototypical implementation and performance evaluation.

REFERENCES

[1] 3rd Generation Project Partnership, available at http://www.3gpp.org.

[2] A. Calvagna and G. D. Modica, "A user-centric analysis of vertical handovers," in WMASH '04: Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots, (Philadelphia, PA, USA), pp. 137–146, October 2004.

[3] B. Moore, E. Ellesson, J. Strassner, and A.Westerinen. Policy Core Information Model. Internet RFC rfc3060.txt, Work in Progress, February 2001.

[4] C. Perkins., "Mobility Support in IPv6", IETF RFC 3220, Jan. 2002.

[5] D. Johnson et al., Mobility Support in IPv4, IETF RFC 3775, Jun.2004

[6] E. Stevens-Navarro and V. W. Wong, "Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks," in IEEE Vehicular Technology Conference (VTC-Spring), May 2006.

[7] F. Zhu and J. McNair, "Optimizations for Vertical Handoff Decision Algorithms," in Wireless Communications and Networking Conference (WCNC), pp. 867–872, March 2004.

[8] H. J. Wang, R. H. Katz, and J. Giese, "Policy-Enabled Handoffs Across Heterogeneous Wireless Networks," in WMCSA, (New Orleans, LA, USA), February 1999.

[9] H. Marques, J. Ribeiro, P. Marques, and J. Rodriguez, Simulation of 802.21 Handovers Using ns-2, Journal of Computer Systems, Networks, and Communications, Volume 2010 (2010), Article ID 794749, 11 pages

[10] ICT ATOI proiect, available at http://www.ict-atoi.eu.

[11] ICT HURRICANE project, available at http://www.ict-hurricane.eu.

[12] ICT WINNER project, available at http://www.winner.org.

[13] IEEE Std 802.21-2008, IEEE Standard for Local and metropolitan area networks - Part 21: Media Independent Handover Services, January 2009.

[14] J. Rosenberg et al., SIP: Session Initiation Protocol,IETF RFC 3261, June 2002.

[15] M. Handley and V. Jacobson, SDP: Session Description Protocol,IETF RFC 4566, July 2006.

[16] M. Kassar, B. Kervella, and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," Comput. Commun., vol. 31, pp. 2607–2620, June 2008

[17] M. Kassar, B. Kervella, and G. Pujolle, "Architecture of an Intelligent Inter-system HandoverManagement Scheme," in Future generation communication and networking (fgcn 2007), (Jeju, Korea), pp. 332–337, December 2007.

[18] Mircea Axente-Stan, Eugen Borcoci, Integrating MPLS and Policy Based Management Technologies in Mobile Environment. EuroNGI Workshop 2004: 166-175.

[19] ns-2, http://www.isi.edu/nsnam/ns.

[20] O. Ormond, J. Murphy, and G.-M. Muntean, "Utility-based Intelligent Network Selection in Beyond 3G Systems," in IEEE International Conference on Communications, 2006. ICC '06, (Istanbul, Turkey), pp. 1831–1836, June 2006.

[21] Q. Guo, J. Zhu, and X. Xu, "An adaptive multi-crit eria vertical handoff decision algorithm for radio heterogeneous network," in IEEE International Conference on Communications, 2005. ICC 2005, (Istanbul, Turkey), pp. 2769–2773, May 2005.

[22] Q. Wei, K. Farkas, C. Prehofer, P. Mendes, and B. Plattner, "Context-aware handover using active network technology," Comput. Netw., vol. 50, no. 15, pp. 2855–2872, 2006.

[23] NIST ns-2 add-on modules for 802.21 (draft 3) support, http://www.nist.gov/itl/antd/emntg/ssm_tools.cfm

Design and Implementation of a Cooperative Protocol for Extending Coverage in Wireless Mesh Networks

Andres Cabrera-Lozoya, Fernando Cerdan, Sergio Lujan, Diego Garcia-Sanchez
Department of Information and Communications Technologies
Universidad Politécnica de Cartagena, UPCT
Plaza del Hospital, 1, 30202, Cartagena, SPAIN
{andres.cabrera, fernando.cerdan, sergio.lujan, diego.gsanchez}@upct.es

***Abstract*—Wireless mesh networks (WMNs) have attracted great attention in the last few years because of their advantages over traditional wireless networks. WMNs can be seen as a mixture of ad hoc and infrastructure networks, with all the underlying benefits of such hybrid architecture. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops through intermediate nodes which not only boost the signal, but cooperatively act extending the network coverage and even forwarding decisions based on their knowledge about the network itself. This paper presents the main design and implementation aspects of a cooperative protocol that allows the coverage extension in these WMNs. It also provides a power saving mechanism for nodes which mainly operate as gateways by simply relaying data from or to neighbouring nodes. Simulation results show that the introduction of the protocol drastically increases the volume of carried traffic on the network due to its coverage extension capabilities. They also show that the power saving mechanism works properly, thus introducing key configuration parameters in the design of WMNs.**

Keywords - wireless mesh network; coverage extension; power saving mechanism; performance evaluation

I. INTRODUCTION

Recent economic emergence of wireless communication and portable computing devices together with the advances in communication infrastructures have produced the rapid growth of today mobile wireless networks. This has led to an exponential growth of cellular networks based on a combination of wired and wireless technologies.

However, the interest of scientific and industrial communities in the telecommunications field has recently changed towards the development of mobile networks with no fixed infrastructure. In this sense, ad hoc networks have become the cutting-edge technology in wireless communications. Indeed, these networks constitute the first step towards providing cost effective and dynamic high-bandwidth solutions over specific coverage areas. They allow the interconnection of the network nodes directly using wireless transceivers (usually through *multihop* paths) without the existence of a fixed infrastructure. This is a very distinctive feature of ad hoc networks compared to traditional wireless networks like cellular or wireless local area networks (WLANs), where nodes communicate with each other only through fixed stations.

On the other hand, WMNs have attracted great attention in the last few years since they can be seen as a mixture of ad hoc and infrastructure networks. Basically, they are infrastructure networks which allow the connection of devices out of the range of the access points (APs) through a direct connection with any node or device that is directly or indirectly within the coverage range of one of those APs. However, it seems that nowadays one of the main bottlenecks of this technology deals with the power consumption of the nodes and the communication’s energetic efficiency. In this sense, every effort to develop energy-efficient protocols should be considered as an important contribution to the whole technology development.

This paper is structured as follows: Section II presents some related work in the area, enumerating several interesting experiences and investigations conducted in the last years in this field. In this regard, they will be classified depending on their scope and main aims, giving in turn a brief overview of the state of the art in this area of research.

Next, Section III presents the proposed application scenario for the protocol itself. Assumptions referring to the hardware involved and its mode of operation will be presented here. Advantages of using an ad hoc / infrastructure hybrid network will also be discussed.

Section IV deals with the formal specification of the protocol, where the key aspects of its operation will be explained from a qualitative point of view.

Section V presents the simulation’s scenario and shows the results obtained during this process. In this section, the highlights of the protocol and its main advantages will be discussed from a quantitative point of view.

Finally, conclusions and future work are presented.

II. RELATED WORK

In the last few years, mesh networks have become an area of ongoing research due to its nature and potential applications. Nowadays, it is extremely easy to find mesh applications in many different scenarios [1, 2].

Thus, although mesh technology depends on other underlying technologies for the establishment of the network backhaul, these networks can indeed be deployed over almost any existing wireless technology, e.g. WiFi (for LAN environments), WiMAX (for MAN environments), etc. and once done, even coexist [3]. That said, it certainly seems that wireless mesh networks are going to be ubiquitous and a line of intense research in a very near future.

Moreover, although the concept of hybrid cellular / ad hoc network is not new [4, 5], it represents an interesting line of action at present due to its nice features.

Indeed, we are steadily witnessing progress in routing techniques and protocols based on channel allocation and transfer rates in wireless mesh networks such as [6, 7], amongst many others. We are also witnessing that the implementation of proactive, reactive and hybrid protocols for optimizing these network traffics is also attracting great attention, like in [8], but despite of all, there are several aspects dealing with the optimization of the available resources in terms of power saving and energy consumption in these WMNs which currently pose a challenge to the researchers.

Thus, although even the most complex problems of mesh topology such as those related to the conduct of the nodes [9] or the network security itself [10] are progressively being addressed, energy consumption issues constitute a bottleneck for this technology at the moment.

The work presented in this paper attempts to shed some light on the development of coverage extension mesh protocols with power saving features which, in fact, is an area of intense research at the moment.

III. The Proposed Scenario

This section describes the network which has been used to extensively test the protocol. In this sense, every hardware aspect relevant to the protocol implementation will be explained below.

A. *Initial scenario*

In this initial stage we will define the *server* as a single computer or access point that will continuously monitor all the network performance. This topology clearly corresponds to a centrally managed network scheme. This single device will count on a wireless interface and will be responsible for creating and maintaining a point to multipoint network in infrastructure mode to connect the various nodes in the network. All traffic generated by the nodes will always be directed to this server machine, making it possible to count and therefore process all data transactions between every node in the network.

Also, we will define the *nodes* or *mobile terminals* as portable devices powered, in any case, by batteries. Therefore, they will feature low processing power and limited energy resources. Each node will have two pre-configured wireless interfaces, using one for direct connection to the server (in infrastructure mode) and the other for direct communication with the rest of nodes through a multi-node topology, also called ad hoc network.

By default, all nodes will try to communicate through the network in infrastructure mode, using the ad hoc network only for communication with terminals outside the coverage area of the network server (see Fig. 1 below).

In this specific scenario, *covered nodes* (nodes within the coverage area of the server) will use the network in infrastructure mode to send / receive data, and *virtually-covered nodes* (nodes within the coverage range of another node which in turn has direct or indirect access *(through another node)* to the server) will use their ad hoc interface to communicate with their accessible nodes in each case.

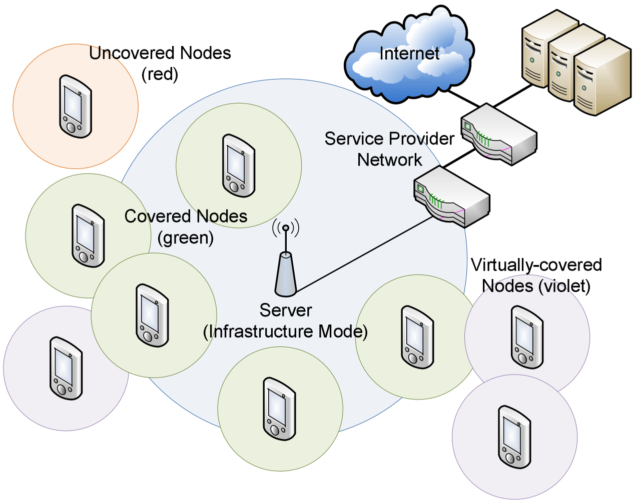


Figure 1. Schema of the application scenario.

Obviously, if a covered node had to communicate with a virtually-covered one, it would use its ad hoc interface since the virtually-covered node is not directly connected to the server and thus not accessible through the former's infrastructure mode interface.

Now, if we see Fig. 1 again, we can make a nice graphical analogy with *Set Theory* to give an idea of the extended coverage of the network using this protocol. Thus, if we considered each circular coverage range of Fig. 1 as a *set*, we could say that the network coverage corresponds to the size of the *union set* of them all (excepting, of course, the range of the uncovered nodes).

Finally, for this scenario to be implemented correctly, it will be assumed that all nodes will be motivated to act selflessly [9], so users are deemed to cooperate with the proper working of the protocol.

B. *Advantages of a mixed network (ad hoc / infrastructure)*

The main reason for testing the protocol over a mixed network is that infrastructure and ad hoc networks are complementary.

Ad hoc networks are almost always exclusively composed of mobile devices while infrastructure networks have at least one device which is not battery-powered. This simple fact makes the nature and operation of both types of networks very different, each one with its own characteristics. With this idea in mind, we can emphasize once again that the fact of using a mixed architecture brings several advantages:

On the one hand, the base station (in infrastructure networks) is usually powered from the mains. This fact allows that the server itself has a greater processing capacity, very powerful wireless interfaces (for signal transmission) and increased sensitivity at reception. In addition, infrastructure mode networks avoid the massive transmissions of data that usually take place in multihopping networks, which can even saturate them when various peripheral nodes generate a large amount of traffic. This advantage comes out from having a really extensive coverage area provided by the base station. In such a situation, connections are made directly to the server, thus obtaining a satisfactory communication between nodes with only two hops in the majority of generated traffic (with the server acting as the only gateway).

On the other hand, the integration of an ad hoc network with the previous infrastructure network can provide several interesting advantages too. For example, multihop functionality provided by ad hoc networks can be used to increase the operating range of a conventional infrastructure network when it is not possible to make a direct connection to the base station through adjacent nodes, i.e., instead of requiring a direct connection between the nodes and the base station, it is possible to reach the server through different paths using multihop compatible wireless devices. In this way, we get to cover "*black spots*" which would be inaccessible in a common infrastructure mode network.

IV. Protocol Baseline

After having highlighted the advantages of using a mixed network, we will proceed to define the main features of the protocol from a formal point of view.

A. *Protocol specification*

When a mobile terminal generates a message to any other node of the network there are two possibilities to send data:

- If the source node is within the coverage range of the server, the mobile terminal will send the message directly to the server in infrastructure mode, with the subsequent receipt confirmation by the latter.
- However, if the mobile terminal has no direct connection to the server, it will broadcast the message through its ad hoc interface.

Any message generated and sent by a mobile terminal will always reach the server: when a node receives any message from any other node, it will act as a gateway in any case, so it will not parse the data. Then, it will simply broadcast the message to make it reach the server. This fact has several relevant consequences: on the one hand, we can guarantee that all data messages will be properly quantified and monitored by the server since they reach it. We can also assure that nodes will not incur any overhead because of this ad hoc operation: every data transmission through this network will be broadcasted without any processing since the server is the only device capable of delivering data to nodes. On the other hand, we find that broadcasting will cause nodes to use a greater amount of resources than nodes which might analyze and accept the message as their own, preventing its spread towards the server.

There may be a multitude of mobile terminals acting as gateways between the server and the source and destination nodes, not only one.

When the server has a message to some node, the former will broadcast a test message to see if the desired node is within its coverage area (in both networks, if necessary):

- If so, it will selectively send the message to the recipient node, the latter replying with a receipt confirmation message.
- On the contrary, if the destination node is not within the coverage area, the server will search the recipient using the ad hoc network created by the nodes through multihop technique. There are two possibilities:
  - If the recipient is located, the server will selectively send data using multihop mechanism.
  - If the recipient is not located, the server will store data for a later retry.

Two approaches can be taken to send messages when the server needs to use the multihop network to reach nodes that are inaccessible through direct connection:

- When locating the mobile terminal, its routing path could be refreshed and stored inside the data message as it goes through the network towards the server. Then, the server could send the data message using that very route. This option allows further optimization of energy resources, but communications turn unstable because, e.g., if any of the gateway nodes used to route the message moves significantly, the transaction will be unsuccessful. This situation would cause the delivery mechanism of the protocol to perform all the steps above to try to transmit the message again. This is a common problem in networks with high mobility, e.g., when mobile terminals are inside vehicles.
- Another option consists of ignoring the route path to the recipient node when locating the mobile terminal. In this case, the reply message will only indicate the presence or absence of connectivity with the destination node. This *broadcasting option* results in a waste of energy by the nodes because the message delivery mechanism will affect a larger number of devices. However, we can ensure with a very high probability that recipient nodes will receive the messages, regardless of the type of network we are working with, since it is a more flexible protocol to network changes (*due to its broadcasting nature*). The cooperative protocol presented in this paper uses this type of location because *in this case* the reliability takes precedence over energy efficiency. Furthermore, in such mesh network environments reliability, self-reconfiguration and self-healing features must be predominant.

Moreover, the protocol includes a power saving mechanism to limit the energy consumption of the nodes which consistently act as gateways relaying messages from other nodes to / from the server (indirect messages) due to its possible location near the border of the coverage area of the fixed network. This mechanism leaves them in idle state during a time interval which is proportional to a *tiredness index* parameter (described in Section V below), that consists of a counter which increases each time the node relays an indirect message.

ISBN: 978-1-61208-147-2

The interaction between the server and the destination node in each case will be independent of the emission mechanism used by the source node.

Fig. 2 below presents the protocol's high-level flowchart.

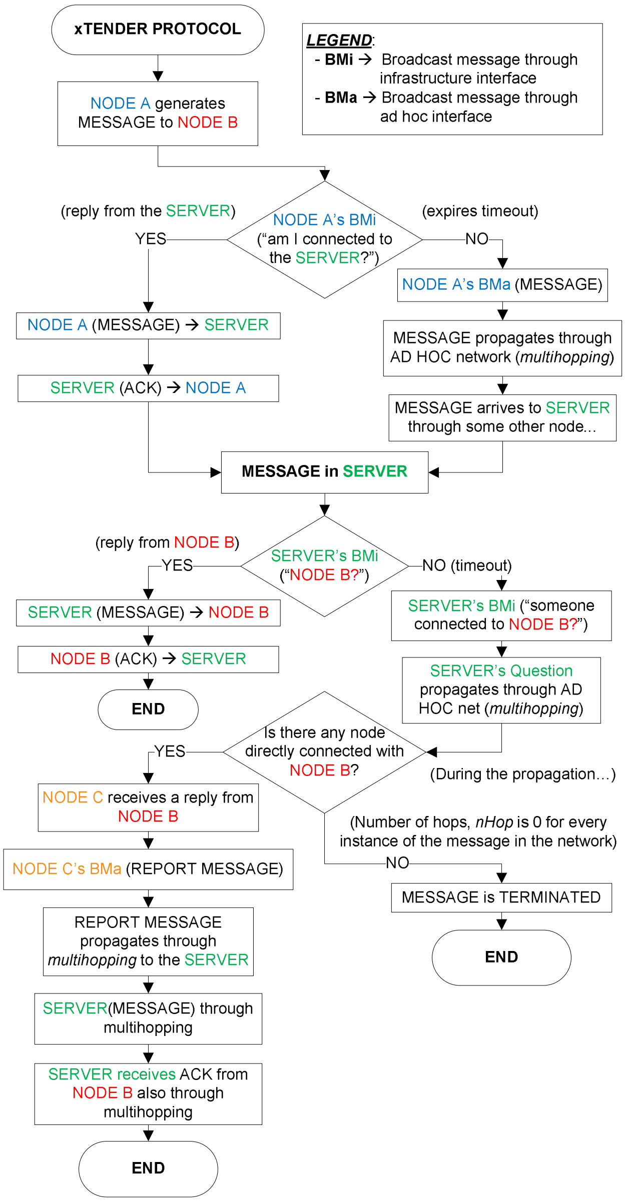

xTENDER PROTOCOL
LEGEND:
- BMi → Broadcast message through infrastructure interface
- BMa → Broadcast message through ad hoc interface
NODE A generates MESSAGE to NODE B
(reply from the SERVER)
YES
NODE A's BMi ("am I connected to the SERVER?")
(expires timeout)
NO
NODE A's BMa (MESSAGE)
NODE A (MESSAGE) → SERVER
MESSAGE propagates through AD HOC network (multihopping)
SERVER (ACK) → NODE A
MESSAGE arrives to SERVER through some other node...
MESSAGE in SERVER
(reply from NODE B)
YES
SERVER's BMi ("NODE B?")
NO (timeout)
SERVER (MESSAGE) → NODE B
SERVER's BMi ("someone connected to NODE B?")
NODE B (ACK) → SERVER
SERVER's Question propagates through AD HOC net (multihopping)
END
YES
Is there any node directly connected with NODE B?
(During the propagation…)
NODE C receives a reply from NODE B
(Number of hops, nHop is 0 for every instance of the message in the network)
NO
NODE C's BMa (REPORT MESSAGE)
MESSAGE is TERMINATED
REPORT MESSAGE propagates through multihopping to the SERVER
END
SERVER(MESSAGE) through multihopping
SERVER receives ACK from NODE B also through multihopping
END

Figure 2. Protocol's high-level flowchart.

Finally, two mechanisms are used to prevent the network collapse:

- Each message will carry a hop counter which will limit the number of hops that a given message can perform.
- Each message will carry a unique identifier (*ID*) that will prevent the same message to be relayed more than once by any mobile terminal, thus avoiding infinite loops.

B. *Message definitions*

After having described the protocol behaviour, we now proceed to define the various messages to be used along with their features.

We could initially make a clear division towards their classification: on the one hand, we can find those messages that are transmitted directly between any node and the server. They will be called *direct messages*. On the other hand, we find those messages that are propagated through the network using multihopping techniques, for communication between terminals. They will be then called *indirect messages*. At this point, it is obvious that every time a terminal receives one of these messages, it will relay it using broadcasting except when the node itself is the destination terminal.

There are different types of messages within each family, and we can differentiate them through the various functions they perform, namely:

- Data transmission
- Receipt confirmation
- Node search

Direct messages (DM) can be sent by the server and the nodes. They count, at best, on the next fields: type of message (*ToM*), source address (*Src*), destination address (*Dst*), unique identifier (*ID*), data length (*Len*) and the data itself (*Data*). Table I below presents each message subtype along with it specific fields:

TABLE I. DIRECT MESSAGES FIELDS

Message subtype	*ToM*	*Src*	*Dst*	*ID*	*Len*	*Data*
Data Transmission	*	*	*	*	*	*
Receipt Confirmation	*	*	*	*		
Node search	*		*			

Indirect messages (IM) are only used for communication between terminals. IMs will only be sent by the server, through multihopping techniques. Thus, if the server receives one of these messages, it will delete it immediately. The fields present in IMs are the same as those of DMs, plus one: the number of hops (*nHop*), indicating in each case the maximum number of hops remaining for a message before it is discarded by the nodes, as a saturation control action. In this way, this mechanism is very similar to the well-known TTL (*Time To Live*) field to be found on many communications systems an protocols. Table II below presents each IM subtype along with it specific fields:

TABLE II. INDIRECT MESSAGES FIELDS

Message subtype	*ToM*	*Src*	*Dst*	*ID*	*Len*	*Data*	*nHop*
Data Transmission	*	*	*	*	*	*	*
Receipt Confirmation	*	*	*	*			*
Node search	*		*				*

In such a scenario, null signalling overhead is always guaranteed since nodes communicate with each other through a flooding mechanism, as explained above in Section IV.A, i.e., using broadcasted messages. Thus, datagrams (see Fig.3 below) do not need extra fields for nodes to know the routing path in each case (which would cause a signalling overhead, affecting the whole system's performance) since they do not even need to process any special headers to transmit or receive messages within the ad hoc network: they simply broadcast every message just as it arrives.

ToM (1)	Src (4)	Dst (4)	ID (4)	Len (4)	Data (variable)	nHop (1)

Figure 3. Detailed datagram structure (numbers in parentheses represent the lenght in bytes of each field).

V. Performance Evaluation

The protocol was developed, implemented and validated using the Specification and Description Language (SDL) and the SDL Tools branch (including SDL Simulator and SDL Validator). The proposed simulation scenario is described in Section III above.

A. Simulation Parameters

Some representative environment variables were externally declared from the outset in order to analyze the protocol behaviour and its efficiency. They were used to launch parametric simulations in which the variation of one or more of them made possible to obtain interesting simulation results. Below are presented each of the variables of the simulation environment along with its meaning and function:

- *nNodes*. It indicates the number of nodes present in a given simulation.
- *nConnec*. It sets the maximum number of connections between nodes, and therefore, in the boundary case, the maximum number of nodes that would be within the coverage area of every single node.
- *PG*. It represents the probability of a node to generate a message to another at a given point in time.
- *PC*. It represents the probability of a direct connection between the nodes and the server.
- *maxHop*. It defines the maximum number of hops that a message can perform when using multihopping technique.
- *indTired*. It indicates the increment of the tiredness rate of each node each time an indirect message is relayed.
- *Sleep*. It indicates how long a node will remain inactive / idle due to its *tiredness*.

(These two last variables are related to the power saving mechanism implemented in the protocol for the nodes).

B. Simulation Results

All the results shown in this section arise from the execution of a number of simulations with the same parameters, so that every result is consistent with the average of those simulations in each case.

We performed the following simulations:

- <u>*Traffic Evolution with a variable PG parameter*</u>*:*

Table III below shows a specific simulation scenario to study the network traffic evolution when the probability of generating messages by nodes, *PG*, varies from 0 to 1.

TABLE III. PARAMETER VALUES FOR SIMULATION 1

Parameter	***Value***	***Parameter***	***Value***
nNodes	15	*nConnec*	3
PC	0.3	*maxHop*	4
PG	Variable	*indTired*	Disabled

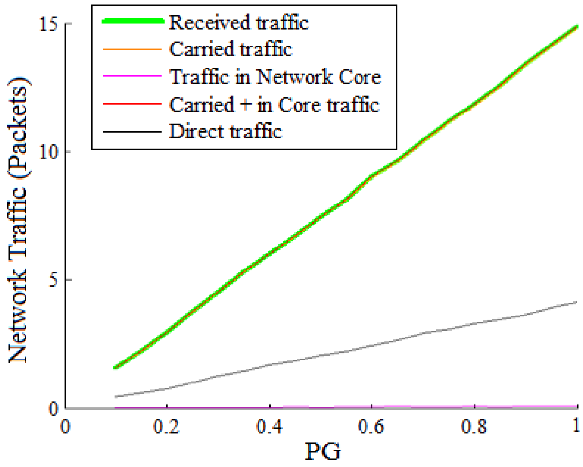


Figure 4. Network traffic evolution based on PG parameter

As can be seen in Fig. 4, obviously all types of traffic increase linearly with traffic generation. Furthermore, in this case all generated traffic is successfully carried since it has direct or indirect access to all nodes. However, the only traffic that could have been carried without the addition of the coverage extension protocol corresponds to the black line (direct traffic) on the figure. In this sense, it is very noteworthy that the addition of the protocol with this specific simulation resulted in a constant increment of around 350% of carried traffic volume coming to a maximum of 383% for PG = 0.2, as can be seen in Fig. 5 below.

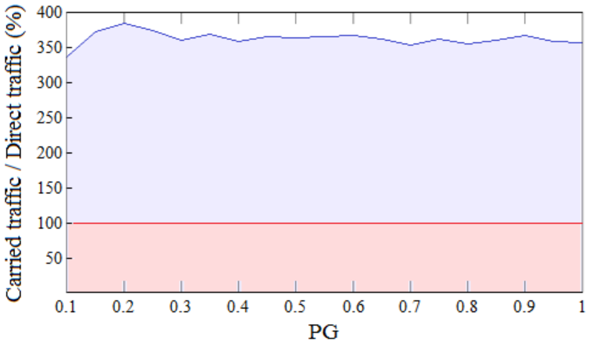


Figure 5. Increment of carried traffic volume when using the protocol compared to a normal situation (without the protocol) (%)

- *Traffic Evolution with a variable nConnec parameter:*

In this case, the simulation parameters shown in Table IV are focused on the study of the network traffic evolution when the maximum number of connections between nodes, *nConnec*, varies from 0 to 10.

TABLE IV. PARAMETER VALUES FOR SIMULATION 2

Parameter	***Value***	***Parameter***	***Value***
nNodes	15	*nConnec*	Variable
PC	0.125, 0.25	*maxHop*	10
PG	0.5	*indTired*	Disabled

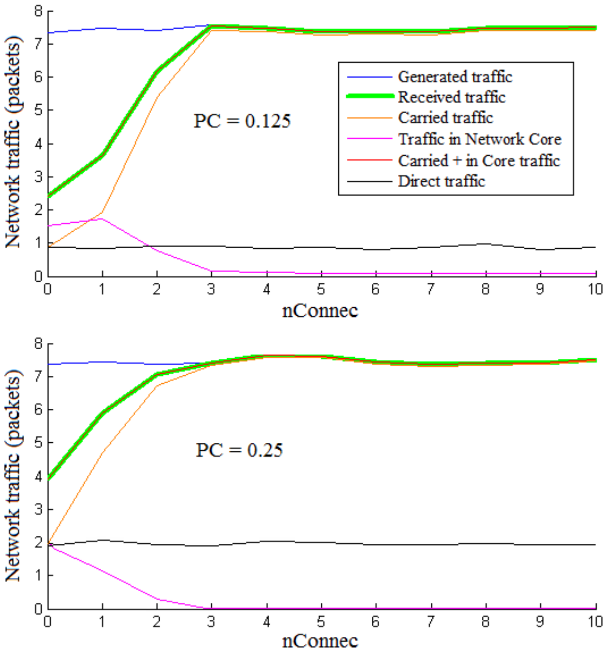


Figure 6. Network traffic evolution based on nConnec parameter with PC = 0.125 and 0.25, respectively

Fig. 6 shows the traffic evolution based on *nConnec* parameter. This simulation aimed to quantitatively analyze the effect of increasing the number of connections between nodes. Conclusions are simple but very meaningful: almost all of generated traffic is carried with an average of 3 connections between nodes although there is a low connectivity to the server in all these simulations (20 and 40% respectively).

- *Traffic Evolution with a variable indTired parameter:*

This third simulation was carried out to test the usefulness and efficiency of the power saving mechanism developed for the protocol. Table V below shows the list of parameters used in this simulation.

TABLE V. PARAMETER VALUES FOR SIMULATION 3

Parameter	***Value***	***Parameter***	***Value***
nNodes	15	*nConnec*	3
PC	0.4	*maxHop*	3
PG	0.8	*indTired*	Variable

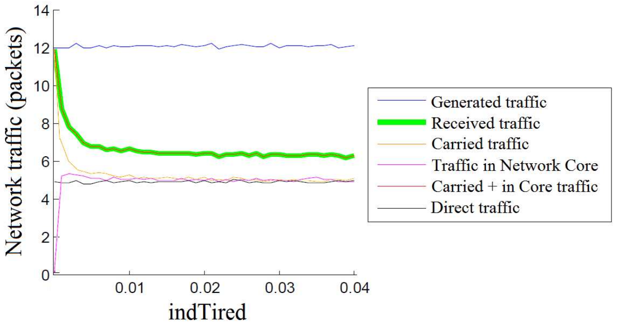


Figure 7. Network traffic evolution based on indTired parameter

Fig. 7 shows the effect of the power saving mechanism implemented for the protocol in the network traffic evolution. Here, as the *tiredness rate* of nodes grows, so does loss rate, slowing down from 0.01 for this specific tiredness index. As already discussed earlier in this paper, losses are due to the existence of nodes that have not direct connectivity to the server. Then, when they transmit data and relay nodes near them are idle, traffic is lost.

From these simulations, we could say that a value between 0 and 0.01 for the tiredness index parameter would be acceptable in terms of traffic losses. In this sense, the selection of a greater or lesser value is a pure design decision depending on every single network deployment and its requirements. Therefore, when designing a network using this cooperative protocol, *indTired* parameter should be carefully chosen to reach a compromise between network losses and energy saving in nodes.

VI. CONCLUSION

In this paper we have presented the main design and implementation aspects of a cooperative protocol that allows the coverage extension in wireless mesh networks. This protocol also includes power saving features for terminals which mainly operate as gateways by simply relaying data from or to neighbouring nodes. Simulation results show that the introduction of the protocol drastically increases the volume of carried traffic on the network due to its coverage extension capabilities. Moreover, they show that the implemented power saving mechanism works as expected, introducing a series of configuration parameters to be taken into account in the design process of wireless mesh networks using this protocol.

Its design has been as generic as possible, so it can be applied to any client-server communication system, from a conventional wireless local area network (WLAN, WiFi) to a mobile phone network or even a WiMAX link. In this sense, although radio technology is not part of the protocol itself, tests and simulations present in the article were conducted using WiFi technology.

Several important advantages arise from its flooding nature (already explained in Section IV.A, e.g., an increased reliability or better self-reconfiguration and self-healing features, etc.), but the extensive use of these techniques could incur excessive energy consumption for the nodes' batteries, which would be compromised. For this reason, the implementation of an efficient power saving mechanism in the protocol itself is of vital importance to minimize the impact of its potentially energy-consuming nature. In this way, the main idea consists of reaching a compromise between energy savings derived from neither having to route nor to process data packets by the nodes, and the extra number of (re)transmissions derived from using such a flooding mechanism.

Keeping all this in mind, it is obvious that this protocol would not be suitable for every possible application since its battery requirements are quite high, but there are many scenarios (where batteries are not the network's bottleneck) in which this protocol could be perfectly used to exploit all its potential advantages over a normal WMN's protocol, e.g., in terms of carried traffic improvements, increased robustness or coverage extension, amongst many others. For example, this protocol could be very useful for mobile phone companies since although it is common for their networks to reach 80% of coverage quite easily, increasing that coverage area to 95% becomes a very difficult and expensive task. In this sense, it is very common to find small specific locations in urban areas with no coverage (due to signal fading effects when propagating through irregular metropolitan areas); however, a short distance from these areas is excellently covered. In these cases, the perceived quality of service of users (*QoE, Quality of Experience*) near that area could be very low. The fact of using the protocol described in this paper could provide a "virtual coverage" to users in a totally transparent way, avoiding such unwanted situations.

ACKNOWLEDGMENT

This research was supported by project grants CALM TEC2010-21405-C02-02 (TCM subprogram) and it was also developed under the framework of "programa de becas asociadas a la realización de proyectos en I+D, innovación y transferencia de tecnología 2009, de la Fundación Séneca, Agencia de Ciencia y Tecnología de la RM, (exp. No 10621/BPS/09)", and "Programa de Ayudas a Grupos de Excelencia de la Región de Murcia, Fundación Seneca".

REFERENCES

[1] F.-M. Zou, T.-S. Wang, X.-H. Jiang, and Z.-X. Lin, "A banyan-tree topology based railway wireless mesh network architecture," Tiedao Xuebao/Journal of the China Railway Society, vol. 32, no. 2, pp. 47-54, April 2010.

[2] Z. Yu, X. Xu, and X. Wu, "Application of wireless mesh network in campus network," 2nd Int. Conf. on Communication Systems, Networks and Applications, ICCSNA'10, vol. 1, pp. 245-247, 2010.

[3] N. Ghazisaidi, K. Hossein, and M. S. Bohlooli, "Integration of WiFi and WiMAX-mesh networks," 2nd Int. Conf. on Advances in Mesh Networks, MESH 2009, pp. 1-6, 2009.

[4] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated cellular and ad hoc relaying systems: iCAR," IEEE JSAC, vol. 19, no. 10, 2001.

[5] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "UCAN: a unified cellular and ad-hoc network architecture," in ACM MOBICOM, 2003.

[6] S.-H. Kim, D.-W. Kim, and Y.-J. Suh, "A cooperative channel assignment protocol for multi-channel multi-rate wireless mesh networks," Ad hoc Networks Journal, vol. 9, no. 5, pp. 893-910, Jul. 2011.

[7] S. Pediaditaki, P. Arrieta, and K. M. Mahesh, "A learning-based approach for distributed multi-radio channel allocation in wireless mesh networks," Int. Conf. on Network Protocols, ICNP'09, IEEE Computer Society, pp. 31-41, 2009.

[8] D.-W. Kum, J.-S. Park, Y.-Z. Cho, B.-Y. Cheon, and D. Cho, "Mobility-aware hybrid routing approach for wireless mesh networks," Proceedings, 3rd Int. Conf. on Advances in Mesh Networks, MESH 2010, pp. 59-62, 2010.

[9] F. Martignon, S. Paris, and A. Capone, "A framework for detecting selfish misbehavior in wireless mesh community networks," Proceedings, 5th ACM Int. Symp. on QoS and Security for Wireless and Mobile Networks, Q2SWINET'09, pp. 65-72, 2009.

[10] K.-H. Lee and C. S. Hong, "A PKI based mesh router authentication scheme to protect from malicious node in wireless mesh network," Management Enabling the Future Internet for Changing Business and New Computing Services, pp. 405-413, 2009.

IQRF Street Lighting - A Case Study

Rostislav Spinar | Martin Spiller | Petra Seflova | Vladimir Sulc
MICRORISC s.r.o.
Jicin, Czech Republic
spinar | spiller | seflova | sulc @microrisc.com

Radek Kuchta | Radimir Vrba
Faculty of Electrical Engineering and Communication
Brno University of Technology
Brno, Czech Republic
kuchtar | vrbar @feec.vutbr.cz

***Abstract*— In this paper, we present main features of IQRF, new communication framework specifically developed for wireless sensor mesh networks and its applications such as intelligent lighting systems. Basic components and functions of IQRF are described. The case study evaluates the existing work on wireless sensor mesh networks for a street lighting scenario and shows number of key mesh network parameters having influence on overall performance of a deployed system. The key parameters were also practically and successfully verified in a test experiment.**

Keywords- frameworks; wireless mesh; intelligent lighting systems; sensors network

I. Introduction

Street lighting control systems are centralized systems which control and monitor the status of street lamps installed along a road. Lights are switched on/off by the system control commands, or, if equipped by light sensitive photocell, then lights are being automatically turned on at dusk and off at dawn. Its local status information is also monitored by control system and reported back to municipal control centre via a communication channel. Among many information being monitored, there might be light status information (on/off), energy saving status (dimming percentage), lifetime period of key lamp elements (maintenance purposes) and safety related information (failures at pedestrian crossing), etc.

To convey control commands and status information between street lighting control system and remote light control terminal installed at each light pole, various types of communication medium and protocols are being used. Regarding the communication media, Power Line Communication PLC or Radio Frequency RF is used commonly [2].

The rationale for these communication media being widely used is their easy installation and low maintenance procedures. In both cases, there is no need to install additional wiring and therefore they are more economically viable than other type of communication media.

Comparing PLC lines with RF channels, both have their own pros and cons. PLC type of communication suffers from an interference from nearby electrical systems, signal attenuation by transformers and DC-DC converters and short circuit problem. On the other hand, RF communication channel parameters tend to deteriorate with worsen weather conditions such as heavy rain or snowfall. Longer communication ranges along with support for dynamic WSMN are essential key factors to maintain certain degree of redundancy in RF communication and thus deliver high reliability of the control lighting system.

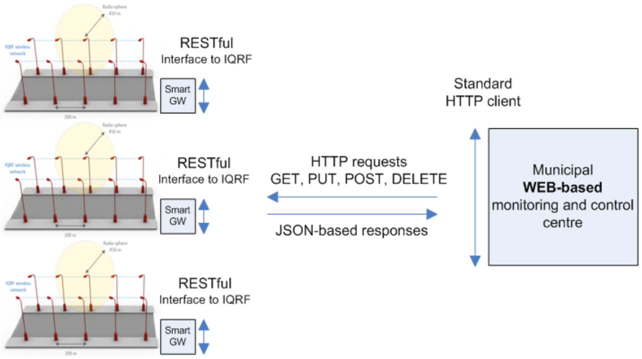


Figure 1. Towards a service-oriented IQRF architecture – street lighting scenario

Maintenance is another important factor. With automatic lights monitoring in place, the system is able to predict lamps failures before they actual happen. This enables to develop more efficient maintenance scheduling plans. In order to further reduce cost and number of maintenance persons, lighting control systems should have high stability and provide required information when needed. For these reasons, reliable communication technique is essential. In this paper, the technology which lays solid foundation for intelligent lighting systems is being further discussed.

The focus of this paper is more on RF communication for our ability to show already gained experience with available RF technology relevant to the selected scenario.

The paper is outlined as follows: First, we present related work in the area of wireless sensors frameworks. We describe new features of IQRF framework in Section 3. Simple implementation of on/off control with status monitoring, a partial task in many street lighting systems, is presented and discussed in Section 4. We conclude with remarks and plans for future work.

II. RELATED WORK

Many solutions supporting low power communication and advanced network topologies are available on the market nowadays. Many of them are based on Low-Rate Wireless Personal Area Networks (LR-WPAN) 802.15.4 [3], Zigbee [4], and 6LoWPAN [5] standards. Following are described platforms based on the mentioned standards.

Arduino [6] is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. The platform was designed for artists, designers, hobbyists, and anyone interested in creating interactive objects or environments.

Jennic [7] is a commercial platform which offers a complete set of wireless microcontrollers, modules, design and development tools. This is complemented by a suite of software that includes network protocol stacks, profiles and APIs as well as application reference examples.

Epic [8] is a open mote platform for application-driven design. A key goal of the Epic project is to develop a composable hardware architecture for WSMN modules that specifically supports prototyping, measurement, and reuse. Epic facilitates prototyping through componentized hardware with flexible interconnections between both the components themselves and third-party hardware.

SuRF [9] is type of module which is based on principles of open-source model and brings the state-of-the-art IPv6 implementation into possibly any electronic device. It is also among first modules which takes advantage of single chip solution (MCU and RF combined together) working in sub GHz band.

IQRF [10] communication framework introduced in this paper takes similar approach as the platforms mentioned above, however IQRF explores more the space of sub GHz bands (868 MHz and 915 MHz) and is equipped by routing mechanism supporting unique 240 routing hops. Further, it brings with itself the merit of simplicity to be applied and as a result of it very fast prototyping and final wireless design. It is a purpose of this case study to also pinpoint and analyze the key parameters of IQRF communication framework and show their influence on the selected scenario.

III. IQRF FRAMEWORK

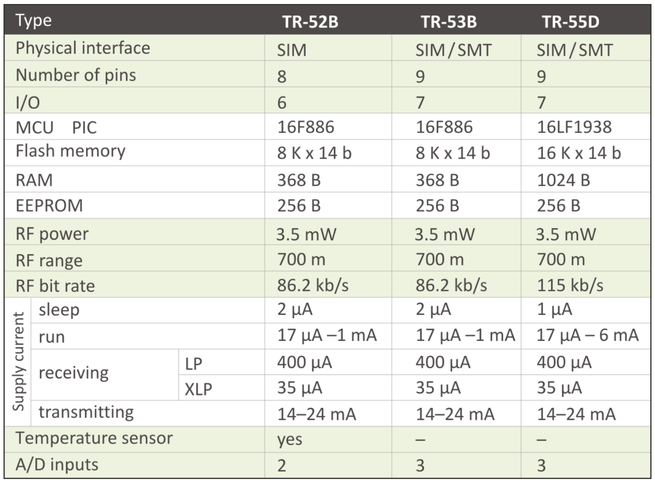
IQRF is the communication framework. The name IQRF stands for an Intelligent Radio Frequency. IQRF is the framework integrating variety of components for building LR-WPAN in an easy way, simplifying and shortening design phase of a wireless communication system. Basic system components and functions will be described in next sections.

A. *Transceiver modules*

A transceiver module (TR) is the basic communication component of the IQRF framework. The TR is a tiny intelligent electronic board with complete circuitry needed for realization of wireless RF connectivity. A micro-controller with a built-in operating system having debug functionality enabled together with an integrated LDO regulator and temperature sensor dramatically reduce a time of an application development. The low power consumption in receive mode (XLP 35uA) predetermines these modules to be used in battery powered applications. Complete set of modules parameters are shown in Figure 2.

A highly integrated design in the SIM card format (25 x 14.9 mm) requires no external RF components and provides efficient way for application firmware development. The modules can be easily integrated into any electronic device via inexpensive and commonly used SIM card connector. An electronic device printed circuit board (PCB) would be populated by the SIM connector and optionally equipped with the TR module. This approach enables manufacturers utilizing the TR modules to sell both either non-communicating versions of the electronic products or optionally equip them with wireless connectivity. The versions with an integrated antenna perfectly support this option.

Solderable versions of the TR modules (TR-53B) fully compatible with their SIM versions would address the applications facing higher mechanical stress. A compatibility with their SIM versions enables easy application development and final seamless migration to solderable versions.



Type			TR-52B	TR-53B	TR-55D
Physical interface			SIM	SIM / SMT	SIM / SMT
Number of pins			8	9	9
I/O			6	7	7
MCU PIC			16F886	16F886	16LF1938
Flash memory			8 K x 14 b	8 K x 14 b	16 K x 14 b
RAM			368 B	368 B	1024 B
EEPROM			256 B	256 B	256 B
RF power			3.5 mW	3.5 mW	3.5 mW
RF range			700 m	700 m	700 m
RF bit rate			86.2 kb/s	86.2 kb/s	115 kb/s
Supply current	sleep		2 μA	2 μA	1 μA
	run		17 μA –1 mA	17 μA –1 mA	17 μA – 6 mA
	receiving	LP	400 μA	400 μA	400 μA
		XLP	35 μA	35 μA	35 μA
	transmitting		14–24 mA	14–24 mA	14–24 mA
Temperature sensor			yes	–	–
A/D inputs			2	3	3

Figure 2. Key parameters of the TR modules

The TR modules are available in several families, each utilizing different peripherals and functions, to fit different user's requirements. Different frequencies in the license-free ISM bands would be utilized: 868 MHz in EU, 915 MHz in US.

Overall parameters for every TR module, specific datasheets and cross-table parameters overview, are shown in Figure 2.

B. *IQRF Operating System*

Every TR module is equipped with the operating system (IQRF OS) implementing basic functionality. IQRF OS is buffer oriented and its block scheme is shown in Figure 3.

IQRF OS controls a radio frequency integrated circuit (RFIC) and supports all communication processes: transmitting (TX), receiving (RX), network bonding, routing, etc.

Data processing (encoding, encryption, check-sums, adding headers, etc.) is made automatically by IQRF OS during communication processes, parameters affecting such processing would be setup before calling communication function. Setting, e.g., variable DLEN (data length in the packet) to be equal to 16 and a consequent call of a RF transmit function would result that the first 16B from bufferRF would be encapsulated to the packet and transmitted.

All RF parameters are software tunable and their setting depends solely on the application requirements. Options of having: 868MHz/916MHz bands; 62/189 channels; 1,2 kb/s up to 86,2 kb/s rates and transmit power up to 3,5 mW. Receiver sensitivity is also adjustable and allows to filter incoming signal according to application need for particular environment. The signal strength can be also periodically checked even while TR being in a receive mode and thus enabling to use clever techniques to increase communication reliability and at the same time to lower power consumption.

In current version of IQRF OS [11], set of addressing and routing options was extended yet simplified for an end user. There might be up to 65000 active devices in a single IQMESH network [13] with routing capability up to 240 hops (700m/hop). The addressing and routing schemes are separated from each other. The addressing is fully under the control of an application developer and on the other hand routing is fully transparent (no need to select routing path) and operating in real-time.

Another new feature of IQRF OS is a discovery mechanism. The discovery allows a network to be logically reconfigured in optimal way for a particular routing option. This further enables to deploy devices without consideration of placing devices in certain way from network coordinator. The discovery mechanism itself is also transparent and very fast. IQRF OS implements support for general mesh network (full MESH) but also supports different set of routing algorithms according to specified topology (Reduced MESH, Optimized MESH, Tree, etc.).

A flexible power management is crucial factor for battery operated devices. There are two important elements which influence power consumption of the TR module. Firstly, it is power consumption in sleep mode and secondly in receive mode. Well designed TR has in sleep mode power consumption of a few uA which yields battery lifetime around 10 years. In most WSN applications, there is a big disproportion in time the transceiver is RX compare to TX during an application life cycle. Thus power consumption in RX mode contributes the most to overall power consumption of the TR. IQRF OS allows the application developer to select among 3 options for receiving modes: standard (STD), low power (LP) and extra low power (XLP). Each of the receiving mode has a corresponding transmitting mode to match up to. Mode selection is driven by application requirements and depends on many factors such as: network throughput, response, length of the packets , use of battery, etc. TR modules consume 2 uA in sleep mode and unique 35 uA in XLP mode. The sleep mode is implemented by turning off all the TR components and then enabling interrupt on change on the MCU input.

There is no special buffer strategy implemented in IQRF OS. There are dedicated buffers for each communication channel (RF, SPI, EEPROM) as shown in Figure 3. It is up to an application to handle correctly these buffers.

In a nutshell, IQRF OS substantially simplifies the design phase and allows a programmer to fully focus on application logic. Besides its basic functionality, IQRF OS provides also a mechanism for application upload when an application is compiled. The programmer will set the TR module into the programming mode and via SPI interface the application code is uploaded to the module as shown in Figure 5. Another method for application upload is via RF and called ICWP (In-Circuit Wireless Programming). ICWP allows multiple TR modules to be programmed simultaneously.

An additional layer on top of IQRF OS so-called plug-ins [13]. An idea of the plug-ins concept is to tailor IQRF OS functionality according to user’s requirements instead of exposing complete set of functions implemented by IQRF OS. A user would not be able to use both UART or I2C and SPI at the same time since these microcontroller (MCU) pins are multiplexed. Therefore, the only one communication plug-in will be used at a time to avoid wasting of the program memory by having all protocols included in the OS built.

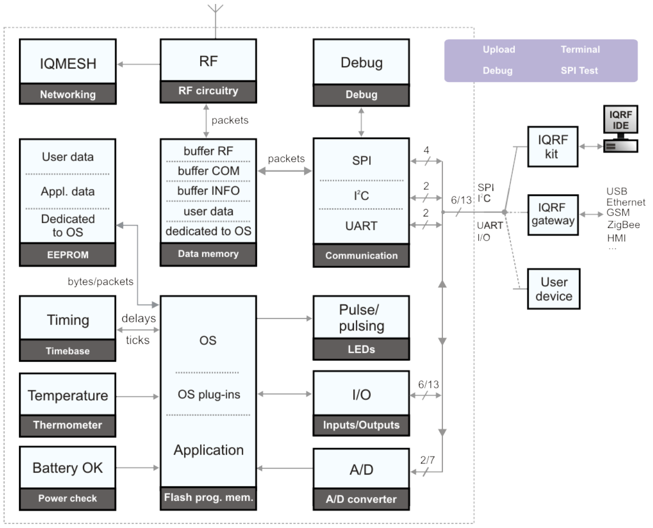


Figure 3. IQRF OS structure

A complete set of functions can be found in [1].

C. Gateways

An external access to the IQRF WSMN is enabled through the gateways. Generic and static types of gateways are distinguished in the IQRF framework [12].

The static gateways provide external connectivity to the IQRF WSMN based on defined fixed protocols. The gateway consists of the TR module providing wireless connectivity together with a dedicated MCU implementing a specific protocol. An Ethernet gateway GW-ETH-01 has Ethernet interface supporting TCP and UDP communication. Based on the gateway’s configuration the packets coming from IQRF WSMN can be stored in a round buffer of the gateway and later picked up by an external server application or directly sent via Ethernet. In opposite direction, data is encapsulated to the IQRF packets and sent directly to the IQRF WSMN. An application layer and function of TR module might be fully customized.

The generic gateways would be customized completely. Both the application layer of the TR module and gateway's MCU would be fully programmed. Based on this mechanism, the generic gateways can provide custom specific functions. Advantages would be seen in the GW-QVGE-01, a human interface device implementation. The objects such as menus, buttons or texts and their specific events will be usually different for every customer's application.

D. *Development tools*

As it was mentioned, the TR modules have built-in OS therefore the only application layer needs to be developed. The simpler applications and examples for the TR modules can be directly downloaded from the website [1], while specific and customized functionality should be developed and programmed. A typical development process based on this concept is shown at figure Figure 5.

To effectively develop, program and debug applications for the TR modules, wide range of hardware and software development tools has been introduced - programmers, development kits and development sets.

The programmers such as CK-USB-04 [1] used in the case study are dedicated to upload compiled application into the modules and also to provide debugging interface during the application development. The development kits such as DK-EVAL-04 [1] used in the case study are modular ready-to-use pieces of HW which would be used for debugging and communication or range testing.

IQRF integrated development environment (IDE) should be mentioned as a basic tool providing complete functionality for the application development - system debug, SPI debug Terminal and Programming/Upload.

E. *Function Specific Components*

Next IQRF components with specific function were added to the IQRF portfolio to help with maintenance task on a site.

The solution is being prepared and is going to be based on graphical IQVCP type of device [14] which is able to join street lighting IQRF network and send diagnostic requests to each lamp. For the field operations, an IQVCP device is able to run from the battery. Shown in Figure 4.

Figure 4. IQVCP scanner

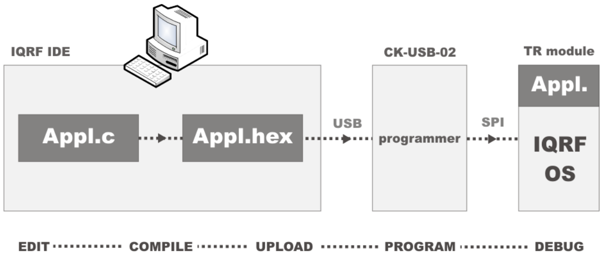


Figure 5. The development process and tools

IV. THE CASE STUDY

Radio waves are affected by the same phenomena like light waves: reflections, absorptions, diffraction, etc. These phenomena strongly influence signal propagation. Radio waves on the frequencies used nowadays in LR-WPAN (sub GHz ISM bands and 2.4GHz band) are influenced by many factors such as the height above ground the modules are deployed, noisy environments usually found in cities (public transport systems, wireless door bells, etc.) and also outside weather conditions (fog, heavy rain, snow). The purpose of the case study is to prove on a simple example the convenient use of WSMN for street lighting systems and show key mesh network parameters along with techniques that influence overall system performance. For the demonstration purposes, the only standard IQRF components and development tools have been used.

A. *SIMULATION SCENARIO*

The simulations of the signal propagation were made for free space which is relevant to street lighting scenario. The TR-52BA-868 [1] modules at 868MHz band were availed and following conditions were applied for the test scenario: 1.60m over the ground, TX on maximum power 3.5 mW, antennas with gain 1.10dBi used both on TX and RX module and ground reflections 45%. The simulated graph is presented in Figure 6. Only near field is shown since far field linearly declines with distance. Based on the simulations and receiver sensitivity for 19.2 kb/s data rate, communication range was calculated as 470 m for a free space.

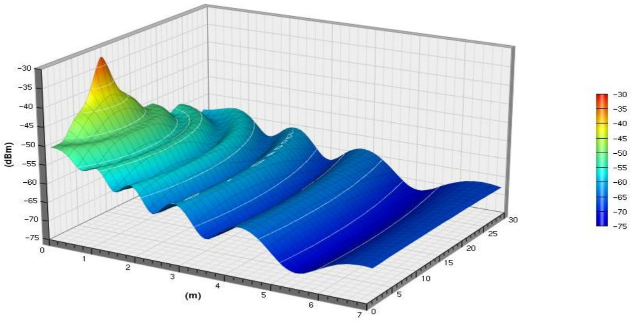


Figure 6. Near field simulation for 868 MHz free space with parameters relevant to the TR-52BA

B. *EXPERIMENTS*

A) Free space communication range measurement was realized with two new TR-52BA-868 modules each placed separately in the evaluation board DK-EVAL-03. An example E03-TR.c available from the website [1] was used, sending repeatedly packets with set data rate 19.2 kb/s and with maximum transmitting power 3.5 mW from one device to the other and back. The communication range was noted down when losing the packets were detected by a LED – 450 m communication range was measured.

TR-52BA-868 with its on-board mini PCB antenna has same radiating pattern as a usual whip antenna. The omni-directional radiating pattern is depicted on Figure 7 (right side).

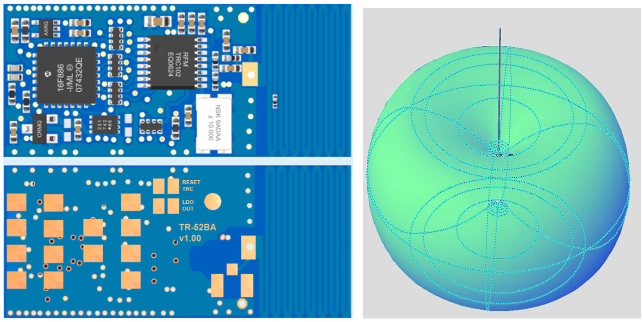


Figure 7. TR-52BA with its omni-directional antenna

B) A wireless network was built-up in the airport environment consisting of 20 modules TR-868-52BA placed to the evaluation boards DK-EVAL-04 and one CK-USB-04 establishing IQRF connection to PC running IQRF IDE.

An example E11-IQMESH-N.c available from the website [1] was tailored for the test scenario and used in the modules N1 - N20 simulating 20 street lamps. All modules were spread in two rows, having 10 of them in a row as depicted on Figure 8. For a network coordinator, E11-IQMESH-C.c was used and loaded into TR module placed in CK-USB-04.

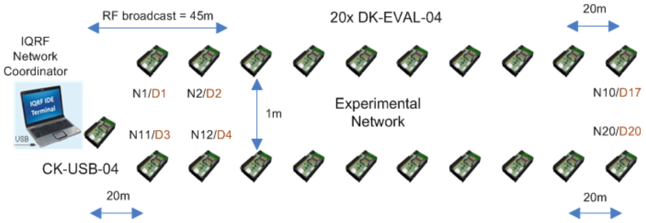


Figure 8. The experimental network

C) Installation phase: a real-life network was setup in the airport environment with a topology shown in Figure 8. The sensitivity of all receivers (all devices) was adjusted to 10th of normal value. Doing that, the RF range was lowered to 45m, along with an assumption that all devices transmit at maximum power. To lower RF selectivity was decided based on a fact that it has much more fine-grained scale in comparison with output RF power. That resulted in better control over the network topology. Next is being discussed all necessary steps to setup and operate the network.

Firstly before actual deployment, all nodes simulating the lamps must be BONDED to the coordinator using standard bonding procedure which is well documented in an user guide to IQRF OS [1]. In our case, the coordinator is TR module placed in CK-USB-04. The bonding procedure assigns addresses to the bonded devices (N1-N20) and is fully under the user control. Bonding must be done within a direct RF range of the devices. It is a recommended practice to label each device with its assigned address.

Secondly, actual DEPLOYMENT of devices takes place. Since recommending to use routing algorithm Discovered Full Mesh (RTDEF = 2) there is no need to place the devices in specific order such as in Figure 8. They might be placed in random fashion. However, keep a map of the deployed devices (N1-N20) and its locations.

Thirdly, a DISCOVERY procedure is initiated by the network coordinator. Complete network is discovered and a virtual routing number VRN (D1-D20) is assigned to each device. D1-D20 are shown here only for an illustration and are not needed to be known for the routing purposes. To address a street lamp, the addresses N1-N20 are used and the routing itself is completely transparent for the user. It is a recommended practice to run the discovery procedure at lower TX power to avoid having same of the devices close to communication edge. It is also recommended to keep track of RSSI traces from the deployed devices at the coordinator and have them available for a comparison during the course of the year. If there is a change in physical network topology (replacement, adding new device, etc.) it is advised to initiate the discovery procedure again.

Finally, after the discovery procedure is finished it is recommended to POLL each device in the network in order to confirm that there is a RF link to every device. If succeed the network is ready to be used.

D) Routing: having full mesh routing supported brings the advantage of multiple redundant paths being available and thus lowering a likelihood of a packet not reaching its set destination. If the topology shown in Figure 8 is considered then the routing mechanism performs as follows. A command is transmitted from the network coordinator and in a first step is received by the devices N1, N2, N11 and N12. In order to avoid collisions to each device is assigned a time slot in which retransmits received command. Since the retransmission is also by broadcast, all devices in RF vicinity receive this retransmission. Next device to retransmit after the coordinator is N1 followed by N2 and so on. The command is being forwarded to its destination in described fashion. It is also important to mention that if a device receives same command twice it just simply discards the last one and keeps the original which to be retransmitted once there is a device's turn. A length of the time slot is set by the coordinator in a parameter RTDT1 (units of OS ticks) and might be variable depending on the length of the commands and expected responses. It is also worth mentioning that

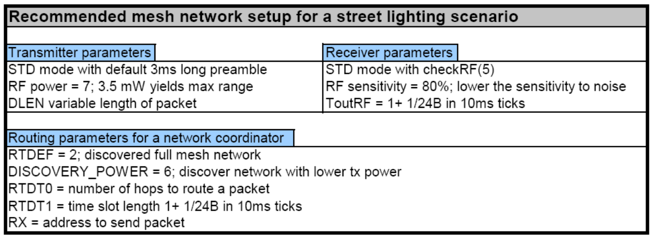
RTDT1 is inherited by all devices in the network once set by the coordinator.

Another important parameter is RTDEF which specifies type of routing mechanism. It is recommended to pick Discovered Full Mesh (RTDEF = 2) routing for the street lighting scenario. As described in the installation phase, once the network is discovered VRNs (D1-D20) are assigned. The sequence, in which the command is being forwarded in type of routing, is derived from VRNs (D1-D20) and not from bonded addresses (N1-N20). This allows the network to be further optimized in a sense of routing topology.

The last important parameter is RTDT0 specifying number of hops the command should be forwarded. It is possible to select RTDT0 according to number of bonded devices in the network. However, this would be only necessary in a case of having a chain mesh network. In other types of network, certain optimization techniques might be applied. More on the optimization might be found in a reference guide to IQRF OS [1]. There is always a trade-off being present between the level of redundancy and the command latency for the particular network topology.

E) For the field deployment as shown in Figure 8., the band 868 MHz and data rate 19,2 kb/s were configured. STD transmitting/receiving mode was used since there is no real emphasis on any power saving mechanism for the street lighting networks but rather maximum number of hops along with the packet latency is being considered. As described in previous paragraph, there are two routing parameters directly proportional to maximum configured hops and overall packet latency. In the field deployment, RTDT0 is equal to 20 and RTDT1 is equal to 1. With this setup in place, the coordinator is able to send short packets (up to 24B) and receive acknowledgment back from N20 within 0.5 s time frame. Further, the coordinator was configured to contact each node (N1-N20) in regular fashion. A pulling cycle was repeated every 5 min for 4 hours. During this run only HW related issue on N15 was encountered, which had no influence on correct performance of network primitives. The coordinator was able to collect all valid responses for the sent requests except for N15.

F) General recommendations for the street lighting networks are shown in Tab. 1. It is recommended to run a street lighting network in STD mode. Other modes such as LP and XLP are more suitable for battery operated devices. Others parameters are described in the table.



Recommended mesh network setup for a street lighting scenario	
Transmitter parameters	Receiver parameters
STD mode with default 3ms long preamble	STD mode with checkRF(5)
RF power = 7; 3.5 mW yields max range	RF sensitivity = 80%; lower the sensitivity to noise
DLEN variable length of packet	ToutRF = 1+ 1/24B in 10ms ticks
Routing parameters for a network coordinator	
RTDEF = 2; discovered full mesh network	
DISCOVERY_POWER = 6; discover network with lower tx power	
RTDT0 = number of hops to route a packet	
RTDT1 = time slot length 1+ 1/24B in 10ms ticks	
RX = address to send packet	

Table 1. IQRF street lighting recommendations

V. Future work

The future work within this project will be aiming at elaborating more on the idea of service-oriented architecture for IQRF and eventually for modern cities as shown in Figure 1. More specifically, the design of a smart gateway with RESTful interface [15] to IQRF will be further pursued along with practical verification of its usability in common cities environment.

VI. Conclusion

The main features and components of the IQRF communication framework were presented. Based on the standard IQRF components the IQRF-based WSMN was built to demonstrate basic operations in the street lighting systems and to experimentally verify the convenient use of WSMN in this application domain.

This network was used for the experiments presented in the case study. On this network, key mesh network parameters were shown and practically discussed. The recommendations for the key parameters were given to application designers in order to easy their task of developing WSMN network.

The experiments have proved WSMN topology to be also at best convenience for the street lighting applications.

Acknowledgement

This research has been supported and co-financed by the Ministry of Industry and Trade of the Czech Republic under a contract FR—TI3/27, project Open Platform for Modern Cities.

Many thanks to Jaroslav Spicka and Jaromir Mastik for their practical insights.

References

[1] Datasheets and examples from http://www.iqrf.org [March 31, 2011]

[2] J. D. Lee, K.Y. Nam, S.H. Jeong, S.B. Choi, H.S. Ryoo, D.K. Kim, “Development of Zigbee based Street Light Control System” IEEE, Atlanta, 2006

[3] IEEE 802.15.4, http://ieee802.org/15/pub/TG4.html [March 31, 2011]

[4] Zigbee Alliance, http://zigbee.org/ [March 31, 2011]

[5] IETF 6lowpan, http://6lowpan.org/ [March 31, 2011]

[6] Arduino platform, http://www.arduino.cc/ [March 31, 2011]

[7] Jennic platform, http://www.jennic.com/ [March 31, 2011]

[8] Epic platform, http://www.eecs.berkeley.edu/~prabal/projects/epic/ [March 31, 2011]

[9] SuRF platform, http://www.peoplepowerco.com/surf_module.html [March 31, 2011]

[10] R. Kuchta, R. Vrba, and V. Sulc, “Smart platform for wireless communication - case study", Seventh International Conference on Networking, Cancun, 2008

[11] J. Pos, "Mesh wireless networks", Sdelovaci technika 3/2011, Czech Republic, 2011

[12] J. Pos, "Communication gateways of IQRF network", Sdelovaci technika 5/2009, Czech Republic, 2009

[13] V. Sulc, R. Kuchta, and R. Vrba, “IQMESH implementation in IQRF Wireless Communication Platform", 2nd International Conference on Advances in Mesh Networks, Glyfada, Greece, 2009

[14] IQVCP platform, http://iqvcp.org/iqvcp/index.php [March 31, 2011]

[15] R. T. Fielding, Phd dissertation, 2000, http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

TenDoc: Network Coding-based Software for Wireless Ad hoc Networks

David Lim, Stéphane Rousseau, Farid Benbadis, Damien Lavaux
Thales Group, Colombes, France
david.lim@fr.thalesgroup.com
stephane.rousseau@fr.thalesgroup.com
farid.benbadis@fr.thalesgroup.com
damien.lavaux@fr.thalesgroup.com

***Abstract*—This work builds upon previous studies that highlight the benefits of Network Coding for all to all traffic patterns. This is the case within the framework of an optimized link state routing protocol (OLSR) where topology control messages are flooded in the entire network in order to provide a precise knowledge of the topology to all single nodes in the network. The flooding efficiency is often measured either in terms of successful dissemination delay or the number of transmissions needed to achieve this goal. In this paper we present the new TenDoc software that has been first designed to support any applications and that has been adapted especially for this OLSR use case. After recalling our own previous simulation-based investigations, we detail the architecture of this TenDoc software and finally present results from our results from our experimental platform.**

Keywords - network coding; wireless network; topology dissemination; multi-point relays.

I. Introduction

A Public Safety Network (PSN) is a multi-hop wireless Network specially used for emergency service organizations (e.g., police, fire services). The ease of deployment and self-management features make such networks very attractive and useful during emergency interventions in crisis areas where any other means of communications are often no longer available (e.g., earthquake, flood). Due to the multi-hop nature of Public Safety Networks, the design of routing protocols is central to optimizing network capacity and usage efficiency. In the literature, two kinds of routing protocols emerge: i) reactive protocols where routes are computed only when needed, and specially adapted for; ii) pro-active protocols where routing tables are maintained. The former are well suited for Mobile Ad-Hoc Networks while the later are tailored to infrastructure-like networks such as Mesh networks [1]. Public Safety Networks, where the time for communication establishment is critical, clearly belong to the second category.

One of the most used pro-active protocols is OLSR [6]. OLSR protocol consists of two distinct parts: i) local topology gathering and dissemination; ii) routing table updates based on the topology deduced from the gathered topology information. Within the framework of this study, we focus on the first part and examine how topology information is disseminated.

In OLSR, local topology information is collected by each node and aims at evaluating the link quality between each node and its neighbors. The protocol is based on bi-directional exchange of messages, called *Hello messages*. The link quality is estimated by taking into account both the successful transmission and reception of those messages. Once this local information is gathered, it must to be disseminated to all nodes in the network by *Topology Control messages (TC).* A naïve approach consists in simply flooding these messages to the entire network. In [6] authors present a distributed Connected Dominating Set algorithm that reduces dramatically the amount of needed transmissions to achieve a successful dissemination. In contrary to flooding dissemination wherein all nodes forward all messages, the distributed Connected Dominating Set algorithm consists in selecting a subset of nodes in charge of forwarding. This algorithm significantly outperforms the flooding dissemination [5].

Optimizing the topology information dissemination based on TC forwarding within OLSR has been the subject of many studies [2], [3], [4]. The most recent ones aim at reducing the number of transmissions needed to achieve a successful dissemination (when all nodes have the knowledge of the entire topology) by introducing Network Coding techniques. The advantage of this method lies in the transmission. Indeed it does not just relay messages to other nodes but combines several messages together before transmitting them. In this way, we have more information in each message.

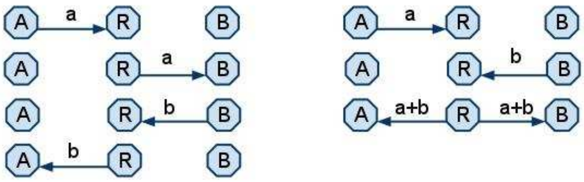


Figure 1. This figure depicts an application example of network coding technique onto three nodes, A, R, B. A resp. B has to send one packet towards B resp. A via R. On the left, without network coding; On the right with network coding. The benefits of using network coding in this case is 25%.

In figure 1, we consider 3 nodes A, B and R (the relay node). In the normal network context, only one packet may be transmitted at a time. However, with the network coding

ISBN: 978-1-61208-147-2

technique, once A and B have transmitted, the relay node can broadcast the coded information to both nodes, thus transmitting two packets simultaneously.

In a preliminary study, several message dissemination protocols (MPR-based forwarding, pure flooding, dominant pruning and network coding) were for the first time compared. As a main result, network coding was shown to outperform other protocols in terms of number of transmissions [2].

In this paper, we extend our previous study by implementing the concept proposed in [2] and run an experiment within our 7 node lab test-bed described on Figure 3. This software implementation enables the use of network coding for topology information dissemination in OLSR. This software is fully technology independent and does not require any modification within OLSR. Furthermore, this software can be used for other applications such as sensing dissemination in Cognitive Radio Networks or Common Operational Picture applications in the context of PSNs. The main contributions are twofold:

- The software architecture for network coding for all to all traffic patterns.
- Software design for the special case of OLSR.

This paper is organized as follows: we first present the related work that motivates this software development, then we detail the architecture of this software, and finally, we present the first experimental results of this novel approach conducted in a7 nodes wireless test-bed.

II. RELATIED WORK

Recent studies have been done in the framework of TC message dissemination improvement by using Network Coding. In [4], Kadi and Al Agha evaluated the benefits to use network coding for TC messages dissemination in the context of OLSR [6]. They focus on the determinist network coding that consists in combining messages in order to maximize at each step the number of neighbor nodes that will be able to decode. The benefits of such methods are also demonstrated in CODEB in [8]. However, an additional information exchange protocol is required to inform neighbor of each node of the set of TC messages already collected. Using simulations, the authors show that network coding applied to MPR-based dissemination [7] significantly reduces the number of transmitted TC messages. In [3], Kadi and Al Agha proposed an additional study by using Random Network Coding which consists in combining messages randomly without any knowledge of the set of TC messages already collected by the neighborhood. Once again, results are dramatically better when dissemination combines MPR-tree and Random Network Coding. Relying on those first results, in [2], an overview of dissemination techniques is done either based on Connected Dominating Set algorithms or network coding (Determinist, Random). All relevant previous works and novel combinations are investigated and compared with each other. Finally, performance gains assessed by simulations show that network coding for TC message dissemination can improve the efficiency in terms of delay of information delivery and of the number of transmissions needed.

III. TENDOC ARCHITECTURE DESIGN

We first describe the TenDoc modules that compose its architecture and then modules interactions. They are illustrated by the different steps in the case of OLSR application. Although the TenDoc software is designed for the OLSR protocol, it can also be used for other applications.

A. Architecture description

In this section we present the modules that compose TenDoc software.

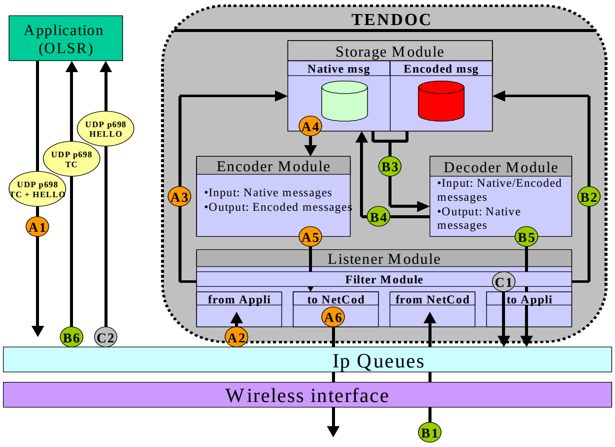


Figure 2. The software architecture.

1) Listener Module

This module aims at fetching TC messages from the IP queue, either from the local OLSR application or from the wireless interface. It is composed of sub-modules that interface with the Linux IP queues at a kernel/user space level and 1 sub-module in charge of dispatching fetched messages.

- **'From appli'** listens to UDP traffic on port *698* that is generated locally. Both TC and Hello messages are sent on this port.
- **'To appli'** sends native messages that are extracted by decoded module towards OLSR applications.
- **'From TenDoc'** listens UDP traffic on an unassigned port (1024 for example), forwards it to be stored into encoded message buffer in the Storage Module.
- **'To TenDoc'** sends encoded messages to neighbor nodes within the radio coverage area, by using a UDP broadcast socket opened on port *1024*.
- **'Filter'** identifies and dispatches messages to the proper sub-module. In the context of OLSR, TC and Hello messages are sent on the same port using the protocol. It is necessary to identify TC from Hello and redirect Hello messages towards their defined destinations.

2) Storage Module

This module is composed of two buffers. The first one aims at storing native TC messages that have been either created by the local OLSR daemon or received from neighbor nodes. The second buffer, Encoded message buffer, stores all messages that are not decoded at this time, either because needed native messages have not been received yet or the decoder module does not treat them at this step.

3) Encoder Module

The goal of this module is to encode two TC messages together from *native message buffer* by xoring two messages contained in the storage module into encoded messages to be sent. The number of encoded messages is a parameter which can be tuned for the experiment. Then, the created encoded messages are sent to the listener module.

4) Decoder Module

This module regularly checks if some encoded messages stored in the *encoded message buffer* (storage module) could be decoded by using native messages contained in the *native message buffer* (storage module). If this is possible, the decoded module removes the considered encoded message from the *encoded message buffer* and stores the native messages into the native message buffer. Moreover, those native messages are also sent towards the OLSR application via the listener module.

5) Module interactions

To emphasize module interactions, all single steps of OLSR TC message dissemination are enumerated, by starting with the first sending of one TC message from the local daemon of OLSR towards the IP queues. Neighbor node TenDoc software exchanges are presented and finally the forwarding of recovery TC messages from encoded messages towards OLSR applications. As illustrated in Figure 2, those steps are ordered into three groups: the A_x steps describe the treatment of TC messages from the local OLSR application, the B_x steps describe the exchanges between TenDoc software running onto neighbor nodes and finally, the C_x steps deal with unexpected fetched messages treatment.

Herein, we present those steps in details:

- ➢ **A1**: OLSR sends TC and Hello messages by using broadcast UDP traffic on port 698.
- ➢ **A2**: Before sending, the Listener Module fetches those messages.
- ➢ **A3**: TC messages are filtered, extracted and sent towards the Storage Module to be stored into *native message buffer*.
- ➢ **A4:** Encoder Module takes some native messages from the *native message buffer* and encodes them. An encoded message is created, with a header indicating the number and the sequence number of the TC messages encoded and within the payload the result of the encoding function.
- ➢ **A5**: The encoded message is sent towards the Listener Module.
- ➢ **A6**: The Encoded message is broadcast towards all neighbor nodes by using a UDP socket on port 1024.

This is the conclusion of the first step of the TenDoc software. The second step begins when an encoded message is received from a neighbor node.

- ➢ **B1**: The Listener Module gets all messages from port 1024 that have been sent as UDP traffic.
- ➢ **B2**: Encoded messages are identified and sent to the storage Module to be stored into the *encoded message buffer*.
- ➢ **B3**: The Decoder Module decodes encoded messages from *encoded message buffer* by using native messages from *native message buffer*.
- ➢ **B4**: Native messages decoded are stored into *native message buffer*.
- ➢ **B5**: A copy of the native messages decoded is sent towards Listener Module.
- ➢ **B6**: Local OLSR application receives TC messages as a UDP traffic on port 698 that makes this software fully seamless from the application point of view.

This ends the second steps of the TenDoc software process. The last one is mainly designed for an OLSR application that sends TC and Hello messages onto the same port number that makes a special filter necessary to distinguish TC from Hello messages before treatment. The following steps deal with the Hello messages once they have been fetched by the 'from appli' sub-module within the Listener Module.

- ➢ **C1:** The Filter sub module extracts Hello messages from fetched messages and sends them towards neighbor nodes
- ➢ **C2:** The local OLSR application receives Hello messages from neighbor nodes as UDP traffic on port 698.

As mentioned before, OLSR is only one of many possible applications of the TenDoc software. The next section deals with the experiment that will be conducted to prove the software concept and assess the performance gains.

IV. EXPERIMENTAL ENVIRONMENT

A. Test-bed description

Seven nodes equipped with wireless interfaces (Atheros wireless Card) are deployed to form the topology depicted in Figure 3. A version of Ubuntu is running on each node and the interface is configured in Ad Hoc mode on channel 2 (channel that is used by no other nodes in the radio coverage range). On each node, the OLSR daemon is running. We use OLSR Version 0.5.6.

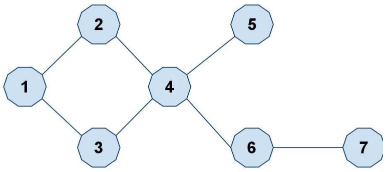


Figure 3. Our 7 node indoor test-bed topology.

B. *Scenario description*

To evaluate the performance gains of using TenDoc instead of OLSR, we focus on two scenarios: (i) standard OLSR running alone, and (ii) TenDoc software running on all nodes of the platform. In both cases we measure the number of transmissions during a 1 day period.

In order to measure this information, we use “iptables” Linux command that can keep track of how many messages have been sent on an interface. We complete this information by using the wireshark software to scan traffic generated within an area (i.e., the platform area).

V. Result Analysis

First, we present last year’s simulation results. Then we introduce the new data from our experiment. For our test, we wanted to consider the number of messages and the delay of a successful dissemination. The two following figures provide us evidence about the advantages of network coding.

A. *Preliminary Results*

Figure 4 shows the comparison of the message dissemination in the network between MPR-based and network coding based method.

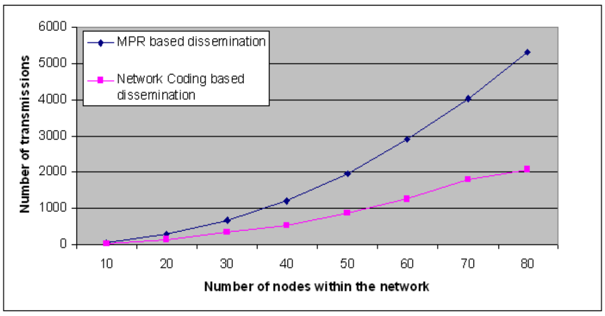


Figure 4. Number of transmissions of MPR based compared to the network coding dissemination

The first thing that we can notice is the number of transmissions is significantly lesser than the MPR based with almost a gain of fifty percent. The result is expected because the network coding process combines packets together and broadcast them. Therefore more information is transmitted per broadcast. Furthermore, the gain depends on the number of the nodes.

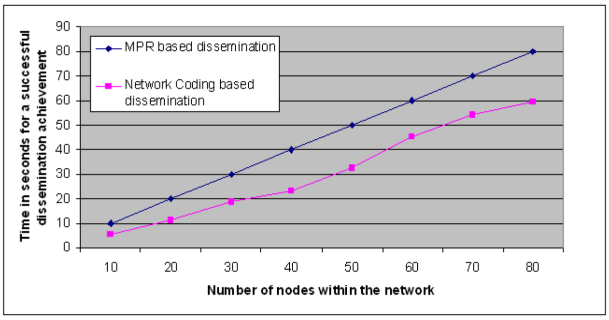
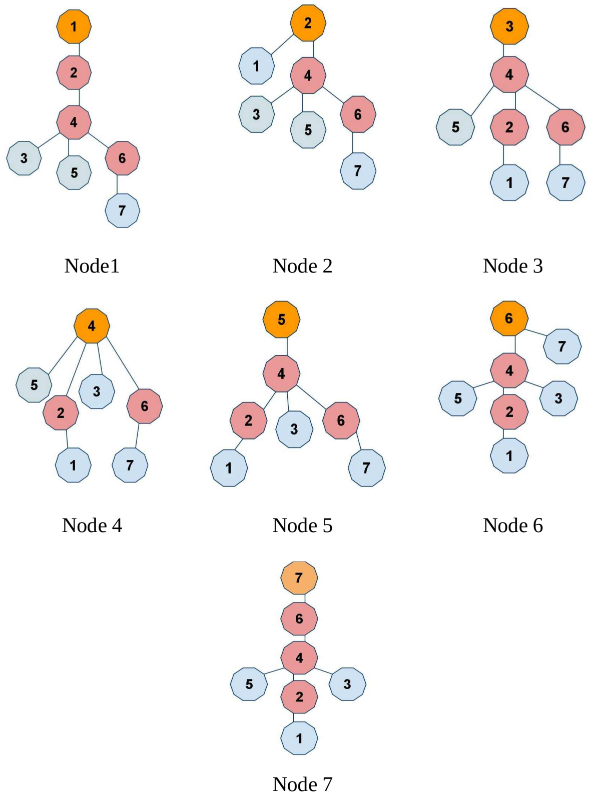


Figure 5. Total time achievement of dissemination of MPR based compared to the network coding.

In figure 4, the noticeable gap starts at 20 nodes. This result indicates that the density of the mesh network should be considered. In figure 5, we consider the time of dissemination achievement. We can see the network coding has an advantage; the completion time is lesser than the MPR-based network. In term of delay, the result is almost the same, but the number of packets which pass through the network is lesser to have a total dissemination.

B. *Experiment results*

In this section, we compare MPR based and network coding based dissemination of TC messages. This experiment is conducted on our 7 indoor test-bed nodes –see Figure 3. The MPR based dissemination requires 23 transmissions for a successful dissemination.


Node1

Node 2

Node 3

Node 4

Node 5

Node 6

Node 7

Figure 6. MPR diffusion tree.

We conduct this experiment by calculating the number of transmissions from the diffusion tree. We consider that each node has to diffuse its own information. Therefore, we select each node one by one to calculate the number of packets which circulate in the network. In figure 6, the root node is the orange node, the red ones are the MPR nodes and the blue one is the terminal node. We calculate the number of the messages that each node disseminates in the network by counting the number of hops from each root node to the terminal nodes.

Table I shows the comparison of all methods that we have used. As we can see the pure flooding method is high. With MPR-based method there were 23 messages which were disseminated in the network. When we use TenDoc software, it combines the pure flooding and the network coding method. We did not expect these results in the practical way. The number of the transmitted messages is higher than for pure flooding.

TABLE I. CLASSIFICATION OF DIFFUSION METHODS

Methods	Number of transmissions
PF	49
MPR based	23
PF+NC	53

As we observed before, in the simulation result the number of messages that each node diffuses depends also on the mesh network density. The experiment that we conducted with seven nodes was not very significant. We would make some other experiments with more than fifty nodes to observe the same performance gains as those obtained in our previous work [2].

VI. SUMMARY

In this paper, we introduced the implementation of network coding in the OLSR protocol for minimizing the number of required transmissions. This was a natural combination. Indeed OLSR is the standard for ad-hoc routing in mesh networks, while the network coding concept is a really efficient way to optimize the number of transmissions and the use of the rare wireless spectrum.

We also investigate on the TC message dissemination by using the Network coding. Moreover we wanted to be application independent (without any modifications onto OLSR). Finally, this method could optimize the radio resource usage.

In this paper, first we introduce the network coding and the OLSR protocol in the ad-hoc mesh network which is the way to optimizing the message dissemination in the mesh. The network coding is added to the routing protocol to minimize the number of required messages. We go beyond the state of art of the network coding to propose a practical solution to implement the application. In the theoretical approach [2], when we associated OLSR and network coding, the simulation results showed that network coding could improve the performance of the message dissemination by fifty percent, thereby avoiding avoiding the waste of radio resources.

Furthermore, to implement our solution, we strive to be seamless from the application point of view and develop our solution as a module that we can plug or unplug whenever we want. It connects to the OLSR framework. In this solution we have two levels: the connection between the OLSR and the inter-module connection. The first one we use the OLSR port connection the 698 to get the packet of TC and hello message by listening the port. We have created a listener and the sender for communicate with the OLSR the packet is transferred to the second level to send in the network through another port connection. Basically we do not use the OLSR port connection to communicate with another nodes but TenDoc's port. The second level is in the part where we have the network coding treatment for encoding and decoding the message that we want to send. Basically, only random network coding is available but we plan to enrich this software by integrating deterministic one.

As we can see, the results are not very significant with a study of seven nodes dissemination. And we think about further work to increase the number of nodes to have a high density of a mesh network. Because previously in [2] in the theoretical way, we saw the density was very important and it can transfer more messages at each time. And the implementation in a practical solution could improve the radio communication by introducing this concept of message dissemination.

Finally, this software will be combined with an efficient control plane that will enable to activate or not some nodes to be network coding active in order to optimize network capacity usage.

ACKNOWLEDGEMENT

This work was supported in part by the European Commission through ICT project CONECT (Cooperative Networking for High Capacity Transport Architectures), FP7 ICT-2009.1.6, and by CELTIC Office through project HNPS (Heterogeneous Network for European Public Safety), CP5-010.

REFERENCES

[1] S. Jan, I.A. Shah, H.S. Al-Raweshidy, "Performance Analysis of Proactive and Reactive Routing Protocols for Mobile Ad-hoc Grid in e-health Applications," Communication Software and Networks, 2009. ICCSN '09. International Conference on, pp.484-488, 27-28, Feb. 2009.

[2] S. Rousseau, F. Benbadis, D. Lavaux, and L. San, Thales Communication France "Overview and optimization of flooding techniques in OLSR", HotMESH 2011, third IEEE International Workshop on Hot Topics in Mesh Networking, June 2011.

[3] N. Kadi, K. Al agha, "MPR-based flooding with distributed fountain network coding," Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 The 9th IFIP Annual Mediterranean, pp.1-5, 23-25, June 2010.

[4] N. Kadi, K. Al agha, "Optimized MPR-based flooding in wireless ad hoc network using network coding," Wireless Days, 2008. WD '08. 1st IFIP, pp.1-5, 24-27 ,Nov. 2008.

[5] A. Qayyum, L. Viennot, A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, pp. 3866- 3875, 7-10 Jan. 2002.

[6] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized link state routing protocol for ad hoc networks," Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International , pp. 62- 68, 2001.

[7] P. Jacquet, Ed. T. Clausen, Ed. The Internet Engineering Task Force (IETF). "Optimized Link State Routing Protocol (OLSR)" Project Hipercom, in INRIA, October 2003.

[8] L. Li, R. Ramjee, M. Buddhikot, S. Miller, "Network Coding-Based Broadcast in Mobile Ad-hoc Networks," INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , pp.1739-1747, 6-12 May 2007.

Review of Trust-based File Sharing in Cloud Computing

Edna Dias Canedo and Robson de Oliveira Albuquerque
Electrical
Engineering Department – ENE – University
of Brasília – UNB
Brasília – DF, Brazil, 70910-900.
E-mails: {ednacanedo@unb.br}{robson@unb.br}

Rafael Timóteo de Sousa Junior
Electrical
Engineering Department – ENE – University
of Brasília – UNB
Brasília – DF, Brazil, 70910-900.
{desousa@unb.br}

***Abstract*—The recent advances in cloud computing have risen a number of unforeseen security related issues in different aspects of cloud environments. Among these, the problem of guaranteeing secure access to computing resources in the cloud is gathering special attention. In this paper, we address open issues related to trust in cloud environments proposing a new trust model for cloud computing which considers a higher level view cloud resources.**

***Keywords*-Cloud Computing; Distributed Computing; Security; Integrity; Confidentiality; Trust and Availability.**

I. Introduction

The widespread use of Internet connected systems and distributed applications has triggered a revolution towards the adoption of pervasive and ubiquitous cloud computing environments. These environments allow users and clients to purchase computing power according to necessity, elastically adapting to different performance needs while providing higher availability. Several web-based solutions, such as Google Docs and Customer Relationship Management (CRM) [2] applications, now operate in the software as a service model. Much of this flexibility is made possible by virtual computing methods, which can provide adaptive resources and infrastructure in order to support scalable on-demand sales of such applications. Virtual computing is also applied to stand-alone infrastructure as a service solutions, such as Amazon Elastic Cloud Computing (EC2) and Elastic Utility Computing Architecture Linking Your Programs to Useful Systems (Eucalyptus) [2].

As a result, the cloud computing frameworks and environments are able to address different issues in current distributed and ubiquitous computing systems.

The availability of infrastructure as a service and platform as a service environments provided a fundamental base for building cloud computing based applications. It also motivated the research and development of technologies to support new applications. As several large companies in the communications and information technology sector have adopted cloud computing based applications, this approach is becoming a de facto industry standard, being widely adopted by different organizations.

Since the adoption of the cloud computing paradigm by IBM Corporation around the end of 2007, other companies such as Google (Google App Engine), Amazon (Amazon Web Services (AWS), EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service)), Apple (iCloud) and Microsoft (Azure Services Platform) have progressively embraced it and introduced their own new products based on cloud computing technology [11]. However, cloud computing still poses risks related to data security in its different aspects (integrity, confidentiality and authenticity).

In this paper, we review the main cloud computing architecture patterns and identify the main issues related to security, privacy, trust and availability. In order to address such issues, we present a high level architecture for trust models in cloud computing environments.

This paper is organized as follows. In Section II, we present an overview of cloud computing, presenting a summary of its main features, architectures and deployment models. In Section III, we present related works. In Section IV, we introduce the proposed trust model. Finally, in Section V, we conclude with a summary of our results and directions for new research.

II. Cloud Computing

Cloud computing refers to the use, through the Internet, of diverse applications as if they were installed in the user's computer, independently of platform and location. Several formal definitions for cloud computing have been proposed by industry and academia. We adopt the following definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [14]. This definition includes cloud architectures, security, and deployment strategies.

Cloud computing is being progressively adopted in different business scenarios in order to obtain flexible and reliable computing environments, with several supporting solutions available in the market. Being based on diverse technologies (e.g. virtualization, utility computing, grid computing and service oriented architectures) and constituting a whole new computational paradigm, cloud computing requires high level management routines. Such management activities include: (a) service provider selection; (b) virtualization technology selection; (c) virtual resources allocation; (d) monitoring and auditing in order to guarantee Service Level Agreements (SLA).

Computational trust can be leveraged in order to establish an architecture and a monitoring system encompassing all these needs and still supporting usual activities such as planning, provisioning, scalability and security. Chang et al. [15] present a few challenges related to security, performance and availability in the cloud.

A. *Characteristics of Cloud Computing*

One advantage of cloud computing is the possibility of accessing applications directly from the Internet, with minor requirements of user computing resources. There are other significant advantages and disadvantages [13], as shown in Table I.

In cloud computing environments, the user does not need to know all the structure of the system that he is part of. For instance, the user does not need to be aware of information such as how many servers execute a given tool, hardware and software configurations, scalability measures physical data center location. Being relieved of managerial duties, the user can simply and transparently access the applications and tools necessary for performing his main business activities.

TABLE I. ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING

Advantages	Disadvantages
Lower IT infrastructure cost	Requires a constant Network connection
Increased computing power	Dependable of network bandwidth
Unlimited storage capacity	Features might be limited
Improved compatibility between operating Systems	Stored data might not be secure
Easier group collaboration	If the cloud loses your data, you will not have access to your information.
Universal access to documents	

Cloud computing combines a shared and statistical service model. It presents three basic characteristics [1]: a) hardware infrastructure architecture – based on low cost scalable clusters. The computing infrastructure in the cloud is composed of a great number of low cost servers, such as standard X86 server nodes; b) collaborative development of basic services and applications with maximal resource utilization, thus improving traditional software engineering processes. In the traditional computational model, applications become completely dependent on the basic services; c) the redundancy among several low cost servers is guaranteed through software. Since a large number of low cost servers is used, individual node failures cannot be ignored. Therefore, node fault tolerance must be taken into account in the design of software.

B. *Cloud Computing Architecture*

Cloud computing architecture is based on layers. Each layer deals with a particular aspect of making application resources available. Basically there are two main layers: a lower and a higher resource layer. The lower layer comprises the physical infrastructure and is responsible for the virtualization of storage and computational resources. The higher layer provides specific services. These layers may have their own management and monitoring system, independent of each other, thus improving flexibility, reuse and scalability. Figure 1 presents the cloud computing architectural layers [11].

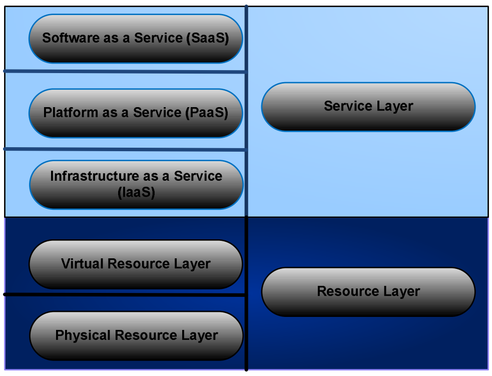

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Layer
Virtual Resource Layer
Physical Resource Layer
Resource Layer

Figure 1. Cloud Computing Architecture [11]

C. *Software as a Service*

Software as a Service (SaaS) provides all the functions of a traditional application, but provides access to specific applications through Internet. The SaaS model reduces concerns with application servers, operating systems, storage, application development, etc. Hence, developers may focus on innovation, and not on infrastructure, leading to faster software systems development.

SaaS systems reduce costs since no software licenses are required to access the applications. Instead, users access services on demand. Since the software is mostly Web based, SaaS allows better integration among the business units of a given organization or even among different software services. Examples of SaaS include [2]: Google Docs and Customer Relationship Management (CRM) services.

D. *Platform as a Service*

Platform as a Service (PaaS) is the middle component of the service layer in the cloud. It offers users software and services that do not require downloads or installations. PaaS provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations [4].

PaaS provides an operating system, programming languages and application programming environments. Therefore, it enables more efficient software systems implementation, as it includes tools for development and collaboration among developers. From a business standpoint, PaaS allows users to take advantage of third party services, increasing the use of a support model in which users subscribe to IT services or receive problem resolution instructions through the Web. In such scenarios, the work and the responsibilities of company IT teams can be better managed. Examples of SaaS [2] include: Azure Services Platform (Azure), Force.com, EngineYard and Google App Engine.

E. Infrastructure as a Service

Infrastructure as a Service (IaaS) is the portion of the architecture responsible for providing the infrastructure necessary for PaaS and SaaS. Its main objective is to make resources such as servers, network and storage more readily accessible by including applications and operating systems. Thus, it offers basic infrastructure on-demand services. IaaS has a unique interface for infrastructure management, an Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. Eventually he can also select network components such as firewalls.

The term IaaS refers to a computing infrastructure, based on virtualization techniques that can scale dynamically, increasing or reducing resources according to the needs of applications. The main benefit provided by IaaS is the pay-per-use business model [4]. Examples of IaaS [2] include: Amazon Elastic Cloud Computing (EC2) and Elastic Utility Computing Architecture Linking Your Programs To Useful Systems (Eucalyptus).

F. Roles in Cloud Computing

Roles define the responsibilities, access and profile of different users that are part of a cloud computing solution. Figure 2 presents these roles defined in the three service layers [3].

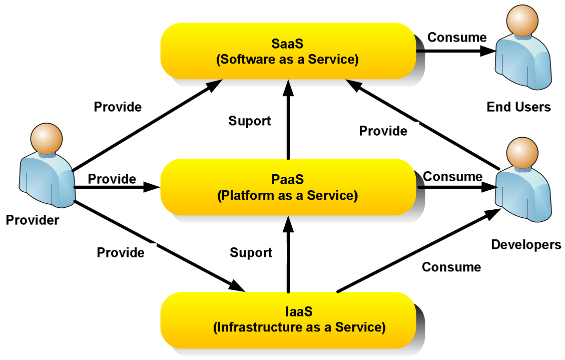


Figura 2. Roles in cloud computing [3].

The provider is responsible for managing, monitoring and guaranteeing the availability of the entire structure of the cloud computing solution. It frees the developer and the final user from such responsibilities while providing services in the three layers of the architecture.

Developers use the resources provided by IaaS and PaaS to provide software services for final users.

This multi-role organization helps to define the actors (people who play the roles) in cloud computing environments. Such actors may play several roles at the same time according to need or interest. Only the provider supports all the service layers.

G. Cloud Computing Deployment

According to the intended access methods and availability of cloud computing environments, there are different models of deployment [4]. Access restriction or permission depends on business processes, the type of information and characteristics of the organization. In some organizations, a more restrict environment may be necessary in order to ensure that only properly authorized users can access and use certain resources of the deployed cloud services. A few deployment models for cloud computing are discussed in this section. They include private cloud, public cloud, community cloud and hybrid cloud, which are briefly analyzed below.

Private: In this model, the cloud infrastructure is exclusively used by a specific organization. The cloud may be local or remote, and managed by the company itself or by a third party. There are policies for accessing cloud services. The techniques employed to enforce such private model may be implemented by means of network management, service provider configuration, authorization and authentication technologies or a combination of these.

Public: Infrastructure is made available to the public at large and can be accessed by any user that knows the service location. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used.

Community: Several organizations may share the cloud services. These services are supported by a specific community with similar interests such as mission, security requirements and policies, or considerations about flexibility. A cloud environment operating according to this model may exist locally or remotely and is normally managed by a commission that represents the community or by a third party.

Hybrid: Involves the composition of two or more clouds. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds.

III. RELATED WORKS

In this section, we present related works in the fields of security, file systems and trust in the cloud.

A. Security in the Cloud

A number of technologies have been employed in order to provide security for cloud computing environments. The creation and protection of security certificates is usually not enough to ensure the necessary security levels in the cloud. Cryptographic algorithms used with cloud applications usually reduce performance and such reduction must be restricted to acceptable levels [21].

Cloud computing offers users a convenient way of sharing a large quantity of distributed resources belonging to different organizations. On the other hand, the very nature of the cloud computing paradigm makes security aspects quite more complex. Trust is the main concern of consumers and service providers in a cloud computing environment [7]. The inclusion of totally different local systems and users of quite diverse environments brings special challenges to the security of cloud computing. On one hand, security mechanisms must offer users a high enough level of guarantees. On the other hand, such mechanism must not be so complex as to make it difficult for users to use the system. The openness and computational flexibility of popular commercially available operating systems have been important factors to support the general adoption of cloud computing. Nevertheless, these same factors increase system complexity, reduce the degree of trust and introduce holes that become threats to security [7].

Huan et al. [22] investigate the different security vulnerability assessment methods for cloud environments. Experiments show that more vulnerabilities are detected if vulnerable tools and servers are in the same LAN. In other word, the hackers can find an easier way to get the target information if it is on the same LAN of compromised systems. Experimental results can be used to analyze the risk in third party compute clouds.

Popovic et al. [23] discuss security issues, requirements and challenges that Cloud Service Providers (CSP) face during cloud engineering. Recommended security standards and management models to address these are suggested both for the technical and business community.

B. Filesystem Security

As the number of devices managed by users is continually increasing, there is a growing necessity of synchronizing several hierarchically distributed file systems using ad-hoc connectivity. Uppoor et al. [6] present a new approach for synchronizing of hierarchically distributed file systems. Their approach resembles the advantages of peer-to-peer synchronization, storing online master replicas of the shared files. The proposed scheme provides data synchronization in a peer-to-peer network, eliminating the costs and bandwidth requirements usually present in cloud computing master-replica approaches.

The work in [9] presents CDRM, a scheme for dynamic distribution of file replicas in a cloud storage cluster. This scheme periodically updates the number and location of file block replicas in the cluster. The number of replicas is updated according to the actual availability of cluster nodes and the expected file availability. The dynamic distribution algorithm for replica placement takes into account the storage and computational capacity of the cluster nodes, as well as the bandwidth of the communication network. An implementation of the proposed scheme using an open source distributed file system named HDFS (Hadoop Distributed File System) is discussed. Experimental measurements point out that the dynamic scheme outperforms existing static file distribution algorithms.

C. Trust

The concepts of trust, trust models and trust management have been the object of several recent research projects. Trust is recognized as an important aspect for decision-making in distributed and auto-organized applications [19] [20]. In spite of that, there is no consensus in the literature on the definition of trust and what trust management encompasses. In the computer science literature, Marsh is among the first to study computational trust. Marsh [19] provided a clarification of trust concepts, presented an implementable formalism for trust, and applied a trust model to a distributed artificial intelligence (DAI) system in order to enable agents to make trust-based decisions. Marsh divided trust into three categories: **1. Basic Trust** – This is the level of trust which represents the general trust disposition of agent X ∈ 2 A at time t. 2. **General Trust** – Given agents x, y ∈ A, the general trust $Tx(y)^t$ represents the amount of trust that x has in y at time t. 3. **Situational Trust** – Given agents x, y ∈ A, and a situation α, the situational trust $Tx(y,\alpha)^t$ represents the amount of trust that x has in y in situation α at time t.

Beth et al. [20] also proposed a trust model for distributed networks. They derived trust recommendations from direct trust and gave them formal representations, as well as rules to derive trust relationships and algorithms to compute trust values. Josang et al. [24] describe a trust model where positive and negative feedback about a specific member is accumulated. The model is based on the Bayesian network model, using the beta probability density function to calculate a member's expected future behavior.

Trust is considered to be more than the authorized nature of security relations between human societies, which achieve stable and healthy operation, to a large extent thanks to the trust relationship between the individuals, groups and organizations. Therefore, in a large number of dynamic user-oriented open network environments, the study of the trust relationships between the trust-based security mechanisms to ensure the safe operation of distributed applications has become a fundamental topic. Currently, most scholars have reached a consensus that trust should have three important features [25], which are discussed bellow.

1) Subjectivity (different entities of the same view of things which will be affected by factors such as individual preferences may vary);

2) The expected probability (the degree of trust can be extracted and formalized as the estimated likelihood of a given event);

3) Relevance (trust is an aspect of things, for specific content).

In recent works on trust, mainly two distinct methods are used for subjective trust reasoning: probabilistic reasoning based on statistical hypothesis testing; and approaches based on fuzzy theory, expert systems and artificial intelligence techniques. However, these methods do not fully reflect the essential nature of trust. Subjective trust, in essence, is based on the belief that it has great uncertainty. In the subjective, objective world, random and fuzzy uncertainties are the two main forms that have become the industry consensus [26]. Thus, the axiomatic methods based on probability theory or fuzzy set theory do not achieve a comprehensive assessment of trust information.

D. Trust in the Cloud

Trust and security have become crucial to guarantee the healthy development of cloud platforms, providing solutions for concerns such as the lack of privacy and protection, the guarantee of security and author rights.

Privacy and security have been shown to be two important obstacles concerning the general adoption of the cloud computing paradigm. In order to solve these problems in the IaaS service layer, a model of trustworthy cloud computing which provides a closed execution environment for the confidential execution of virtual machines was proposed [5]. This work has shown how the problem can be solved using a Trusted Platform Module. The proposed model, called Trusted Cloud Computing Platform (TCCP), is supposed to provide higher levels of reliability, availability and security. In this solution, there is a cluster node that acts as a Trusted Coordinator (TC). Other nodes in the cluster must register with the TC in order to certify and authenticate its key and measurement list. The TC keeps a list of trusted nodes. When a virtual machine is started or a migration takes place, the TC verifies whether the node is trustworthy so that the user of the virtual machine may be sure that the platform remains trustworthy. A key and a signature are used for identifying the node. In the TCCP model, the private certification authority is involved in each transaction together with the TC [5].

Shen et al. [7] presented a method for building a trustworthy cloud computing environment by integrating a Trusted Computing Platform (TCP) to the cloud computing system. The TCP is used to provide authentication, confidentiality and integrity [7]. This scheme displayed positive results for authentication, rule-based access and data protection in the cloud computing environment.

Cloud service providers (CSP) should guarantee the services they offer, without violating users' privacy and confidentiality rights. Li et al. [8] introduced a multi-tenancy trusted computing environment model (MTCEM). This model was designed for the IaaS layer with the goal of ensuring a trustworthy cloud computing environment to users. MTCEM has two hierarchical levels in the transitive trust model that supports separation of concerns between functionality and security. It has 3 identity flows: a) the consumers, who hire the CSP cloud computing services; b) the CSP, that provides the IaaS services; c) the auditor (optional, but recommended), who is responsible for verifying whether the infrastructure provided by the CSP is trustworthy on behalf of users. In MTCEM, the CSP and the users collaborate with each other to build and maintain a trustworthy cloud computing environment.

Zhimin et al. [12] propose a collaborative trust model for firewalls in cloud computing. The model has three advantages: a) it uses different security policies for different domains; b) it considers the transaction contexts, historic data of entities and their influence in the dynamic measurement of the trust value; and c) the trust model is compatible with the firewall and does not break its local control policies. A model of domain trust is employed. Trust is measured by a trust value that depends on the entity's context and historical behavior, and is not fixed. The cloud is divided in a number of autonomous domains and the trust relations among the nodes is divided in intra and inter-domain trust relations. The intra-domain trust relations are based on transactions operated inside the domain. Each node keeps two tables: a direct trust table and a recommendation list. If a node needs to calculate the trust value of another node, it first checks the direct trust table and uses that value if the value corresponding to the desired node is already available. Otherwise, if this value is not locally available, the requesting node checks the recommendation list in order to determine a node that has a direct trust table that includes the desired node. Then it checks the direct trust table of the recommended node for the trust value of the desired node. The process continues until a trust value for the desired node is found in a direct trust table of some node. The inter-domain trust values are calculated based on the transactions among the inter-domain nodes. The inter-domain trust value is a global value of the nodes direct trust values and the recommended trust value from other domains. Two tables are maintained in the Trust Agents deployed in each domain: form of Inter-domain trust relationships and the weight value table of this domain node.

In [17] a trusted cloud computing platform (TCCP) which enables IaaS providers to offer a closed box execution environment that guarantees confidential execution of guest virtual machines (VMs) is proposed. This system allows a customer to verify whether its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity. The TCCP guarantees the confidentiality and the integrity of a user's VM, and allows a user to determine up front whether or not the IaaS enforces these properties.

The work [18] evaluates a number of trust models for distributed cloud systems and P2P networks. It also proposes a trustworthy cloud architecture (including trust delegation and reputation systems for cloud resource sites and datacenters) with guaranteed resources including datasets for on-demand services.

IV. High Level Trust Model For File Sharing

According to the review and related research [5] [6] [7] [8] [10] [12] [17], it is necessary to employ a cloud computing trust model to ensure the exchange of files among cloud users in a trustworthy manner. In this section, we introduce a trust model to establish a ranking of trustworthy nodes and enable the secure sharing of files among peers in a public cloud.

We propose a trust model where the selection and trust value evaluation that determines whether a node is trustworthy can be performed based on node storage space, link and processing capacity. For example, if a given client has access to a storage space in a public cloud, it still has no selection criterion to determine to which cloud node it will send a particular file.

When a node wants to share files with other users, it will select trusted nodes to store this file through the following metrics: processing capacity (the average workload processed by the node, for example, if the node's processing capacity is 100% utilized, it will take longer to attend any demands), storage capacity and link (better communication links and storage resources imply greater trust values, since they increase the node's capacity of transmitting and receiving information). The trust value is established based on queries sent to nodes in the cloud, considering the metrics previously described.

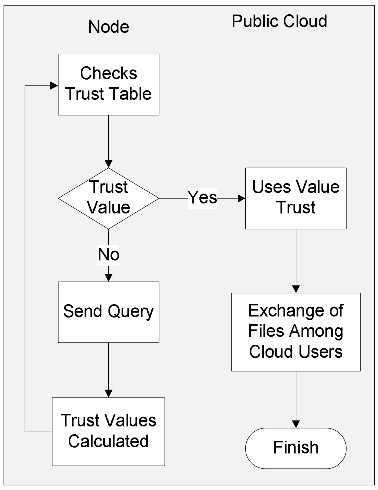


Figure 3. Proposed Trust Model.

Each node maintains two trust tables: direct trust table and the recommended list. a) If a node needs to calculate the trust value of another node, it first checks the direct trust table and uses the trust value if the value for the node exists. If this value is not available yet, then the recommended lists are checked to find a node that has a direct trust relationship with the desired node the direct trust value from this node's direct trust table is used. If there's no value attached, then it sends a query to its peers requesting information on their storage space, processing capacity and link. The trust values are calculated based on queries exchanged between nodes.

b) The requesting node will assign a greater trust value to nodes having greater storage capacity and / or processing and better link.

The trust value of a node indicates its suitability for storage and cloud operations. This value is calculated based on the historical interactions of the node, being represented by T_{np}, for a given node. Its value may range from 0 to 1. As we have previously stated, the value of T_{np} is calculated from queries exchanged between nodes regarding their overall system capacities. Figure 3 presents a high level view the proposed trust model, where the nodes query their peers to obtain the information needed to build their local trust table.

In this model, a trust rank is established, allowing a node A to determine whether it is possible to trust a node B to perform storage operations in a public cloud. In order to determine the trust value of B, node A first has to obtain basic information on this node. Figure 4 depicts the query exchange process used for gathering the necessary trust information from a node B by a node A.

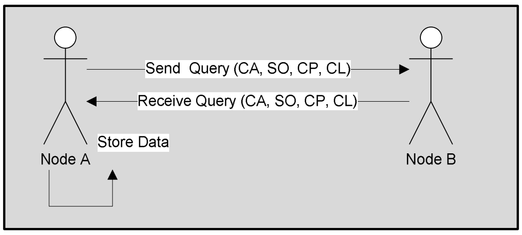


Figure 4. Scenario of Information Request

Node A needs to exchange a file in the cloud and wants know if the node B can be trusted to store and send the file. The protocol Trust Model can be described as follows: In step 1, A sends a query to B regarding its storage capacity, operating system, processing capacity and link. In step 2, B sends a response to he query sent by A, providing the requested information. In step 3, node A evaluates the information received from B and, if the information is consistent, it is stored in A's local trust table. In general, the trust of node A in node B, in the context of a public cloud NP, can be represented by:

$$T_{a,b}^{np} = V_{np}^{b} \tag{1}$$

Where V_{np}^{b} is the trust value of B in the public cloud NP analyzed by A and $T_{a,b}^{np}$ represents the trust of A in B, in the public cloud NP. According to the definition of trust, V_{np}^{b} equals the queries sent and received (interaction) by A and B in the cloud NP.

The trust information may be stored as individual records of interaction with the respective node, being recorded in a local database that contains information about the behavior of each node in the cloud. Thus, the trust of node A in node B in the cloud NP can be represented by:

$$T_{a,b}^{fnp} = \frac{\sum_{i=1}^{j} V_{npi}^{b}}{j}\text{, for j > 0} \tag{2}$$

$T_{a,b}^{fnp}$ represents the final trust of A in B in the cloud NP, while j represents the number of interactions / querys between nodes A and B in the cloud NP.

V. CONCLUSION

We have presented an overview of the cloud computing paradigm, as well as its main features, architectures and deployment models. Moreover, we identified the main issues related to trust and security in cloud computing environments.

In order to address these issues, we proposed a trust model to ensure reliable exchange of files among cloud users in public clouds. In our model, the trust value of a given node is obtained from a pool of simple parameters related to its suitability for performing storage operations. Nodes with greater trust values are subsequently chosen for further file storage operations.

As a future work, we plan to implement the proposed trust model and analyze node behavior after the ranking of trustworthy nodes is established.

ACKNOWLEDGMENT

This work resulted from applyed research supported by Dell Computers of Brazil and the Brazilian Ministry of Planning, Budget and Management.

REFERENCES

[1] Chen Kang and Zen WeiMing, “Cloud computing: system instance and current research,” Journal of Software, pp. 20(5):1337-1347. 2009.

[2] Minqi Zhou, Rong Zhang, Dadan Zeng, and Weining Qian, “Services in the cloud computing era: a survey,” Software Engineering Institute. Universal Communication. Symposium (IUCS), 4th International. IEEE Shanghai, pp. 40-46. China. 978-1-4244-7821-7 (2010).

[3] A. Marinos and G. Briscoe, “Community cloud computing,” in First International Conference Cloud Computing, CloudCom, volume 5931 of Lecture Notes in Computer Science, pp. 472–484. Springer (2009).

[4] P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft). National Institute of Standards and Technology. http://csrc.nist.gov/groups/SNS/cloud-computing. 2009. 30 may 2011.

[5] Wang Han-zhang and Huang Liu-sheng, “An improved trusted cloud computing platform model based on DAA and Privacy CA scheme,” IEEE International Conference on Computer Application and System Modeling (ICCASM 2010). 978-1-4244-7235-2. 2010.

[6] S. Uppoor, M. Flouris, and A. Bilas, “Cloud-based synchronization of distributed file system hierarchies,” Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS), IEEE International Conference, pp. 1-4. 2010.

[7] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, “Cloud Computing System Based on Trusted Computing Platform,” Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[8] Xiao-Yong Li, Li-Tao Zhou, Yong Shi, and Yu Guo, “A Trusted Computing Environment Model in Cloud Architecture,” Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, 978-1-4244-6526-2. Qingdao, pp. 11-14. China. July 2010.

[9] Qingsong Wei, Bharadwaj Veeravalli, Bozhao Gong, Lingfang Zeng, and Dan Feng, “CDRM: A Cost-Effective Dynamic Replication Management Scheme for Cloud Storage Cluster,” 2009 IEEE International Conference on Cluster Computing (CLUSTER), pp. 188-196, 2010.

[10] Kai Hwang, Sameer Kulkareni, and Yue Hu, “Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement,” 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC ’09), pp. 717-722, 2009.

[11] Xue Jing and Zhang Jian-jun, “A Brief Survey on the Security Model of Cloud Computing,” 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), Hong Kong IEEE, pp. 475 – 478. Aug 2010.

[12] Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, and Guangming Wan, “A collaborative trust model of firewall-through based on Cloud Computing,” Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China. pp. 329-334, 14-16. 2010.

[13] M. Miller, Cloud Computing – Web-Based Applications That Change the Way You Work and Collaborate Online, Que Publishing, Pearson Education, Canada 2008.

[14] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," 21. Aug 2009.

[15] T. Dillon, Chen Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 27-33. Australia, 2010.

[16] Li Xiaoqi, Lyu M R, and Liu Jiangchuan. “A trust model based routing protocol for secure AD Hoc network,” Proceedings of the 2004 IEEE Aerospace Conference, pp. 1286-1295. 2004.

[17] N. Santos, K. Gummadi, and R. Rodrigues, “Towards Trusted Cloud Computing,” Proc. HotCloud. June 2009.

[18] Kai Hwang, Sameer Kulkareni, and Yue Hu, “Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement,” 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Chengdu, pp.717-722. China 2009.

[19] S. P. Marsh, “Formalising Trust as a Computational Concept”, Ph.D. Thesis, University of Stirling, 1994.

[20] T. Beth, M. Borcherding, and B. Klein, “Valuation of trust in open networks,” In ESORICS 94. Brighton, UK, November 1994.

[21] H. Takabi, J. B. D. Joshi, and G. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Nov./Dec. 2010, doi:10.1109/MSP.2010.186.

[22] Huan-Chung Li, Po-Huei Liang, Jiann-Min Yang, and Shiang-Jiun Chen, “Analysis on Cloud-Based Security Vulnerability Assessment,” 2010 IEEE 7th International Conference on e-Business Engineering (ICEBE), pp. 490-494, 2010.

[23] K. Popovic and Z. Hocenski, “Cloud computing security issues and challenges,” MIPRO, 2010 Proceedings of the 33rd International Convention, pp. 344-349, 24-28 May 2010 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533317&isnumber=5533310.

[24] A. Jøsang and R. Ismail, “The Beta Reputation System,” In Proceedings of the 15th Bled Electronic Commerce Conference, pp. 17-19. June 2002.

[25] A. Abdul-Rahman and S. Hailes, “A distributed trust model,” In Proceedings of the 1997 New Security Paradigms Workshop, pp. 48-60, 1998.

[26] A. Jφsang and S. J. Knapskog, “A metric for trusted systems,” Global IT Security, pp. 541-549, 1998.

[27] Zhao-xiong Zhou, He Xu, and Suo-ping Wang, “A Novel Weighted Trust Model based on Cloud,” AISS: Advances in Information Science and Service Sciences, Vol. 3, No. 3, pp. 115- 124, April 2011.

Connecting the Unconnected

Bluetooth and 802.11 in harmony

Curtis Sahd
Department of Computer Science
Rhodes University
Grahamstown, South Africa
curtissahd@gmail.com

Hannah Thinyane
Department of Computer Science
Rhodes University
Grahamstown, South Africa
h.thinyane@ru.ac.za

***Abstract*—Many new cell phones on the market come with 802.11 enabled, along with standard Bluetooth functionality. A large percentage of working class people in South Africa typically cannot afford 802.11 enabled cell phones, and thus the most applicable form of wireless data transfer is achieved through the Bluetooth protocol. This paper investigates bridging Bluetooth and 802.11 protocols on low cost wireless routers equipped with a Broadcom chip and a USB port, as well as bridging on high end cell phones. For the router component of this research, the BlueZ protocol stack will be implemented on top of the OpenWrt platform and experiments relating to the feasibility and scalability of SIP voice calls between clients on the Bluetooth network and clients on the wireless mesh network will be investigated. For the cell phone component of this bridging, Java Mobile will be used as the development platform of choice, and a comparison between bridging on the cell phone and on the wireless router will be conducted, with metrics such as latency, scalability, and minimum throughput will be considered. This paper proposes a low cost solution to building community telephone networks in rural South Africa, through the bridging of 802.11 and Bluetooth interfaces.**

Keywords – Wireless; SIP; Community telephone networks; BlueZ.

I. INTRODUCTION

The Bluetooth protocol has been around since 1994, and its primary function is to replace wires and serve as lightweight wireless implementation for data transfer. Even though most high end cell phones are equipped with 802.11, Bluetooth still serves as the primary data transfer protocol between cell phones in South Africa. Based on a survey conducted on the streets of Grahamstown, South Africa, it was discovered that most people called someone in Grahamstown or in the surrounding region on a daily basis. Currently, the only way to make phone calls, whether local or inter-town, is to make use of a fixed landline, which the vast majority of the underprivileged do not have access to, or to make use of the ever increasingly expensive mobile service providers. Paying sky high cellular network rates to make local phone calls places an enormous burden on already financially constrained rural communities. Bluetooth alone cannot be used in a full scale implementation which would enable free local phone calls. However, the combination of Bluetooth and 802.11 mesh networks could, in the context of South African rural communities, create a system which saves rural communities millions of Rand each year. Wireless mesh networks (WMNs) are dynamic, self-configuring networks which are design to span large geographical areas. WMNs could therefore be used to span the geographical area of the rural community, and possibly even connect remote rural communities to one another.

This paper aims to explore inexpensive means to creating low cost community telephone networks with existing technology in rural areas. We propose a system which enables the seamless integration of Bluetooth and 802.11 on the OpenWrt and Java Mobile (JME) platforms. We begin with an introduction to Bluetooth and in particular, Bluetooth networking with piconets and scatternets. We then provide a brief overview of the OpenWrt platform and focus on mesh networking, as well as reviewing related work in this area. Section IV then describes the Mesh Potato, and the possibilities it presents in rural areas. This overview is then followed by an in depth analysis of the proposed infrastructure of the Blue Bridge, and the associated advantages and disadvantages of various implementations. Section VI describes the context of this paper and how the proposed technology can be beneficial to rural communities and coincides with objectives of various social reconstruction programmes. Section VII then concludes this paper.

II. BLUETOOTH PERSONAL AREA NETWORKS

A. Overview

At initial conception Bluetooth was considered the future of Personal Area Networks (PANs), due to it being a lightweight protocol and the inexpensive manufacturing of Bluetooth chips [1]. The Bluetooth specification clearly defines PANs and associated roles of the nodes in the PAN in the case where two devices are communicating directly. The Bluetooth specification also defines the roles of nodes in multi-hop environments, but less research has been conducted in this field [1]. Asthana and Kalofonos [2] have developed a custom protocol which enables the seamless communication of existing Piconets within a Scatternet. Specifically, their research allows for the creation of Ethernet and IP local links on top of scatternets through the use of a standard PAN profile implementation, without the need for ad hoc forwarding protocols [2].

Plenty of research has been done in the field of providing Internet Access to rural communities. There has been little to no research in the field of making use of low cost hardware infrastructure to bridge Bluetooth and 802.11 which enables large scale service provision to local and remote rural communities. Bluetooth Piconets and Scatternets are an important component of bridging Bluetooth and 802.11 mesh networks, as in some cases devices will be able to communicate directly with one another (Piconets) and in other cases devices may only be able to communicate by sending traffic through a number of other nodes before reaching the desired node (more applicable to Scatternets). With that said, many researchers have investigated the formation and limitations of Mobile Ad-hoc Networks (MANETs) with the Bluetooth protocol [1].

B. *Piconets and Scatternets*

According to Bisdikian [3] a piconet is simply defined as a collection of Bluetooth devices which can communicate with one another. A piconet consists of one master node and one or more slave nodes, and exists for as long as the master communicates with the slaves. Piconets are formed in an ad-hoc manner, and need a minimum of one master node and maximum of seven active slave nodes. Although only seven active nodes are able to transmit based on coordination of the master node, other nodes are able to connect to the piconet, and are said to be in a parked state [3].

Scatternets are based on piconets and are said to exist when one device is a member of multiple piconets. In the case of scatternets, a node can only serve as the master node for one piconet.

For the purposes of this research it is important to understand the functioning of piconets and scatternets in order to handle the association of clients to the Bluetooth access point.

III. OPENWRT

OpenWrt is defined as Linux for embedded devices [4]. OpenWrt provides a plethora of opportunities for robust application development and service provision on embedded devices, and for the purposes of this research, specifically on wireless routers. In order to grasp the functioning of OpenWrt it is necessary to understand the various components of the software which manages wireless routers and for that matter any embedded device. The software which runs on computer chips or on embedded device chips is known as firmware [5]. The following are a few of the many types of chips which have firmware installed on them: read-only memory (ROM); programmable read-only memory (PROM); erasable programmable read-only memory (EPROM). PROMs and EPROMs are designed to allow firmware updates through a software update [5]. In order to compile custom Linux firmwares on embedded devices, a technique known as cross compiling is used, where a new compiler is produced, which is capable of generating code for a particular platform, and this compiler is then able to compile a linux distribution customized for a particular device [6]. Generally, the cross-compiling process begins with a binary copy of a compiler and basic libraries, rather than the daunting task of creating a compiler from scratch [6]. The remainder of this section describes mesh networking principles and practices on the OpenWrt platform, as well as the state of the art in rural mesh networks.

OpenWrt contains a number of packages which assist with the implementation of mesh networks. Optimized Link State Routing Protocol (OLSR) is an example of a routing protocol developed by Andreas Tønnesen which has been implemented in the form of a package for OpenWrt [7]. Another Open Source mesh networking implementation known as ROBIN (ROuting Batman Inside) has been developed on top of OpenWrt Kamikaze [8]. ROBIN is self-configuring and self-maintaining, which enables the seamless creation of wireless mesh networks. ROBIN requires a minimum of one Digital Subscriber Line (DSL) connection, a Dynamic Host Configuration Protocol (DHCP) enabled router which is connected to the DSL line and serves as the gateway node [4]. Client repeater nodes simply have to be powered on and a mesh network is dynamically configured [4]. With that said, open mesh networking protocols, which simplify the creation and extension of mesh networks, can be utilized in rural communities. Mesh networks thus serve as a low cost alternative to information technology service provision in rural areas, providing significantly more benefits than drawbacks. The benefits of mesh networks in rural communities have been extensively discussed [8] [9]. Reguart et al. [8] suggest that mesh networking technologies in urban areas are often unsuited to rural areas due to the high cost of equipment and maintenance. They proposed and tested Wireless Distribution System (WDS) by making use inexpensive wireless hardware (Linksys WRT54AG and Linksys WRT54G). Through a prototype deployment of their infrastructure they found that inexpensive wireless equipment is capable of providing fourty people with internet access, and at any one point in time there are between fifteen and thirty active clients [8]. The aforementioned implementation performs surprisingly well for sparsely situated rural communities, but would not suffice for the purposes of South African rural communities for the following reasons: Rural communities in South Africa are densely populated; laptops are seldom found in rural areas, as most of the people are living below the breadline and cannot afford such equipment; even if everyone had access to laptops, the use of inexpensive wireless equipment as used above would be overloaded and the end result would most likely be malfunction; also the use of secured outdoor equipment is imperative in the context of South Africa due to crime levels.

IV. THE MESH POTATO

The Mesh Potato is a new device which merges the ideas of current telephony (analog phones) and future technology (reliable wireless communications). The Mesh Potato combines a wireless access point (AP) with an Analog Telephony Adapter (ATA), and thus enables cheap communications using existing technology [17]. Routers by Meraki [18] and OpenMesh [19] are gaining popularity due to their low cost and robustness, but they however lack the functionality contained within the Mesh Potato in terms of integration with existing telephonic infrastructure.

Although rural areas in South Africa are often on the outskirts of town, plenty of remote and isolated settlements exist, and more often than not, these settlements lack infrastructure such as running water, sewage and waste removal, and electricity. In such cases where electricity is scarce or non-existent, the Mesh Potato is ideal since it can be powered by a 10w solar panel [17].

The Mesh Potato is powered by Open Source firmware (Linux, OpenWrt, B.A.T.M.A.N and Asterisk) which removes vendor lock in and makes the Mesh Potato cost effective and highly configurable [17]. The Mesh Potato enables the seamless connection of analog telephones, as well as wired and wireless IP phones. Cellular technology is the primary form of communication in rural areas in South Africa, and although analog phones are inexpensive and could be subsidized by the government, the Mesh Potato is currently unable to cater for the existing needs of people in rural areas.

V. PROPOSED BRIDGING INFRASTRUCTURE

After extensive literature reviews we found that there is a lack of knowledge in the field of Bluetooth and 802.11 bridging in the context of rural communities in Africa, and as such we propose a system (Blue Bridge) which not only deals with remote access to such communities, but also enables service provision through the use of inexpensive and readily available technology thus connecting the unconnected. The system will be centered around the OpenWrt firmware, which is to be installed on the Ubiquiti AirRouter [10]. The AirRouter will not only serve as an interface for 802.11 connections, but will also become a Bluetooth access point through the use of the BlueZ protocol stack which controls the functioning of the Bluetooth dongle inserted into the USB port of the AirRouter. Asterisk [11] will be installed as a package on the OpenWrt platform, and will serve as the SIP controller. A package will be developed for the OpenWrt platform which will bridge the connections between the 802.11 and Bluetooth interfaces. Fig. 1 shows the proposed infrastructure involving one AirRouter:

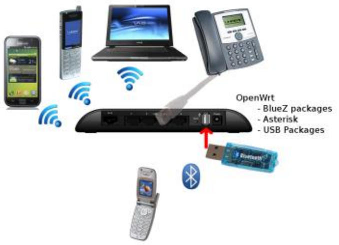


Figure 1. Proposed OpenWrt infrastructure for low cost community telephone network.

Any cell phone on the Bluetooth interface of the Blue Bridge should be able to place SIP calls to any other phone on the Bluetooth interface, as well as to any phone on the 802.11 interface. Of course as mentioned in Section B a maximum of seven active connections can exist on the Bluetooth interface, which clearly places limitations on the scalability of the proposed system.

With the aforementioned, the components of the proposed system include the AirRouter (running OpenWrt); the USB Bluetooth dongle; and a JavaME enabled cell phone, which the majority of the surveyed population possesses. The aim of this research is to provide Bluetooth access (via the connected Bluetooth USB dongle) as well as 802.11 access to multiple geographically dispersed routers which in turn enables the creation of community telephone networks, thus connecting the unconnected, and significantly decreasing the burden of expensive cellular calls.

The ideal scenario is the use of minimal equipment, while still maintaining an acceptable level of service provision. This translates to decent quality voice calls, with minimal downtime. In order to achieve this, an understanding of the Bluetooth protocol and its scalability limitations is vitally important. Sahd [12] conducted a study which investigated the real throughput achieved by the Bluetooth protocol on mobile devices. Sahd [12] found that the average transfer speed of the Logical Link Control and Adaptation Protocol (L2CAP) when transferring a 6.6 MB M4A audio file twice between two cell phones is 136.39 KBps [12]. If a maximum of seven clients are connected to the Bluetooth interface each client would be allocated a bandwidth of 19.48 KBps. Based on the assumption that seven simultaneous connections are active on the Bluetooth interface, the minimum accumulated bandwidth for these connections is 27.35 KBps, which would allow a theoretical number of thirty five clients to be connected [13].

This research will also investigate the differences in performance of Blue Bridge implementations on the JME platform and on the OpenWrt platform. Of course the most prominent difference between implementations on the two platforms is the class of Bluetooth device. The OpenWrt platform implementation of the Blue Bridge will make use of a class one Bluetooth device which is capable of a distance of 100m, whereas cell phones typically contain class two Bluetooth chips which enables transmission at distances of 10m. Sahd [12] found that even though the Bluetooth specification states a distance of 10m, transmission is possible at distances as high as 15m.

Fig. 2 shows the proposed Blue Bridge infrastructure on the cell phone:

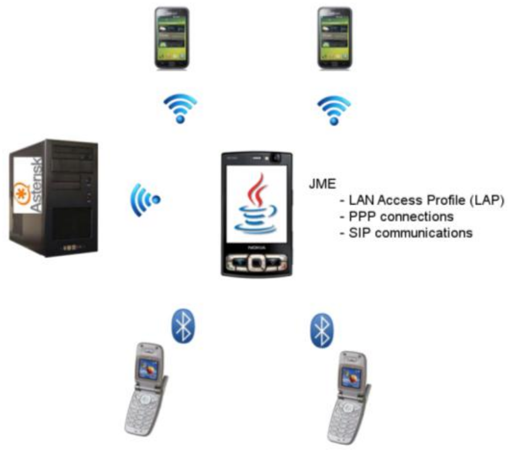


Figure 2. Proposed cell phone based infrastructure for low cost community telephone network.

From Fig. 2 it can be seen that an external asterisk server would have to substitute the asterisk server contained within the OpenWrt packages. The scalability of the internal asterisk server would have to be researched and compared to that of the external asterisk server. On the other hand, the Nokia N95 8GB could pose to be a severe bottleneck under load.

In order to determine which platform will serve as the basis for a community telephone network, a number of metrics would have to be compared. These metrics can be seen in Table I:

TABLE I. KNOWN METRICS OF PROPOSED BLUE BRIDGE PLATFORMS

Metrics	OpenWrt	Blue Bridge on cell phone
Cost	Cheap	More expensive
Compactness	Average	Very compact
Complexity	High	Medium
Platform	Linux	Java Mobile

Based on the information currently available, assumptions from the data in Table I could lead one to believe that the Blue Bridge on the cell phone would be the better alternative as a whole. However, metrics such as performance under load, scalability, and multi-hop capability can only be determined once the implementation and necessary research has been completed.

With the above overview of the equipment needed for the implementation of the Blue Bridge, subsection A provides information regarding the costs involved, and a means for funding the Blue Bridge.

A. *Costs and implementation considerations*

There are two important factors to consider when determining the cost, and the number of units necessary for the implementation of community telephone networks: the geographical area and the proposed number of connected clients. The geographical area plays a large role in determining the strength of the devices needed to transmit a good quality signal. Mountains, trees, buildings, and other obstructions have to be considered. The number of connected clients dictates the scalability of the system, and thus the overall cost of implementation. Table II provides an overview of the costs involved:

TABLE II. KNOWN METRICS OF PROPOSED BLUE BRIDGE PLATFORMS

Device	Cost	Means of funding
AirRouter 150Mbps WiFi Router	R313.50	Government
Mecer Class 1 USB Bluetooth (ENUBT-C1EM)	R169.00	Government
Basic machine for Asterisk server (1.8 GHz, 2GB RAM, 500GB HD)	R2700.00	Government

Based on the costs in Table II, the maximum total cost for a prototype system catering for seven connected nodes will come to a total of R3182.50. This value is of course inclusive of the Asterisk server machine, which would not be necessary if the Asterisk server were to be implemented on the AirRouter itself.

The average voice call from the Vodacom cellular network to another network costs R2.75 per minute [20]. Based on the assumption that seven people spend five minutes on the phone each day for one month, the total cost incurred is R2983.75. Even though the Bluetooth protocol only permits seven active clients, more than seven people could connect to one AirRouter, due to the unlikeliness of everyone placing calls simultaneously. With that said, it can be seen that in just one month, the costs incurred by impoverished communities can be drastically reduced. This rate is the highest rate per minute rate on the Vodacom prepaid plan, and was chosen to estimate the maximum amount of money spent on cell phone calls.

Section VI provides an overview of government initiatives to introduce equality in impoverished areas, as such all equipment and implementation costs would be government subsidized.

VI. CONTEXT

The reconstruction and development program (RDP) of South Africa is a program implemented by the African National Congress (ANC) which addresses socioeconomic problems which exist as a result of the Apartheid regime [14]. The RDP program is of great benefit to all South Africans and in particular, South Africans living in rural areas without basic necessities such as adequate housing, water and electricity. Traditionally RDP housing was built on plots of 250m^2 which placed tremendous strain on the fair land distribution due to special constraints [15]. Recently, there has been a movement from traditional RDP housing to more cost effective multi-storey RDP housing which reduces plot sizes from 250m^2 to 80m^2 [15][16]. With that said this poses as an ideal situation for the successful implementation of the Blue Bridge, as signal penetration will be higher and this type of RDP housing would prove more effective from a point of view of device mounting as well as line of sight access for surrounding residents. The Blue Bridge will benefit such communities immensely in terms of cost savings, and possible expansions could include educational resources and Internet access.

VII. Conclusion and Future work

In this paper, we proposed an inexpensive means to creating a community telephone network, which utilizes existing technology and infrastructure. We demonstrated an innovative approach to merging two independent technologies to achieve maximum penetration in all spheres of society. We proposed an infrastructure for the implementation of the Blue Bridge on the OpenWrt platform, as well as on the JME platform, and determined the metrics necessary for large scale implementation. This paper demonstrated an understanding of the social inequality and the effects of overpriced communications on impoverished communities.

The Mesh Potato lacks functionality which caters for the existing needs of people in rural areas. Similarly, the Blue Bridge lacks the functionality of providing an analog telephony interface, which is still widely used. As such, future work which adds functionality to the OpenWrt component of the Blue Bridge could involve connecting the Mesh Potato to the AirRouter via cable, and ensuring that both devices are on the same subnet, thus enabling the utilization of the analog interface of the Mesh Potato. In terms of the cell phone component of the Blue Bridge, the Mesh Potato could be connected to the cell phone via the wireless interface.

Another proposal for future work regarding this research could involve the use of low cost, high powered wireless equipment which could solve the need for large numbers of AirRouters or similar devices, since one device could provide access to a larger area. Future implementations of the aforementioned could involve connecting powerful wireless equipment to the AirRouter via the LAN interface, and in the case of the cell phone based Blue Bridge, via the wireless interface. The proposed expansion of the original infrastructure can be seen in Fig. 3.

Fig. 3(a) shows the expansion of the OpenWrt based infrastructure through the use of an external high powered wireless device, which is connected to the AirRouter via cable. This device then expands the wireless network, which then enables a larger number of clients to connect to the mesh and reap the benefits of a community telephone network. Of course the AirRouter will still serve as an access point for nearby 802.11 and Bluetooth clients.

Fig. 3(b) depicts the expansion of the cell phone based infrastructure for the Blue Bridge. Since the cell phone is unable to connect to the external wireless device via LAN cable, a connection needs to be made wirelessly. As such, the external high powered wireless device will transmit signal over a greater distance accomplished by the cell phone and will serve as the primary AP for 802.11 based clients.

Acknowledgment

I would like to thank my 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] Zaruba, G.V., Basagni, S., and Chlamtac, I., “Bluetrees-Scatternet formation to enable Bluetooth-based ad hoc networks,” IEEE International Conference on Communications, ICC 2001, vol. 1, 2001, pp. 273-277.

[2] Asthana, S. and Kalofonos, D., “Secure ad-hoc group collaboration over bluetooth scatternets,” Applications and Services in Wireless Networks, 2004. ASWN 2004. 2004 4th Workshop, pp. 199-124.

[3] Bisdikian, C., “An overview of the Bluetooth wireless technology,” IEEE Communications Magazine, vol. 39, 2001, pp. 86–94.

[4] OpenWrt. Available at: http://openwrt.org, 2011. [Accessed 04-04-2011].

[5] Apple. What is Firmware?. Available at: http://support.apple.com/kb/ht1471, 2008. [Accessed 01-04-2011].

[6] Fainelli, F., “The OpenWrt embedded development framework,” 2008.

[7] OpenWrt. Available at: http://wiki.openwrt.org/inbox/mesh.olsr, 2011. [Accessed 06-04-2011].

[8] Reguart, A., Cano, J.C., Calafate, C.T., and Manzoni, P., “Providing Internet Access in Rural Areas: A Practical Case Based on Wireless Networks,” The 2006 IFIP WG 6.9 Workshop on Wireless Communications and Information Technology in Developing Countries (WCIT 2006), 20-25 August 2006, Santiago, Chile.

[9] Parikh, T.S., and Lazowska, E.D., “an architecture for delivering mobile information services to the rural developing world,” Proceedings of the 15th international conference on World Wide Web, 2006, pp. 791-800.

[10] UBNT. Available at: http://ubnt.com, 2011. [Accessed 04-04-2011].

[11] Asterisk. Available at: http://asterisk.org, 2011. [Accessed 07-04-2011].

[12] Sahd, C., “Bluetooth Audio and Video Streaming on the J2ME Platform,” 2010.

[13] AsteriskGuru. Available at: http://www.asteriskguru.com/tools/bandwidth_calculator.php, 2011. [Accessed 09-04-2011].

[14] Metagora. Reconstruction and Development Programme (RDP) of South Africa. Available at: http://www.metagora.org/training/encyclopedia/rdp.html, 2006. [Accessed 10-04-2011].

[15] Alexandra. Another RDP first from the Alexandra Renewal Project. Available at: http://www.alexandra.co.za/05_housing/article_0610_rdp_housing.htm, 2006. [Accessed 09-04-2011].

[16] Joshco. Sol Plaatje. Available at: http://www.joshco.co.za/solplaatje.html, 2011. [Accessed 10-04-2011].

ISBN: 978-1-61208-147-2

[17] VillageTelco. Mesh Potato. Available at: http://www.villagetelco.org/mesh-potato/, 2011. [Accessed 11-04-2011].

[18] Meraki. Meraki. Available at: http://meraki.com/, 2011. [Accessed 11-04-2011].

[19] Open-Mesh. Open-Mesh. Available at: http://www.open-mesh.com/, 2011. [Accessed 11-04-2011].

[20] Vodacom. 4U Prepaid. Available at: http://www.vodacom.co.za/vodacom/Deals/Prepaid/Prepaid+Price+Plans/4U+Prepaid, 2011. [Accessed 23-05-2011].

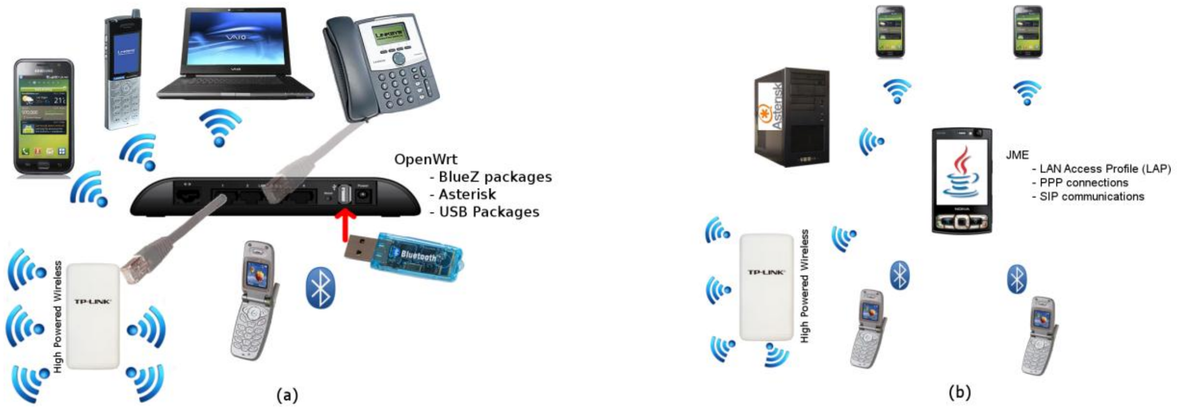


Figure 3. (a) Proposed wireless expansion of OpenWrt based Blue Bridge (b) Proposed wireless expansion of cell phone based Blue Bridge

ISBN: 978-1-61208-147-2