Journal of Computer Systems, Networks, and Communications

Lightweight Mobile and Wireless Systems: Technologies, Architectures, and Services

Guest Editors: Charalabos Skianis, Fabrizio Granelli, Periklis Chatzimisios, Christos Verikoukis, and Michael Devetsikiotis

Lightweight Mobile and Wireless Systems: Technologies, Architectures, and Services

Journal of Computer Systems, Networks,
and Communications

Lightweight Mobile and Wireless Systems: Technologies, Architectures, and Services

Guest Editors: Charalabos Skianis, Fabrizio Granelli,
Periklis Chatzimisios, Christos Verikoukis,
and Michael Devetsikiotis

Contents

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 420806, 2 pages
doi:10.1155/2010/420806

Editorial

Lightweight Mobile and Wireless Systems: Technologies, Architectures, and Services

Charalabos Skianis,[1] Fabrizio Granelli,[2] Periklis Chatzimisios,[3] Christos Verikoukis,[4] and Michael Devetsikiotis[5]

[1] *Department of Information and Communication Systems Engineering (ICSE), University of the Aegean, 81100 Mytilene, Greece*
[2] *Department of Information Engineering and Computer Science (DISI), University of Trento, 38123 Trento, Italy*
[3] *Department of Informatics, Alexander Technological Educational Institute of Thessaloniki, Thessaloniki, 574 00 Macedonia, Greece*
[4] *Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), 08860 Barcelona, Spain*
[5] *North Carolina State University (NCSU), Raleigh, NC 27695, USA*

Correspondence should be addressed to Charalabos Skianis, cskianis@aegean.gr

Received 31 December 2010; Accepted 31 December 2010

Wireless communications are becoming increasingly pervasive, as the number and diffusion of portable wireless equipped devices are exponentially increasing (ranging from cellular phones to handheld game consoles, from personal digital assistant and personal navigation devices to still and video cameras). This results in an unprecedented request for lightweight, wireless communication devices with high usability and performance able to support added-value services in a highly mobile environment. Such devices follow the users everywhere they go (at work, at home, while travelling, in a classroom, etc.) and result in exciting research, development, and business opportunities as evidenced from a plethora of currently undergoing European and national funded projects and consortiums (e.g., ICARUS, NEWCOM++, MIMAX, OMEGA, MOBILIA, REWIND, and SELFNET).

The above scenario clearly demands significant upgrades to the existing communication paradigm in terms of infrastructure, devices, and services to support the "anytime, anywhere, any device" philosophy, providing novel and fast-evolving requirements and expectations on research and development in the field of information and communication technologies. The core issue is to support wireless users' desire for 24/7 network availability and transparent access to "their own" services.

This issue gathers together a selection of recent original research in the field comprising of six diverse papers that reflect the variety of concerns and latest advances relating to lightweight mobile and wireless systems.

In the first paper "*Hidden Anchor: A Lightweight Approach for Physical Layer Location Privacy,*" R. El-Badry et al. propose an algorithm that provides anchor physical layer location privacy for different classes of localization algorithms in wireless sensor networks. The performance of the proposed algorithm is evaluated through analysis and simulation experiments and it is shown that it can hide the location and identity of anchor nodes with very low overhead and without limiting the localization accuracy for trusted nodes. The authors also provide a technique that significantly enhances the privacy of the network without affecting the localization accuracy at trusted nodes.

The second paper "*Simulation of 802.21 Handovers Using ns-2*" by H. Marques et al. presents a short description of the 802.21 standard, its implementation in ns-2 as well as the employed signaling in a handover between WiMAX and Wi-Fi networks. Moreover, the paper evaluates the reliability and scalability of ns-2 tool in simulating multiple vertical handover scenarios under the scope of IEEE 802.21 and also proposes a novel and very simple approach to determine the expected number of handovers in an ns-2 simulation.

In the paper "*Service-Aware Retransmission Control in Cellular Networks,*" N. B. Halima et al. propose a service-aware cross-layer approach between application/transport layers on the mobile terminal and link layer on the wireless

base station to enable dynamic control on the level of per-packet hybrid ARQ (HARQ) protection for multimedia data streams. Experimental results demonstrate the potential benefits deriving from the proposed strategy, underlining relevant improvements for audio and video flows as well as for TCP-based data transfers.

In the paper "*Crafting a Real-Time Information Aggregator for Mobile Messaging,*" J.-S. Leu develops a real-time information aggregator called visualizing SMS and MMS messages system (VSMMS) in order to visualize instant SMS/MMS messages openly on a larger device, instead of a limited-sized screen on personal cellular phones in the past. VSMMS includes an optional web-based interface to help the administrator verify the incoming contents and, thus, appears to be suitable for public mass media broadcasting and real-time information sharing.

The paper "*Optimized Hybrid Resource Allocation in Wireless Cellular Networks with and without Channel Reassignment*" by X. Wu et al. presents two efficient integer linear programming formulations for the hybrid channel assignment (HCA) problem in wireless cellular networks. The proposed approaches optimally allocate a channel (from a pool of available channels) to an incoming call such that both hard (i.e., cosite and adjacent channel constraints) and soft constraints (i.e., the packing condition, resonance condition, and limiting channel reassignment) are satisfied.

Finally, in "*Spatial Diversity Scheme to Efficiently Cancel ISI and ICI in OFDM-OQAM Systems,*" N. Zorba and F. Bader propose a spatial diversity scheme to cancel the intersymbol interference (ISI) and intercarrier interference (ICI) in the system through low-complexity operations in order to enable the implementation of an offset quadrature amplitude modulation (OQAM) orthogonal frequency division multiplexing (OFDM) transmission scheme. The authors formulate the performance of the proposed scheme in terms of data rate and BER and mathematically obtained the SNR expression. The performance results indicate that the OFDM-OQAM proposal increases the system data rate comparing to the classical cyclic prefix (CP) OFDM systems.

Acknowledgments

We would like to thank all the authors for contributing papers to this special issue and the external reviewers for their tireless work and efforts during the reviewing process. We also would like to thank the Editorial Staff of Journal of Computer Systems, Networks, and Communications for their continuous support in editing this special issue. This special issue has been organized with the support of the FP7 Network of Excelence NEWCOM++ (216715).

Charalabos Skianis
Fabrizio Granelli
Periklis Chatzimisios
Christos Verikoukis
Michael Devetsikiotis

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 749298, 12 pages
doi:10.1155/2010/749298

Research Article

Hidden Anchor: A Lightweight Approach for Physical Layer Location Privacy

Rania El-Badry, Moustafa Youssef, and Ahmed Sultan

Wireless Intelligent Networks Center, Nile University, 12677 Cairo, Egypt

Correspondence should be addressed to Moustafa Youssef, mayoussef@nileu.edu.eg

Received 1 February 2010; Accepted 15 May 2010

Academic Editor: Christos Verikoukis

In hybrid wireless sensor networks, where trusted and un-trusted nodes coexist, it becomes important to allow trusted nodes to share information, especially, location information and prevent un-trusted nodes from gaining access to this information. We focus on anchor-based localization algorithms in WSNs, where a small set of specialized nodes, that is, anchor nodes, broadcast their location to the network and other nodes can use the broadcast information to estimate their own location. The main challenge is that both trusted and un-trusted nodes can measure the physical signal transmitted from anchor nodes and use it to estimate their locations. In this paper, we propose Hidden Anchor, an algorithm that provides anchor physical layer location privacy for different classes of localization algorithms. The Hidden Anchor algorithm exploits the inherently noisy wireless channel and uses identity cloning of neighboring trusted nodes to make anchors unobservable to un-trusted nodes while providing complete information to trusted nodes. Evaluation of the Hidden Anchor algorithm through analysis and simulation shows that it can hide the identity, and hence the location, of anchor nodes with very low overhead. In addition, the results show that by adding artificial noise, we can achieve significant improvement in anchor's location privacy.

1. Introduction

Location discovery has been an active area of research in wireless sensor networks (WSN) due to its critical need in many applications including location-based routing [1], coverage [2], node identification, and information tagging. Localization algorithms can be categorized as either anchor-based or anchor-free [3]. Anchor-based algorithms, for example, [4, 5], assume the existence of a small set of nodes with known locations, that is, anchor nodes, that broadcast their location information to the network in special *beacon* frames. A node with an unknown location estimates its distance to the anchor node, in a process known as ranging, and combines the estimated distance to at least three anchor nodes with the broadcast anchors' locations in beacon frames to estimate its location in 2D (Figure 1). On the other hand, anchor-free localization algorithms, for example, [6, 7], do not assume the existence of anchor nodes and estimate the relative topology of the network, in which the coordinate system is established by a reference group of nodes. This paper focuses on anchor-based localization algorithms using Received Signal Strength (RSS) for ranging.

In many hybrid wireless sensor networks' (HWSNs) applications, sensor nodes are deployed in hostile environments where trusted and un-trusted nodes co-exist. In such hybrid networks, it becomes important to allow trusted nodes to share information while, at the same time, prevent un-trusted nodes from gaining access to this information.

An anchor node may encrypt its beacon frames with a key shared only with trusted nodes. This will prevent un-trusted nodes from getting the information contained in the beacon frames. Although encryption can provide location information secrecy, it does not provide *physical layer* location privacy, where a group of un-trusted nodes can measure the received signal strength (RSS) of encrypted messages and cooperate to determine the anchor nodes' locations through trilateration. This paper proposes an algorithm, termed *Hidden Anchor*, that addresses the physical layer location privacy problem. In particular, the *Hidden Anchor* algorithm provides *anchor nodes unobservability*, where un-trusted nodes cannot detect (observe) the existence of anchor nodes.

In [8, 9], we proposed the *HyberLoc* algorithm for addressing the physical layer location privacy problem.

HyberLoc depends on the anchor nodes to dynamically change their transmission power and to include the used transmission power in the encrypted beacon frame. However, *HyberLoc*'s advantage is limited because of the current limitations of the sensor hardware as we elaborate in Section 5.1.

Our novel approach in the *Hidden Anchor* algorithm is to exploit the noisy characteristics of the wireless channel to hide the location of anchor nodes from un-trusted nodes, while providing complete information to trusted nodes. The idea is for anchor nodes to randomly use the identity of the *nearby*, that is, within a given distance, trusted nodes when broadcasting their beacon frames. As a result, un-trusted nodes will not be able to distinguish between anchor traffic and trusted node traffic. Shared information between the anchor and trusted nodes is used to give complete location information to trusted nodes. We evaluate the performance of the *Hidden Anchor* algorithm using analysis and simulation with metrics for both deterministic and probabilistic anchor-based location determination systems. The results show that the *Hidden Anchor* algorithm can hide the location and identity of anchor nodes while maintaining very low overhead.

Since the *Hidden Anchor* algorithm depends mainly on exploiting the noisy characteristics of the wireless channel, we further extend it by inducing artificial noise to the network in a way that does not affect the localization accuracy at trusted nodes. Analysis of the proposed noise induction technique shows significant improvement of the security of the proposed techniques. This is particularly important in handling the case when the un-trusted node uses a probabilistic location determination technique, which is known to give higher accuracy than deterministic location determination techniques [10, 11].

The rest of this paper is organized as follows. Section 2 discusses some related work. Section 3 highlights some background information. Section 4 presents the problem statement. Section 5 details the *Hidden Anchor* algorithm and analyzes its performance. Section 6 discusses our artificial noise extension to the basic *Hidden Anchor* algorithm. Section 7 evaluates the *Hidden Anchor* algorithm through simulation. Finally, Section 8 concludes the paper.

2. Related Work

In this section, we discuss different work related to the *Hidden Anchor* algorithm. The authors in [12, 13] proposed a technique that uses sophisticated PHY-layer measurements in a wireless network for location distinction. The proposed technique, temporal link signature, is a multipath-based location distinction technique. The main goal was to detect whether a node has moved from its location or not. Using link signature, this technique can determine that a node has changed its location, for example, when the anchor node clones the ID of a neighboring node in the *Hidden Anchor* algorithm. However, the technique depends on collecting training data, which makes it unsuitable for use with non-cooperating nodes, which is the case in hybrid WSNs.

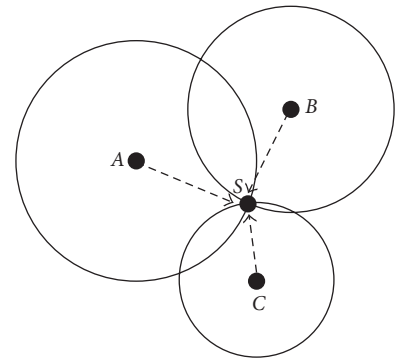

Figure 1: Node S can estimate its location in 2D using the location messages received from the three anchor nodes A, B, and C and the estimated range to them. Similarly, we can understand this figure as three un-trusted nodes A, B, and C cooperating to estimate the location of an anchor node S.

Therefore, it cannot be used as an attack on the *Hidden Anchor* algorithm.

The authors in [14] proposed *SlyFi*, an 802.11-like wireless link layer protocol that encrypts entire frames, including addresses, to remove explicit identifiers that could be used by third parties to link together frames from the same transmitter. It was proposed to improve wireless privacy. *SlyFi*, although suitable for a WiFi network, is based on a number of assumptions that may not fit the nature of sensor networks. First, *SlyFi* requires each node to keep a set of shared keys for every node that it may communicate with and a table of the possible incoming addresses for every time interval. Second, *SlyFi* requires all nodes in the network to be synchronized. These are considered a high overhead for sensor nodes which are limited in memory, processing power, and battery.

As will be discussed in Section 5, *HyberLoc* [8, 9] provides a weaker notion of location privacy, that is, location anonymity, than the unobservability provided by the *Hidden Anchor* algorithm.

3. Background

In this section, we provide background information on localization algorithms for WSNs. For more details, the reader is referred to [3].

3.1. Anchor-Based versus Anchor-Free Algorithms. Location discovery algorithms for sensor networks can be classified as anchor-based or anchor-free algorithms. Anchor-based algorithms, for example, [4, 5], assume that a small percentage of the nodes, that is, anchor nodes, are aware of their positions. Anchor nodes broadcast their location information to their neighbors which use this information to estimate their own location. In anchor-free algorithms, for example, [6, 7], no special anchor nodes exist in the network. In this case, the algorithm estimates relative positions, in which the coordinate system is established by a reference group of nodes. Relative positioning is suitable for

some applications, for example, location-aided routing [15]. However, the accuracy of anchor-free algorithms is typically less than anchor-based algorithms. This paper focuses on anchor-based algorithms.

3.2. Range Estimation Method. Ranging is the process of estimating node-to-node distances or angles. In order to determine its location in 2D, a sensor node needs to estimate its range to three or more anchor nodes. The most popular methods for estimating the range between two nodes are Time-based methods, for example, Time-of-Arrival (ToA), Angle-of-Arrival methods (AoA), and Received-Signal-Strength (RSS) methods. This paper focuses on RSS-based range estimation methods where the propagation loss can be calculated based on the difference in power between the transmitted and received signals. Theoretical and empirical models are used to translate this loss into a distance estimate. Combining the positioning information received from at least three anchor nodes with the estimated distances, a sensor node can estimate its location in 2D (Figure 1).

3.3. Wireless Channel-Based Security. The broadcast nature of wireless communications makes them vulnerable to many security attacks. Many researchers have used the characteristics of the wireless channel to solve this intrinsic security problem of wireless communications. For example, the authors in [16] exploit the multipath fading characteristic of wireless communication to facilitate secret key sharing between a sender and a receiver.

In this paper, we exploit the noisy characteristic of the wireless channel to provide physical layer location privacy for wireless devices. We start by exploiting the environment noise to secure the location of anchor nodes and then extend the idea by inducing artificial noise.

4. Problem Statement

This section outlines the network model and security and privacy requirements. We also delineate the different ways an un-trusted node can use to identify the existence of an anchor node.

4.1. Network Model. We assume a hybrid wireless sensor network where anchor, trusted, and un-trusted nodes co-exist. We also assume that nodes use an RSS anchor-based localization algorithm. Thus, anchor nodes continuously broadcast beacon frames containing their position information.

Any node in the network can observe any frame transmitted by other nodes within its range. Sensor nodes are randomly distributed in the area of interest. Trusted nodes can use standard encryption algorithms to hide the anchor nodes' position information where both anchor nodes and trusted nodes share the required common information, for example, cryptographic keys, prior to deployment.

Un-trusted nodes use the same radio hardware used by anchor nodes and trusted nodes. We further assume that there is no correlation between the frame information, such as size and content, and the frame type. Therefore, un-trusted nodes cannot differentiate between the frames from trusted nodes and those from anchor nodes. This can be achieved by encrypting the contents or padding the frames as needed.

We also assume that the goal of the un-trusted nodes is to estimate their range to anchor nodes based on the physical signal transmitted by anchor nodes.

4.2. Security and Privacy Requirements. By considering the network model discussed in the previous section, we have two main requirements that should be considered.

4.2.1. Location Information Secrecy. Anchor nodes should be able to broadcast their position information periodically and trusted nodes should be able to use this information to estimate their position. On the other hand, un-trusted nodes should not be able to use anchor nodes' beacon frames to gain information about anchor nodes' locations. This can be achieved, for example, by encrypting the anchor nodes' beacon frames.

4.2.2. Physical Layer Location Privacy. Un-trusted nodes should not be able to exploit the measured physical signal to estimate the location of anchor nodes. This paper focuses on this privacy requirement.

4.3. Identifying Anchor Nodes. An un-trusted node may exploit one or a combination of the following vulnerabilities to identify the existence of an anchor node. Note that detecting the existence of the anchor node is a necessary prelude to determine its location.

4.3.1. Separate ID-Space for Anchor Nodes. If the WSN is designed such that the ID-space for anchor nodes is separate from the ID-space of trusted nodes, an un-trusted node can identify the existence of an anchor node by its ID in the frame header.

4.3.2. Type of Transmission—Broadcast/Unicast. Beacon frames are broadcast in the network. If only anchor nodes broadcast messages in the network, their frames can be distinguished from the frames of other nodes by noting the broadcast destination address. However, regular sensor nodes use both broadcast and unicast to transmit their own messages, making this way less useful for the un-trusted node.

4.3.3. Periodicity of Frames. Even if other nodes send broadcast frames, the periodicity of the beacon frames make them easier to detect and hence expose the anchor node.

4.3.4. Frame Size. Beacon frames usually have a fixed size. This can make them easily distinguishable by the un-trusted node.

4.3.5. Type Field in Frame Header. If there is a field in the frame header to identify the different message types, this can be used to determine the anchor node by the type of messages it sends.

Except for the last two vulnerabilities, which can be easily mitigated by padding the frame with random data and encrypting the frame, respectively, the *Hidden Anchor* algorithm mitigates the remaining three vulnerabilities to achieve anchor node unobservability as discussed in the next section.

5. The Hidden Anchor Algorithm

In this section, we start by a possible technique that addresses the physical layer location privacy problem. We show that this technique has shortcomings, thus motivating the need for a the *Hidden Anchor* algorithm.

5.1. Possible First-Cut Solution. Anchor nodes can confuse un-trusted nodes using variable transmission power. For example in [8, 9], we proposed a light-weight algorithm that provides secure anchor-based localization in hybrid wireless sensor networks. The idea is for anchor nodes to continuously and randomly change the transmit power and to include the transmit power encrypted in the frame using the shared information between itself and trusted nodes. This change of transmit power will reduce the localization accuracy at the un-trusted nodes, achieving location anonymity (location anonymity refers to hiding the true location of an anchor node. This is a weaker notion than anchor node unobservability, where the anchor node existence is not detected at all). Trusted nodes can use the shared information to extract the transmit power from the frames and, therefore, their localization accuracy is not affected by the transmit power change.

Based on the current sensor network hardware, for example, [17], transmit power can be selected from a set of prespecified discrete power levels. This has the disadvantage that after receiving a sufficient number of frames, an un-trusted node will be able to distinguish between the different discrete received power levels, thus removing the ambiguity introduced by the random change of transmit power. As a result, un-trusted nodes will be able to localize anchor nodes accurately. In addition, location anonymity provided by this technique is a weaker privacy notion than the unobservability of anchor nodes provided by the *Hidden Anchor* algorithm.

In the next section, we propose the *Hidden Anchor* algorithm as a light-weight algorithm that provides physical layer location privacy and allows trusted nodes to accurately estimate their positions at a low overhead.

5.2. Hidden Anchor Algorithm. The *Hidden Anchor* algorithm exploits the noisy wireless channel to hide the existence of anchor nodes. The idea is for anchor nodes to use the identity of the nearby trusted nodes when broadcasting their beacon frames. This way, un-trusted nodes cannot differentiate between anchor nodes and trusted nodes. On receiving a frame with ID a, an un-trusted node cannot determine whether this frame is from trusted node a or from an anchor node with the same ID. Note that since the anchor node chooses its ID from nearby nodes, its location is hidden within the noise of the wireless channel. The algorithm operates in two phases: the neighbor discovery phase and the location hiding phase.

5.2.1. Neighbor Discovery Phase. The purpose of this phase is for the anchor node to discover the IDs of the nearest neighbors so that the anchor node can select which IDs to use during the next phase.

The anchor node may broadcast an encrypted identity-request message using a random ID to all its neighbors within a certain radius. This can be controlled by a hop count parameter. All trusted nodes in the network that receive this message reply with an identify-reply message.

The anchor node waits for a certain time to collect the identify-reply messages along with their received signal strength. After that, the anchor node sorts the nodes in an ascending order with respect to their received signal strength and saves the identities of the k nearest trusted nodes in a set ($\mathbb{S}$).

The anchor node can also discover the IDs of the nearest neighbors by passively monitoring the network traffic for a sufficient time period.

5.2.2. Location Hiding Phase. In this phase, and when it is time to send a beacon frame, the anchor node chooses one ID from the set $\mathbb{S}$ randomly and uses it as its *unencrypted* identity. The true identity of the anchor node, along with the type of the message can be sent encrypted in the body of the message, if needed. Upon receipt of a broadcast beacon frame, a trusted node decrypts the frame and can determine the identity and location of an anchor node. On the other hand, an un-trusted node, not knowing the decryption key, cannot differentiate between the frames from the anchor nodes and trusted nodes, as they have the same identity and the difference in their signal strength is within the wireless transmission noise.

5.3. Discussion. For the vulnerabilities identified in Section 4.3, the *Hidden Anchor* algorithm eliminates any chance for un-trusted nodes to identify anchor nodes using their IDs as anchor nodes never use their real IDs in clear, which is equivalent to using only the trusted nodes ID-space. Also, the proposed algorithm removes the periodicity of beacon frames by using a different ID every time for the frames transmitted from anchor nodes. Finally, since anchor nodes clone the identity of trusted nodes, their traffic pattern, as seen by the un-trusted nodes, becomes indistinguishable.

Note also that, even if un-trusted nodes cooperate to determine the location of all trusted nodes, they cannot determine the location of anchor nodes, as anchor nodes are unobservable. Statistical analysis is not useful here too as anchor nodes use the IDs of trusted nodes for sending their own traffic.

Compared to *HyberLoc*, the *Hidden Anchor* algorithm does not depend on changing the power levels and therefore, it is not affected by the current sensor network hardware limitations. Also, while the *HyberLoc* algorithm provides anchor node location anonymity, the *Hidden Anchor* algorithm provides the stronger notion of anchor nodes unobservability.

5.4. Analysis. In this section, we derive expressions for the difference in received signal power, which is directly related to the average difference in estimated distance, and the statistical Kolmogorov-Smirnov (KS) test value at the un-trusted receiver both when the *Hidden Anchor* algorithm is used and without using it in the presence of noise.

5.4.1. Difference in Estimated Distance. The difference in estimated distance metric represents the error in estimated distance when the trusted node is sending by itself on one hand and when both the trusted node and the anchor node share the same ID, that is, using the *Hidden Anchor* algorithm. The distance estimate is based on the average received signal strength at the un-trusted node. The lower the value of this metric, the better in terms of privacy requirement as the un-trusted node will be unlikely to detect that both trusted node and anchor node are sharing the same ID.

5.4.2. KS Test Value. This metric represents the value of the Kolmogorov-Smirnov (KS) statistical test. The KS test value gives a measure of similarity between the probability distribution of the signal strength received at the un-trusted node with and without using the *Hidden Anchor* algorithm. It gives an insight about how a probabilistic location determination algorithm would perform with and without using the *Hidden Anchor* algorithm. A lower value of this metric represents better security as the un-trusted node will be less likely to differentiate between the signal strength distributions of the trusted node and anchor node.

5.4.3. Notation. We use the following notation.

(i) We consider a signal propagation model that has a dominant line-of-sight (LOS) component. In the presence of Additive White Gaussian Noise (AWGN), the probability density function (PDF) of the received signal power [18] is

$$f(P_r \mid h, x) = \frac{1}{2\sigma^2} \exp\left(-\frac{P_r + hx}{2\sigma^2}\right) I_0\left(\frac{\sqrt{P_r hx}}{\sigma^2}\right), \quad (1)$$

where P_r is the received signal power, h is the channel gain which is a function of distance, x is the transmission power, $2\sigma^2$ is the total noise variance, and $I_0(x)$ is the modified Bessel function of order zero.

Thus, the mean of the received signal power is

$$\mu = 2\sigma^2 + hx, \quad (2)$$

and the CDF of the received signal power follows a non-central chi-square distribution given by

$$\chi(P_r \mid h, x) = \sum_{j=0}^{\infty} \exp\left(\frac{-hx}{2\sigma^2}\right) \frac{(hx/2\sigma^2)^j}{j!} Q(P_r; 2 + 2j), \quad (3)$$

where $Q(m, n)$ is the CDF of a central chi-square distributed random variable with n degrees of freedom.

(ii) v_{HA}. A random variable representing the average received power from the same ID over n samples at the un-trusted receiver when the *Hidden Anchor* algorithm is used.

(iii) $v_{\overline{\mathrm{HA}}}$. A random variable representing the average received power from the same ID over n samples at the un-trusted receiver when the *Hidden Anchor* algorithm is not used.

(iv) P_r. A random variable representing the power received from the same ID at the un-trusted node, whether from the trusted node or the anchor node.

(v) P_{r_t}. A random variable representing the power received at the un-trusted node from the trusted node.

(vi) P_{r_a}. A random variable representing the power received at the un-trusted node from the anchor node.

(vii) r. Traffic ratio, that is, ratio of the traffic from the trusted node to the traffic from the anchor node.

(viii) α. In the KS test, the parameter α controls the probability of rejecting the null hypothesis that the samples are from the same distribution.

5.5. Metric 1: Difference in Received Power. In this section, we derive an expression for the difference in received power with and without using the *Hidden Anchor* algorithm, which is directly related to the average in estimated distance. Using the above notation, the average received power when the *Hidden Anchor* algorithm is used, v_{HA}, over n samples is given by

$$\begin{aligned} v_{\mathrm{HA}} &= \frac{1}{n}\sum_{i=1}^{n} P_{r_i} \\ &= \frac{1}{n}\left(\sum_{i=1}^{nr/(1+r)} P_{r_{t_i}} + \sum_{i=1}^{n/(1+r)} P_{r_{a_i}}\right), \end{aligned} \quad (4)$$

where P_{r_i} represents the ith sample from the corresponding random variable. From (4),

$$\begin{aligned} E[v_{\mathrm{HA}}] &= \frac{1}{n}\left[\sum_{i=1}^{nr/(1+r)} E\left(P_{r_{t_i}}\right) + \sum_{i=1}^{n/(r+1)} E\left(P_{r_{a_i}}\right)\right] \\ &= \frac{1}{r+1}\left(rE[P_{r_t}] + E[P_{r_a}]\right) \\ &= \frac{r}{r+1}\left(2\sigma^2 + h_t x_t\right) + \frac{1}{r+1}\left(2\sigma^2 + h_a x_a\right) \\ &= 2\sigma^2 + \frac{r}{r+1}\left(h_t x_t\right) + \frac{1}{r+1}\left(h_a x_a\right). \end{aligned} \quad (5)$$

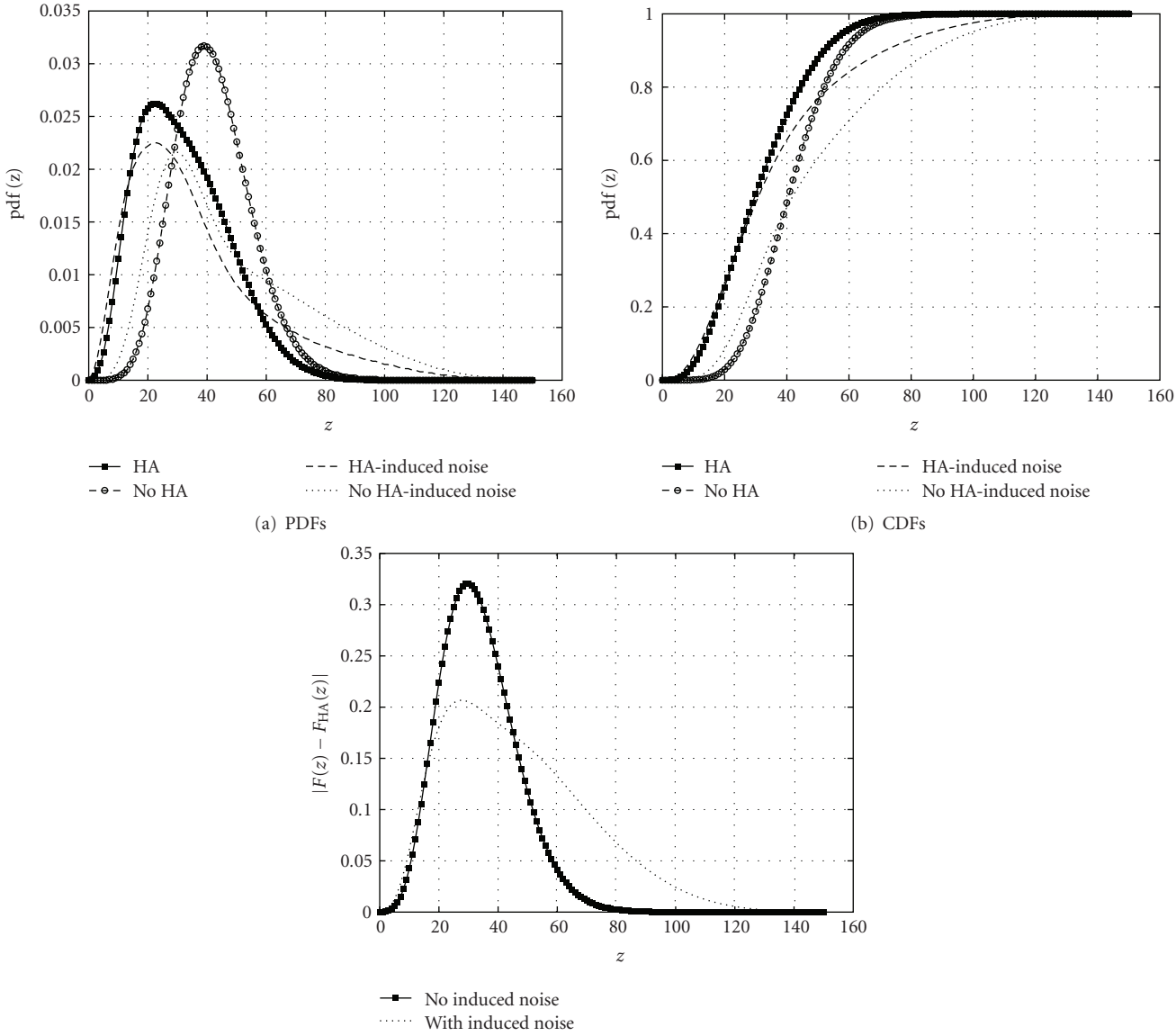

Figure 2: Performance of the *Hidden Anchor* algorithm with and without induced noise for low receiver noise.

Similarly, when the *Hidden Anchor* algorithm is not in use, the expected average received power, $E(v_{\overline{\text{HA}}})$, over n samples is given by

$$E[v_{\overline{\text{HA}}}] = 2\sigma^2 + h_t x_t. \tag{6}$$

By subtracting (5) from (6), the expected difference in received power between using the *Hidden Anchor* algorithm and not using it is given by

$$\begin{aligned} &E\,[\text{Difference in Power Received}] \\ &= \frac{1}{r+1}(h_t x_t - h_a x_a). \end{aligned} \tag{7}$$

5.6. Metric 2: Kolmogorov-Smirnov Test Value. The Kolmogorov-Smirnov statistic is used to test whether two underlying one-dimensional probability distributions differ. It is based on quantifying the distance between the empirical cumulative distribution functions, F_1 and F_2 of two sets and is defined as

$$\text{KS Test Value} = \sup|F_1(x) - F_2(x)|. \tag{8}$$

Using the above notation, the cumulative distribution function of the power received from the same ID when the *Hidden Anchor* algorithm is used, is given by

$$\begin{aligned} F_{\text{HA}}(P_r) &= \frac{1}{r+1}F_a(P_r) + \frac{r}{r+1}F_t(P_r) \\ &= \frac{1}{r+1}\chi_a(P_r \mid h_a, x_a) + \frac{r}{r+1}\chi_t(P_r \mid h_t, x_t). \end{aligned} \tag{9}$$

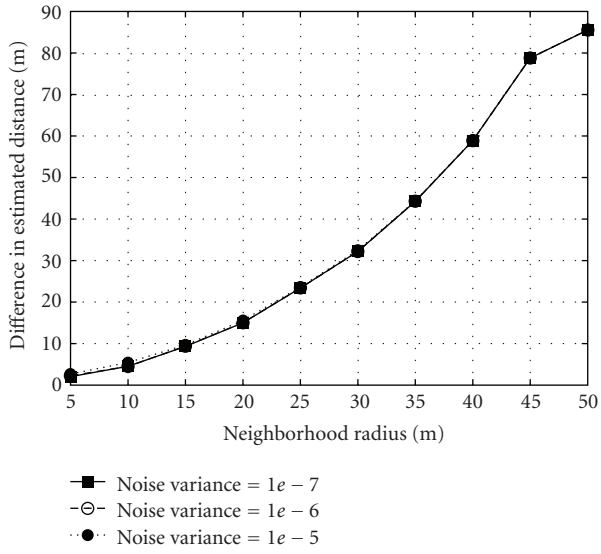

Figure 3: Effect of changing the noise level and the neighborhood radius on estimated distance at the un-trusted node.

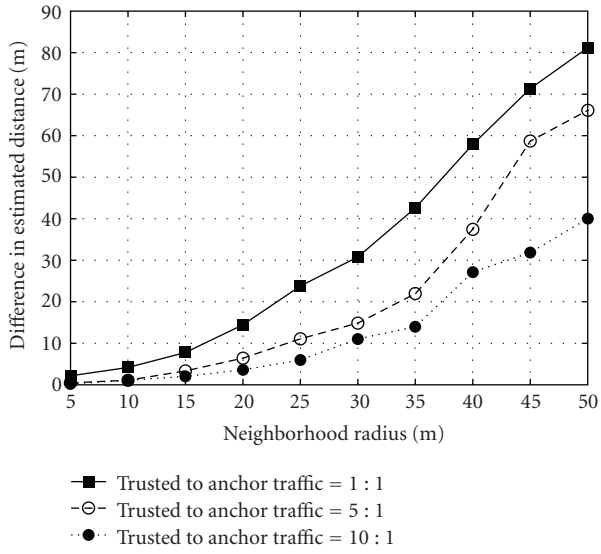

Figure 4: Effect of changing the traffic ratio and the neighborhood radius on estimated distance at the un-trusted node.

Similarly, the cumulative distribution function of the power received from the same ID when the *Hidden Anchor* algorithm is not used is given by

$$F_{\overline{\mathrm{HA}}}(P_r) = \chi_t(P_r \mid h_t, x_t) \tag{10}$$

From (9) and (10), the KS test value is given by

$$\text{KS Test Value} = \frac{1}{r+1} \sup \left| \chi_t(P_r \mid h_t, x_t) - \chi_a(P_r \mid h_a, x_a) \right|. \tag{11}$$

5.7. Discussion. The performance of the *Hidden Anchor* algorithm depends on many parameters including the noise level, the ratio between the traffic sent by the anchor and the traffic sent by the nearest trusted nodes, and the distance between the anchor node and the un-trusted node which affects the channel gain. For both metrics, the performance of the *Hidden Anchor* algorithm can be arbitrary enhanced by controlling the traffic ratio and the distance between the anchor node and trusted nodes (neighborhood radius parameter). For the deterministic metric, the performance is independent from the noise at the receiver. This is expected as averaging removes the effect of noise at the receiver. This is not true however for the probabilistic metric, where the entire signal strength distribution makes an effect on performance. Note that probabilistic location determination techniques are known to produce higher accuracy than deterministic techniques as they use more information [10, 11].

In Section 7, we validate our analysis and show the effect of each parameter on the performance of the algorithm in more detail.

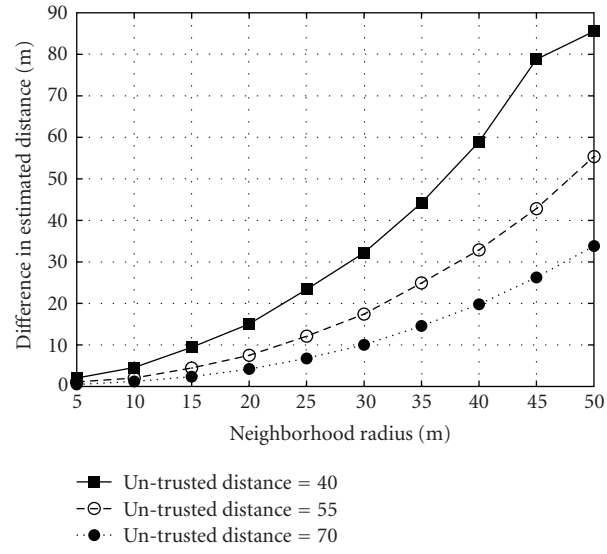

Figure 5: Effect of changing the un-trusted distance and the neighborhood radius on estimated distance at the un-trusted node.

6. Adding Artificial Noise

The KS test value metric evaluates the performance of the *Hidden Anchor* algorithm when un-trusted nodes use a probabilistic location determination technique. Intuitively, this metric should decrease, indicating better security, as the noise level increases (Figure 6). Thus, if we can increase the noise level artificially, we can achieve better anchor's location privacy. The challenge is to increase the ambiguity at the un-trusted nodes without affecting the localization accuracy at the trusted nodes. In this section, we present two techniques that can be used to achieve this goal.

6.1. Symbol-Level Noise. Trusted nodes and anchor nodes can intentionally add a noise vector to the transmitted signal in a way that guarantees statistically independent, identically

distributed, Gaussian random signal samples at the receiver. This induced noise can be picked out of a predetermined noise codebook. Knowing the noise vector used by an anchor node, any trusted node can easily subtract the added noise to accurately localize this anchor node. For the un-trusted nodes, the added noise vector is unknown. Thus, the noise level is higher than the actual level.

To clarify the idea, assume that the received signal (Z) can be represented as:

$$Z = Xh + n, \tag{12}$$

where X is the transmitted signal, h is the channel gain, and n is Additive White Gaussian noise.

Using the proposed technique, the transmitted signal is now composed of the actual transmitted signal and the added noise. Therefore, the received signal can be represented as

$$Z = (X + n_a)h + n, \tag{13}$$

where n_a is the noise added by the anchor node.

For trusted nodes, both X and n_a are known. Thus, trusted nodes can easily estimate the distance to anchor nodes by estimating h. For un-trusted nodes, not knowing the added noise vector, the received signal is given by

$$Z = Xh + n_a h + n, \tag{14}$$

$$Z = Xh + v. \tag{15}$$

As shown in (15), v is now the summation of two noise components. By applying this technique, the noise at the un-trusted receiver will be increased, leading to better privacy, without affecting the localization accuracy at trusted nodes.

6.2. Frame-Level Noise. Adding noise at the symbol-level requires changing the hardware. To use the same hardware, trusted nodes and anchor nodes can add a frame-level noise by randomly changing their transmission power. Using this technique, not knowing the transmission power used, un-trusted nodes can only estimate some noisy estimates of the distance to trusted node. If both trusted and anchor nodes randomize their transmission power at the same time, the un-trusted nodes will not be able to detect any changes in the received signal strength when both trusted and anchor nodes share the same ID, thus, increasing anchors' location privacy.

Note that this induced frame-level noise technique is different from the power randomization technique used in *HyberLoc* [8, 9] as in *HyberLoc*, only anchor nodes change their transmission power while in the induced frame-level noise techniques, both trusted and anchor nodes change their transmission power. The average transmission power of the distribution used can be constrained to a certain value to meet the energy efficiency requirements of the WSN.

6.3. Analysis. For the symbol-level induced noise, the analysis of the performance of the *Hidden Anchor* algorithm is identical to the analysis of Section 5.4 with increased noise. In this section, we analyze the performance of the *Hidden Anchor* algorithm with induced frame-level noise.

6.3.1. Metric 1: Difference in Received Power. The average received power when the *Hidden Anchor* algorithm with induced frame-level noise is used, v_{HA}, over n samples is given by

$$\begin{aligned} v_{\mathrm{HA}} &= \frac{1}{n}\sum_{i=1}^{n} P_{r_i} \\ &= \frac{1}{n}\left(\sum_{i=1}^{nr/(1+r)} P_{r_{t_i}} + \sum_{i=1}^{n/(1+r)} P_{r_{a_i}}\right), \end{aligned} \tag{16}$$

where P_{r_i} represents the ith sample from the corresponding random variable

$$\begin{aligned} E[v_{\mathrm{HA}}] &= \frac{1}{n}\left[\sum_{i=1}^{nr/(1+r)} E\left(P_{r_{t_i}}\right) + \sum_{i=1}^{n/(r+1)} E\left(P_{r_{a_i}}\right)\right] \\ &= \frac{1}{n}\left[\sum_{i=1}^{nr/(1+r)} \left(2\sigma^2 + h_t x_{t_i}\right) + \sum_{i=1}^{n/(r+1)} \left(2\sigma^2 + h_a x_{a_i}\right)\right] \\ &= 2\sigma^2 + \frac{1}{n}\left[h_t \sum_{i=1}^{nr/(1+r)} x_{t_i} + h_a \sum_{i=1}^{n/(r+1)} x_{a_i}\right]. \end{aligned} \tag{17}$$

Similarly, when the *Hidden Anchor* algorithm is not in use, the expected average received power, $E(v_{\overline{\mathrm{HA}}})$, over n samples is given by

$$E\left[v_{\overline{\mathrm{HA}}}\right] = 2\sigma^2 + \frac{h_t}{n}\sum_{i=1}^{n} x_{t_i}. \tag{18}$$

From (17) and (18), given an average power constraint, as $n \to \infty$, the difference in received signal converges to (7). Thus, for the deterministic case, the frame-level-induced noise gives no privacy advantage.

6.3.2. Metric 2: Kolmogorov-Smirnov Test Value. The cumulative distribution function of the power received when the *Hidden Anchor* algorithm with induced frame-level noise is used is given by

$$\begin{aligned} F_{\mathrm{HA}}(P_r) &= \frac{1}{r+1}\sum_{i=1}^{i_{\max}} P(x_{a_i}) F_a(P_r \mid x_{a_i}) \\ &\quad + \frac{r}{r+1}\sum_{i=1}^{i_{\max}} P(x_{t_i}) F_t(P_r \mid x_{t_i}) \\ &= \frac{1}{r+1}\sum_{i=1}^{i_{\max}} P(x_{a_i}) \chi_a(P_r \mid h_a, x_{a_i}) \\ &\quad + \frac{r}{r+1}\sum_{i=1}^{i_{\max}} P(x_{t_i}) \chi_t(P_r \mid h_t, x_{t_i}), \end{aligned} \tag{19}$$

where $i_{\max}$ is the number of power levels used.

Similarly, the cumulative distribution function of the power received when the *Hidden Anchor* is not used is given by

$$F_{\overline{\mathrm{HA}}}(P_r) = \sum_{i=1}^{i_{\max}} P(x_{t_i})\chi_t(P_r \mid h_t, x_{t_i}). \tag{20}$$

Thus, the KS test value is

$$\text{KS Test Value} = \frac{1}{r+1} \sup \left| \sum_{i=1}^{i_{\max}} P(x_{t_i})\chi_t(P_r \mid h_t, x_{t_i}) - \sum_{i=1}^{i_{\max}} P(x_{a_i})\chi_a(P_r \mid h_a, x_{a_i}) \right| \tag{21}$$

Note that (11) is a special case of (21) when $i_{\max} = 1$, that is, without randomization.

6.4. Numerical Evaluation. In this section, we numerically compare the performance of the proposed original *Hidden Anchor* algorithm (11) against the same algorithm with induced artificial noise (21). Figure 2 shows the PDF, CDF, and difference of CDFs (the maximum of this difference is proportional to the KS test value). The probability distribution used to induce the artificial noise is a discrete exponential distribution over three discrete power levels (i.e., $i_{\max} = 3$). The discrete exponential distribution is the entropy maximizing distribution under a given average power level constraint [9]. The figure shows that the proposed randomization technique reduces the KS test value, which is equivalent to better privacy. We will investigate the effect of different parameters on the performance of the *Hidden Anchor* algorithm in the next section.

7. Simulation Study

In this section we evaluate the performance of the *Hidden Anchor* algorithm and show the effect of changing different parameters on its performance. We also evaluate the performance of the *Hidden Anchor* algorithm with induced artificial noise.

7.1. Simulation Environment. The *Hidden Anchor* algorithm was implemented using Matlab. The sensor nodes were randomly distributed over a square of $100 \times 100\,\mathrm{m}^2$. Results represent the average over five different network topologies where every network was randomly generated with a different seed. Without loss of generality, we show the results for only one un-trusted node. We use the "difference in estimated distance" and "KS test value" metrics, described in Section 5.4.

7.2. Simulation Parameters. We evaluate the effect of different parameters on the difference in estimated distance metric and the KS test value. The parameters that we considered in this simulation are the following.

7.2.1. Noise Level. This parameter represents an additive white Gaussian noise with zero mean and total power of $2\sigma^2$.

7.2.2. Traffic Ratio. This parameter (r) represents the ratio of the traffic sent by the trusted node to the traffic sent by the anchor node.

7.2.3. Neighborhood Radius. This parameter represents the maximum distance between the anchor node and the trusted nodes whose IDs it clones. Note that the anchor nodes pick its identity randomly from this set of neighbors.

7.2.4. Un-Trusted Distance. This parameter represents the distance between the anchor node and the un-trusted node.

7.3. Results for the Hidden Anchor Algorithm

7.3.1. Effect of the Parameters on Metric 1: the Difference in Estimated Distance. Figure 3 verifies that the difference in estimated distance metric is not affected by the noise level at the receiver (7). Thus, we fix the noise level in this part to $1e-6$.

Figure 4 shows the effect of changing the neighborhood radius for different traffic ratios. The un-trusted distance is fixed to 70 m. The results show that as the traffic sent by the trusted node increases, relative to the traffic sent by the anchor node, the difference in the estimated distance decreases. Since typical anchor-based algorithms use low anchor traffic to trusted nodes traffic ratio, this shows the promise of the proposed *Hidden Anchor* algorithm.

Figure 5 shows the effect of changing the neighborhood radius with different un-trusted distance values. The traffic ratio is fixed to 1 : 1. The figure shows that as the distance between the anchor node and the un-trusted node increases, the difference in the estimated distance decreases. Consequently, the un-trusted node will not be able to differentiate between the physical signal transmitted by the anchor node and the physical signal transmitted by the trusted node. The reason is that the effect of the distance difference on signal strength between the anchor node and the neighboring trusted nodes diminishes as we go away from the anchor node.

7.3.2. Effect of the Parameters on Metric 2: the KS Test Value. Figure 6 shows the effect of changing the neighborhood radius on the KS test value for different noise levels. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively. Other parameters were fixed at un-trusted distance = 70 m, and traffic ratio = 1 : 1. As the noise level increases, the KS test value decreases. This indicates that the difference between the distribution of the received signal strength using the *Hidden Anchor* algorithm and without using it decreases as the noise level increases.

Figure 7 shows the effect of changing the neighborhood radius for different traffic ratios. Other parameters were fixed at un-trusted distance = 70 m, and noise variance = $1e-6$. The results show that as the traffic sent by the trusted node increases, with respect to the traffic sent by the anchor node,

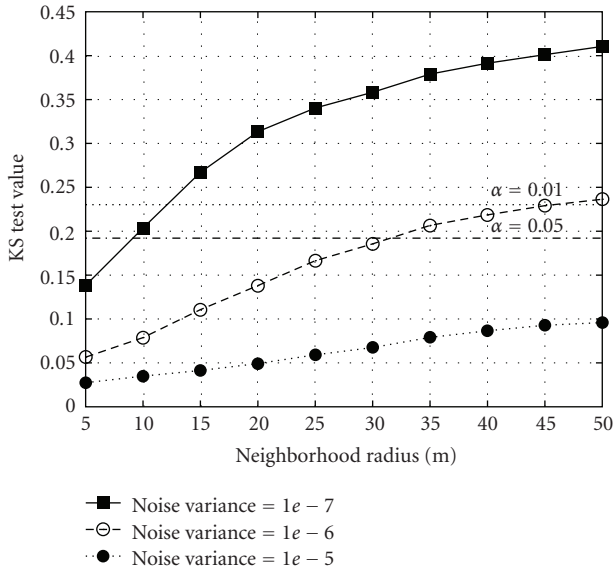

Figure 6: Effect of changing the noise level and the neighborhood radius on the KS test value. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

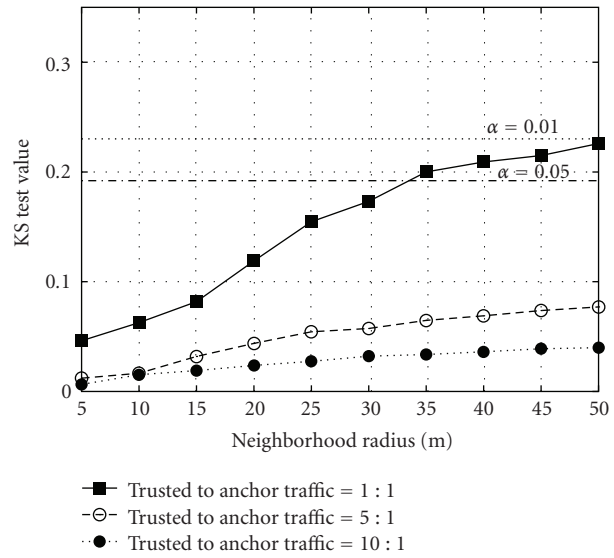

Figure 7: Effect of changing the traffic ratio and the neighborhood radius on the KS test value. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

the KS test value decreases. This means that we can improve the performance of the algorithm dramatically by reducing the traffic sent by the anchor, which is typical for anchor-based algorithms.

Figure 8 shows the effect of changing the neighborhood radius for different un-trusted distance values. Other parameters were fixed at traffic ratio = 1 : 1, and noise variance = $1e - 6$. The figure shows that as the distance between the anchor node and the un-trusted node increases, the difference in the estimated distance decreases. Consequently, the un-trusted node will not be able to distinguish between

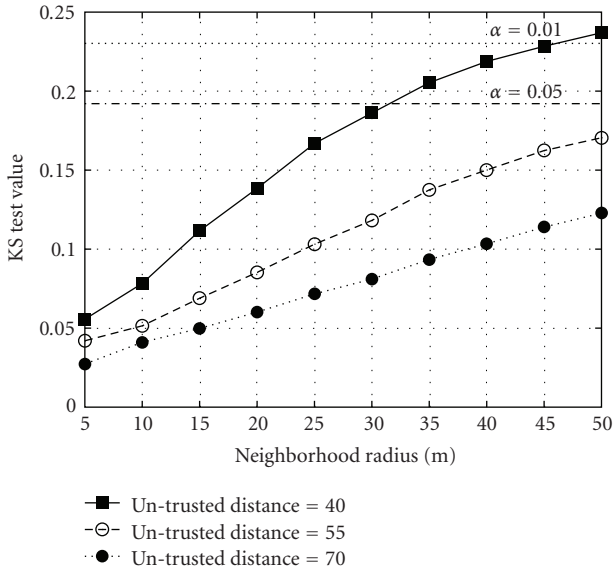

Figure 8: Effect of changing the neighborhood radius and the un-trusted distance on the KS test value. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

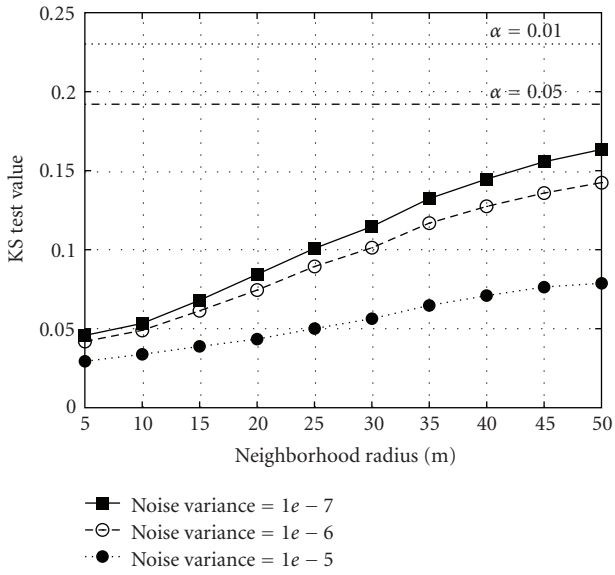

Figure 9: Effect of randomizing the transmission power on the KS test value for different noise levels. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

the physical signal transmitted by the anchor node and the physical signal transmitted by the trusted node.

7.4. Results for the Hidden Anchor Algorithm with Induced Artificial Noise. For Metric 1, as indicated by the analysis in Section 6, there is no advantage of randomizing the transmit power, since averaging over a large number of samples reduces the effect of randomization. The rest of this section

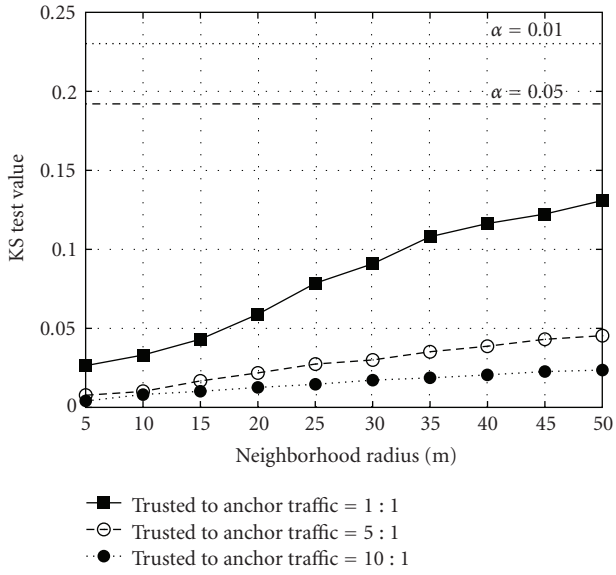

Figure 10: Effect of randomizing the transmission power on the KS test value for different traffic ratios. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

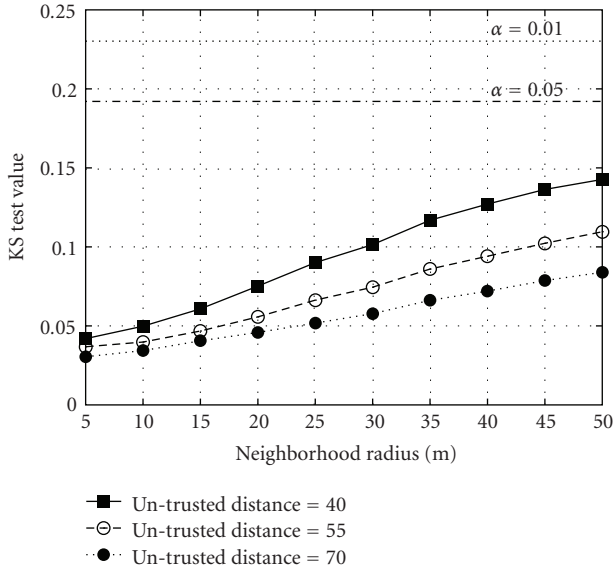

Figure 11: Effect of randomizing the transmission power on the KS test value for different un-trusted distances. The two horizontal lines represent the critical values for the test for $\alpha = 0.01$ and $\alpha = 0.05$, respectively.

evaluates the advantage of using induced artificial noise on Metric 2: the KS Test Value.

Figures 9, 10, and 11 evaluate the performance when the *Hidden Anchor* with induced artificial noise is used. The results show significant improvement in the KS test value when the anchor and trusted nodes randomize their power given an average power constraint. The simulation parameters used in Figures 9, 10, and 11 are the same parameters used in Figure 6, 7, and 8, respectively.

7.5. Summary. In this section, we have evaluated the performance of the *Hidden Anchor* algorithm for different parameters: the noise level, traffic ratio, the maximum distance between the anchor node and the neighboring trusted nodes, and the distance between the anchor node and the un-trusted node.

We have also evaluated the performance of the network when we added artificial noise to the *Hidden Anchor* algorithm by randomizing the transmission power. The results show significant improvement in anchors' location privacy when the un-trusted nodes use a statistical localization method like the KS test.

In all cases, the designer of the network can control the traffic ratio and the maximum distance between the anchor node and the neighboring trusted nodes. Reducing the anchor node to trusted nodes traffic ratio enhances security but may decrease the localization accuracy at trusted nodes. The results show that we can make the performance metric arbitrary small, indicating better privacy, by controlling these two parameters.

8. Conclusion

In this paper, we focused on the physical layer location privacy problem, where an anchor node wants to hide its physical signal information from un-trusted nodes, while at the same time allows trusted nodes to benefit from this information. We proposed the *Hidden Anchor* algorithm for solving the physical layer location privacy and evaluated its performance through analysis and simulation experiments. Our results show that the *Hidden Anchor* algorithm can effectively hide the location and identity of anchor nodes without limiting the localization accuracy for trusted nodes, thus providing anchor nodes' unobservability. The *Hidden Anchor* algorithm can underlie higher layer anchor-based localization algorithms that, when *Hidden Anchor* is employed, would not have to consider the physical layer threats to their operation. We also described a technique for improving the performance of the *Hidden Anchor* algorithm, when the un-trusted node employs a probabilistic location determination system, based on adding artificial noise to the network. The proposed technique significantly enhances the privacy of the network without affecting the localization accuracy at trusted nodes.

Acknowledgments

This research is supported in part by a grant from the Qatar National Research Fund (QNRF)—Grant number NPRP-1-7-7-3—and in part by the Egyptian National Telecommunication Regularity Authority (NTRA).

References

[1] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, August 2000.

[2] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '01)*, pp. 1380–1387, April 2001.

[3] A. Youssef and M. Youssef, "A taxonomy of localization schemes for wireless sensor networks," in *Proceedings of the International Conference on Wireless Networks*, 2007.

[4] P. Liu, X. Zhang, S. Tian, Z. Zhao, and P. Sun, "A novel virtual anchor node-based localization algorithm for wireless sensor networks," in *Proceedings of the 6th International Conference on Networking (ICN '07)*, April 2007.

[5] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Computer Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[6] S. Capkun, M. Hamdi, and J.-P. Hubaux, "Gps-free positioning in mobile adhoc networks," in *Hawaii International Conference on System Sciences (HICSS-34)*, pp. 3481–3490, January 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28–34, 2000.

[8] M. Adel, M. Ibrahim, K. Abulmakarem, M. Youssef, and M. Eltoweissy, "Hyberloc: demonstrating secure localization in hybrid sensor networks," in *Proceedings of the International Conference on Mobile Computing and Networking*, San Francisco, Calif, USA, September 2008.

[9] R. Elbadry, A. Sultan, and M. Youssef, "Hyberloc: providing physical layer location privacy in hybrid sensor networks," in *IEEE ICC '10—The Ad-Hoc, Sensor and Mesh Networking Symposium (ICC '10)*, 2010.

[10] M. Youssef and A. Agrawala, "The *Horus* location determination system," *Wireless Networks*, vol. 14, no. 3, pp. 357–374, 2008.

[11] M. A. Youssef and A. Agrawala, "Analysis of the optimal strategy for wlan location determination systems," *International Journal of Modelling and Simulation*, vol. 27, no. 1, pp. 53–59, 2007.

[12] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '07)*, pp. 111–122, September 2007.

[13] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 26–37, September 2008.

[14] B. Greenstein, T. Kohno, D. McCoy, S. Seshan, J. Pang, and D. Wetherall, "Improving wireless privacy with an identifier-free link layer protocol," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, pp. 40–53, June 2008.

[15] I. Stojmenovic and X. Lin, "Loop-free hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 12, no. 10, pp. 1023–1032, 2001.

[16] M. A. Latif, A. Sultan, and H. El Gamal, "ARQ-based secret key sharing," in *IEEE International Conference on Communications (ICC '09)*, June 2009.

[17] "Telosb mote platform," http://www.xbow.com/.

[18] J. Proakis, *Digital Communications*, McGraw-Hill Science, New York, NY, USA, 2000.

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 794749, 11 pages
doi:10.1155/2010/794749

Research Article

Simulation of 802.21 Handovers Using ns-2

Hugo Marques,[1] José Ribeiro,[1] Paulo Marques,[2] and Jonathan Rodriguez[2]

[1] *Instituto Politécnico Castelo Branco, Escola Superior de Tecnologia, Avenida do Empresário, 6000-767 Castelo Branco, Portugal*
[2] *Instituto de Telecomunicações, Universidade de Aveiro, Campus de Santiago, 3810-193 Aveiro, Portugal*

Correspondence should be addressed to Hugo Marques, hugo@ipcb.pt

Received 1 February 2010; Accepted 2 June 2010

Academic Editor: Charalabos Skianis

The new IEEE 802.21 standard specifies link layer intelligence and other related network information to upper layers in order to optimize handovers between networks of different types, such as WiMAX, Wi-Fi, and 3GPP. This paper makes a short description of 802.21 standard, how it is implemented in ns-2, and the signaling used in a handover between WiMAX and Wi-Fi. The paper also proposes a novel and very simple approach to determine the expected number of handovers in an ns-2 simulation and also evaluates the reliability and scalability of ns-2 when simulating 802.21 scenarios with multiple nodes.

1. Introduction

As wireless users constantly demand for more mobility and bandwidth, a solution was needed that allows their mobile devices to use "any" network in range in order to get coverage or better service. The IEEE 802.21 standard [1] is a first step in order to allow mobile devices to successfully make a handover (HO) between networks of different technologies, such as WiMAX, Wi-Fi, UMTS, Bluetooth, or Ethernet.

The most basic way of describing an HO is when a phone call in progress is redirected from its current cell to a new cell. This normally happens when the mobile device making the call is in movement and detects that it is losing coverage, so it needs to "jump" to another antenna. When the HO is within the same technology, for example, between Wi-Fi cells, it is called a horizontal HO. If it is executed between different technologies, for example, WiMAX to Wi-Fi, then it is called vertical HO. Horizontal HOs are easy to implement because the operation is typically made under the same operation domain. Vertical HOs, on the other hand, are typically executed between different operators, and require a much more complex signaling.

This paper is an attempt to evaluate the reliability and scalability of the network simulator-2 (ns-2) [2] tool in simulating multiple vertical HOs under the scope of IEEE 802.21. Currently the 802.21 functionality can be incorporated in ns-2 by using external add-on modules developed by the National Institute of Standards and Technology (NIST) (NIST is a nonregulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.), that are based in 802.21 (draft 3).

The paper is structured as follows. Section 2 explains the current implementation of IEEE 802.21 in ns-2. Section 3 describes relevant related work published by research projects and the academic community. Section 4 provides a general description of the signaling involved in a handover between WiMAX and Wi-Fi technologies and presents a message sequence chart for the correspondent events in ns-2. Section 5 describes our simulation scenario, presents a novel approach to determine the expected number of handovers in an ns-2 simulation and also presents simulation results. Section 6 deals with result analysis and conclusions and future work. Finally, Section 7 is for acknowledgments.

2. Related Work

Since the release of the mobility package by NIST, as part of their joint work with IEEE 802.21 and the IETF, numerous research studies have used these modules. Reference [3] evaluates the performance of an adaptive channel scanning algorithm for IEEE 802.16 using a previous version of the WiMAX module that is used in this paper. In [4] the handover latency for the cases where UDP and TCP carry

MIH signaling messages is compared and some of the design tradeoffs are presented. The evaluation of the performance of a vertical handoff scheme between 802.11 and 802.16 wireless access networks with respect to signaling cost, handoff delay, and QoS support can be found in [5]. Reference [6] evaluates a proposed cross-layer mechanism for making intelligent handover decisions in FMIPv6 in terms of handover latency, packet loss and handover signaling overhead, and [7] evaluates a new enhanced Media Independent Handover Framework (eMIHF) that allows for efficient provisioning and activation of QoS resources in the target radio access technology during the handover preparation phase.

The use of ns-2 with NIST modules has also been used to propose new implementation guidelines to the new security extension for IEEE 802.21 that is yet to come (IEEE 802.21a). Reference [8] compares different authentication techniques, namely, reauthentication and preauthentication, that may be used in order to reduce the time and resources required to perform a vertical handover. Reference [9] measures the performance of the authentication process in media independent handovers and considers the impact of using IEEE 802.21 link triggers to achieve seamless mobility, and [10] proposes an extension to current network selection algorithms that takes into account security parameters and policies and compares the handover performance with and without the proposed extension.

3. Heterogeneous Handovers in ns-2

The support for vertical HO scenarios is available, but limited, in ns-2 through the use of NIST add-on modules [11]. These modules were developed for version 2.29 of ns-2. NIST added and changed numerous files in the standard release of ns-2 in order to support mobility scenarios. The following are some of these changes:

(i) development of a new IEEE 802.21 add-on module [12], based on draft 3 of IEEE 802.21;

(ii) development of a new IEEE 802.16 add-on module [13], based on IEEE 802.16g-2004 standard [14] and the mobility extension 802.16e-2005 [15] (both updated in 2007);

(iii) development of a new Neighbor Discovery add-on module [16] for IPv6 (limited functionality);

(iv) update of the existing IEEE 802.11 MAC implementation [17].

3.1. IEEE 802.21 Support in ns-2. The 802.21 add-on module contains an implementation of the Media Independent Handover Function (MIHF) based on draft 3 of IEEE 802.21 specification. An overview of the MIHF interaction with the different components of the mobile node (MN) is shown in Figure 1.

The MIHF and MIH Users are implemented as Agents. An Agent is a class defined in ns-2, extended by NIST, that allows communication with both the lower layers (i.e., MAC) and the higher layers (i.e., MIH Users), providing the mapping between the media independent interface service access point (MIH_SAP) and the media-dependent interface (MIH_LINK_SAP and media-specific primitives). Because of this, the MIHF can send layer 3 packets to remote MIHF and MIH User can register with the MIHF to receive events from local and remote interfaces. The MIHF is also responsible of getting the list and status of local interfaces and control their behavior. The MIH User class is hierarchy organized according to Figure 2.

From Figure 1, we can see that MIH Users make use of the functionalities provided by the MIHF in order to optimize the HO process. MIH Users typically will send commands to the MIHF and receive events or messages. The Interface Management class (IFMNGMT), depicted in Figure 2, provides flow management functions which facilitate the HO module in finding the flows that need to be redirected. The IFMNGMT also receives events from the Neighbor Discovery (ND) agent when a new prefix is detected or when it expires. The MIPV6 Agent adds the redirection capability to the MIH User. When a flow needs to be redirected, a message can be sent to the source node to inform it of the new address or interface to use. The Handover class provides a template for HO modules and computes a new address after a successful HO.

3.2. 802.21 *Supported Technologies in ns-2.* Currently ns-2 supports the following technologies in IEEE 802.21 scenarios: WiMAX (802.16), Wi-Fi (802.11), and UMTS and ethernet (802.3). In the scope of the work described in this paper only WiMAX and Wi-Fi will be used in the simulation scenario described in Section 4.

3.2.1. Implementation of Nodes with Multiple Interfaces in ns-2. Supporting nodes with multiple interfaces is not intuitive in ns-2, because external packages do not necessarily follow the same node structure as the one defined in the basic model (i.e., routing algorithms are different). To resolve this issue, NIST created the concept of *multiFace* node, which is a node who links to other nodes. The other nodes are considered interfaces for the *multiFace* node, and the *multiFace* node can be viewed as a "supernode". This concept is illustrated in Figure 3.

The interface nodes trigger events and send them to the *multiFace* node. The MIH Users on the *multiFace* node can register to receive these events. Additionally each of the interface nodes will also run an instance of the Neighbor Discovery (ND) agent, detailed in Section 3.2.5, in order to detect layer 3 movement.

3.2.2. Integration of WiMAX. The WiMAX module was developed entirely by NIST, the supported features are shown in Table 1.

A limitation of the implemented WiMAX model is that, when using WiMAX cells, at the beginning of the simulation there must be at least one MN within each cell range in order for the BS to function correctly. Due to this condition, a WiMAX simulation scenario has to include "phantom" nodes. Figure 4 illustrates this concept.

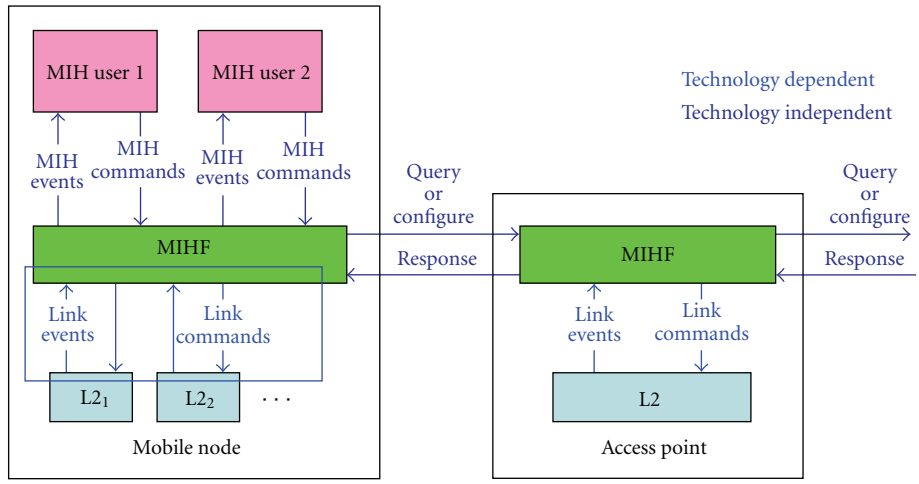

Figure 1: MIH implementation in ns-2 [12].

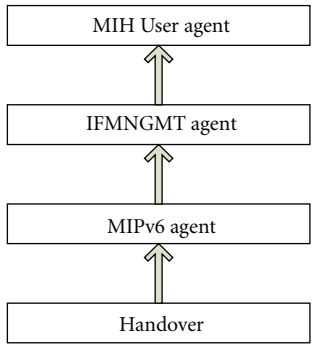

Figure 2: MIH User class hierarchy [12].

3.2.3. Integration of Wi-Fi. Regarding the Wi-Fi module, the following features were changed in order to support basic 802.21 functionality [17].

(i) *Backoff and Defer Timers*. The modifications made include the separation of the defer time (such as SIFS, DIFS, or EIFS in IEEE 802.11 standard) and the backoff time. Another modification is that after receiving an ACK, a backoff is triggered only if there is no beacon to be sent.

(ii) *Management Frames—Beacons*. The beacon messages have been added to the implementation. They can be used by an AP to inform the MN about its presence, and are sent at a specific interval (typically every 100 ms).

(iii) *Management Frames—Association Request and Response*. The Association Request and Response frames have been added to allow an MN to connect to an AP at layer 2 and to add the possibility of an AP to reject the MN from accessing the network (e.g., as part of a congestion control mechanism).

(iv) *Support for Multiple APs and Scanning*. Modifications were made to resolve the scanning functionality and the interference model when using multiple APs. As a result all MNs share the same channel object which is responsible of knowing the frequency used by each MN's physical layer. Only the MNs using the same frequency will communicate with each other. With these new capabilities, it is possible to implement scanning mechanisms at the MAC layer.

3.2.4. Integration of Information Services, Command Services, and Event Services. IEEE 802.21 standard defines three types of services: Information Services (ISs), facilitate discovery and selection of multiple types of networks that exist within a geographical area; Command Services (CSs), enable higher layers to control the physical, data link, and logical link layers and; Event Services (ESs), indicate changes in state and transmission behavior of the physical, data link, and logical link layers or predict state changes of these layers. ISs are currently not supported in ns-2 802.21 implementation. Both CS an ES are supported, Table 2 shows the correspondent primitives.

3.2.5. Support for Subnet Discovery and Change of Address. For supporting subnet discovery and change of address when making an HO, ns-2 makes use of *Router Advertisement* (RA), *Router Solicitation* (RS), and ND messages. RA messages are broadcasted periodically by Access Points (APs) or base stations (BSs) to inform MNs about the network prefix. In ns-2, each AP (Wi-Fi) or BS (WiMAX) is on a different subnet (domain or cluster in ns-2 nomenclature) and therefore will require a layer 3 HO, so the prefix is the address of the AP/BS that sends the RA.

The ND agent located in each MN is responsible for receiving RA messages and determines if it contains a new prefix; if yes the ND agent informs the interface manager; if not, the timer associated with the current prefix is refreshed. If an MN loses the connection with its current point of attachment (PoA), AP or BS, it will not receive more RAs from that PoA therefore the current prefix expires; in this case a notification is also sent to the interface manager.

RS messages are used by MNs to discover new APs or BSs after the HO.

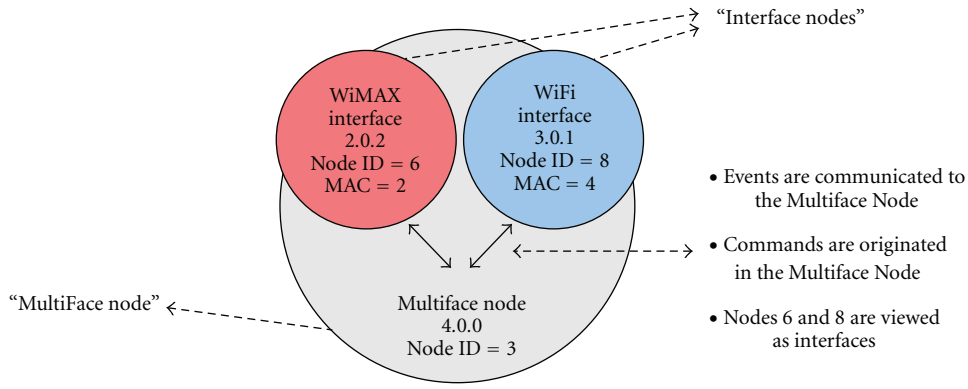

Figure 3: High level overview of a *multiFace* node.

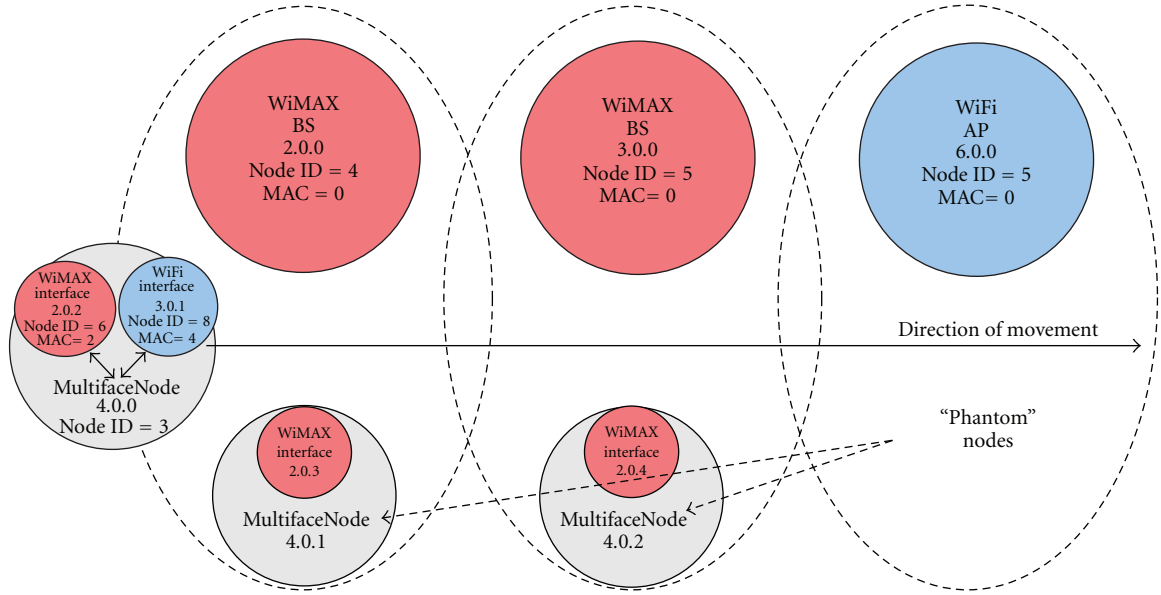

Figure 4: "Phantom nodes" in WiMAX simulation.

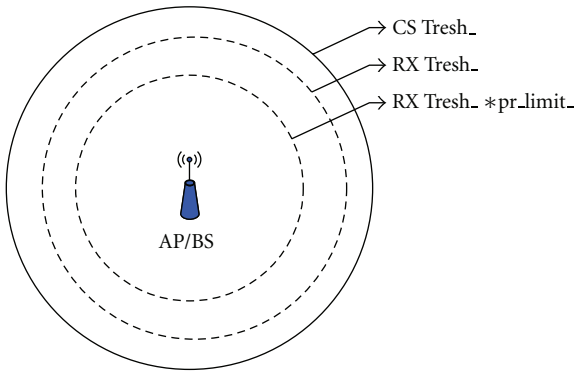

Figure 5: Power boundaries defined in ns-2.

3.2.6. Power Boundaries in Wi-Fi and WiMAX Cells in ns-2. In order to identify power boundaries to be used in the simulation, three variables were defined [17]; see Figure 5. The description of the power boundaries is as follows.

(i) *CSTresh* defines the minimum power level to sense wireless packets and switch the MAC from idle to busy;

(ii) *RX Tresh* defines the minimum power level to receive wireless packets without error;

(iii) *pr_limit* is always equal or superior to 1 and is used in the equation $(RX\ Tresh\_)*(pr\_limit\_)$; this equation defines the minimum power level that an interface senses before triggering a *Link_Going_Down* event. The higher the *pr_limit_* coefficient, the sooner the event will be generated.

4. General Description of a Handover between WiMAX and Wi-Fi

This section provides a short description of the sequence of events that a MN and network perform in order to make a successful HO. The power received at MN's interfaces, depicted in Figure 6, and the message sequence chart

Table 1: Supported and unsupported features in ns-2 WiMAX module.

Available features	Features not implemented
(i) Wireless MAN-OFDM physical layer with configurable modulation	(i) Wireless MAN-OFDMA
(ii) Time Division duplexing (TDD)	(ii) Frequency Division duplexing (FDD)
(iii) Management messages to execute network entry (without authentication)	(iii) (ARQ) Automatic Repeat Request
(iv) Default scheduler providing round robin uplink allocation to registered Mobile Stations (MSs) according to bandwidth requested	(iv) Service Flow and QoS scheduling
(v) IEEE 802.16e extensions to support scanning and handovers	(v) Periodic ranging and power adjustments
(vi) Fragmentation and reassembly of frames	(vi) Packing
	(vii) Error Correction

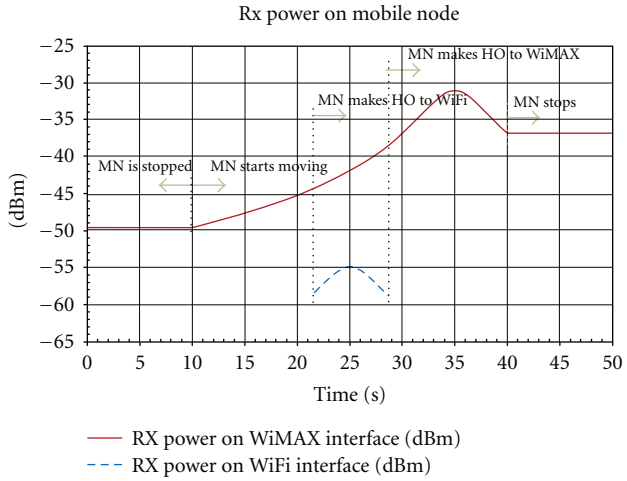

Figure 6: Received power on both MN's interfaces.

Table 2: Supported MIH commands and events in ns-2.

MIH commands	MIH events
Link event subscribe	Link UP
Link event unsubscribe	Link down
Link configure threshold	Link going down
Link get parameters	Link detected
MIH get status	Link event rollback
MIH link scan	Link parameters report
	Link handover imminent
	Link Handover Complete

depicted in Figure 7 are important to better understand the description that follows.

Figure 6 shows that a particular MN started in a WiMAX cell and in the first 10 s the MN is stopped. Then it started to move in direction of the center of the BS, and in its way a Wi-Fi network was detected. Since the used HO algorithm considers Wi-Fi a better network than WiMAX, the MN makes the HO to the Wi-Fi network ($t = 22$ s). MN stays in this network for approximately 7 s, when it senses that it is losing coverage. Since the WiMAX signal is still available the MN makes a new HO to the WiMAX network (because it has no better network). The MN is the closest to the BS at instant $t = 35$, when the Rx power is at its highest value. The MN then continues its way and stops at instant $t = 40$ s.

A more detailed description of the sequence of events is as follows.

(1) MIH user on the MN sends *MIH Get Status Request* to MN's MIHF.

(2) MN's MIHF responds with an *MIH Get Status Response*, saying that two interfaces are available: one is *link type 27* (WiMAX) and the other is *link type 19* (Wi-Fi); both interfaces support commands and events.

(3) MIH user subscribes for events on both MN's interfaces.

(4) MN's WiMAX interface receives a *Download Context Descriptor* (DCD) and an *Upload Context Descriptor* (UCD) from the BS and triggers a *Link Detected* event.

(5) MIH User Agent in the MN receives the *Link Detected* and since this is the only interface detecting a possible PoA, it commands MN's WiMAX interface to connect to the BS.

(6) MN's WiMAX interface connects to BS and triggers a *Link Up* event that is received by MN's MIHF that then commands MN's MIPv6 agent to request the ND Agent to send an RS.

(7) MN's WiMAX interface sends an RS; BS detects that this is a new neighbor, it then sends an RA including: router-lifetime (1.800 s), prefix valid_lifetime (5 s), network prefix (ex. 2.0.0), and advertisement interval (10 s).

(8) MN's WiMAX interface receives the RA. This interface will now reconfigure its address according to the received prefix (i.e., interface address = 2.0.1). MN's MIH Agent is notified and commands the WiMAX interface to send an *MIH Capability Request* to the BS.

(9) BS receives the *MIH Capability Request* and sends an *MIH Capability Response* including its MIHF identification; MIH Agent now knows the identification of the remote (PoA) MIHF identification.

(10) At $t = 5$ s, CN starts to send CBR traffic to the MN. Traffic is received through the WiMAX interface.

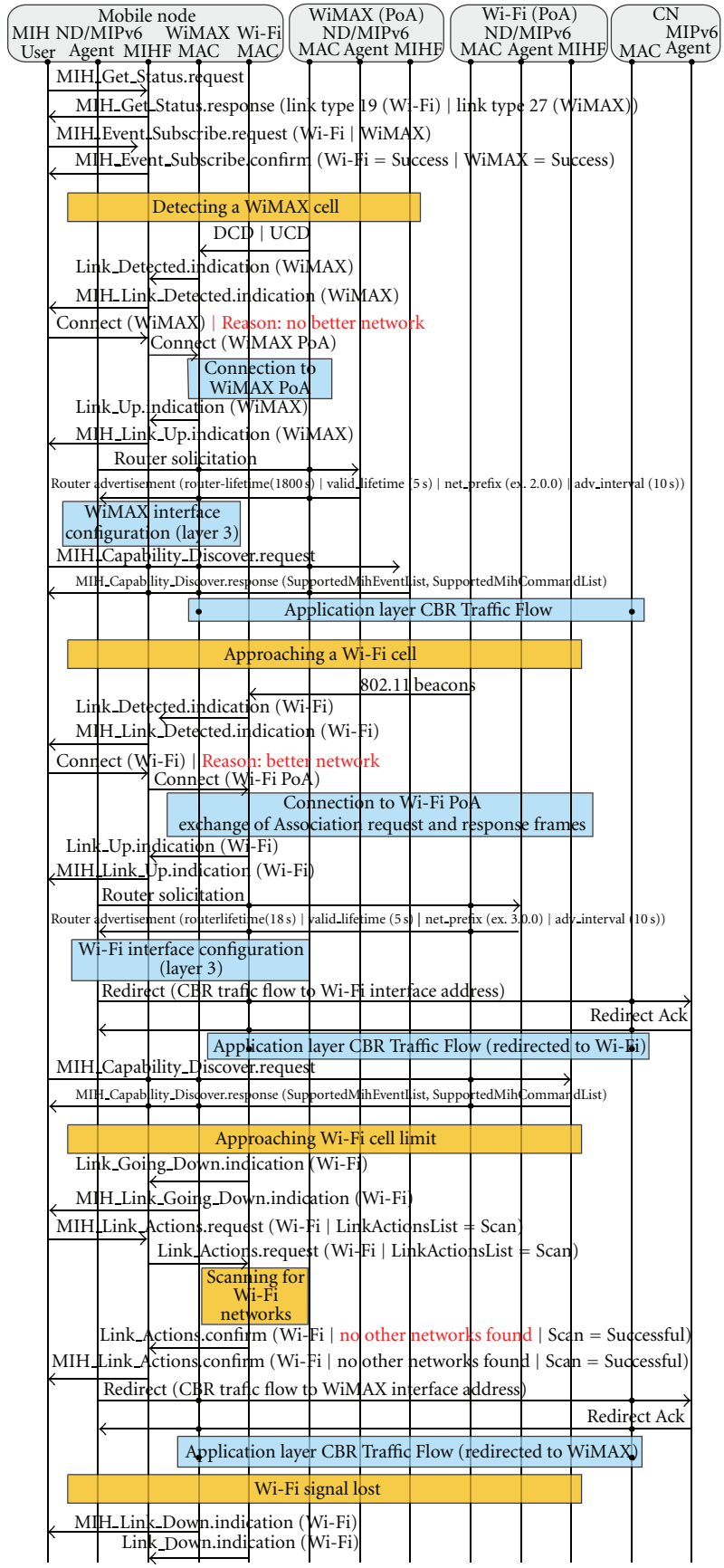

Figure 7: Sequence of events triggered by WiMAX-Wi-Fi-WiMAX handover using NIST modules in ns-2.

(11) At $t = 10$ s, MN starts moving towards Wi-Fi cell.

(12) At approximately $t = 22$ s, MN's Wi-Fi interface starts detecting 802.11 beacons and triggers a *Link Detected* event when the received power of the beacon frames is above the threshold value; MIH Agent in the MN receives the *Link Detected* event and, since this is a better interface, it commands MN's Wi-Fi interface to connect to the AP.

(13) MN's Wi-Fi interface and the AP exchange *Association Request* and *Response* frames in order to connect the MN to the Wi-Fi cell. After MN's Wi-Fi interface receives the *Association Response*, it will trigger a *Link Up* event; MIH Agent in MN receives the *Link Up* event and commands MN's MIPv6 agent to request the ND Agent to send an RS.

(14) MN's WiFi interface sends an RS; AP receives the RS and detects that this is a new neighbor, it then sends a RA including router lifetime (18 s), prefix valid lifetime (5 s), network prefix (ex. 3.0.0), and advertisement interval (10 s).

(15) MN's Wi-Fi interface receives the RA. This interface will now reconfigure its address according to received prefix (i.e., interface address = 3.0.1). MN's MIH Agent is notified.

(16) MN's MIPv6 Agent commands the Wi-Fi interface to send a *Redirect* message to the CN in order to inform the CN of the new MN location; CN's MIPv6 Agent receives the *Redirect* message and sends an *Ack* message that is later received by MN's Wi-Fi interface which then notifies MN's MIH Agent. This behavior is considered a make-before-break, that is, the MN will use both interfaces at the same time in order to perform a seamless HO.

(17) At approximately $t = 22$ s MN's MIH Agent has the confirmation that the CN has been notified of MN's new address and redirects the reception of CBR traffic from the WiMAX interface (2.0.1) to the Wi-Fi interface (3.0.1); traffic comes in using the link between Wi-Fi interface and AP.

(18) MN's MIH agent commands the Wi-Fi interface to send a *MIH Capability Request* to the AP; AP responds with a *MIH Capability Response* including its MIHF identification; this process is similar to what was described to WiMAX.

(19) MIH Agent receives the MIH Capability Response with the identification of the new remote (PoA) MIHF identification.

(20) At approx. $t = 28$ s the MN is approaching the boundary of Wi-Fi cell so the Wi-Fi interface triggers a *Link Going Down* event (based on the received power of the beacon frames); due to MN's speed the probability that the Wi-Fi link goes down starts to increase. When it reaches a specified value (90% in our case), and since MN's WiMAX interface is still active, the MN MIPv6 Agent commands the WiMAX interface to send a *Redirect* message to the CN in order to inform the CN of the new MN location (2.0.1). Additionally the MN's MIH Agent commands the Wi-Fi interface to execute a *Link Scan* in order to search for other nearby Wi-Fi networks.

(21) MN's Wi-Fi interface executes the scan sending a *Probe Request* in each of the defined IEEE 802.11 channel frequencies. A *Probe Response* is only received in channel 2 (where the MN currently is). Based on this, MN's MIH Agent is notified that this is the only available Wi-Fi network.

(22) CN's MIPv6 Agent receives the *Redirect* message and sends *Ack* message that is received by MN's WiMAX interface; MIH Agent is notified.

(23) At approximately $t = 29$ s MN's MIH Agent has the confirmation that the CN has been notified of MN's new address and redirects the reception of CBR traffic from the Wi-Fi interface (3.0.1) to the WiMAX interface (2.0.1); traffic now comes in using the link between the WiMAX interface and BS.

(24) Almost at the same time MN's Wi-Fi interface triggers a *Link Down* event, and the MN is disconnected from Wi-Fi cell.

5. Simulation Scenario

The simulation of 802.21 HOs between heterogeneous networks using ns-2 has two main purposes: (i) evaluating 802.21 NIST add-on modules for ns-2 and (ii) evaluating the reliability and scalability of ns-2 in simulating 802.21 scenarios.

In order to achieve these goals, a network topology consisting of one WiMAX base station, three Wi-Fi access points and a variable number of MNs was created. Choosing for a variable number of MNs allows us to measure ns-2 scalability in simulating 802.21 scenarios. Figure 8 presents the network topology, and Table 3 presents values for the most relevant variables.

5.1. Determining the Number of IEEE 802.21 Handovers in ns-2. When simulating IEEE 802.21 scenarios in ns-2 with a variable number of nodes with random start and end positions, it is important to determine the number of HOs that would be triggered by MNs. Comparison between this value and the effective number of HOs that were produced in ns-2 simulation is important because it is an indication of the HO success rate as the number of MNs increases in the simulation. Since ns-2 does not provide this information, a new innovative way of determining such a value is proposed in this paper. Taking in consideration Figure 8 and knowing that MNs have a rectilinear movement (Table 3), a handover happens when a MN crosses the boundary of a 802.11 cell; this is independent of the start and end positions of the MN.

Using the MN positioning data obtained from ns-2 simulation, it is possible to draw the trajectories of each simulated MN. The total number of intersections between the MNs trajectories and 802.11 boundaries gives the theoretic number of handovers in the simulation.

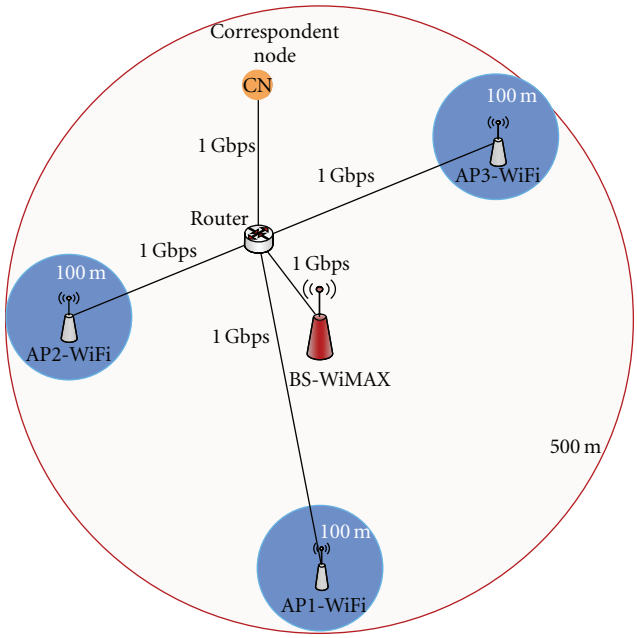

Figure 8: Simulation scenario.

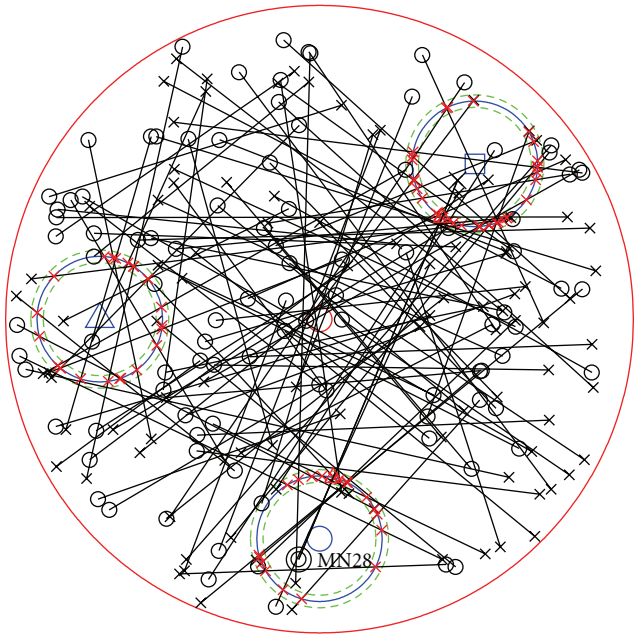

Figure 9: Determining no. of HOs by geometric calculation.

The trajectories for 100 MNs triggering a total of 79 handovers can be seen in Figure 9; the big circle corresponds to the WiMAX coverage area, the three small circles correspond to the three Wi-Fi cells coverage and the lines correspond to MN trajectories. Each line starts with a small circle (MN start position) and ends with a cross (MN end position). The intersections between lines and the three Wi-Fi circles are indicated by small triangles. Each Wi-Fi cell has also two doted circles representing the power boundaries described in Section 3.2.6.

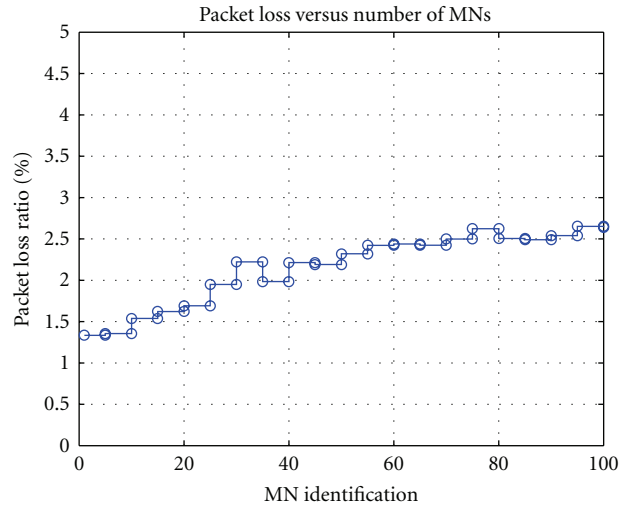

Figure 10: Percentage of packet loss versus no. of MNs

5.2. Simulation Results. To evaluate ns-2 as a platform for simulating handovers in 802.21 scenarios, we measure (i) system packet loss, (ii) handover time (delay), and (iii) the impact of higher traffic bit rates in the system.

Figure 10 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 all MNs (including both WiMAX and Wi-Fi interfaces).

Figure 11 shows the evolution of HO time from WiMAX to Wi-Fi and vice versa as the number of MNs increases in the system. The HO time is the amount of time that elapses between an interface sending an MIPv6 *Redirect Request* to the CN and receiving the correspondent *Redirect Ack* from the CN.

For the specific simulation of 100 MNs in the system, Figure 12 identifies the MNs that executed an HO, the wireless networks to which a particular MN has made the HO, and the specific time it took for that specific handover. As an example, we can see that MN number 10 executed two HOs, one to the WiMAX cell and the other to Wi-FI cell (AP3). MN number 60 has not made any HO. Figure 12 also shows that for 100 MNs in the system the average HO time to Wi-Fi cell (less sensitive to the number of MNs in the simulation) is approximately 5 ms, and the average HO time to WiMAX cell is approximately 230 ms (also see Figure 11 for 100 MNs).

Figures 12, 13, and 14 show how the increase in bit rate and the number of MNs in the simulation affect the packet loss and the HO time (delay).

6. Conclusions and Future Work

IEEE 802.21 uses a significant amount of signaling in the nodes themselves and between the nodes and network infrastructure. Even considering the fact that the NIST 802.21 add-on modules only support limited functionality of the standard, the amount of signaling generated by this

Table 3: Simulation parameters.

Number of mobile nodes	Between 1 and 100
Mobile movement	Rectilinear movement at 50 Km/h
Propagation channel model	Two-Ray Ground
Wired links	All wired links support 1 Gbps
Traffic parameters	UDP, constant bit rate at (Kbps) 50, 100, 200, 300, 500, and 1000.
WiMAX coverage	500 m
WiMAX parameters	Technology: 16QAM (10 Mbps) BS Tx power: 15 W (41 dBm) @ 3.5 GHz *RX Thresh_*: 1.215 e-9 W (~ −60 dBm) *CSTresh_*: Level 80% of *RX Thresh_*
Wi-Fi coverage	100 m
Wi-Fi parameters	Technology: 802.11 b (11 Mbps) AP Tx power: 100 mW (20 dBm) @ 2.417 GHz *RX Thresh*: 0,989 e-9 W (~ −60 dBm) *CSThresh_*: Level 90% of *RX Thresh_* *pr_limit_*: 1.2

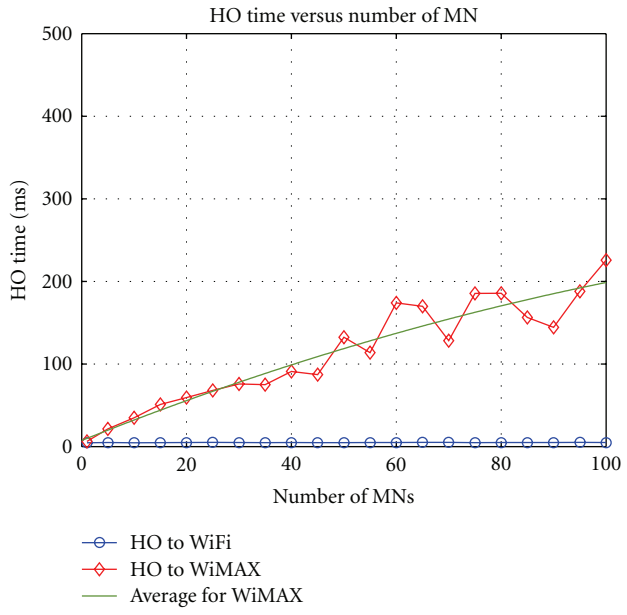

Figure 11: HO time versus no. of MNs.

module is significant. Adding to this, there is also all the signaling from 802.11 and 802.16 (including management and beacon frames). Beacons frames are mandatory in the simulation, because MN's interface uses them to trigger MIH events such as "*Link Detected*" or "*Link Going Down*" (see Table 2); they are a fundamental part of the network discovery process MNs do in order to discover networks (better coverage or better service).

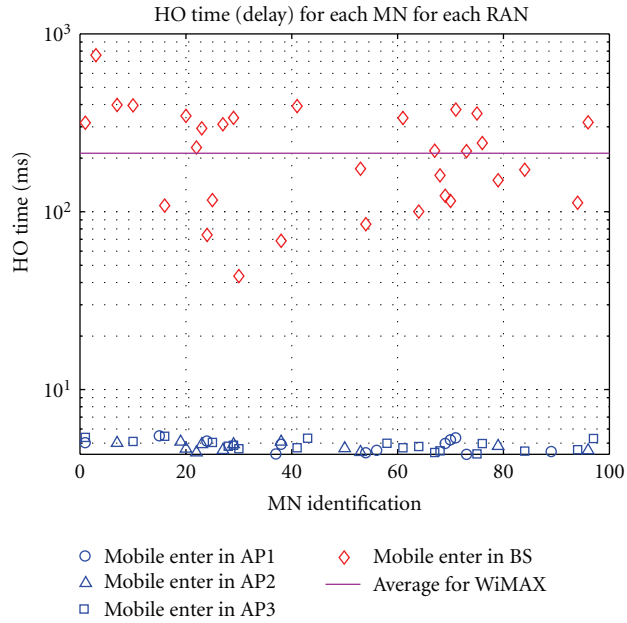

Figure 12: HO time for each MN (total of 100 MNs in topology).

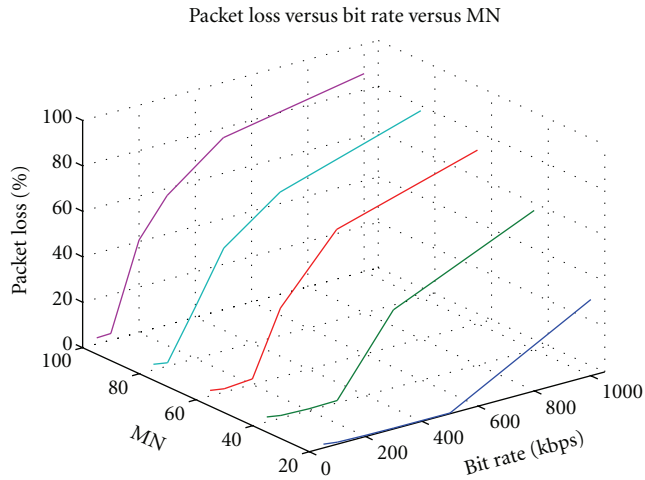

Figure 13: Packet loss versus bit rate versus no. of MNs.

From our analysis, packets are lost mainly due to (i) address resolution issues, in which case ARP must run every time a MN enters a new cell, (ii) the handover operation and, (iii) insufficient bandwidth in the deployed radio access technologies. It is also possible to see this effect in Figure 13.

For audio, lost packets produce choppy, broken audio. The IEEE 802.20 Working Group [18] recommends less than 2% packet loss for mobile voice.

For video in mobile networks, packet loss tolerance heavily depends on the scenario. A packet loss of 1% [18] is accepted for noninteractive video; for interactive video, such as in a videoconference, the recommended is less than 0.1%.

Looking at the obtained results for packet loss in our simulated scenario, see Figure 10, we can see that if more than 40 MNs are present in the topology, voice would degrade

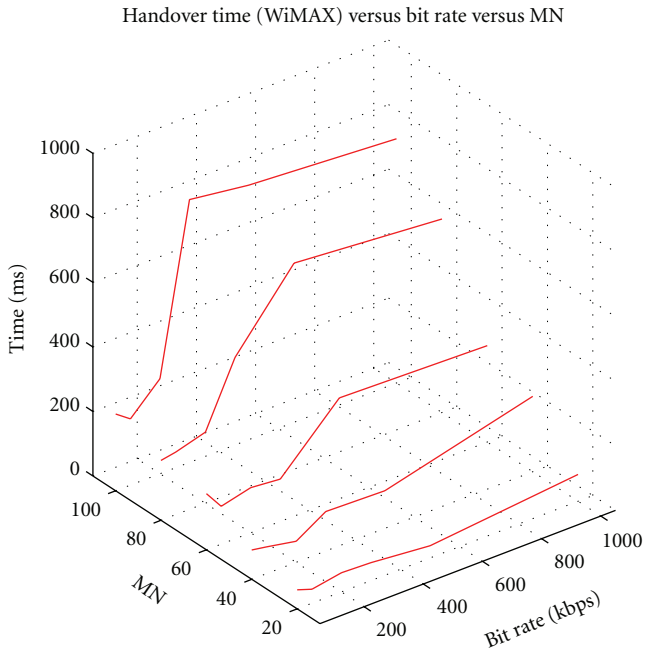

Figure 14: HO time (WiMAX) versus bit rate versus no. of MNs.

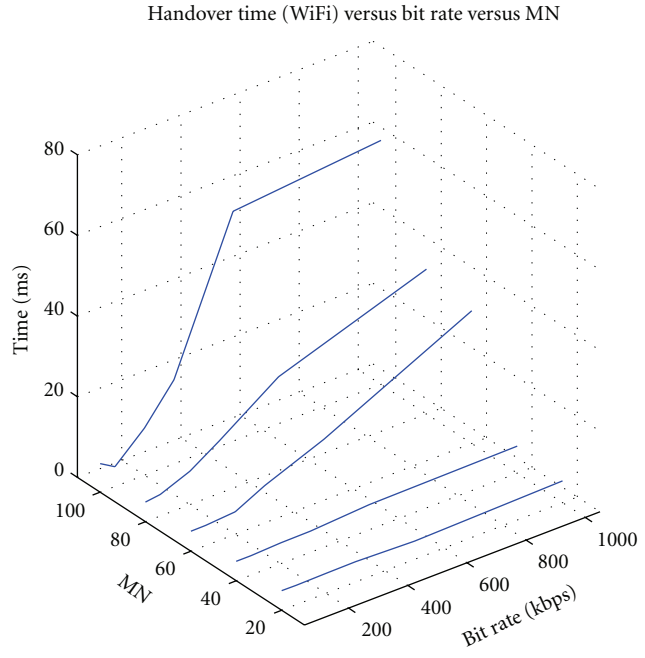

Figure 15: HO time (Wi-Fi) versus bit rate versus no. of MNs.

to bad quality. For video, only non-interactive applications would be allowed, because buffering and retransmission of lost packets are possible. If traffic flow has an increased bit rate, see Figure 13, video support would degrade to unacceptable quality.

Regarding the handover time, results depicted in Figures 11 and 12 show that HO to the WiMAX cell is more sensitive to the number of MNs in the simulation than the Wi-Fi cells. This can be explained by the fact that the WiMAX cell is bigger than the Wi-Fi cells, so is the total number of MNs inside the WIMAX cell. Since each MN is receiving traffic from the CN, more traffic is being supported by the WiMAX cell. Additionally, we observed that the delay associated with the first part of the handover (till redirect message reaches the CN) has the same tendency as the ones in Figure 11. We concluded that this difference in behavior is related to how, in ns-2, these two technologies implement the uplink and downlink scheduler and the contention resolution/avoidance for the wireless shared medium.

Considering IEEE 802.20 Working Group recommendations for mobile voice, the one-way network delay should be less than 150 ms. By looking to the evolution of the handover delay to WiMAX depicted in Figure 11 we could think that in the simulated scenario the obtained results were acceptable to guarantee such recommendation; however the measured HO time does not take in consideration that some HO features, such as user authentication, resource query, and resource reservation in the target network, are not currently implemented in NIST add-on modules for ns-2. If such features were supported, the HO delay would increase; as shown in [10] by including authentication and some additional primitives for Information Services, the handover delay can reach up to 1 second.

According to [18] a delay of 150 ms and 200 ms is acceptable for low- and high-quality voice, respectively, in mobile networks. For non-interactive video a one-way network delay of 280 ms [18] is acceptable, and for interactive video, the delay will depend on the class of interactivity. According to ITU-T Recommendation Y.1541 [19], a network delay of 100 ms is acceptable for class 0 and up to 400 ms is acceptable for class 1.

Results depicted in Figures 11, 12, 14, and 15 show that such recommendations can be achieved during handover by both WiMAX and Wi-Fi technologies, given that the number of associated MNs and traffic flow volume are in acceptable values.

We can say that ns-2 with NIST add-on modules proved to be a valuable tool to simulate IEEE 802.21 handover scenarios and better understand the basic signaling of IEEE 802.21 standard. NIST add-on modules however, only support part of the standard (based on draft 3) and were not conceived to simulate a high number of MNs as some adaptations in ns-2 were needed in order to run the simulations described in this paper. Nevertheless obtained results have proven an acceptable approximation to what could be expected in real case scenarios.

Considering that add-on modules, such as WiMAX, Wi-Fi, UMTS, Bluetooth, FMIPv6, amongst others, are constantly being added and updated by the ns-2 community, the importance of ns-2 for 802.21 simulations becomes clear. It will not only allow simulating complex vertical handover scenarios, prohibitive to do in a real testbed, but also allow modifying such modules in order to model missing primitives and better predict results for a real scenario. As shown by our experiments, both WiMAX and Wi-Fi modules need improvements in the scheduling mechanisms and the contention resolution/avoidance for the shared medium in order to better reflect the technology's real behavior.

As future work, new contributions could appear on the following topics: (i) implementation of missing IEEE 802.21 primitives in ns-2 using the current NIST modules in order to better simulate seamless HOs in conformance to the IEEE 802.21 standard; (ii) implementation of a retransmission mechanism for MIP messages in order to improve the success ratio of handovers; (iii) implementation of Information Services and a Media Independent Information Server (MIIS) that MNs could query in order to obtain neighbor network information.

Acknowledgment

The work presented in this paper was supported by the European Project ICT-HURRICANE and the Portuguese Foundation for Science and Technology (FCT) through Project AGILE.

References

[1] IEEE P802.21-2008, "Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," IEEE, January 2009.

[2] "The network simulator tool," ns-2, http://nsnam.isi.edu/nsnam/.

[3] R. Rouil and N. Golmie, "Adaptive channel scanning for IEEE 802.16e," in *Proceedings of IEEE Military Communications Conference (MILCOM '06)*, October 2006.

[4] D. Griffith, R. Rouil, and N. Golmie, "Performance metrics for IEEE 802.21 media independent handover (MIH) signaling," *Wireless Personal Communications*, vol. 52, no. 3, pp. 537–567, 2010.

[5] Y. Zhang, W. Zhuang, and A. Saleh, "Vertical handoff between 802.11 and 802.16 wireless access networks," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 584–589, December 2008.

[6] Q. B. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized FMIPv6 using IEEE 802.21 MIH services in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6 I, pp. 3397–3407, 2007.

[7] P. Neves, F. Fontes, S. Sargento, M. Melo, and K. Pentikousis, "Enhanced media independent handover framework," in *Proceedings of the 69th IEEE Vehicular Technology Conference*, Barcelona, Spain, April 2009.

[8] A. Izquierdo, N. Golmie, K. Hoeper, and L. Chen, "Using the EAP framework for fast media independent handover authentication," in *Proceedings of the Wireless Internet Conference (WiCON '08)*, Maui, Hawaii, USA, November 2008.

[9] A. Izquierdo, N. Golmie, and R. Rouil, "Optimizing authentication in media independent handovers using IEEE 802.21," in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, August 2009.

[10] A. Izquierdo and N. T. Golmie, "Improving security information gathering with IEEE 802.21 to optimize handover performance," in *Proceedings of the 12th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM '09)*, pp. 96–105, 2009.

[11] "NIST ns-2 add-on modules for 802.21 (draft 3) support," http://www.antd.nist.gov/seamlessandsecure/pubtool.shtml#tools.

[12] "The Network Simulator NS-2 NIST add-on—IEEE 802.21 model (based on IEEE P802.21/D03.00)," National Institute of Standards and Technology (NIST), January 2007.

[13] "The Network Simulator NS-2 - NIST add-on—IEEE 802.16 model (MAC+PHY)," National Institute of Standards and Technology (NIST), January 2009.

[14] IEEE 802.16 WG, "IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Std. 802.16-2004, October 2004.

[15] IEEE 802.16 WG, "Amendment to IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems–Physical and Medium Access Control Layer for Combined Fixed and Mobile Operation in Licensed Bands," IEEE Std. 802.16e-2005, December 2005.

[16] "The Network Simulator NS-2 - NIST add-on – Neighbor discovery"," National Institute of Standards and Technology (NIST), January 2007.

[17] "The Network Simulator NS-2 - NIST add-on - Mac 802.11," National Institute of Standards and Technology (NIST), January 2007.

[18] IEEE 802.20 Working Group, "Mobile Broadband Wireless Access (MBWA)," ITU-T Recommendation Y.1541, Network Performance Objectives for IP-Based Services. ITU-T Recommendation Y.1541, Network Performance Objectives for IP-Based Services, http://www.ieee802.org/20/.

[19] ITU-T Recommendation Y.1541, "Network Performance Objectives for IP-Based Services".

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 256964, 8 pages
doi:10.1155/2010/256964

Research Article

Service-Aware Retransmission Control in Cellular Networks

Nadhir Ben Halima,[1] Dzmitry Kliazovich,[2] and Fabrizio Granelli[1]

[1] *Department of Information Engineering and Computer Science, University of Trento, via Sommarive 14,38050 Trento, Italy*
[2] *University of Luxembourg, 6 rue Couden-hove Kalergi, L-1359, Luxembourg*

Correspondence should be addressed to Dzmitry Kliazovich, kliazovich@disi.unitn.it

Received 1 February 2010; Accepted 30 June 2010

Academic Editor: Charalabos Skianis

This paper proposes a service-aware cross-layer approach between application/transport layers on the mobile terminal and link layer on the wireless base station to enable dynamic control on the level of per-packet error protection for multimedia data streams. Specifically, in the context of cellular networks, the proposed scheme enables the mobile terminal to specify to the base station the desired level of Hybrid ARQ (HARQ) protection by using an in-band control feedback channel. Such protection is dynamically adapted on a per-packet basis and depends on the perceptual importance of different packets as well as on the reception history of the flow. Experimental results demonstrate the potential benefits deriving from the proposed strategy either for audio and video real-time streams as well as for TCP-based data transfers.

1. Introduction

Nowadays, IP networks and the Internet in particular are used as transport facilities for a whole plethora of novel applications that go far beyond the data transfer for which IP was originally designed. Those applications introduce specific requirements in terms of delivery performance of the underlying transport infrastructure. Indeed, as services are evolving to a "triple play" vision, implying delivery of data, voice, and video to the end user using the same IP transport facility, strong emphasis is put on providing a satisfactory user experience and as a consequence on identifying techniques able to control packet losses and delay.

In addition, more than 30% of the current Internet users are mobile, that is, use wireless networks to access the Internet and its services. The usage of a wireless access technology increases the complexity in the management of delivery of data and multimedia flows, due to the time-varying performance of the wireless medium, handover management, and so forth.

While no solution for end-to-end quality of service (QoS) assurance over heterogeneous networks is available, still several approaches are available for improving data transfer performance on the wireless access trunk [1]. However, most of the available solutions are flow-based (i.e., intended to differentiate services based on flows) and furthermore need to introduce relevant modifications to the protocol stacks on the mobile node and wireless base stations—which reduces the possibility of deployment of such schemes.

In the specific framework of multimedia (e.g., voice and video), several works are available based on the Unequal Error Protection (UEP) paradigm [2–6]. The goal of UEP is to provide higher protection to the most perceptually relevant data, where protection can be achieved through means of adaptive power levels, forward error correction codes, retransmission control, and so forth. Nevertheless, since UEP is usually performed or managed at source level and thus without specific knowledge of the contingent operating scenario, such solutions (while increasing the complexity of multimedia codecs) can lead to nonoptimal performance due to waste of available capacity in case network/channel conditions are good (and no packet drops are experienced) or time-varying performance of the transport infrastructure (particularly true in the case of wireless networks).

The proposed scheme represents a novel paradigm of dynamic and "link-level" UEP, focused on the access network and the actual "reception history" at the receiver. The

scenario is "triple-play" service delivery over 3G cellular networks, with specific focus on the wireless link between the Base Station and the User Terminal. The core idea is to adaptively tune the level of Hybrid ARQ (HARQ) protection based on the relative importance on the overall user experience of the packet being transmitted by the base station. The introduction of such term enables to differentiate protection on the basis of the actual content of the packet; for voice and video flows, the impact of losing the current packet (and the corresponding required level of protection) is estimated in terms of the potential decrease in audio or visual quality as measurable by Mean Opinion Score (MOS) or Peak Signal-to-Noise Ratio (PSNR), respectively. The authors agree that other automatic means for finer and more accurate evaluation of the multimedia quality are available in the literature (e.g., E-model for audio, V-model for video). However, the method is presented using PSNR for sake of simplicity (as the focus in on the overall approach and not on the specific building blocks), while the introduction of more sophisticated algorithms based on finer models or Rate-Distortion characteristic is possible due to the modular architecture of the proposed solution.

An important aspect to be underlined is that the above concept is applicable also in the case of data transfer. In this case, assuming data flows are transported by TCP (which is true for more than 80% of the Internet traffic), packet losses can have a different impact on the overall performance (in terms of time required to complete the delivery) due to the corresponding modifications of the congestion window evolution.

The proposed scheme (Service-Aware Retransmission Control—SARC) is inspired, first, by basic ideas of adjusting ARQ/HARQ over the lossy links for multimedia traffic [7–9], second, by multiple studies adapting TCP data transfer performance to wireless environment [10], and, finally, by cross-layer optimization in wireless and mobile networks [11, 12] However, one of the main design features which differentiates the proposed approach is the availability of the feedback channel between the MN where the decision on ARQ tuning is taken and the BS where it is actually implemented.

The structure of the paper is as follows: Section 2 describes in detail the proposed framework, while performance evaluation is presented in Section 3. Finally, Section 4 concludes the paper with final remarks and outlines about future work on the topic.

2. Proposed Approach

The main idea of the proposed approach, called Service-Aware Retransmission Control (SARC), is to allow the mobile terminal receiver to control the level of HARQ protection applied by the base station for every frame transmitted on the radio link. The decision of the mobile terminal is based on the potential benefit in correctly receiving the next packet given the current reception history and the actual perceptual relevance of the packet itself.

Automatic Repeat Request (ARQ) is an error detection mechanism used in UMTS, where the transmitter uses a stop-and-wait procedure, transmitting a data block and waiting for a response from the receiver before sending a new data block or retransmitting an incorrectly received data block. As an evolution of such approach, Hybrid ARQ (HARQ) scheme is used in High Speed Downlink Packet Access (HSDPA), an evolution of UMTS where incorrectly received data blocks are not discarded but stored and soft-combined with successive retransmissions of the same information bits.

3GPP specifications have defined two HARQ processes for HSDPA: Incremental Redundancy and Chase Combining [13]. In the former scheme, successive retransmissions of an incorrectly received data block are sent with additional redundancy—that is, increased with each consecutive retransmission. The retransmissions consist of redundant information in order to increase the chances of successful delivery. Since each transmitted block is not the same as the previous transmission, it is demodulated and stored at the receiver and subsequently soft-combined to reproduce the original data block [14]. In the chase combining strategy, an erroneously received data packet is stored and soft-combined with later retransmissions that are an exact copy of the original transmission.

HSDPA uses HARQ (Hybrid Automatic Repeat Request) retransmission mechanism with Stop and Wait (SAW) protocol. HARQ mechanism allows the User Equipment (UE) to rapidly request retransmission of erroneous transport blocks until they are successfully received. HARQ functionality is implemented at MAC-hs (Medium Access Control—high speed) layer, which is a new sublayer introduced in HSDPA. MAC-hs is terminated at node B, instead of RLC (Radio Link Control) which is terminated at RNC (Radio Network Controller). This enables a smaller retransmission delay (<10 ms) for HSDPA rather than UMTS Rel. 99 (up to 100 ms).

In this paper, the level of HARQ protection (also indicated as "HARQ Strength" in the following) is considered in terms of the maximum number of retransmission attempts taken for a packet delivery in case of failure.

Figure 1 illustrates architectural principles of the proposed SARC approach. As outlined in the previous sections, SARC operates on the wireless 3G link. At the mobile terminal side, whenever a packet is received by the application, the latter can specify packet importance for subsequent incoming packets for a given flow.

The information about the importance of the next packet is then transferred into corresponding values of HARQ protection by the SARC module (implemented within the protocol stack of the mobile terminal) and delivered to the HARQ entity at the link layer of the Base Station using cross-layer signaling. At the link layer, the specified HARQ protection parameter is sent along with HARQ acknowledgement, which is generated for every frame received according to stop-and-wait HARQ type.

The SARC module implemented at the BS analyses incoming traffic (assuming to have access to TCP and IP protocol headers) and specifies the HARQ entity to use the requested HARQ protection on a per-packet basis.

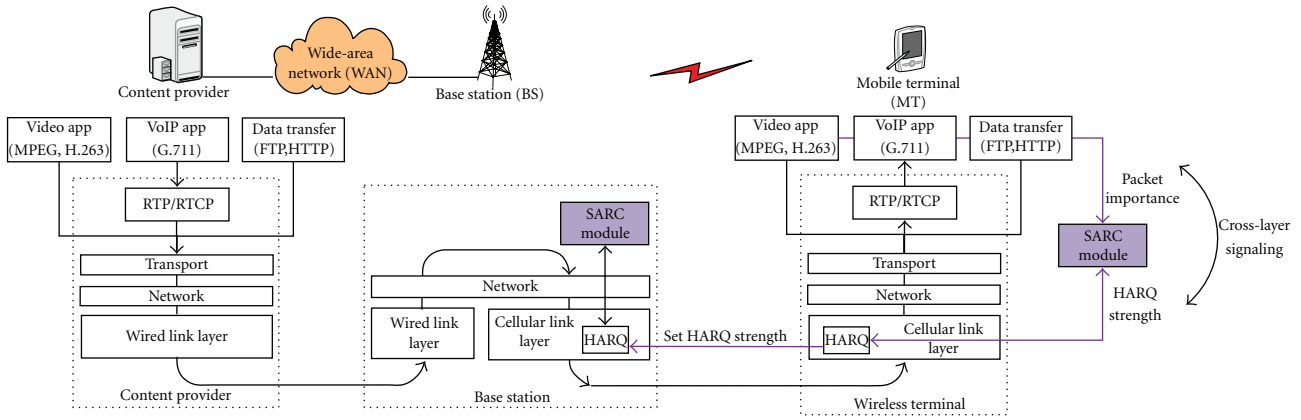

Figure 1: Architectural principles of SARC in a 3G cellular network. Blocks and links highlighted in "blue" underline the modules and signaling links employed by SARC approach.

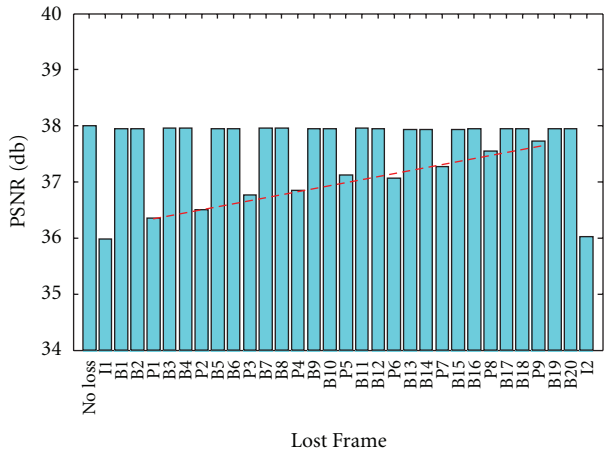

Figure 2: Quality of the received video flow for different frames lost.

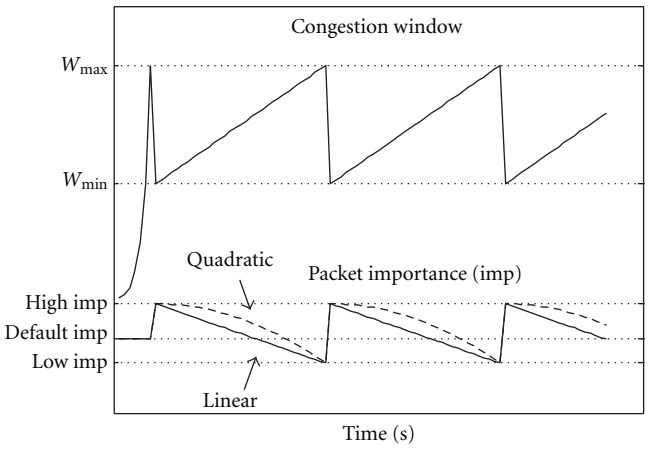

Figure 3: Variation of HARQ strength used for TCP packet transmission based on the congestion window parameter estimated at the receiver.

2.1. Packet Importance Metric. The adaptation of the level of HARQ protection based on the content carried in the packet payload represents a solution belonging to the framework of cross-layer service-aware networking solutions, which optimize "pure" networking techniques based on services and their traffic demand.

In this paper, we address three different classes of service—voice, video, and data transfer—improving delivery performance by adapting network response to the relevance of packet being delivered over the radio link.

The level of HARQ protection in the proposed approach varies on the basis of a packet importance metric, which consists of two components.

(i) Initial packet importance corresponds to the level of quality reduction for a given flow in case the packet is lost during transmission or corrupted at the receiver [15]. The quality of the flow is determined by end-to-end application requirements and user demands. For example, commonly used metric for VoIP is Mean Opinion Score (MOS), for video is Peak Signal-to-Noise Radio (PSNR), and for TCP-based data is transfer throughput level.

(ii) Dynamic packet importance component accounts for the "reception history" of the flow and adjusts initial packet importance. For example, the importance of frame i in a video sequence can be dynamically adjusted in case its decoding depends on the neighboring frames $i-1$ and $i+1$ and frame $i-1$ is not correctly received.

2.2. Packet Importance Metric in Video Streams. For sake of a clear explanation, we consider a scenario with a mobile node receiving MPEG-4 video flows from a streaming server located in the wired Wide-Area Network (WAN). However, similar reasoning can be applicable to H.263 and H.264 encoded video streams, as well as embedded video streams. The Base Station (BS) serves as a gateway between fixed and wireless network segments.

An MPEG-4 video is composed of Groups of Pictures (GOPs), consisting of video frames of three types. I-Frames (Intra coded frames) are encoded without reference to any other frame in the sequence, and are usually inserted every 12 to 15 frames as well as at the beginning of a sequence. Video decoding can start at an I-frame only. P-Frames (Predicted frames) are encoded as differences from the last I- or P-frame. The new P-frame is first predicted on the basis of the reference I- or P-frame through motion compensation and encoding of the prediction error. B-Frames (Bidirectional frames) are encoded as the difference from the previous or following I- or P-frames. B-frames use prediction as for P-frames but for each block either the previous or the following I- or P-frame is used.

Due to the correlation property of P- and B-frames, the effective impact deriving from the loss of an I-frame can be clearly considered much higher than that of P- or B-frame. In addition, the loss of one I- or P-packet may generate error propagation: while the loss of a B-frame does not affect the quality of the consecutive frames, the loss of an I-frame may disable correct decoding of subsequent P- and B-frames. This leads to the conclusion that I-frames are more important than P-frames, which are more important than B-frames.

To validate the above considerations, Figure 2 shows the quality reduction of a real video flow transmitted using VideoLan software [16] in terms of PSNR measured at the receiver versus the loss of different types of packets within a GOP. The horizontal scale indicates which frame within the GOP was lost, while the first value (obtained with no losses) serves as a reference point.

The highest loss in PSNR quality corresponds to the case when the I-frame is lost-making decoding of the entire GOP either not possible or prone to error propagation. On the other hand, the loss of any of B-frame does not degrade the quality by more than a minor fraction. However, the loss of a single P-frame has high influence on the video quality and the level of its degradation depends on the relative position of the lost P-frame within the transmitted GOP sequence: higher quality degradation is measured for P-frames losses located closer to the beginning of the GOP.

Following such observation, the importance of P-frames P_{imp} is defined ranging linearly from I_{imp} to B_{imp}, where I_{imp} is the importance level of I-frames and B_{imp} is the importance level of B-frames with $I_{imp} \geq P_{imp} \geq B_{imp}$. Indeed, the loss of P1 (which follows immediately after the reference I-frame) leads to almost the same drop in PSNR as the loss of the I-frame, while the loss of P9 which is transmitted right before the last pair of B-frames leads to PSNR loss comparable with those caused by B-frame losses. The bold line presented in Figure 2 is obtained by curve fitting with the first order polynomial RSM model for PSNR values achieved for different P-frames lost. The obtained R-square equal to 0.97 shows good match between the experimental data and the proposed linear model and, as a result, for the chosen P-frame packet importance.

2.3. Packet Importance Metric in VoIP Flows. A large variety of Voice-over-IP (VoIP) encoders are available, representing different tradeoffs between quality and bandwidth consumption. Encoders can be either sample based (e.g., G.711) or frame based (e.g., G.729), periodically coding individual speech samples or grouping a certain number of samples within a time window, respectively. VoIP speech payload is typically encapsulated into RTP/UDP/IP packets.

At the receiver side, speech frames are demultiplexed and inserted into a playout buffer. The playout buffer plays an important role in perceived speech quality, since it enforces speech frames delivery at the same interval at which they are generated by the encoder. This is done through reordering, delaying or even dropping the frames which arrive later than their expected playback time. However, whenever the frame is dropped, it causes a relevant decrease of the quality of the voice stream.

Based on the above, initially, equal packet importance (i.e., "initial packet importance") is associated to all transmitted speech frames. However, in case the receiver detects frame losses after out-of-order frame reception, it increases importance (and error redundancy) for the subsequent packets of the stream (i.e., increases the "dynamic packet importance"). Summarizing, SARC aims at avoiding bulk frame losses, which are critical for the quality of the speech stream, while single frame losses can be easily compensated or concealed by the decoder.

2.4. Packet Importance Metric in File Transfer. TCP is the most widely used protocol in Internet and it provides a flow of equally-important packets for the user viewpoint. However, depending on the context (e.g., the evolution of the TCP congestion window), packet losses can severely decrease the data transfer performance.

The proposed SARC scheme dynamically adapts the level of HARQ protection used on the radio link based on the value of the TCP congestion window computed at the receiver node.

The core idea is to provide higher protection on the radio link (and more retransmission attempts) when congestion window is small and lower protection for high window values. Indeed, when congestion window is small, any link error will trigger window reduction to its half-unnecessarily reducing the throughput of the TCP flow. In the opposite case, the impact of link errors becomes less significant, since the window will be possibly reduced due to congestion-related losses.

Figure 3 presents congestion window evolution in TCP New Reno $f(w)$ and the corresponding proposed variation of the packet importance metric $\mathrm{Imp}(w)$. Specifically, the proposed approach assigns the highest importance ("High Imp") to TCP segments produced right after each window reduction and decreases it down to the "Low Imp" threshold following linear or any other monotonically decreasing function and defined as follows:

$$\mathrm{Imp}(w) = \begin{cases} -f(w) \cdot k & \text{if linear,} \\ -f^2(w) \cdot m & \text{if quadratic,} \end{cases} \quad (1)$$

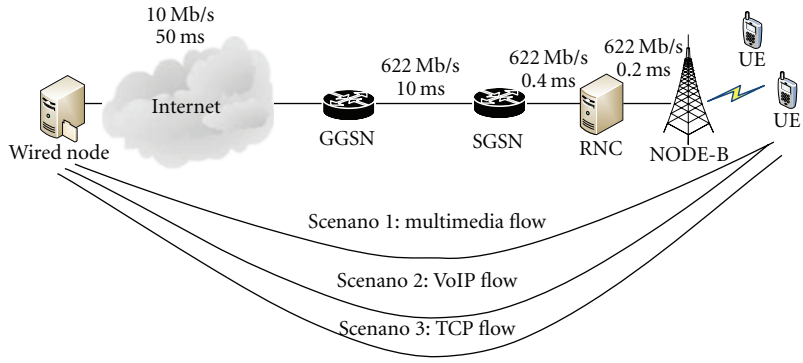

Figure 4: Simulation scenario used for ns-2 experiments.

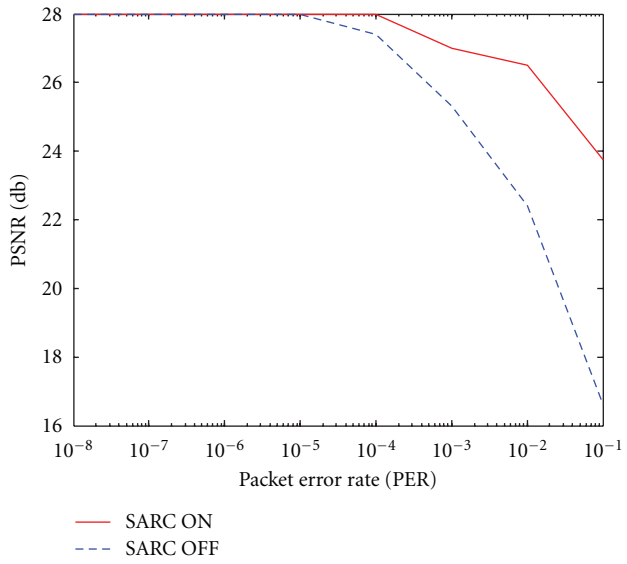

Figure 5: Quality of "Foreman" video clip for different error rates.

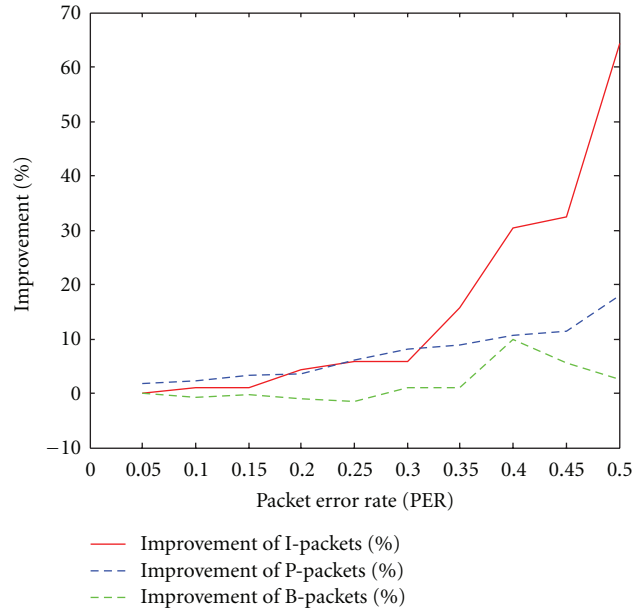

Figure 6: Percentage of improvement in corretly delivered I-, P-, and B- packets against PER.

where

$$k = \frac{\left|\mathrm{Imp}_{\max} - \mathrm{Imp}_{\min}\right|}{|W_{\max} - W_{\min}|}, \qquad m = \frac{k^2}{\mathrm{Imp}_{\min}}. \tag{2}$$

In summary, SARC provides higher protection for low congestion window values or flow sending rates. This reduces the probability of packet losses due to link errors on the wireless channel, which is a well-known reason for TCP performance degradation [17].

3. Performance Evaluation

3.1. Simulation Scenario. The proposed scheme is evaluated in the context of an UMTS/HSDPA cellular network. Network Simulator 2 (NS-2) [18] is used to perform experiments, with the additional Enhanced UMTS Radio Access Network Extensions (EURANE) module [19] for HSDPA implementation.

Figure 4 illustrates the reference scenario and the main parameters employed in the experiments. All considered flows originate from a server (the Fixed Host—FH) on the Internet and are delivered to the User Equipment (UE) located in a 3G cellular network. SARC approach is implemented between the Node-B and the UE.

3.2. Video Transfer Performance. In the first scenario, the FH is a video server which transmits video streams to the video receiver located at UE. Results are presented for the "Foreman" video sequence, using MPEG-4 (open-source ffmpeg [20]) video coding. The video format is Quarter Common Intermediate Format (QCIF, 176 ∗ 144). The GOP structure is IBBPBBPBBPBBPB. Stored in YUV format, the video clip is processed by MPEG-4 encoder which generates the encoded video stream.

The Video Sender (VS) reads the encoded video stream and generates the trace file containing information related

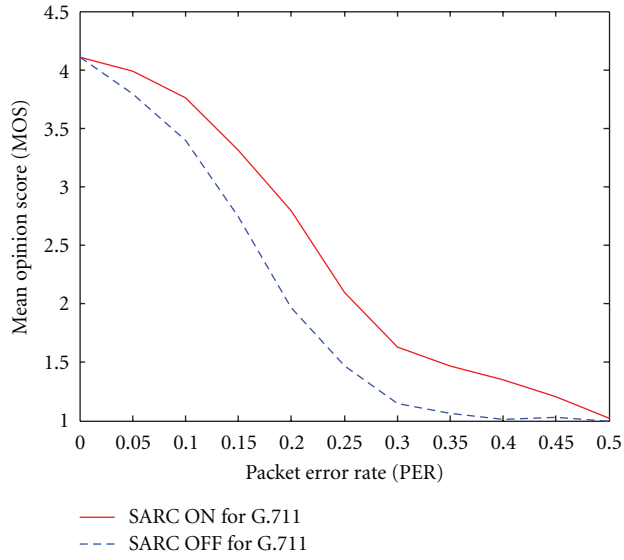

Figure 7: G.711 Voice MOS against Packet Error Rate.

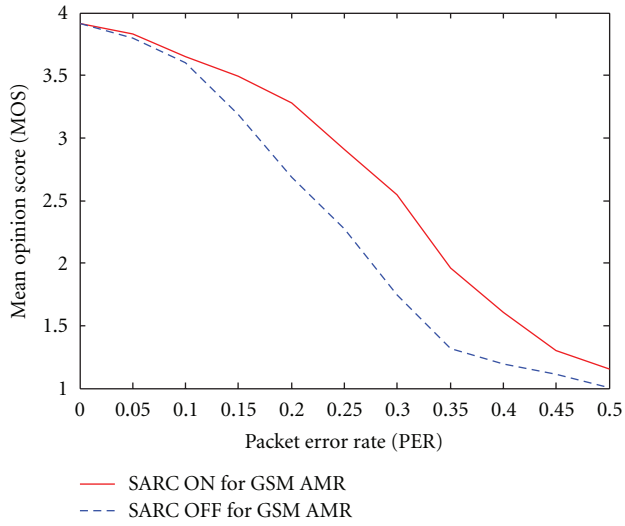

Figure 8: GSM AMR MOS against Packet Error Rate.

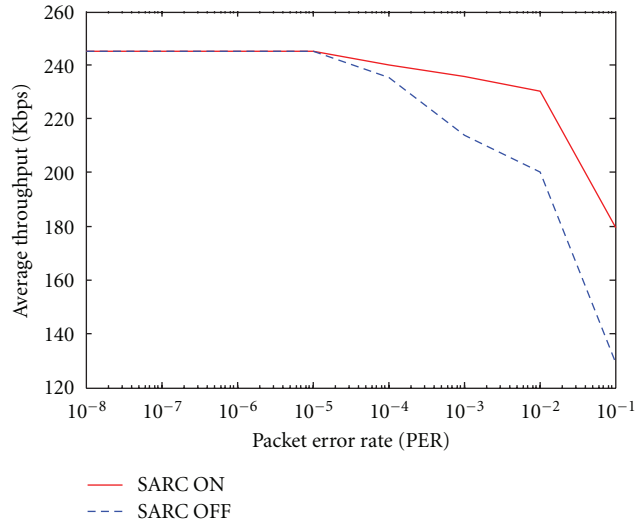

Figure 9: Average TCP Throughput as a function of Packet Error Rate on the wireless channel.

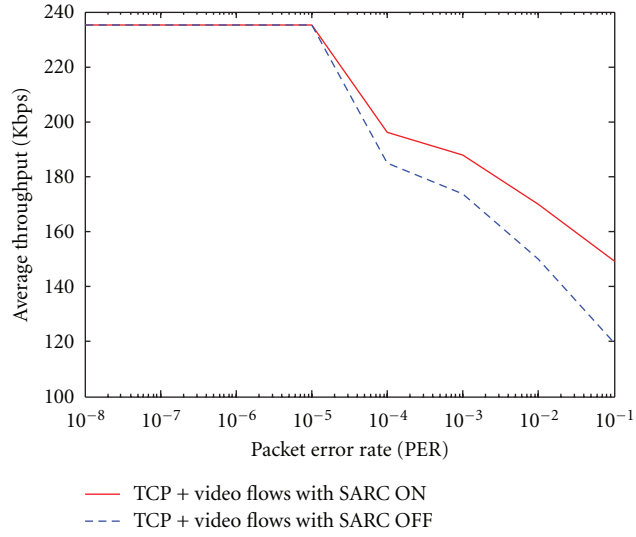

Figure 10: Average TCP Throughput against Packet Error Rate in presence of video flows.

to frame type, size, and so forth, for each video frame. Based on this trace file, the NS-2 streaming server application generates the data—which is encapsulated at all the protocol layers and sent over the network.

The effect of streaming video over the network is captured in the streaming client log file generated by NS-2. It contains timestamp, size, and ID for each transmitted and received packet. The trace file and the log files are used by the Evaluate Trace (ET) program to generate an output corresponding to the result of video file transmission over the error prone network. In order to examine the video quality obtained at the receiver, the original video file and the one obtained after transmission over the network are compared using PSNR calculation module. The employed simulation methodology was proposed and developed within the framework of EvalVid [21], enhanced as in [22] for including NS-2.

The portion of the multimedia stream which is crucial to the overall quality is retransmitted by SARC with a higher HARQ strength; that is, packets belonging to an I-frame are retransmitted with HARQ Strength = 8, while packets belonging to B-frames are retransmitted with a HARQ strength = 2. P-frames are retransmitted with a variable HARQ strength ranging from 8 to 3 depending on the position of the frame in the GOP. Default value of HARQ strength is set to 4 for all packets in the legacy scenario (i.e., without SARC).

Achieved results are illustrated in Figure 5, where SARC increases the range of packet error tolerance to 10^{-2}-10^{-1}. The detailed behavior of the proposed scheme with respect

to the legacy approach is described in Figures 6 and 7 where it is possible to clearly identify the unequal and dynamic protection implemented by SARC on I- and P-frames.

3.3. VoIP Transfer Performance. Experiments on VoIP flows are performed using the simulation model presented in [23]. The sender and the receiver side are separately modeled. The sender includes a customizable codec, which generates generic speech frames (the latter being either voice samples of voice frames, depending on the codec) and a multiplexer, which aggregates several speech frames into one payload. The most common codecs employed in network simulation (e.g., G.711, GSM.AMR) are supported by the VoIPSender, while others can be easily added.

Initially, an HARQ strength equal to 3 is associated to all transmitted speech frames. However, in case the receiver detects frame losses after out-of-order frame reception, it increases HARQ strength linearly for the subsequent packets of the stream (with HARQ strength max equal to 8) in order to avoid bulk frame losses. Once no loss is detected, SARC decreases the HARQ strength to the initial value.

Achieved results (Figures 7 and 8) demonstrate that SARC is able to provide a relevant improvement in terms of MOS both for G.711 and GSM AMR speech flows. In average, application of SARC scheme enables the codec to deliver the same speech quality for error rate of 5% higher if compared with the case when SARC is not enabled.

3.4. File Transfer Performance. In this scenario, a TCP sender located at FH connects to the receiver implemented at UE. For the entire duration of the flow, the receiver maintains up-to-date value of the congestion window (cwnd) computed by counting the number of packets received during the current RTT. Whenever the loss detection signal (three duplicate acknowledgements) is sent to the sender, packet importance is increased according to the function presented in Section 2—introducing higher HARQ protection and, as a result, producing higher resistance to the link errors.

Figure 9 presents TCP throughput achieved by the flows for different PERs of the wireless link. As expected, higher protection against the link errors for low congestion values of the congestion window brings evident performance improvement and underlines advantages of dynamic error protection techniques based on application awareness introduced by SARC.

Figure 10 analyzes a scenario where both video and data flows are delivered on the wireless link. In this scenario, two UEs are considered: one is receiving a video stream, while the other is receiving data via FTP. The same parameters are used as in the previous scenarios. It is possible to observe that while video performance remains as in Figure 5, data transfer is affected by relatively lower protection—while still achieving better results than in the legacy scenario (without SARC).

4. Conclusions and Future Work

This paper proposes a cross-layer approach between application/transport layers on a mobile terminal and link layer on the wireless base station to enable dynamic control on the level of per-packet HARQ protection. The level of protection is dynamically adapted on a per-packet basis and depends on the perceptual importance of different packets as well as on the reception history of the flow. Experimental results demonstrate the potential benefits deriving from the proposed strategy, underlining relevant improvements either for audio and video flows as well as for TCP-based data transfers.

Clearly, further improvement is possible on the building blocks of the proposed scheme, for example by introducing a more precise user quality assessment. However, such aspects are left out of the scope of the paper, as they are well reported and analyzed in the scientific literature.

Future work will be aimed at validating and optimizing the proposed scheme in the framework of embedded multimedia streams.

References

[1] F. Granelli, D. Kliazovich, and N. L. S. da Fonseca, "Performance limitations of IEEE 802.11 networks and potential enhancements," in *Wireless LANs and Bluetooth*, Y. Xiao and Y. Pan, Eds., Nova Science, New York, NY, USA, 2005.

[2] U. Horn, K. Stuhlmüller, M. Link, and B. Girod, "Robust internet video transmission based on scalable coding and unequal error protection," *Signal Processing: Image Communication*, vol. 15, no. 1, pp. 77–94, 1999.

[3] Z. Wu, A. Bilgin, and M. W. Marcellin, "Unequal error protection for transmission of JPEG2000 codestreams over noisy channels," in *Proceedings of the International Conference on Image Processing (ICIP '02)*, pp. 213–216, September 2002.

[4] M. van der Schaar and H. Radha, "Unequal packet loss resilience for fine-granular-scalability video," *IEEE Transactions on Multimedia*, vol. 3, no. 4, pp. 381–394, 2001.

[5] X. K. Yang, C. Zhu, Z. G. Li, G. N. Feng, S. Wu, and N. Ling, "A degressive error protection algorithm for MPEG-4 FGS video streaming," in *Proceedings of the International Conference on Image Processing (ICIP '02)*, pp. 737–740, Rochester, NY, USA, September 2002.

[6] Q. Zhang, W. Zhu, and Y.-Q. Zhang, "Network-adaptive scalable video streaming over 3G wireless network," in *Proceedings of IEEE International Conference on Image Processing (ICIP '01)*, pp. 579–582, October 2001.

[7] Z. Miao, "Rate-distortion optimized streaming of packetized media," *IEEE Transactions on Multimedia*, vol. 8, no. 2, pp. 390–404, 2006.

[8] G. Cheung, W.-T. Tan, and T. Yoshimura, "Rate-distortion optimized application-level retransmission using streaming agent for video streaming over 3G wireless network," in *Proceedings of the International Conference on Image Processing (ICIP '02)*, pp. 529–532, September 2002.

[9] F. Yang, Q. Zhang, W. Zhu, and Y.-Q. Zhang, "Bit allocation for scalable video streaming over mobile wireless internet," in *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, pp. 2142–2151, March 2004.

[10] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 756–769, 1997.

[11] G. Liebl, H. Jenkac, T. Stockhammer, and C. Buchner, "Radio Link Buffer Management and Scheduling for Video Streaming over Wireless Shared Channels," in *Proceedings of the International Packet Video Workshop*, December 2004.

[12] Q. Zhang, W. Zhu, and Y.-Q. Zhang, "QoS-adaptive resource allocation for video transmission over 3G wireless network," *IEEE Transactions on Circuit and System for Video Technology*, vol. 14, no. 8, pp. 1049–1063, 2004.

[13] D. Chase, "Code combining—a maximum-likelihood decoding approach for combining an arbitrary number of noisy packets," *IEEE Transactions on Communications*, vol. 33, no. 5, pp. 385–393, 1985.

[14] P. J. A. Gutíerrez, *Packet scheduling and quality of service in HSDPA*, Ph.D. dissertation, Aalborg University, October 2003.

[15] C. Hoene, B. Rathke, and A. Wolisz, "On the importance of a VoIP packet," in *Proceedings of ISCA Tutorial and Research Workshop on th Auditory Quality of Systems*, Herne, Germany, April 2003.

[16] VLC media player, http://www.videolan.org/vlc/.

[17] H. Lim, K. Xu, and M. Gerla, "TCP performance over multipath routing in mobile ad hoc networks," in *Proceedings of the International Conference on Communications (ICC '03)*, vol. 2, pp. 1064–1068, May 2003.

[18] NS-2 simulator tool, http://www.isi.edu/nsnam/ns/.

[19] "Enhanced UMTS Radio Access Extensions," http://www.ti-wmc.nl/eurane/.

[20] "FFmpeg multimedia system," http://ffmpeg.mplayerhq.hu/.

[21] J. Klaue, B. Rathke, and A. Wolisz, "EvalVid–a framework for video transmission and quality evaluation," in *Proceedings of the 13th International Conference on Modeling, Techniques and Tools for Computer Performance Evaluation*, Urbana, Ill, USA, 2003.

[22] C.-H. Ke, C.-H. Lin, C.-K. Shieh, and W.-S. Hwang, "A novel realistic simulation tool for video transmission over wireless network," in *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06)*, pp. 275–281, Taichung, Taiwan, June 2006.

[23] A. Bacioccola, C. Cicconetti, and G. Stea, "User-level performance evaluation of VoIP using ns-2," in *Proceedings of the Workshop on Network Simulation Tools (NSTools '07)*, Nantes, France, October 2007.

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 209617, 7 pages
doi:10.1155/2010/209617

Research Article

Crafting a Real-Time Information Aggregator for Mobile Messaging

Jenq-Shiou Leu

Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan

Correspondence should be addressed to Jenq-Shiou Leu, jsleu@mail.ntust.edu.tw

Received 7 December 2009; Revised 30 July 2010; Accepted 12 August 2010

Academic Editor: Periklis Chatzimisios

Mobile messaging is evolving beyond SMS (Short Message Service) text messaging with the introduction of MMS (Multimedia Messaging Service). In the past, such a scheme is used for peer-to-peer communication. Messages are generally displayed on a cellular phone with a limited-sized screen. However, such a visualizing process is not suitable to broadcast real-time SMS/MMS messages to people in public. To facilitate the instancy and publicity, we develop a real-time information aggregator—Visualizing SMS and MMS Messages System (VSMMS)—to realize the concept by integrating SMS and MMS messaging over GSM/GPRS/UMTS onto a remote display device. The device exhibits messages on a larger display device in public. VSMMS features a revolutionized variation of mass media broadcasting. In this paper, we practically illustrate how to design and implement VSMMS and use a M/M/1 model to conduct a theoretical analysis about the message delay in the system queue. Meanwhile, we make an empirical performance evaluation about the message transmission time over different networks.

1. Introduction

SMS [1] enables mobile subscribers to send and receive instant messages of up to 160 bytes. Some real-time information can be delivered to message receivers by SMS messages from applications, for example, delivering system failure information to the administrators [2], monitoring remote data [3]. SMS also supports many interdisciplinary applications, like Classroom Feedback Systems (CFSs) [4] to raise large-class interactivity among teachers and students. It has exploded in popularity with cell phones and other communications devices that support text messaging. A general SMS messaging system architecture includes a Short Message Service Center (SMSC), a SMS broker, and a content provider [5]. Compared with SMS, MMS [6] provides a richer message service within images, audio, text, video clips, and combinations of these. However, the screen size of cellular phone on which messages are shown is very limited. Therefore, a comprehensive displaying mechanism can enrich the visualization of mobile message communications.

Based on the above, we combined the Java Web Service, Java Secure Socket Extension, and Java Swing [7] to develop the VSMMS on a larger display device such as PDP within a computer. Additionally, the system contains an optional interface of previewing all incoming messages by an administrator to prevent the device from displaying improper contents in public. This system can be applied to broadcast instant information sent from cellular phones onto the display device.

The rest of this paper is organized as follows. Section 2 depicts the system architecture of VSMMS and how to implement such a system, including the process flow and related system components. Section 3 presents system service analyses. Section 4 shows the comparisons between the modern messaging communication systems and VSMMS as well as some potential applications of VSMMS. Concluding remarks are finally drawn in Section 5.

2. Architecture Design and Implementation

2.1. System Components. VSMMS is composed of four modules as follows and the system architecture is shown in Figure 1:

(1) SMS/MMS Messages Receiver,

(2) Message Queue,

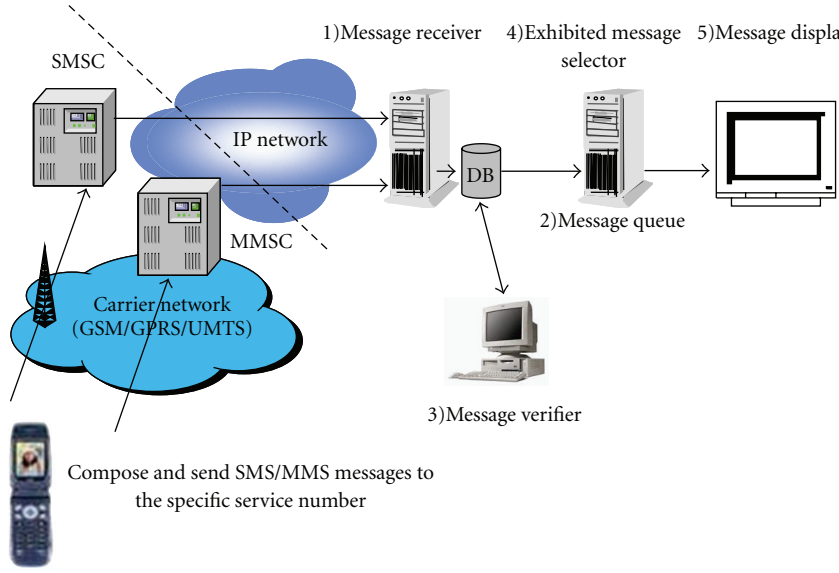

Figure 1: VSMMS system architecture.

(3) Message Verifier (Optional),

(4) Message Displayer,

(5) Exhibited Message Selector.

2.2. Processing Flow. Figure 2 describes the message processing logic flow.

(1) SMS messages and MMS messages are composed and sent by mobile handsets and then delivered to SMSC and MMSC, respectively.

(2) These incoming messages are forwarded to "Message Receiver" first and stored in the unverified message queue.

(3) After the administrator preview by using "Message Verifier" and then designate these messages to be approved or disapproved for display.

(4) "Exhibited Message Selector" then selects the candidate messages for "Message Displayer" to display based on different algorithms and applications.

2.3. Detailed Descriptions for System Component

2.3.1. SMS/MMS Message Receiver. This module is responsible for receiving all incoming messages from GSM and GPRS/UMTS networks. Two significant submodules—SMS Message Receiver and MMS Message Receiver, connect to SMSC and MMSC, respectively, to receive incoming messages. The former one links up with SMSC (SMS Centre) via SMPP [8] over IP. The latter one communicates with MMSC (MMS Centre) via MM7 interface [9] over SOAP/HTTP/IP. Detailed protocol stacks are illustrated in Figure 3. All messages targeting at the specific service ID are conveyed from SMSC/MMSC to such a receiver and put into the message queue to be further processed.

2.3.2. SMS/MMS Message Queue. Message Queue stores all incoming messages. Each entity in the queue contains the generic information listed in Table 1. Such information can provide necessary parameters to the latter Exhibited Message Selector on a selection basis, for example, "MessageType", "CreatedTime", and "LastDisplayedTime" according to different scheduling mechanisms.

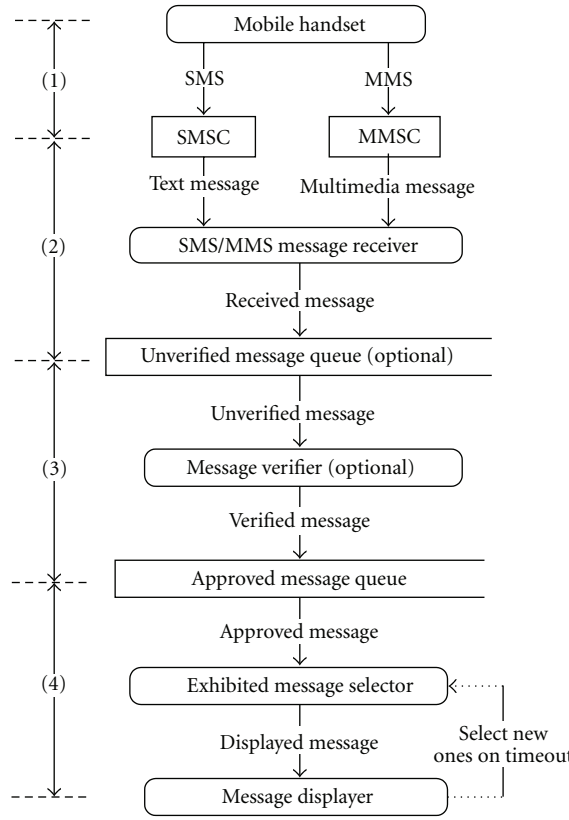

Figure 2: Message Processing Logic Flow.

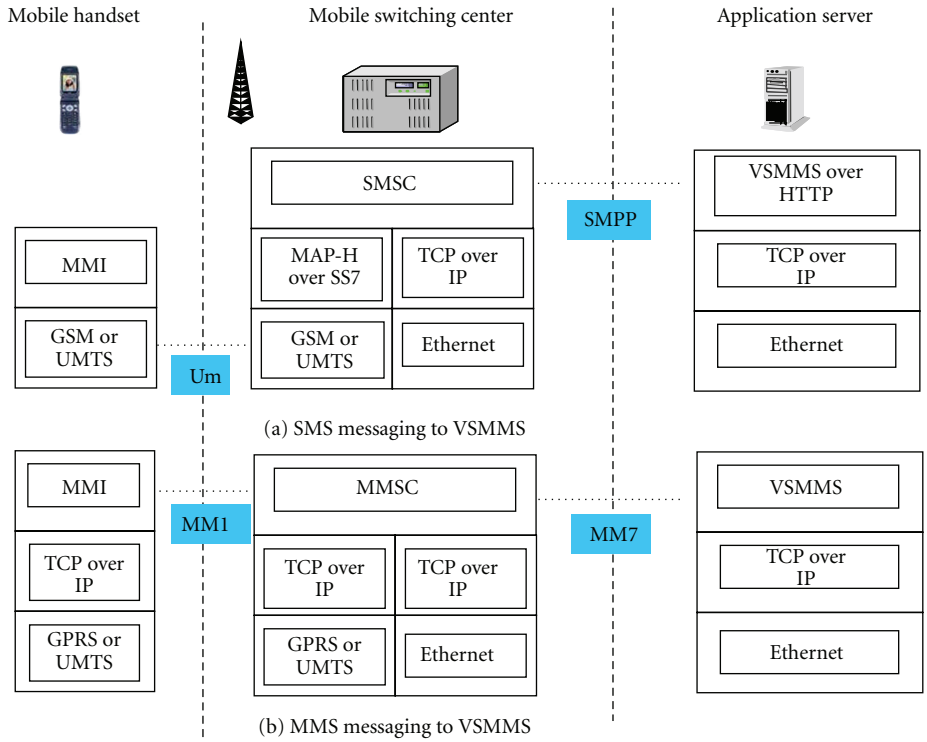

Figure 3: SMS/MMS messaging to VSMMS protocol stack.

Table 1: Attributes of messages.

Attributes	Description
ID	Message entity ID
Message ID	SMS/MMS message ID
CreatedTime	message created time
Priority*	Selected to be exhibited priority
MSISDN	Sender's phone number
Text	Text part in message
Image	Image part in message
MessageType	What type the message is
LastExhibitedTime	Last exhibited time
Flag**	Verification state

*For priority driven selection.
**If the message does not need to be verified before exhibited, the "Flag" for messages in the queue is set to be "Approved" by default.

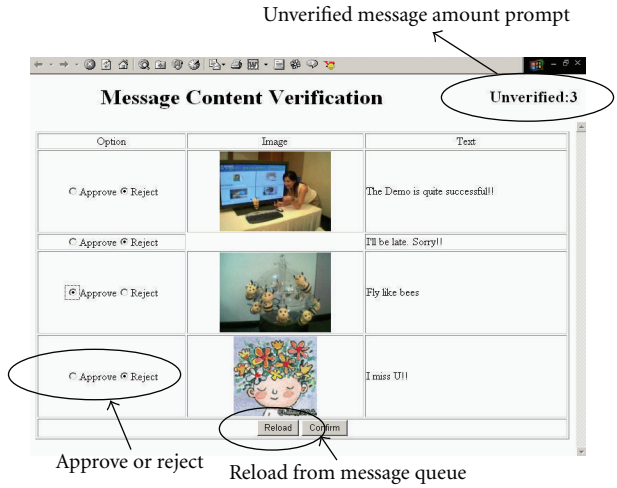

Figure 4: An optional web-based interface to preview message contents.

2.3.3. Message Verifier (Optional). Since the service ID is opened for all users, a simple mechanism to administer contents in messages can avoid displaying improper contents from malicious senders. An authorized checker can utilize Message Verifier to verify all incoming messages via a web-based interface. After finding out thatthere exist some unverified messages in the system, the checker can examine all constituents in each message, including the text description or media content, to decide which message can be approved or disapproved to publish. By selecting the "Approve" or "Disapprove" radio button as shown in Figure 4, all verified messages can be submitted to the system for displaying.

2.3.4. Exhibited Message Selector. Exhibited Message Selector performs a selection among approved messages for Message Displayer. Each region in the layout of Message Displayer has an independent message assigned by Exhibited Message Selector. Such a component can be implemented by different scheduling algorithms, such as First-Come-First-Served (FCFS), Round-Robin manner, or priority-driven manner by referring to necessary fields, such as "CreatedTime" and "Priority". In order to conduct a selection with fairness for all approved messages for exhibition, we exploit a hybrid

```
// Select K messages in the approved message queue as
requested

(1) Count all fresh messages, which are not yet exhibited,
    (with NULL value in "LastExhibitedTime" field) and set
    such the said count to N

(2) If N > K
    Then
      2.1 Designate the preceding K messages among these N
    messages by referring to "CreatedTime" as selected ones
    Else
      2.2 Designate these N messages as selected ones
      2.3 Designate the preceding K-N messages among old
messages (with non-NULL value in "LastExhistedTime"
field) by referring to "LastExhibitedTime" as selected ones
    End IF

(3) Update "LastExhibitedTime" values for these K
    .messages as the current time

(4) Return these K messages IDs
```

Algorithm 1: Algorithm of FCFS-based selection with LRU re-exhibition.

way of the FCFS mechanism for fresh messages and Least Recent Used (LRU) mechanism for old messages by referring to "LastExhibitedTime" as an aging factor for re-exhibition. The detailed scheme is depicted in Algorithm 1.

2.3.5. Message Displayer. This module is used to exhibit approved message contents, which are selected by Exhibited Message Selector, in the Approved Message Queue. The physical layout may depend on different applications and comprise several independent regions. Figure 5 illustrates a sample display layout. The top area is a marquee, which exhibits text message contents. The bottom area consists of four regions. MMS message contents are displayed concurrently in these four regions which include an image part and a text one accordingly. These regions can have their own display durations determined by Message Displayer. Additionally, these independent regions always ask for a new message content to display toward Exhibited Message Selector when the corresponding display durations are expired. Figure 6 shows VSMMS implemented on a computer-embedded PDP.

3. System Service Analysis

3.1. Message Delay Analysis. We analyze the message delay in the message queue of VSMMS by a M/M/1 queuing conceptual model shown in Figure 7. The assumptions and parameters exploited in the model are illustrated below.

(1) The new SMS and MMS message arrival into the approved message queue of VSMMS SMS/MMS are Poisson distributions with rates λ_{SMS} and λ_{MMS}, respectively. The total message arrival rate is $\lambda = \lambda_{SMS} + \lambda_{MMS}$.

(2) The exhibition time of a message is assumed to be exponentially distributed with mean $1/\mu$. All stored messages are displayed according to FIFO scheduling.

(3) The message queue in VSMMS is a finite storage with a capacity of M messages.

Performance analysis of the VSMMS message queue can be induced by describing the queue as a Markov chain. Figure 8 shows the transitions among different states where the state i indicates that there are i messages in the queue.

Let P_i denote the steady-state probability of being in the state i. Using balance equations, we can get the following result:

$$P_i = \prod_{j=1}^{i} \left(\frac{\lambda}{\mu}\right) P_0 = P_0 \left(\frac{\lambda}{\mu}\right)^i, \quad 1 \le i \le M+1, \tag{1}$$

where P_0 can be as $\sum_{i=0}^{M+1} P_i = 1$.

Let a_i denotes the probability of having i messages in the queue just before a message arrives and gets accepted by the VSMMS. Such a message never sees the queue in the state $M+1$, that is, blocking state. a_i can be shown by the following result [10, 11].

$$a_i = \frac{P_i}{1 - P_{M+1}}. \tag{2}$$

The message delay (W) is defined as the time between the acceptance of a message in VSMMS and the time the message starts to be transmitted. Two notations $F_z(t)$ and $f_z(t)$ are used for the following analyses. $F_z(t)$ and $f_z(t)$ denote the distribution and density function of a random variable z, where

$$f_z(t) = \frac{d}{dx} F_z(t). \tag{3}$$

Figure 5: Layout of message displayer.

Figure 6: VSMMS on a computer-embedded PDP.

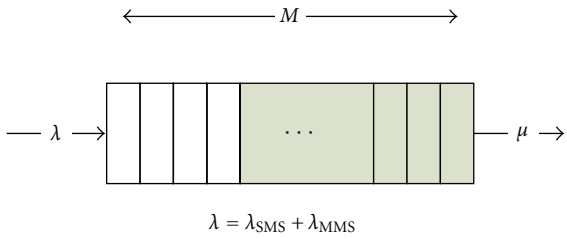

Figure 7: A queuing model for the VSMMS message queue.

Assume that a message arrives to the queue when there are i messages in the queue (i.e., the queue is in the state i). Let m_i denote this message. If $1 \le i \le M+1$, then m_i is accepted and the queue state would change into $i+1$. If $i = 0$, then m_i would be immediately processed, otherwise it must wait in the queue till the i message has been processed. Suppose the queue is consisted of these i messages which are ahead of m_i at some moment. Let t_i denote the time required for the message population to decrease from i to $i-1$ $(1 \le i \le M)$. Then, t_i is exponentially distributed with the rate parameter μ, and we can obtain

$$f_{t_i}(t) = \mu e^{-\mu t}. \tag{4}$$

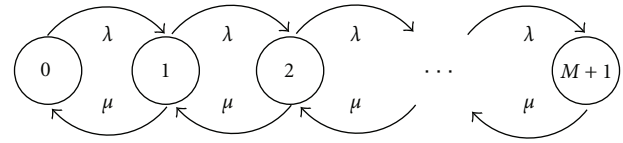

Figure 8: An M/M/1 Markov chain representation for the VSMMS message queue.

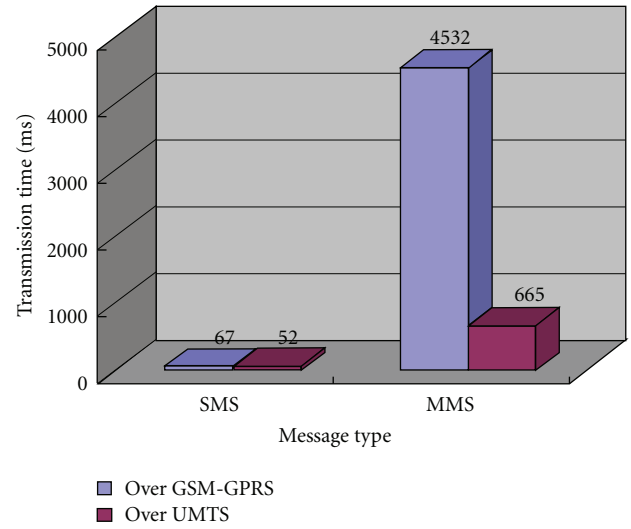

Figure 9: Average transmission time of SMS/MMS messaging over GSM/GPRS/UMTS.

Let T_i denote the message delay of m_i, that is, the amount of time m_i must wait before its transmission starts. Then we can get

$$T_i = t_1 + t_2 + \cdots + t_i = T_{i-1} + t_i, \quad \text{for } i \ge 1,\ T_0 = 0. \tag{5}$$

The mean message delay is therefore given by

$$E[T_i] = \sum_{j=1}^{i} E\left[t_j\right] = \sum_{j=1}^{i} \frac{1}{\mu} = \frac{i}{\mu}. \tag{6}$$

3.2. Transmission Time Analysis. VSMMS offers an instant way to gather and broadcast instant messages from anywhere under cellular network coverage, for example, 53.6 kbps over GPRS or 384 kbps over UMTS for a limited radio resource. The consumed time of message transmission may be an attractive issue. Normally SMS messages fly over SS7 control channels, the transmission time for SMS messages is far below the one consumed by transmitting MMS messages. (Figure 9 shows the average transmission time of SMS/MMS messaging over GSM/GPRS/UMTS while delivering 102-byte SMS messages and 24-kbyte MMS message to VSMMS.) Hence, the focusing scenario is to compose and deliver MMS messages to VSMMS. The consumed time for such a scenario is shown by

$$\left(\frac{\text{Size}_{\text{MMS}}}{\text{TR}_{\text{GPRS/UMTS}_{\text{UL}}}} + \frac{\text{Size}_{\text{MMS}}}{\text{TR}_{\text{GPRS/UMTS\_DL}}}\right) \times 8 \text{ seconds}, \tag{7}$$

Table 2: Comparisons of the contemporary messaging communication systems and VSMMS.

	Mobile messaging system	VSMMS	Digital broadcasting system
Communication model	1 to 1	1 to Many in One Centralized Receiver	1 to Many with scattered receivers
Mobility for message creator	High	High	Low
Immediateness of message delivery	High	High	Low
Scale for message receiving	Small	Medium	Large
Carrier network	Cellular network (GSM/GPRS/UMTS)	Cellular network (can be easily extended to any all-IP networks)	Broadcasting network (DAB/DVB)
Message capacity	Low (limited by handset form factor)	High (System-based, extendable)	High (System-based, extendable)

where Size_{MMS} denotes the MMS message size in kbyte; $\text{TR}_{\text{GPRS/UMTS\_DL}}$ and $\text{TR}_{\text{GPRS/UMTS\_UL}}$ denote GRPS/UMTS transmission rates in kbits per second for the downlink and uplink, respectively.

For example, the size of an MMS message is 26.8 kbytes and the GPRS transmission rate is 53.6 kbps. The total consumed time from posting to being received by VSMMS is 4∼5 seconds.

4. Analytical Comparison and Potential Applications

Compared to modern messaging communication systems, such as Mobile Messaging System and Digital Broadcasting System [12], VSMMS features one-to-many medium-sized broadcasting on a centralized display device with high mobility and instancy support via cellular networks. Furthermore, VSMMS can be easily extended and adapted to the future all-IP networks. The major differences between the contemporary messaging communication systems and VSMMS are depicted in Table 2.

VSMMS can be one of the following variations but not limited.

4.1. Real-Time Traffic Information Sharing. Traffic jam is getting worse for lack of real-time traffic information. Drivers can use MMS-enabled handsets within a digital cam to capture and advertise the visible traffic condition in public, instead of only oral reporting.

4.2. Home Appliance within a Family Bulletin Board. A dedicated channel in a traditional TV allocated for unfolding SMS/MMS messages enables people to communicate with one another like a family bulletin board.

4.3. Dynamic Poster Framework. To substitute for the traditional public bulletin board, a multimedia display terminal with wireless instead of wired communication capability enables the flexibility of dynamic advertisement or announcement in a public area, especially for location-oriented affairs like community information, weather information.

4.4. Real-Time Visualization for Televoting Statistics. Televoting service can establish direct connections with radio-stations listeners, TV viewers, and readers of newspapers and magazines. Such a visualization process can make mobile voting mechanism more evident.

5. Conclusion

The prototype system presented in this paper has been successfully implemented and demonstrated. We have realized an extended idea to visualize instant SMS/MMS messages openly on a larger device, instead of a limited-sized screen on personal cellular phones in the past. Such an implementation also improves the traditional peer-to-peer mobile communication. Users compose SMS or MMS messages within real-time information by handset and send them to a specific service ID via SMSC/MMSC. Afterward all incoming messages are processed by VSMMS and shown on a remote display device. VSMMS is suitable to be deployed for real-time information sharing in public. To avoid displaying improper contents in public, the system includes an optional web-based interface to help the administrator verify the incoming contents. VSMMS features a novel messaging communication scheme for mass media broadcasting.

References

[1] 3GPP TS 23.040, "Technical realization of the short message service (SMS), release 5," v5.2.0, 2001.

[2] M. Ghasemzadeh and V. A. Foroushani, "Remote management of computer networks by short message service," in *Proceedings of the International Conference on Computer and Communication Engineering (ICCCE '08)*, pp. 300–305, May 2008.

[3] H. Yan and H. Pan, "Remote data monitoring system design based on GSM short message service," in *Proceedings of IEEE International Symposium on Industrial Electronics*, pp. 364–367, 2009.

[4] E. Scornavacca, S. Huff, and S. Marshall, "Mobile phones in the classroom: if you can't beat them, join them," *Communications of the ACM*, vol. 52, no. 4, pp. 142–146, 2009.

[5] J. Brown, B. Shipman, and R. Vetter, "SMS: the short message service," *Computer*, vol. 40, no. 12, pp. 106–110, 2007.

[6] 3GPP TS 22.140, "Multimedia messaging service (MMS); stage 1; release 6," v6.6.0, June 2004.

[7] For Java Developers, 2010, http://www.oracle.com/technetwork/java/index.html.
[8] SMPP Forum, "Short Message Peer-to-Peer Protocol Specification v5.0," 2010, http://www.smsforum.net/.
[9] 3GPP TS 23.140, "Multimedia messaging service (MMS); functional description; stage 2; release 6," v6.6.0, June 2004.
[10] D. Gross, et al., *Fundamentals of Queueing Theory*, John Wiley & Sons, New York, NY, USA, 4th edition, 2008.
[11] M. Ghaderi and S. Keshav, "Multimedia messaging service: system description and performance analysis," in *Proceedings of the 1st International Conference on Wireless Internet (WICON '05)*, pp. 198–205, July 2005.
[12] ETSI and EN 300 744, "Digital video broadcasting (DVB): framing structure, channel coding and modulation for digital terrestrial television," vol. 1.5.1, pp. 9–39, November 2004.

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 524854, 11 pages
doi:10.1155/2010/524854

Research Article

Optimized Hybrid Resource Allocation in Wireless Cellular Networks with and without Channel Reassignment

Xin Wu, Arunita Jaekel, Ataul Bari, and Alioune Ngom

School of Computer Science, University of Windsor, 401 Sunset Avenue, Windsor, ON, Canada N9B 3P4

Correspondence should be addressed to Ataul Bari, bari1@uwindsor.ca

Received 14 February 2010; Revised 23 July 2010; Accepted 26 July 2010

Academic Editor: Fabrizio Granelli

In cellular networks, it is important to determine an optimal channel assignment scheme so that the available channels, which are considered as "limited" resources in cellular networks, are used as efficiently as possible. The objective of the channel assignment scheme is to minimize the *call-blocking* and the *call-dropping* probabilities. In this paper, we present two efficient integer linear programming (ILP) formulations, for *optimally* allocating a channel (from a pool of available channels) to an incoming call such that both "hard" and "soft" constraints are satisfied. Our first formulation, ILP1, does not allow channel reassignment of the existing calls, while our second formulation, ILP2, allows such reassignment. Both formulations can handle hard constraints, which includes *co-site* and *adjacent channel* constraints, in addition to the standard *co-channel* constraints. The simplified problem (with only co-channel constraints) can be treated as a special case of our formulation. In addition to the hard constraints, we also consider soft constraints, such as, the *packing condition, resonance condition,* and *limiting rearrangements*, to further improve the network performance. We present the simulation results on a benchmark 49 cell environment with 70 channels that validate the performance of our approach.

1. Introduction

In recent years, there has been a great development in the field of the cellular networks due to the tremendous growth in the demand of mobile wireless communication services. The cellular principle partitions a geographical area into *cells* where each cell has a *base station* and a number of *mobile terminals* (e.g., mobile phone). The base station is equipped with radio transmission and reception equipment. A group of base stations are connected to the *Mobile Switching Center* (MSC). The MSC connects the cellular network to other wired or wireless networks. The base station is responsible for the communication between a mobile terminal and the rest of the information network. A typical cellular system architecture is illustrated in Figure 1.

In order to start a communication with a base station, a mobile terminal must obtain a *channel* from the base station. A channel consists of a pair of frequencies: one frequency (the *down-link*) for transmission from the base station to the mobile terminal, and another frequency (the *up-link*) for the transmission in the reverse direction. The *channel assignment problem* deals with assigning an appropriate channel for each communication request that arrives in a cell.

Radio transmission in a channel may cause radio frequency interference in other channels, resulting in the degradation of the signal quality. Therefore, to alleviate the interference between channels, a channel that can be selected to be assigned to a new call must satisfy the following electromagnetic compatibility constraints [1], also referred to as *hard* constraints.

(i) Cochannel constraint (CCC): the same channel cannot be assigned to two cells that are separated by a distance less than a specified minimum *reuse,* (Some relevant terminologies are discussed in Section 2.) , distance, r_0.

(ii) Cosite constraint (CSC): channels in the same cell must be separated by a minimum amount g. That is, their radio frequencies must be far enough apart.

(iii) Adjacent channel constraint (ACC): channels assigned to neighboring cells must be separated by a minimum amount w.

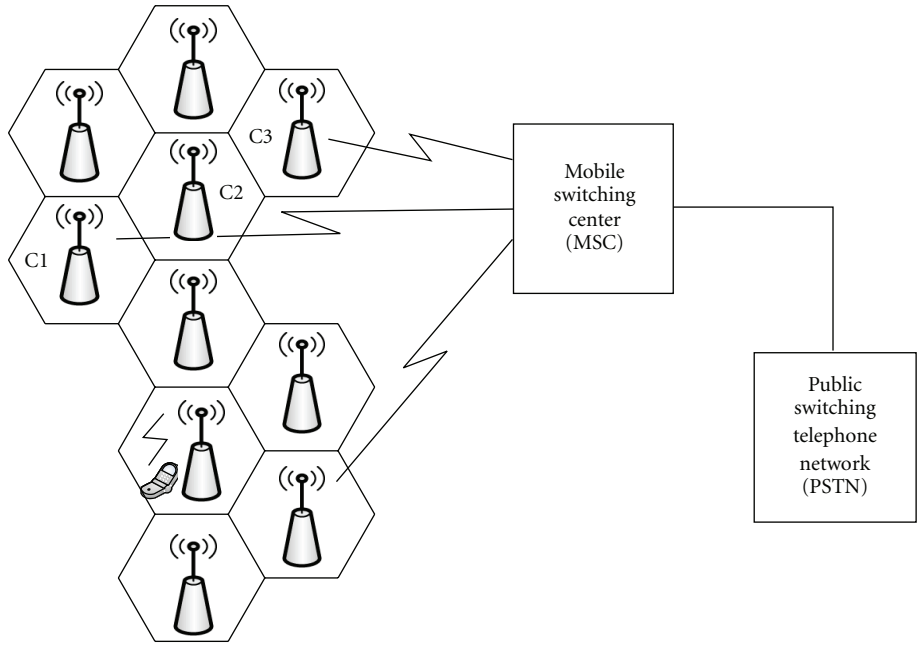

Figure 1: A typical cellular system architecture.

The hard constraints *must* be satisfied for the system to work properly. In addition to the above hard constraints, there are a number of *soft* constraints that can be used to guide the channel assignment process to improve the quality of the solution. However, the soft constraints may be violated if necessary [2]. The soft constraints include the following.

(a) Packing condition: try to use the minimum number of channels every time a call arrives [3]. This condition encourages the selection of channels already in use in other cells as long as the hard constraints are satisfied.

(b) Resonance condition: try to assign the same channels to cells that belong to the same reuse scheme [3]. The purpose of this approach is to leave as many channels as possible to be allocated to other cells belonging to other reuse schemes. Consequently, the probability of causing cochannel interference in the system is reduced.

(c) Limiting rearrangement: try to assign, whenever possible, the same channels assigned before to the existing calls, thus limiting the reassignment of channels. Channel reassignment is the process of transferring an ongoing call to a new channel without call interruption [4]. Such reassignment in the entire cellular network upon the arrival of a new call will obviously result in lower call blocking probability, but it is complex, both in terms of time and computation [3]. Therefore, the reassignment processes should be limited to a low level. On this account, limiting rearrangement condition is used to prevent excessive reassignment in a cell [3].

The packing condition encourages reuse of the channels that are already in use in other cells. The motivation behind this is that the channels that are currently not being used anywhere can be allocated with more flexibility. So, if there is an option between using a channel (say λ_1) that is currently in use in one or more cells, and another channel (say λ_2) that has not been allocated in any cell, the packing condition will promote the use of λ_1 for the current call (assuming no hard constraints are being violated). This leads to increased flexibility, that is, it leaves the more flexible option (i.e., using λ_2) available for any future incoming calls, thus increasing the likelihood that future calls can be accommodated more easily. To see why the packing condition can lead to a lower blocking probability (and hence, to better system performance), we consider a very simple example with three cells (C1, C2, and C3) and two available dynamic channels (λ_1 and λ_2). Suppose the cells are placed one after the other in a straight row (as shown in Figure 1) and the reuse distance $r_0 = 2$, that is, the same channel cannot be used in two adjacent cells, but can be used if there is at least one intervening cell separating the two cells. Assume that there is an ongoing call in C1, which is using channel λ_1. Now a call request arrives in C3. According to the packing condition, it should also use λ_1. If a third request arrives in C2, this can then be accommodated using λ_2. On the other hand, if the packing condition was ignored and the call in the cell C3 was allocated to channel λ_2, then when the third call arrives in C2, it cannot be accommodated using either λ_1 or λ_2, and hence, must be blocked.

The channel assignment schemes proposed in the literature can generally be divided into three categories: fixed channel-assignment (FCA), dynamic channel-assignment (DCA), and hybrid channel-assignment (HCA). In FCA, a fixed number of channels is assigned to each cell beforehand, based on estimated traffic, and in DCA, channels are dynamically allocated based on incoming call and the current network configuration. HCA is a hybrid of both FCA and DCA.

In this paper, we present two *optimal* integer linear programming (ILP) formulations, ILP1 and ILP2, that can be used for the hybrid channel assignment (HCA) problem in wireless cellular networks. The formulation ILP1 does not consider reassignment of existing calls in the cell, while the formulation ILP2 allows such reassignment to further reduce the blocking probability. Our approach can be applied to the dynamic channel assignment (DCA) problem as well. As opposed to the many existing channel assignment schemes [5, 6] that solve a simplified version of the channel assignment problem by addressing the cochannel constraint (CCC) only, our approach not only handles all three hard constraints, but also takes into consideration the soft constraints, mentioned above. In summary, the motivations behind the proposed formulations are as follows.

(1) Although there are many existing schemes for dynamically allocating channels to an incoming call, the vast majority of these only consider the simple cochannel constraint (CCC), but ignore the cosite constraint (CSC) and adjacent channel constraint (ACC) [6–10].

(2) The existing schemes are primarily based on heuristics, with no specified performance bounds. Therefore, it is not easy to analyze the quality of their solutions.

(3) Most existing schemes focus on the standard FCA or DCA techniques and relatively little work has been done on HCA.

In this paper, our objective is to develop novel mathematical formulations (rather than heuristics) capable of generating optimal solutions for HCA. We wanted to develop an approach that jointly considers CCC, CSC and ACC as an integrated part of the channel selection process, rather than simply selecting a channel and then checking if the constraints are satisfied. Since the proposed formulations provide optimal solutions for this complex design problem, these can be used as benchmarks to evaluate existing (or future) heuristics.

An earlier version of this paper appeared in [11]. The remainder of the paper is organized as follows. In Section 2, we review the relevant work on channel assignment schemes for cellular networks. In Section 3, we present our ILP formulations. We discuss our cellular model and experimental results in Sections 4 and 5 and conclude in Section 6.

2. Review

The availability of channels or frequency spectrum is very limited, as compared to the exponential growth of mobile terminals. This requires a method to share these channels for efficient assignment and proper management of channel resources.

As the reuse of channels is inevitable in a cellular system, channels used at one cell site may also be used at other cell sites in the case of absence of cochannel interference. Cochannel interference is the radio interference caused due to the allocation of the same channel to certain pairs of cells with geographical separation not enough to avoid deterioration of signal quality. The minimum distance required between the centers of two cells using the same channel to maintain the desired signal quality is known as the *reuse distance* [3, 6, 12, 13]. Reuse distance determines an interference region marked by gray cells which locate around a given cell x as shown in Figure 2. Figure 3 shows a reuse pattern, with reuse distance equal to three, in which the cells with same number belong to the same reuse scheme and are free from cochannel interference. This reuse scheme is obtained by jumping from one cell to another in steps of length equal to the reuse distance [3, 14, 15]. The longer the reuse distance is, the smaller will be the cochannel interference level. However, a long reuse distance may result in lower reuse efficiency [15]. Thus, the frequency reuse scheme should be determined taking into consideration both the cochannel interference level and the reuse efficiency. Traditionally, channel assignment is made according to the cochannel interference level determined by a fixed reuse distance which is decided during network planning. Many approaches proposed in the literature to solve channel allocation problem are based on such concept [3, 6, 12, 13, 15–17].

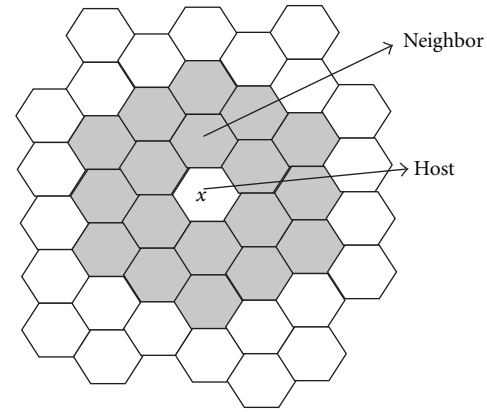

Figure 2: Reuse distance.

The channel assignment problem is the problem of allocating frequencies to mobile terminals and base stations such that the network's capacity, in terms of number of mobile users, is maximal. This is a well-known NP-hard problem [18] and has been widely investigated in the literature. Various channel assignment schemes have been studied widely to find better ways to assign channels to calls and to achieve higher level of channel reuse, which can be broadly classified as FCA, DCA, and HCA schemes.

The FCA schemes [16, 19–22] allocate channels permanently to each cell based on predetermined estimated traffic. FCA scheme is simple but it does not adapt to the changes in traffic conditions. In a cell, a call can be assigned to a channel only if there is a free channel available in the predetermined set for this cell. Otherwise, the call might be rejected, even in some cases when many channels may be available in the network.

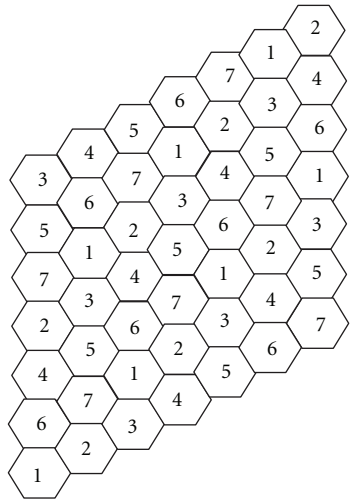

Figure 3: Reuse pattern (reuse distance is 3).

In DCA, there is no permanent allocation of channels to cells. Instead, the whole set of available channels is accessible to all the cells, and the channels are assigned on a call-by-call basis, in a dynamic manner [7–9, 23–26]. Since a cell can use any of the channels in a dynamic way, it is possible that if a cell uses all channels at a given time, then there will be no channel available to its neighboring cells at that time due to the interferences. DCA makes wireless networks more efficient, especially if the traffic load distribution is not known beforehand, or varies with time. The advantage of DCA is the flexibility and the traffic adaptability, since channel assignment is based on the current network conditions. DCA methods have better performance than FCA methods for light to medium traffic load [6]. Most of the proposed DCA algorithms are based on heuristics, and do not guarantee an optimal solution. In addition, many existing DCA schemes consider a simplified problem with only cochannel constraints [7–10, 23–25, 27]. Recently, DCA schemes for multihop wireless communications [28–32] have also been proposed.

In addition to the fact that most DCA techniques use a heuristic approach with possibly suboptimal solutions, the main drawbacks of DCA are as follows.

(i) After a call request arrives, DCA requires some computation since allocation is done based on the "current state" of the network. In FCA the channel allocation is done offline, before the network starts operating, so when a call arrives at a cell k, any of the available channels assigned to the cell can be allocated to the new call immediately, without having to consider how the neighboring cells are being affected. Therefore, FCA is typically faster than DCA.

(ii) In DCA, it is possible for a "greedy" cell to use up too many channels at a given time, so that there are no channels available for the neighboring cells.

HCA [5, 6, 17, 33, 34] combines the features of both FCA and DCA techniques to overcome the drawbacks of FCA and DCA. In HCA, the set of channels is divided into two subsets [6], the Fixed Channels set (or FC set: a set of channels permanently allocated to given cells) and the Dynamic Channels set (or DC set: a set of channels available to all cells). The ratio of the number of channels in each set is fixed a priori by the cellular network designer. For example, the representative ratios, FC : DC, for a set of 70 channels could be 35 : 35, 49 : 21, or 21 : 49 (If FC is empty, then the HCA problem reduces to the classical DCA problem). When a new call arrives in a cell, the system first tries to serve it from the set of fixed channels, FC. If no channel is available in the set of fixed channels FC, then the DCA scheme determines a suitable channel from the set of dynamic channels DC, satisfying the interference constraints and the traffic demands in cells. A channel is selected from the set DC, only if all channels in FC are busy. Therefore, HCA does not require a computation every single time (like DCA) and hence is faster than DCA on average (but not as fast as FCA). In addition, in HCA, a "greedy" cell can use up all the dynamic channels in DC, but it cannot use the fixed channels assigned to its neighboring cells. So, the neighboring cells are not as adversely affected as in the case of DCA.

3. ILP Formulation for Hybrid Channel Assignment

Channel assignment schemes help to increase the network's capacity by efficiently distributing the channels across the network. We assume that each base station in a cellular network has a computer that stores the current state of its cell. The state of the cell includes information about the channels, the mobile elements, and the ongoing calls in the cell. Each base station sends its state to other base stations through a wired network between their computers. Channel assignment is made by the computer of the concerned base station according to the channel usage information stored in the allocation matrix. Let, C be the total number of cells in the network and L be the total number of channels in the network. The allocation matrix A is the binary matrix of size $C \times L$ such that each element of A is defined as

$$a_{i,j} = \begin{cases} 1 & \text{if channel } j \text{ is in use in cell } i, \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

The allocation matrix is updated every time a channel is allocated or released in the network, and each base station receives a copy of the allocation matrix. The total number of channels is divided into two sets: FC and DC. If FC is empty, then the problem reduces to the classical DCA problem.

We solve HCA problem based on reuse distance concept. In this section, we propose two ILP formulations, ILP1 and ILP2, to solve the channel assignment problem, where ILP1 does not allow channel reassignment, but ILP2 allows it. Unlike most existing techniques, we consider all the three hard constraints, that is, cochannel, cosite, and adjacent channel constraints, as well as the soft constraints. Our HCA approach works as follows. When a call arrives in a cell k at time t, we first search for a channel in the FC set that can

serve the call. If no such channel is available from FC, then we apply our ILP formulations on the DC set to obtain a best assignment of channels in cell k. The solution contains channels to be assigned to all ongoing calls in the cell k (ongoing calls maybe reassigned new channels to minimize blocking or dropping of calls, for ILP2) and the channel to be assigned to the new call.

3.1. Notation Used. In our ILP1 and ILP2 formulations, we will use the following symbols to represent input data:

(1) k: cell where a call arrives,

(2) d_k: number of calls in cell k (traffic demand in cell k), including the new call.

(3) r_0: reuse distance,

(4) r_1: minimum distance between cells to avoid adjacent channel interferences,

(5) g: cosite interference channel interval,

(6) w: adjacent site interference channel interval, $g \geq w$,

(7) C: number of cells in the network,

(8) L: total number of channels in the network (including both fixed and dynamic channels),

(9) L_d: number of dynamic channels in the network,

(10) B: set $\{1, 2, \ldots, L_d\}$ of channel numbers for all dynamic channels,

(11) B_f: subset of B, containing the channels currently not in use in cell k,

(12) $\mathcal{K}_i$: subsets of B containing the channels currently in use in cell i, $1 \leq i \leq C$,

(13) W_1, W_2 and W_3: positive constants,

(14) $d_{i,j}$: normalized distance between cell i and cell j, $1 \leq i, j \leq C$,

(15) $res(i, j)$: a function defined as follows:

$$\text{res}(i,j) = \begin{cases} 1 & \text{if cell } i \text{ and cell } j \text{ belong to the} \\ & \text{same reuse scheme,} \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

(16) $a_{i,j}$: an element of a $C \times L$ allocation matrix A, where each element, $a_{i,j}$, is defined as follows:

$$a_{i,j} = \begin{cases} 1 & \text{if channel } j \text{ is in use in cell } i, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

We also define the following binary variables:

$$x_l = \begin{cases} 1 & \text{if channel } l \text{ is selected for the new call} \\ & \text{in cell } k, \quad \forall l \in B_f, \\ 0 & \text{otherwise,} \end{cases} \tag{4}$$

$$y_m = \begin{cases} 1 & \text{if channel } m \in B \text{ is selected for an} \\ & \text{existing call or new call in cell } K, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

3.2. ILP Formulation without Channel Reassignment (ILP1). We now present our first ILP formulation that allocates a free channel to a new call without any reassignment of existing channels. Using the notation given above, we formulate *ILP1* as follows.

Objective Function.

$$\begin{aligned} \text{Minimize} - W_1 \sum_{i=1, i\neq k}^{C} \sum_{l \in B_f} \frac{a_{i,l} \cdot x_l}{d_{i,k}} \\ + W_2 \sum_{i=1, i\neq k}^{C} \sum_{l \in B_f} a_{i,l} \cdot x_l \cdot (1 - \text{res}(i,k)), \end{aligned} \tag{6}$$

subject to

(1) constraint for one channel per call

$$\sum_{l \in B_f} x_l = 1, \tag{7}$$

(2) cochannel constraint

$$x_l + a_{i,l} \leq 1, \quad \forall l \in B_f,\ 1 \leq i \leq C,\ d_{i,k} < r_0,\ i \neq k, \tag{8}$$

(3) cosite constraint

$$x_l + a_{k,q} \leq 1, \quad \forall l \in B_f,\ \forall q \in \frac{B}{B_f},\ |l - q| < g, \tag{9}$$

(4) adjacent channel constraint

$$\begin{aligned} x_l + a_{i,q} \leq 1, \quad \forall l \in B_f,\ \forall q \in \mathcal{K}_i,\ 1 \leq i \leq C,\ i \neq k, \\ d_{i,k} < r_1, \quad |l - q| < w, \quad l \neq q. \end{aligned} \tag{10}$$

In our formulation, the traffic demand and the "hard" constraints are handled by (7)–(10). There may be multiple channels that satisfy these constraints, but, among them, the objective function specified in (6) selects one channel that best meets the requirements of the "soft" constraints. W_1 and W_2 are positive constants and determine the relative significance of the different terms. The first term expresses the packing condition. The objective value decreases if channel l is also in use in cell i which is free from cochannel interference with cell k. The decrease in the value depends upon the distance between the cells i and k. The second term expresses the resonance condition. The objective value decreases if channel l is also in use in cell i, and cells i and k belong to the same reuse scheme. Therefore, the objective function attempts to increase packing and assign the same channel to cells that belong to the same reuse scheme.

We note that, if we were simply minimizing the objective function (without considering any of the constraints) the packing condition could lead to the same channel being assigned to two ongoing calls in adjacent cells, at the same time. However, such an assignment would violate the cochannel constraint (Constraint (8)), and hence would not be selected as a feasible solution, even though it gives a lower objective value.

Constraint (7) ensures that each call is allocated exactly one channel from the pool of available dynamic channels that are currently not in use in cell k.

Constraint (8) enforces the cochannel constraint by ensuring that a channel $l \in B_f$ is not selected for a call in cell k if it is already in use in any neighboring cell i, assuming i and k are separated by a distance less than the reuse distance r_0.

Constraint (9) is the cosite constraint. It ensures that a channel l is selected in cell k only if it separated by at least the cosite interval, g, from any other channel q, currently in use in cell k.

Constraint (10) states the adjacent channel constraint. It ensures that a channel l is selected in cell k only if it separated by at least the adjacent channel interval, w, from any other channel q, currently in use in a neighboring cell i, which is at a distance r_1. Since the channel separation within the same cell should be at least as high as that between adjacent cells, we should always have $g \geq w$ and $r_0 \geq r_1$.

We note that $\mathcal{K}_i$ is valid for all i, $1 \leq i \leq C$ (including cell k). However, the condition $i \neq k$, given in adjacent channel constraint (Constraint (10)), indicates that this constraint is not applicable for cell k. Of course, there will be no problems if the constraint actually is satisfied in cell k, but it need not be enforced. Therefore, the qualifier $i \neq k$ given in Constraint (10) is used to select cells for which the adjacent channel constraint should (or should not) be applied.

3.3. ILP Formulation with Channel Reassignment (ILP2). Channel reassignment, the process of transferring an ongoing call to a new channel without call interruption [4], can improve the quality of service in terms of lowering call blocking probability. Hence it is an important process in dynamic channel allocation. We now present our second ILP formulation that makes use of reassignment of existing channels. Using the notation given above, we formulate *ILP2* as follows.

Objective Function.

$$\begin{aligned}\text{Minimize} &- W_1 \sum_{i=1, i\neq k}^{C} \sum_{m\in B} \frac{a_{i,m} \cdot y_m}{d_{i,k}} \\ &+ W_2 \sum_{i=1, i\neq k}^{C} \sum_{m\in B} a_{i,m} \cdot y_m \cdot (1 - res(i,k)) \\ &- W_3 \sum_{m\in B} a_{k,m} \cdot y_m.\end{aligned} \tag{11}$$

subject to

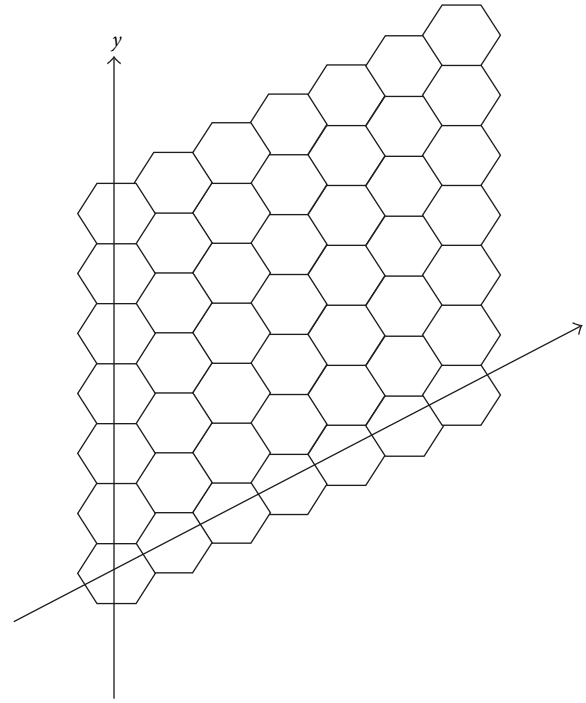

Figure 4: Cellular topological model.

(1) constraint for one channel per call

$$\sum_{m\in B} y_m = d_k, \tag{12}$$

(2) cochannel constraint

$$\begin{aligned} y_m + a_{i,m} \leq 1, \quad \forall m \in B,\ 1 \leq i \leq C, \\ i \neq k,\ d_{i,k} < r_0, \end{aligned} \tag{13}$$

(3) cosite constraint

$$y_m + y_p \leq 1, \quad \forall m, p \in B, |m - p| < g,\ m \neq p, \tag{14}$$

(4) adjacent channel constraint

$$\begin{aligned} y_m + a_{i,p} \leq 1, \quad \forall m, p \in B, |m - p| < w, \\ 1 \leq i \leq C, \quad d_{i,k} < r_1, \quad i \neq k. \end{aligned} \tag{15}$$

Equation (11) is the objective function. The first two terms are similar to those in ILP1. The third term expresses the limiting rearrangement condition. This term results in a decrease in the objective value if the new assignment for the ongoing calls in the cell k is same as the previous allocation. As in ILP1, W_1, W_2, and W_3 are positive constants and determine the significance of different terms.

Constraint (12) ensures that each call is allocated exactly one channel among all dynamic channels.

Constraint (13) enforces the cochannel constraint and is similar to constraint (8) except that here, we consider every dynamic channel $m \in B$.

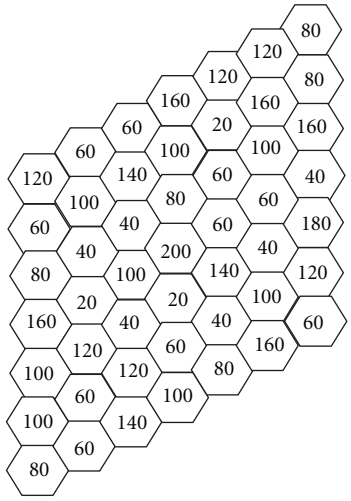

Figure 5: Non uniform traffic distribution pattern.

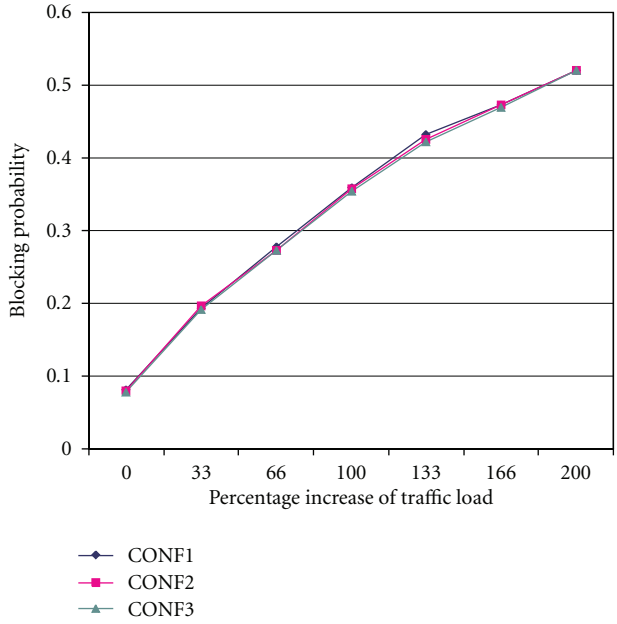

Figure 6: Comparison of performances of ILP2 with different combinations of values of W_1, W_2, and W_3, for ratio 35 : 35 with $g = 4$ and $w = 3$.

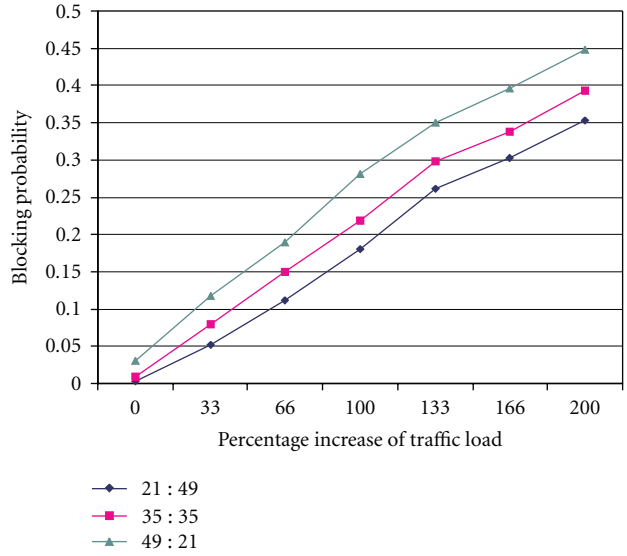

Figure 7: Performances with reassignment for $g = 2$ and $w = 2$.

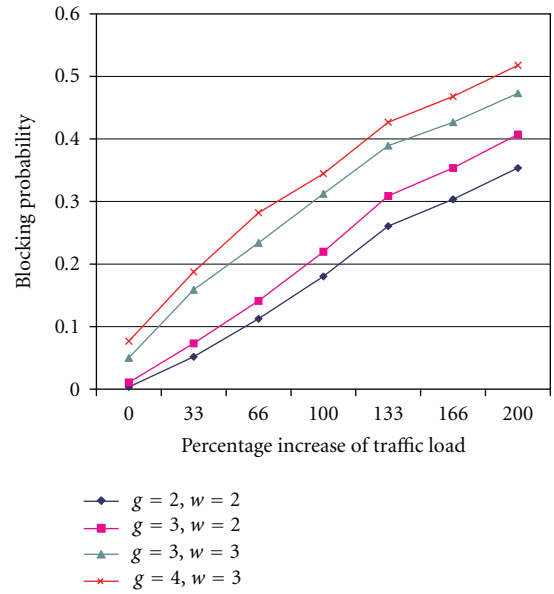

Figure 8: Performances with reassignment for ratio 21 : 49.

Constraint (14) is the cosite constraint. It ensures that two channels $m \in B$ and $p \in B$ are not selected in cell k if they do not have enough cosite interval distance, g.

Constraint (15) is the adjacent channel constraint, similar to constraint (10). But here, we consider every dynamic channel $m, p \in B$.

4. Cellular Model Assumptions

Our ILP approach is applied to the mobile cellular model used in [2]. The basic characteristics of the model are briefly summarized as follows

(1) The topological model is a group of 49 hexagonal cells that form a parallelogram shape, as shown in the Figure 4.

(2) The total number of channels for the network is 70, distributed in FC and DC, that is, $|FC \cup DC| = 70$. A channel serves one call at most. In FCA, the available fixed channels are distributed among the cells, while in DCA, all dynamic channels are put in a central pool. A channel is assigned to an incoming call by a central controller that monitors the whole cellular network.

(3) Incoming calls at each cell may be served by any of the available channels.

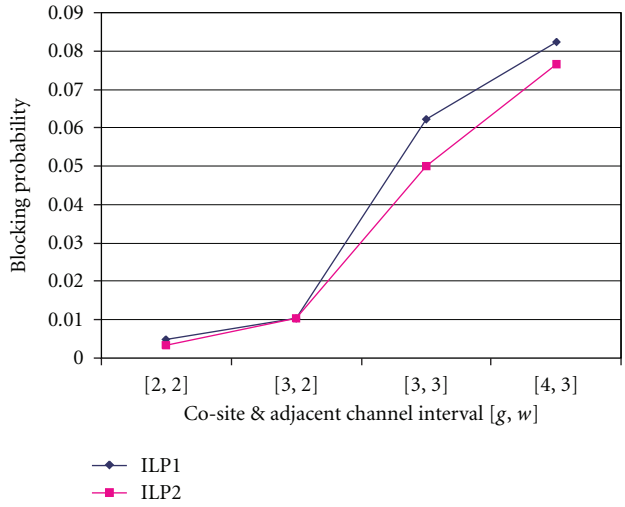

Figure 9: Performances of ILP1 versus ILP2 for ratio 21 : 49 with initial traffic load.

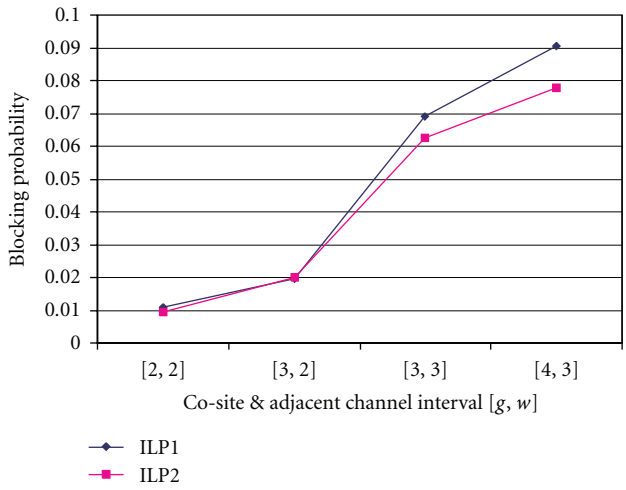

Figure 10: Performances of ILP1 versus ILP2 for ratio 35 : 35 with initial traffic load.

(4) The selection of a channel is subject to cochannel, cosite, and adjacent channel interference.

(5) The basic object of the network model is the link, which is a communication between a base station and a mobile terminal through a channel.

(6) A new call at cell k is blocked if neither a fixed channel nor a dynamic channel is available to satisfy the electromagnetic interference constraints.

(7) Existing calls in a cell involved in a new call arrival may be reassigned new channels (ILP2 only).

In our simulation, we assume the traffic model to follow the blocked-calls-cleared queuing discipline. An incoming call is served immediately if a channel is available, otherwise the new call is blocked and not queued. The most fundamental characteristics of this model include infinite number of users, finite number of channels for the network, no queue

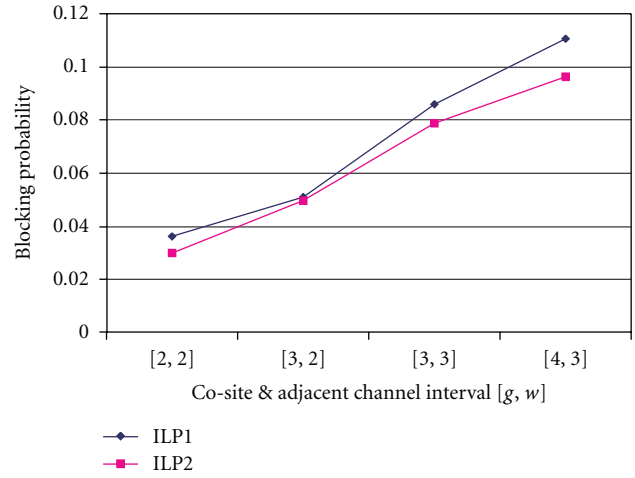

Figure 11: Performances of ILP1 versus ILP2 for ratio 49 : 21 with initial traffic load.

for new calls, call arrival following a Poisson process with mean arrival rate of λ calls/hour. The call duration is a random variable with exponential distribution of the form:

$$f(x) = \begin{cases} b\exp^{-bx} & \text{if } x \geq 0, \\ 0 & \text{otherwise,} \end{cases} \tag{16}$$

where b is the mean duration time of calls [3]. Interarrival time follows a negative exponential distribution with mean b. The product of the mean arrival rate and the mean call duration gives the traffic load offered to the cellular network. We used nonuniform traffic distribution (where each cell may have a different call arrival rate) and considered the traffic pattern used in [3] shown in Figure 5. The entry in a cell represents the mean call arrival rate per hour, under *normal load* condition. In addition, we set the mean call duration to 180 seconds.

5. Simulations and Discussions

In our simulations, similar to the works in [6], we used three representative ratios of fixed and dynamic channels, FC : DC, 21 : 49, 35 : 35, and 49 : 21. The initial load in each cell was set to 60% of the normal load and the results were obtained by increasing the traffic rates by 33% for all cells in each pattern, with respect to the initial rates on each cell. The performance of the ILP formulations is derived in terms of blocking probability for new incoming calls, which is defined as the ratio between the number of blocked calls and the total number of call arrivals in the system. In all of our experiments, set the reuse distance, $r_0 = 3$. We also set $W_1 = 1.5$, $W_2 = 2$, and $W_3 = 1$, which were determined by trial-and-error.

To ascertain the values of $W_1 = 1.5$, $W_2 = 2$, and $W_3 = 1$, we investigated performances of different combinations. Figure 6 shows a comparison of blocking probability of *ILP2* for three configurations, namely, {1, 1, 1}, {1.5, 0.5, 1}, and {1.5, 2, 1}, for ratio 35 : 35 with $g = 4$ and $w = 3$. By

Table 1: Blocking probabilities with no reassignment.

FC : DC	g	w	Percentage increase of traffic load						
			0	33	66	100	133	166	200
21 : 49	1	1	0.00	0.00	0.00	0.03	0.09	0.12	0.18
	2	2	0.00	0.05	0.11	0.18	0.26	0.30	0.36
	3	2	0.01	0.08	0.15	0.23	0.31	0.35	0.40
	3	3	0.06	0.16	0.24	0.32	0.40	0.43	0.49
35 : 35	1	1	0.00	0.00	0.02	0.09	0.16	0.21	0.27
	2	2	0.01	0.08	0.14	0.22	0.31	0.34	0.40
	3	2	0.02	0.10	0.18	0.26	0.34	0.39	0.44
	3	3	0.07	0.17	0.25	0.34	0.40	0.44	0.50
49 : 21	1	1	0.00	0.04	0.10	0.17	0.26	0.30	0.36
	2	2	0.04	0.12	0.20	0.28	0.36	0.40	0.45
	3	2	0.05	0.15	0.23	0.30	0.38	0.42	0.47
	3	3	0.08	0.20	0.27	0.35	0.42	0.46	0.52

Table 2: Performances of ILP1 and the ES approach proposed in [6].

FC : DC	Scheme	Percentage increase of traffic load						
		0	20	40	60	80	100	120
21 : 49	ES	0.00	0.00	0.01	0.02	0.07	0.14	0.17
	ILP1	0.00	0.00	0.04	0.06	0.11	0.17	0.19
35 : 35	ES	0.00	0.00	0.01	0.03	0.08	0.14	0.17
	ILP1	0.00	0.00	0.03	0.05	0.11	0.16	0.19
49 : 21	ES	0.00	0.00	0.03	0.05	0.10	0.16	0.19
	ILP1	0.00	0.01	0.05	0.07	0.12	0.18	0.21

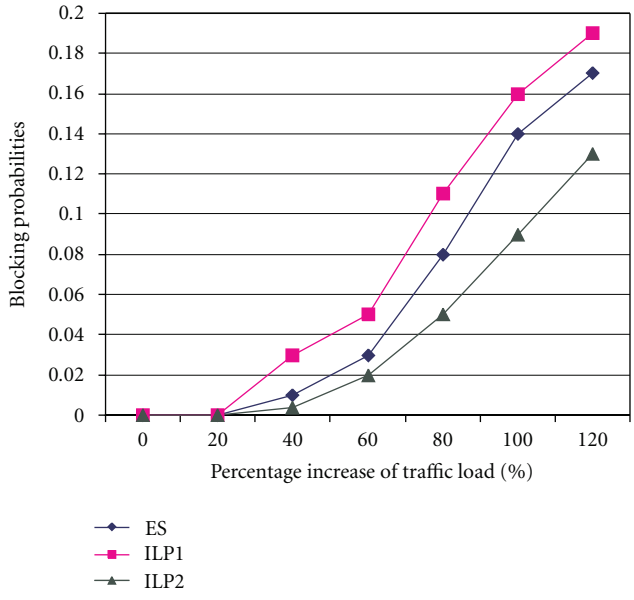

Figure 12: Relative performances of ES [6], ILP1, and ILP2 for ratio 35 : 35 with initial traffic load.

and large, Conf 3, which was taken for the rest of our simulations, works best, but the gap between their performances is inconspicuous. For both *ILP1* and *ILP2*, the similar situation was sustained with other ratios and values of g and w.

Table 1 shows the blocking probabilities for channel allocation without any reassignment of existing calls (obtained using ILP1). As expected the blocking probability increases with increasing traffic load on the network, and with the required channel interval for cosite constraint (g) and adjacent channel constraint (w), but the network performs better as the number of dynamic channels increases. This was expected as the higher number of dynamic channels means that the scheme has more freedom and can choose channels from a larger set to assign to calls.

We have tested ILP2, where channel reassignment is allowed, with different combinations for the values of g and w, each ranging from 1 to 4. Figure 7 shows the blocking probabilities when $g = 2$ and $w = 2$. Results with other values of g and w are similar. As before, blocking probability increases with traffic, and also with required channel intervals for cosite and adjacent channel constraints. However, as shown in the figure, the 21 : 49 ratio consistently gives the best performance, followed by 35 : 35 and 49 : 21.

Figure 8 shows how the blocking probabilities are affected by the requirement of different values of cosite and adjacent channel intervals, for the ratio of 21 : 49, under reassignment scheme. We see that even small changes in the values of g and w can have a significant effect on the blocking probability. The results for the 35 : 35 and 49 : 21 ratios followed a similar pattern, but the overall blocking probabilities were higher.

The effect of channel reassignment on blocking probability with the following representative ratios: 21 : 49, 35 : 35, and 49 : 21 was illustrated in Figures 9, 10, and 11, respectively, under reassignment scheme. Our results indicate that although channel reassignment does reduce blocking probability, the amount of improvement seems to vary with traffic load and the values for g and w. We are conducting further experiments to determine the conditions under which channel reassignment is most beneficial.

Finally, we have compared our approach with the evolutionary strategy- (ES-) based HCA scheme proposed in [6], which considers cochannel constraints only. We note that, the approach in [6] not only provides criteria for selecting among multiple feasible solutions (similar to our approach), but also it has been shown to outperform another well-known approach for HCA [3]. However, like most existing approaches, both [6] and [3], do not consider CSC and ACC. So we had to use a restricted case of our formulation, for CCC only, to get a meaningful comparison. Furthermore, since we use ILP to generate the solutions, we can expect the performance advantage to be consistently greater than (or at least equal to) existing heuristics, for the same parameters.

We simulate this by setting $g = 1$ and $w = 1$ in our formulation. Initial traffic in each cell, percentage increase of load, and other parameters including the values of W_1 and W_2 were set to the same values as in [6]. In Table 2, the rows *ES* and *ILP1* indicate the blocking probabilities in [6] and our ILP1, respectively, under different traffic loads. As shown in the table, our results *without* channel reassignment are close to those in [6] with channel reassignment. A qualitative comparison of the results for ES [6], ILP1, and ILP2 is shown in Figure 12 for the ratio of 35 : 35. The results for the other ratios follow a similar pattern. We note that ILP1 (without any channel reassignment) has a slightly higher blocking probability compared to ES, which is expected, but ILP2 consistently outperforms ES.

6. Conclusions

In this paper, we have presented two new integer linear program formulations for hybrid channel assignment in wireless cellular networks. The first formulation does not allow channel reassignment for existing calls, while the second formulation is capable of performing channel reassignment. To the best of our knowledge, these are the first formulations for optimally solving the hybrid channel assignment problem that take into consideration the cosite and the adjacent channel constraints, in addition to the cochannel constraints. We also integrate soft constraints such as the packing condition, resonance condition and limiting channel reassignment to further optimize the objective function. The results indicate that even without channel reassignment, our approach (in ILP1) produces results comparable to some existing schemes that perform reassignment. Additional improvements are obtained if we allow channel reassignment (in ILP2) as well. We are currently investigating the relative importance of the soft constraints and effect of varying the constants in the objective function, on the overall performance of our formulations.

Acknowledgment

A. Jaekel and A. Ngom thank NSERC for their support.

References

[1] G. Chakraborty, "An efficient heuristic algorithm for channel assignment problem in cellular radio networks," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 6, pp. 1528–1539, 2001.

[2] E. Del Re, R. Fantacci, and L. Ronga, "A dynamic channel allocation technique based on hopfield neural networks," *IEEE Transactions on Vehicular Technology*, vol. 45, no. 1, pp. 26–32, 1996.

[3] H. G. Sandalidis, P. P. Stavroulakis, and J. Rodriguez-Tellez, "An efficient evolutionary algorithm for channel resource management in cellular mobile systems," *IEEE Transactions on Evolutionary Computation*, vol. 2, no. 4, pp. 125–137, 1998.

[4] P. T. H. Chan, M. Palaniswami, and D. Everitt, "Neural network-based dynamic channel assignment for cellular mobile communication system," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 2, pp. 279–288, 1994.

[5] T. Farid, A. Ngom, and A. Jaekel, "Integrated hybrid channel assignment and distributed power control in wireless cellular networks using evolution strategy," in *Proceedings of the IEEE Symposium on Computational Intelligence in Image and Signal Processing (CIISP '07)*, pp. 293–300, 2007.

[6] G. Vidyarthi, A. Ngom, and I. Stojmenović, "A hybrid channel assignment approach using an efficient evolutionary strategy in wireless mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 5, pp. 1887–1895, 2005.

[7] S. L. Chen and P. H. J. Chong, "Dynamic channel assignment with flexible reuse partitioning in cellular systems," in *Proceedings of the IEEE International Conference on Communications (ICC '04)*, vol. 7, pp. 4275–4279, June 2004.

[8] K. Naik and D. S. L. Wei, "Call-on-hold for improving the performance of dynamic channel-assignment strategies in cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 6, pp. 1780–1793, 2004.

[9] S.-M. Senouci and G. Pujoile, "Dynamic channel assignment in cellular networks: a reinforcement learning solution," in *Proceedings of the 10th International Conference on Telecommunications (ICT '03)*, vol. 1, pp. 302–309, 2003.

[10] V. T. Vakili and A. Aziminejad, "Dynamic channel allocation based on compact pattern concept with pattern restoration: performance analysis of a modified approach," in *Proceedings of the 5th European Personal Mobile Communications Conference*, pp. 555–559, 2003.

[11] X. Wu, A. Jaekel, A. Bari, and A. Ngom, "Optimized hybrid resource allocation in wireless cellular networks with and without channel reassignment," in *Proceedings of IEEE/ComSoc International Conference on Information Technology New Generations (ITNG '09)*, pp. 1146–1151, 2009.

[12] R. C. V. Macario, *Cellular Radio: Principles and Design*, Macmillan, New York, NY, USA, 2nd edition, 1997.

[13] A. Hac, "Cellular network model with hand off delays," in *Proceedings of the IEEE International Conference on Communications (ICC '95)*, pp. 1834–1838, June 1995.

[14] W. C. Y. Lee, *Mobile Communications Design Fundamentals*, Wiley, New York, NY, USA, 1993.

[15] G. Vidyarthi, *Integrated channel assignment and power control in wireless mobile network using evolutionary strategy*, M.S. thesis, University of Windsor, 2003.

[16] S. Sarkar and K. N. Sivarajan, "Channel assignment algorithms satisfying cochannel and adjacent channel reuse constraints in cellular mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 5, pp. 954–967, 2002.

[17] G. Vidyarthi, A. Ngom, and I. Stojmenovic, "Evolutionary methods in wireless mobile computing," in *Combinatorial Optimization in Communication Networks*, D.-Z. Du, M. Cheng, and Y. Li, Eds., vol. 18, pp. 33–79, Springer, New York, NY, USA, 2006.

[18] W. K. Hale, "Frequency assignment: theory and applications," *Proceedings of the IEEE*, vol. 68, no. 12, pp. 1497–1514, 1980.

[19] R. Chávez-Santiago, E. Gigi, and V. Lyandres, "Channel assignment for cellular mobile networks with nonuniform cells—an improved heuristic algorithm," *IEE Proceedings: Communications*, vol. 153, no. 1, pp. 61–68, 2006.

[20] S. C. Ghosh, B. P. Sinha, and N. Das, "Coalesced CAP: an improved technique for frequency assignment in cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, pp. 640–653, 2006.

[21] Md. I. Islam and A. B. M. S. Hossain, "Channel allocation of mobile cellular network based on graph theory," in *Proceedings of the IEEE TENCON Region Annual International Conference*, vol. 2, pp. B529–B532, 2004.

[22] Y. Peng, L. Wang, and B. H. Soong, "Optimal channel assignment in cellular systems using tabu search," in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '03)*, vol. 1, pp. 31–35, 2003.

[23] S. L. Chen and P. H. J. Chong, "Capacity improvement in cellular systems with dynamic channel assignment and reuse partitioning," in *Proceedings of the IEEE International Conference on Communications (ICC '03)*, vol. 2, pp. 1441–1445, 2003.

[24] L. Li, J. Tao, and F. Li, "Dynamic channel assignment performance analysis in multiservice hierarchical wireless networks," in *Proceedings of the 1st International Conference on Communications and Networking in China (ChinaCom '06)*, pp. 1–5, 2006.

[25] L. Li, J. Tao, and T. Xiaofang, "Dynamic channel assignment performance analysis in multiservice hierarchical wireless networks," in *Proceedings of the 17th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06)*, pp. 1–5, September 2006.

[26] M. A. C. Lima, A. F. R. Araujo, and A. C. Cesar, "Adaptive genetic algorithms for dynamic channel assignment in mobile cellular communication systems," *IEEE Transactions On Vehicular Technology*, vol. 56, no. 5, pp. 2685–2696, 2007.

[27] I. Koutsopoulos and L. Tassiulas, "Joint optimal access point selection and channel assignment in wireless networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 3, pp. 521–532, 2007.

[28] L. S. El Alami, E. Kudoh, and F. Adachi, "On-demand channel assignment using channel segregation for uplink DS-CDMA multi-hop virtual cellular network," in *Proceedings of the 63rd IEEE Vehicular Technology Conference (VTC '06)*, vol. 2, pp. 713–717, July 2006.

[29] E. Kudoh and F. Adachi, "Distributed dynamic channel assignment for a multi-hop virtual cellular system," in *Proceedings of the 59rd IEEE Vehicular Technology Conference (VTC '04)*, vol. 4, pp. 2286–2290, May 2004.

[30] X. J. Li and P. H. J. Chong, "A dynamic channel assignment scheme for TDMA-based multihop cellular networks," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '07)*, pp. 815–818, September 2007.

[31] A. M. Safwat, "Distributed connection admission control and dynamic channel allocation in ad hoc-cellular networks," in *Proceedings of the International Conference on Digital Telecommunications (ICDT '06)*, p. 52, August 2006.

[32] P. Satahack and C. Chayawan, "A multi-hop borrowing channel assignment for wireless local loop systems," in *Proceedings of the 9th IEEE Singapore International Conference on Communication Systems (ICCS '04)*, pp. 200–204, 2004.

[33] S. Alireza, G. Shirazi, and H. Amindavar, "A hybrid method for channel assignment problems in cellular radio networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '06)*, vol. 3, pp. 1260–1265, 2006.

[34] A. K. Prajapati, R. K. Ghosh, and H. Mohanty, "A self-adaptive hybrid channel assignment scheme for wireless communication systems," in *Proceedings of the 9th International Conference on Information Technology (ICIT '06)*, pp. 94–95, December 2006.

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 576243, 10 pages
doi:10.1155/2010/576243

Research Article

Spatial Diversity Scheme to Efficiently Cancel ISI and ICI in OFDM-OQAM Systems

Nizar Zorba[1] and Faouzi Bader[2]

[1] *Electrical Engineering Department, Faculty of Engineering, University of Jordan, Amman 11942, Jordan*
[2] *Centre Technològic de Telecomunicacions de Catalunya, (CTTC), Avenida Carl Friedrich Gauss 7, 08860 Barcelona, Spain*

Correspondence should be addressed to Nizar Zorba, n.zorba@ju.edu.jo

Received 19 August 2010; Accepted 4 October 2010

Academic Editor: Christos Verikoukis

This paper is based on an Offset Quadrature Amplitude Modulation (OQAM) Orthogonal Frequency Division Multiplexing (OFDM) transmission scheme that is operated without a Cyclic Prefix (CP), where the multiple transmitting antennas are employed to substantially reduce the inherent intersymbol and intercarrier interference. The proposed scheme avoids the use of the CDMA technology to get rid of the interference. The nonemployment of the CP increases the spectral efficiency in comparison with classical CP-OFDM systems, as it does not employ the CP for its correct performance. On the other hand, the non-employment of the CP comes at cost of Intersymbol Interference (ISI). This paper presents a method which cancels the interference terms by employing a multiantenna precoding strategy based on spatial diversity OQAM-OFDM scheme, so that the overall system can get the advantage of the CP removal while no ISI is generated. Moreover, the proposed system benefits from the multiuser gain through an opportunistic scheduler at the transmitter side to select the user with the best channel characteristics at each instant. The resultant scheme OQAM-OFDM-MIMO data rate is obtained in a closed form expression and proved to be higher than the classical CP-OFDM systems.

1. Introduction

Communication rates in broadband wireless systems achieved very high values in multicarrier techniques, that can be combined with the Multiple-Input-Multiple-Output (MIMO) technology to provide both efficiency and Quality of Service (QoS) to the system. Typically, the channel in these broadband systems is frequency selective, and one of the best multicarrier techniques that can be employed together with MIMO is the Orthogonal Frequency Division Multiplexing (OFDM), because OFDM converts the frequency selective channel into a set of parallel frequency flat channels. Therefore, OFDM is already included in several communication standards as the IEEE 802.11n WLAN standard, while its multiuser OFDM Access (OFDMA) version is already within the IEEE 802.16a/e WiMax standards, the cellular Long-Term Evolution (4G-LTE) and the Terrestrial Digital Video Broadcasting (DVB-T) standards [1, 2].

OFDM shows some drawbacks that decrease its efficiency. The largest drawback is the requirement for a CP to tackle the delay in the channel, where the CP constitutes 10%–20% of the symbol time, with the consequent decrease in the system performance and the invested resources [3]. It also needs a block processing to keep the orthogonality among all the subcarriers, which is a serious problem for scalability, as it is impossible to increase the number of allocated subcarriers because they will be asynchronous with the rest of the block. As all modern communication systems are characterized by users running different applications characterized with various data rates, setup times, and QoS demands, OFDM shows a problem to synchronization in such heterogenous systems. OFDM shows several advantages as its low complexity and its familiarity to both the academia and industry, as it is already implemented in a lot of communication standards. But to further increase the system efficiency, the design of alternative multicarrier schemes is currently under study within the cognitive communications arena [4, 5].

An interesting proposal is to modify the OFDM systems by jointly employing it with the Offset Quadrature Amplitude Modulation (OQAM) transmission principle, for what

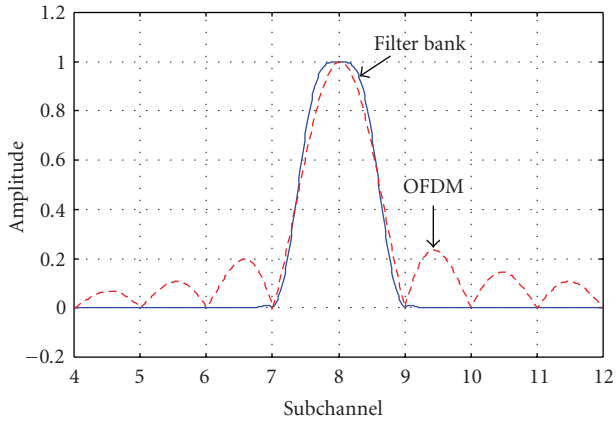

FIGURE 1: The prototype filter advanced basic pulse that reduces the out-of-band frequency leakage.

is known in the literature as the Filter Bank-based Multicarrier (FBMC) transmission [6, 7]. This proposal is shown to enhance the performance and the operational flexibility of OFDM, thanks to its capabilities to exploit the spectral efficiency of filter banks and to enable independence among its subchannels. In OFDM-OQAM, the transmission channel is divided into subchannels, which gives an interesting degree of freedom to control the allocation process, together with the scalability advantage [8]. The main difference of OQAM with respect to OFDM is that instead of rectangular windows, a more advanced basic pulse, also called prototype filter, is used, which can reduce the out-of-band frequency leakage and help to fulfill more stringent spectral masks, as can be seen from Figure 1. The use of OQAM with appropriate filter prototypes allows to obtain an almost negligible ISI and Intercarrier Interference (ICI) assuming that the channel coherence bandwidth is high enough. OFDM-OQAM is mainly characterized by the non-employment of the CP, so that all the system resources are devoted to increase the whole system throughput, thus providing higher spectral efficiency than the classical CP-OFDM [9].

But in OFDM, the CP is employed to avoid the ISI, while OFDM-OQAM removes the CP from its scheme, therefore, the combat of the ISI and the ICI remains as the main challenge in this technique, where these tasks are usually performed by the receiver through some complex operations, representing a main problem for the implementation of this scheme. Therefore, even the study of OFDM-OQAM was initially proposed many years ago [8], but up to now, it has not been included in any commercial standard, mainly due to its large complexity that handicaps its implementation in realistic systems. Recently, an increasing interest in FBMC has again emerged [4–6, 9, 10], which has to start by finding some signal processing techniques to decrease the OFDM-OQAM complexity and to make it commercially viable.

The MIMO technology is already in almost all commercial standards, so that an additional resource is available in the system to be employed to cancel the interference terms without the need for any complex reception techniques and, therefore, to decrease the complexity related to FBMC schemes. Notice that MIMO systems are always proposed to increase the system rate and/or to decrease its error rate, while now, we can face an alternative approach for the implementation of the MIMO systems: the interference cancellation in FBMC. On the other hand, another resource that is employed by the designer to enhance the system behaviour is the multiuser gain, as the availability of multiple users in the system is beneficial to enable the transmitter to select the user with the best channel conditions at each time, and by this way, to increase the system average sum rate. This philosophy is known as the opportunistic scheduler [11], which has already been commercially introduced in the UMTS-HSDPA standard.

Few recent works have been presented to tackle the FBMC systems complexity reduction; the authors in [12] employed the CDMA technology to get rid of the interference without the CP requirement in OFDM-OQAM systems. On the other hand, [13] introduced a MIMO scheme in OFDM-OQAM systems when there exist some uncertainty in the Channel State Information (CSI) at the transmitter side, asking for full CSI to operate the system which is a serious handicap in terms of the feedback load.

Up to the authors' knowledge, no previous schemes have been presented in the literature to benefit from the antennas availability to efficiently cancel the ISI and the ICI in the system through a realistic strategy. Therefore, the objective of this paper is to propose a spatial diversity scheme to cancel the ISI and ICI in the system through low-complexity operations, so that the implementation of the OFDM-OQAM technique can be possible, with all the presented advantages of the OFDM-OQAM systems. In other words, MIMO will accomplish the required task of interference cancellation in the system that is jointly employed with the system multiuser gain [11, 14] to increase the system data rate.

As a summary, the contributions of this work in the field of OFDM-OQAM systems are as follows.

(i) A novel OFDM-OQAM scheme is presented that is operated without the need of the cyclic prefix.

(ii) An intuitive transmission scheme together with low-complexity processing at the receiver side are presented within the introduced OFDM-OQAM strategy.

(iii) The multiuser gain in the system is also considered to enhance the system performance, showing better behaviour that the classical CP-OFDM Alamouti [15] technique.

The remainder of this paper is organized as follows: while Section 2 introduces the OFDM-OQAM system applied to single-input single-output systems, Section 3 presents the proposed spatial diversity technique within OFDM-OQAM, where the employed system model and the opportunistic strategy will be explained there. Section 4 will show the numerical results and simulations, followed by Section 5 with the paper conclusions.

2. Single-Input Single-Output OFDM-OQAM Approach

Orthogonal frequency division multiplexing with the cyclic prefix insertion (CP-OFDM) is the most widespread modulation among all the multicarrier modulations, and this is thanks to its simplicity and its robustness against multipath fading using the CP. Nevertheless, this technique causes a loss of spectral efficiency due to the cyclic prefix. Furthermore, CP-OFDM shape is not compact due to the large side lobe levels resulting from the rectangular pulse. This could be avoided by inserting null subcarriers at frequency boundaries in order to avoid harmful interferences into neighboring communication systems. But these practice results in an important loss of spectral efficiency. To avoid these disadvantages, OQAM-OFDM (or FBMC) was proposed as an alternative approach to multicarrier OFDM mainly in cognitive-based networks [16]. In FBMC, there is no need to insert any guard interval. Furthermore, it uses a frequency well-localized pulse shaping such that provides high spectral efficiency [17–20]. Each sub-carrier is modulated with an Offset Quadrature Amplitude Modulation (OQAM) which consists of transmitting the real and the imaginary parts of a complex data symbol with a shift of half the symbol period between them [21].

Because OQAM orthogonality conditions are considered in the real field, the data at the receiver side is carried only by the real (or imaginary) component of the signal. The imaginary (or real) part appears as an intrinsic interference term although the data is always orthogonal to the interference term. But, this term of interference becomes a source of problems when combining OQAM-OFDM with some MIMO techniques.

In both the transmitter and the receiver, a filter bank is obtained by adding to the Fast Fourier Transform (FFT) unit a specific signal processing module: the polyphase network. The number M of filters in the bank is the size of the FFT and the system is said to have M subchannels, while OFDM has M subcarriers. The filters are frequency-shifted versions of a prototype low-pass filter, satisfying the Nyquist criterion. A family of prototype filters, which have many desirable properties and can be considered as globally optimal have been designed, using the frequency-sampling technique and a few frequency coefficients [21–23].

The multicarrier filter banks are employed in the transmultiplexer configuration using the Synthesis Filter Bank (SFB) at the transmitter, and the Analysis Filter Bank (AFB) at the receiver [23]. In the FBMC application, the use of critically sampled filter banks would be problematic, since the aliasing effects would make it difficult to compensate imperfections of the channel by processing the subchannel signals after the AFB only. Therefore, a factor of two oversampling is commonly applied in the subchannel signals in the AFB, as shown in Figure 3.

In the current paper, we focused on uniform-modulated filter banks in which the prototype filter $g[m]$ of length L is shifted to cover the whole system bandwidth, where the ratio $K = L/M$ is named the overlapping factor because it is the number of multicarrier symbols which overlap in the time domain. The frequency response of any prototype filters is determined by K samples, as given by Table 1 for several values of the overlapping factor. It must be pointed out that in high speed transmission, the value $K = 4$ leads to a good tradeoff between performance and complexity and it is retained as the reference.

Table 1: Frequency coefficients reference for prototype filters, from [4].

K	H_0	H_1	H_2	H_3
2	1	0.707		
3	1	0.911438	0.411438	
4	1	0.971960	0.707	0.235147

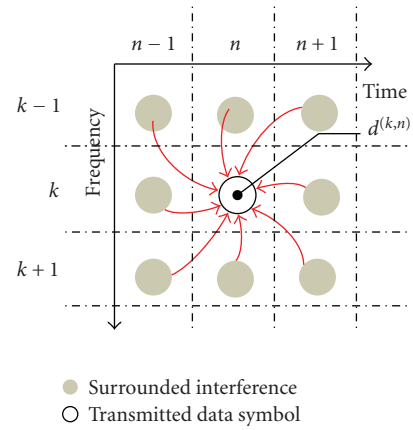

Figure 2: Received ISI and ICI from surrounding data symbols.

Once the prototype filter has been designed, the M filters in the bank are obtained by the frequency shifts k/M, with $0 \le k \le M-1$. The output signal from the synthesis filter bank is constituted by M subcarriers (M = IFFT/FFT size) and the set of active subcarriers, $d^{(k,n)}$ denotes the real-valued symbols at the kth subcarrier during the nth symbol interval, modulated at rate $2/T$. The signalling interval T is defined as the inverse of the subcarrier spacing, that is, $T = 1/\Delta f$. The symbols $d^{(k,n)}$ and $d^{(k,n+1)}$ can be interpreted to carry the in phase and quadrature (I/Q) components of the complex-valued symbol $c^{(k,l)}$ (of rate $1/T$) from a QAM-alphabet.

It should be noted that the signs of the $\theta^{(k,n)}$ ($\theta^{(k,n)} = j^{k+n}$) depicted in the sequence of Figure 3 can be chosen arbitrarily, but the pattern of real and imaginary samples has to follow the shown definition to maintain (near) orthogonality [6]. The synthesized signal burst is, therefore, a composite of multiple subchannel signals each of which consists of a linear combination of time-shifted (by multiples of $T/2$) and overlapping impulse responses of the prototype filter, weighted by the respective symbol values $d^{(k,n)}$. The "$C2R$" and the "$R2C$" blocks in Figure 3 indicate the conversion of the data from complex into real form and the inverse operation, respectively. When a real (imaginary) part of a subcarrier symbol is used, then the unused imaginary (real) part is, at the receiver, a fairly complicated function of surrounding data symbols, as can be seen in Figure 2. We

Table 2: Representation of the time-frequency response of the OFDM-OQAM (FBMC) system considered in this work. Due to the employed offset QAM modulation, the effective time-frequency response will be reduced to only bold values in the table [4].

	−4	−3	−2	−1	0	1	2	3	4
−2	**0**	0.0006	**−0.0001**	0	**0**	0	**−0.0001**	0.0006	**0**
−1	0.0054	$0.0429j$	−0.1250	$-0.2058j$	0.2393	$0.2058j$	−0.1250	$-0.0429j$	0.0054
0	**0**	−0.0668	**0.0002**	0.5644	**1**	0.5644	**0.0002**	−0.668	0
1	0.0054	$-0.0429j$	−0.1250	$0.2058j$	0.2393	$-0.2058j$	−0.1250	$0.0429j$	0.0054
2	**0**	0.0006	**−0.0001**	0	**0**	0	**−0.0001**	0.0006	**0**

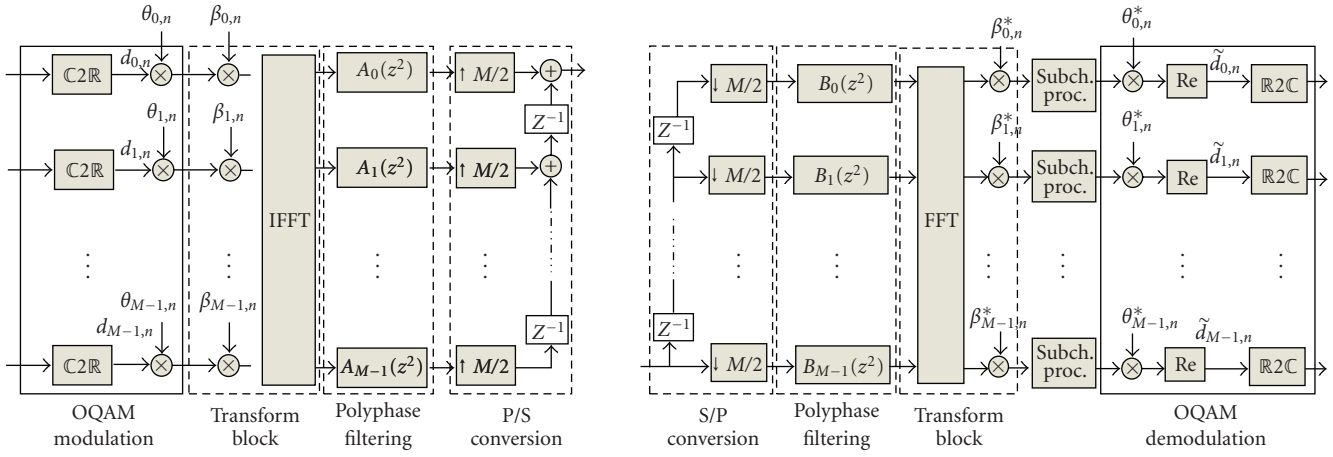

Figure 3: Multicarrier polyphase filter banks for SISO case, (a) synthesis filter banks (SFB), (b) analysis filter banks (AFB).

can write at the transmitter side the baseband equivalent of a discrete time FBMC signal as follows [21, 24]:

$$S[m] = \sum_{k=0}^{M-1} \sum_{n \in z} d^{(k,n)} g^{(k,n)} \left[m - n\frac{M}{2} \right] e^{(2\pi/M)m(m-D/2)} e^{j\psi^{(k,n)}}, \tag{1}$$

where D is the delay term and depends on the length of the prototype filter $g[m]$ and $\psi^{(k,n)}$ is an additional phase term. The transmitted symbols $d^{(k,n)}$ are real-valued symbols. Equation (1) can be written in a more compact form as

$$S[m] = \sum_{M-1}^{k=0} \sum_{n \in z} d^{(k,n)} g^{(k,n)}[m], \tag{2}$$

where $g^{(k,n)}[m]$ are the shifted versions of $g[m]$ in time and frequency. When the transmitter and the receiver are connected back to back, the signal at the receiver output over the kth sub-carrier and the nth time instant is determined using the inner product of $s[m]$ and $g^{(k,n)}[m]$

$$r^{(k,n)} = \sum_{m=-\infty}^{+\infty} \sum_{k'=0}^{M-1} \sum_{n' \in z} d^{(k',n')} g^{(k',n')}[m] g^{(k,n)\star}[m]. \tag{3}$$

The coefficients of their impulse responses in the time-frequency domain are illustrated in Table 2. The phase term $\psi^{(k,n)}$ in (1) guarantees and holds the real orthogonality condition

$$\Re e \left\{ \sum_{m=-\infty}^{+\infty} g^{(k',n')}[m] g^{(k,n)\star} \right\} = \delta^{(k,k')} \delta^{(n,n')}. \tag{4}$$

Considering the SISO FBMC transmission, when passing through the radio channel and adding noise contribution $z^{(k,n)}$, (3) becomes

$$r^{(k,n)} = h^{(k,n)} d^{(k,n)} + u^{(k,n)} + z^{(k,n)}, \tag{5}$$

where $h^{(k,n)}$ is the channel coefficient at subcarrier k and time index n, $u^{(k,n)}$ is defined as an intrinsic interference and is written as

$$u^{(k,n)} = \sum_{(k',n') \neq (k,n)} h^{(k',n')} d^{(k',n')} \sum_{m=-\infty}^{+\infty} g^{(k',n')} g^{(n,k)\star}[m]. \tag{6}$$

According to Table 2, we note that most part of the energy is localized in a restricted set (shown in bold) around the considered symbol. Consequently, we will assume that the intrinsic interference term depends only on this restricted set (denoted by k, n) [21]. Moreover, assuming that the channel

is constant at least over this summation zone, we can write as in [24]

$$r^{(k,n)} = h^{(k,n)}\left(d^{(k,n)} + \underbrace{\sum_{(k',n')\in\Omega^{(k,n)}} h^{(k',n')} d^{(k',n')} \sum_{m=-\infty}^{+\infty} g^{(k',n')}[m] g^{(k,n)\star}[m]}_{u^{(k,n)}}\right) + z^{(k,n)} \tag{7}$$

According to (4), and as $d^{(k',n')}$ is real valued, the intrinsic interference $u^{(k,n)}$ is pure imaginary. Thus, the demodulated signal can be rewritten as

$$r^{(k,n)} \approx h^{(k,n)}\left(d^{(k,n)} + jf^{(k,n)}\right) + z^{(k,n)}, \tag{8}$$

where $f^{(k,n)}$ is real-valued. In the case of n_t multiple antennas at the transmitter side, we transmit real symbols $d_i^{(k,n)}$ at a given time-frequency position (k,n) and at the ith transmit antenna. So, after transmitting through the radio channel, we demodulate at the receiver side as

$$r^{(k,n)} = \sum_{i=1}^{N_t} h_i^{(k,n)}\left(d_i^{(k,n)} + jf_i^{(k,n)}\right) + z^{(k,n)}, \tag{9}$$

where $h_i^{(k,n)}$ is the channel coefficient between the ith transmitting antenna and the receiver. A more extended analysis of the multiple antenna case with the proposed ISI and ICI interference suppression scheme is presented in next section.

3. Spatial Diversity in OFDM-OQAM

The opportunistic scheduling [11, 14] is one of the main transmission techniques in multiuser scenarios, where during the acquisition step, a known training sequence is transmitted from the Base Station (BS). Each one of the users receives the the signal, calculates the received Signal-to-Noise Ratio (SNR), and feeds it back to the BS. In order to benefit from the instantaneous channel situation, and, therefore, improving the average system performance, the BS scheduler accomplishes a smart user selection by choosing the user with the largest SNR value for transmission. This opportunistic strategy is proved to be optimal [11, 14] as it obtains the maximum rate point.

We consider a multiantenna downlink systems where the transmitter at the BS is provided with n_t transmitting antennas, while V receivers exist in the scenario, each one of them equipped with a single-receiving antenna. The case of $n_t = 2$ is considered along the paper for easiness in the results presentation and to align with all commercial implementations of the IEEE 802.11 *pre-n* and the proposals for all 4G-LTE systems. Neglecting the (k,n) components to provide a general system model that can be also employed for the Alamouti scheme, the channel $\mathbf{h}_{[1\times n_t]} = [h_1 \;\; h_2]$ is considered between the transmitting antennas and each one of the users, where a quasistatic block fading model is assumed with independent and identically distributed (i.i.d.) complex Gaussian entries $\sim \mathcal{CN}(0,1)$. Let $\mathbf{x} = [x_1 \;\; x_2]^T$ be the $n_t \times 1$ transmitted vector, while denote $r(v)$ as the received signal at the vth receiver as

$$\begin{aligned} r^{(k,n)}(v) &= \mathbf{h}^{(k,n)}(v)\mathbf{x} + z^{(k,n)}(v) \\ &= h_1^{(k,n)}(v)x_1 + h_2^{(k,n)}(v)x_2 + z^{(k,n)}(v), \end{aligned} \tag{10}$$

where $z^{(k,n)}(v)$ is an additive Gaussian complex noise component with zero mean and a unit variance. The transmitted signal $\mathbf{x}$ is a coded version of the i.i.d. data symbols s_i with $E\{|s_i|^2\} = 1$. For ease of notation, the n component is dropped whenever possible to concentrate on the proposed spatial domain processing.

The generated interference in the system due to the non-employment of the CP is one of the drawbacks due to considering OFDM-OQAM in current commercial systems. On the other hand, the MIMO technology is already available in almost all OFDM-based wireless standards (e.g., IEEE 802.11n, IEEE 802.16e/m and LTE). The MIMO system is mainly devoted to increase the system data rate and/or quality of service, but it can be also employed to accomplish interference mitigation in the system, such mitigation is already known in the research arena through several schemes like space time coding [15] and zero forcing beamforming [25], among others. To apply interference cancellation over OFDM-OQAM systems is a challenging matter due to the time-frequency interference pattern in Table 2, but it would be a very important achievement for the OFDM-OQAM system, as the interference cancellation stands as one of the main milestones to make the OFDM-OQAM to be attractive, avoiding extra interference cancellation complex mechanisms at the receiver side, reducing its complexity and making it suitable for implementation.

Table 3: OFDM-OQAM proposed setup in a two-antenna scenario.

	Subchannel 1	Subchannel 2
Antenna$_1$	d_1 on PPN_1	d_2 on PPN_2
Antenna$_2$	d_1 on PPN_2	d_2 on PPN_1

The consideration of MIMO with $n_t = 2$ enables two simultaneous symbols to travel in the channel at the same time and through the same subchannel. Table 3 shows a possible setup for the OFDM-OQAM transmission over 2 subchannels and on a single time instant (i.e., $k = 1, 2$ and n is dropped from the formulations), where the PPN order is switched over the two antennas.

From Table 3, notice that the two antennas are employed to provide the system with a space-time block coding scheme that will be later employed to cancel the interference at the receiver side through some signal processing. With the shown setup, the second antenna is employed to transmit the same information as in the first antenna, implementing the same principle as the very well-known Alamouti scheme [15]. For sure, some modifications are required to enable

its application to the OFDM-OQAM technology with its characterizing large amount of generated interference.

Considering this setup, the received signal $r^{(1,n)}$ in the first subchannel states as

$$r^{(1,n)} = \left(d^{(1,n)} + jf^{(1,n)}\right)h_1 + \left(d^{(1,n)} + jf^{(1,n)}\right)h_2 + z^{(1,n)}, \tag{11}$$

where as previously explained, $z^{(1,n)}$ is the noise term received in the subchannel 1, and $f^{(1,n)}$ accounts for all the interference components [23] that arise from the filterbank usage at the first subchannel, as presented through Table 2. On the other hand, the received signal in the second subchannel is as

$$r^{(2,n)} = \left(jd^{(2,n)} + f^{(2,n)}\right)h_1 + \left(jd^{(2,n)} + f^{(2,n)}\right)h_2 + z^{(2,n)}, \tag{12}$$

with $f^{(2,n)}$ as the interference terms in the second subchannel.

The reader can consider a hypothetical case that h_1 and h_2 show equal values in magnitude and opposed in phase, killing the received signal, as the two signals coming from the two antennas will cancel each other, and no signal will reach the receiver. We should remark that this situation has a low probability to happen [15], and even of that, this case would fail in the system outage consideration, exactly as the Alamouti scheme does [15].

3.1. Receiver Processing. Through the proposed transmission scheme, now the receiver has two different arriving signals $r^{(1,n)}$ and $r^{(2,n)}$, one on each subchannel. Note that a whole symbol (i.e., both its real and imaginary parts) is transmitted over two antennas operating on two subchannels (i.e., one single OFDM carrier) and on one time instant, then a full diversity rate [15] is obtained. With the proposed scheme, the two antennas are be efficiently employed in the system to help mitigating the generated OFDM-OQAM interference, thus decreasing the OFDM-OQAM complexity.

At the receiver side, the following low-complexity processing is accomplished to obtain the expression from $r^{(1,n)}$ as

$$\begin{aligned} y_1 &= \mathrm{Re}\left\{h_1^* r^{(1,n)} + h_2 r^{(1,n)*}\right\} \\ &= \left(|h_1|^2 + 2\,\mathrm{Re}(h_1^* h_2) + |h_2|^2\right)d_1 \\ &\quad + \mathrm{Re}\left(h_1^* z^{(1,n)}\right) + \mathrm{Re}\left(h_2 z^{(1,n)*}\right), \end{aligned} \tag{13}$$

where we can see that all the interference terms $f^{(1,n)}$ are removed thanks to the receiver processing. This is a very important step for OFDM-OQAM as the interfering terms have disappeared without the need to complex operations at the receiver side. Unfortunately, some dependence on the channel phase is generated with the receiver processing, due to the $2\,\mathrm{Re}(h_1^* h_2)$ term, that can show positive and negative values depending on the instantaneous channel conditions of both h_1 and h_2. A great spatial antenna gain is presented in the system, as the information in $d^{(1,n)}$ is received through both h_1 and h_2. Moreover, the data component $d^{(1,n)}$ is received without any other data components, so that with the simple Matched Filter (MF) receiver, the data can be efficiently extracted. Another equation is required for the detection of $d^{(2,n)}$, as the single symbol is composed from its real part $d^{(1,n)}$ and its imaginary part $d^{(2,n)}$, where both parts are compulsory for a correct detection.

The equation for $d^{(2,n)}$ is obtained by applying a different processing for subchannel 2 at the receiver side, to get

$$\begin{aligned} y_2 &= \mathrm{Im}\left\{h_1^* r^{(2,n)} + h_2^* r^{(2,n)}\right\} \\ &= \left(|h_1|^2 + 2\,\mathrm{Re}(h_1^* h_2) + |h_2|^2\right)d_2 \\ &\quad + \mathrm{Im}\left(h_1^* z^{(2,n)}\right) + \mathrm{Im}\left(h_2^* z^{(2,n)}\right), \end{aligned} \tag{14}$$

where we also notice that there is not any interference term in the equation.

The symbol detection, through its $d^{(1,n)}$ and $d^{(2,n)}$ parts, is now solved as no more OFDM/OQAM interfering terms are shown in the previously presented equations. The only remaining problem to be solved is the channel phase effect due to the $\mathrm{Re}(h_1^* h_2)$ term.

The received SNR for the presented scheme is, therefore, obtained as

$$\mathrm{SNR} = \frac{1}{2}\frac{\left|\,|h_1|^2 + 2\,\mathrm{Re}(h_1^* h_2) + |h_2|^2\,\right|^2}{\left|\,\mathrm{Re}(h_1^* z^{(1,n)}) + \mathrm{Re}(h_2 z^{(1,n)*})\,\right|^2} = \frac{A}{2B}, \tag{15}$$

where the 1/2 value is due to the separate reception of the two parts of the symbol, therefore, the power of $d^{(1,n)}$ is half the power of the original symbol s, which was defined to be unity. Now, we must develop this formulation to see how suitable is the obtained SNR expression and how it can be further improved. Remind that each one of the channel entries (e.g., h_1) is distributed as an i.i.d. complex Gaussian variable $\sim \mathcal{CN}(0,1)$, so that it has both a real and imaginary components $h_1 = h_{11} + jh_{12}$ and $h_2 = h_{21} + jh_{22}$, where each one of these components is distributed as an i.i.d. Gaussian variable $\sim \mathcal{N}(0, 1/2)$. With these clarifications and under the consideration of i.i.id. noise component, the expression of the denominator can be further developed to obtain

$$\begin{aligned} B &= \frac{1}{2}\left(|h_{11}|^2 + 2h_{11}h_{21} + |h_{21}|^2 + |h_{12}|^2 + 2h_{12}h_{22} + |h_{22}|^2\right) \\ &= \frac{1}{2}\left(|h_1|^2 + 2h_{11}h_{21} + |h_2|^2 + 2h_{12}h_{22}\right). \end{aligned} \tag{16}$$

Now, considering the numerator A in order to simplify the SNR expression, the value of $2\,\mathrm{Re}(h_1^* h_2)$ can be formulated as

$$2\,\mathrm{Re}(h_1^* h_2) = 2h_{11}h_{21} + 2h_{12}h_{22}, \tag{17}$$

and, therefore, the SNR expression in (15) stands as

$$\mathrm{SNR} = |h_1|^2 + 2\,\mathrm{Re}(h_1^* h_2) + |h_2|^2. \tag{18}$$

Notice that the channel phase effect can be positive or negative, where the value of $2\,\mathrm{Re}(h_1^* h_2)$ has a symmetric distribution over the zero point, as it is only composed of Gaussian $\sim \mathcal{CN}(0,1)$ variables. Obviously, the receiver is interested in a positive value for the channels phase effect, so that the decoding process is improved.

In order to compare this proposal to current systems, we notice that for a fair comparison, we must consider the Alamouti scheme [15] that is applied over OFDM and following the same power restrictions that are imposed in the system model section. The obtained SNR expression for such strategy [15] is as

$$\mathrm{SNR}_{\mathrm{alam}} = |h_1|^2 + |h_2|^2, \tag{19}$$

which is shown to provide very good system performance, and it is already included in several broadband wireless communication standards. Comparing the SNR expressions in (18) and (19), we notice that the only difference relates to the channel phase effect $2\,\mathrm{Re}(h_1^* h_2)$ value. As already commented, this value can be either positive or negative with an equally distribution for its sign. If we consider the average performance, then the two SNR expressions will be equal on the long run, but with different Bit Error Rate (BER) behaviour, as the variance of the expression in (18) is larger due to the additional phase term, thus with lower BER performance. This is a severe disadvantage of the proposal up to now, so that some improvement must be accomplished in order to make it more suitable and therefore, not only the CP gain, the synchronization and the scalability advantages are presents, but also a gain in terms of the rate and BER behaviours. The only problem that remains to solve is the effect of the phase term, as we only require it to show a positive value, where the solution to this problem is obtained through the multiuser gain, as next shown.

When several users exist in the system, the system administrator can benefit from the channel conditions of the available users in the system to select the user with the best channel conditions, for what is known as the multiuser system gain [11]. Several modern wireless communication standards [26] employ such opportunistic scheduling in its operation to increase their performance, and as OFDM/OQAM is targeted to high data rate systems, then we will tackle our objective through the opportunistic scheduler. This objective can be accomplished if we define the opportunistic scheduling as looking to select the user v showing

$$\max_{v=1:V}\left(|h_1(v)|^2 + 2\,\mathrm{Re}\left(h_1(v)^* h_2(v) + |h_2(v)|^2\right)\right), \tag{20}$$

to guarantee that the phase channel effect is always beneficial to the system performance.

On the other hand, the Alamouti scheme can be also operated with an opportunistic scheduler, where the selected user will be the one showing

$$\max_{v=1:V}\left(|h_1(v)|^2 + |h_2(v)|^2\right), \tag{21}$$

where the Alamouti scheme is proved [27] to highly benefit from the multiuser gain.

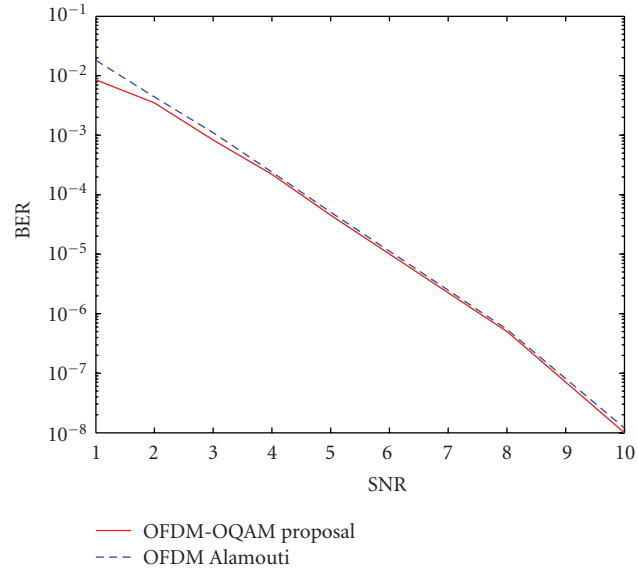

Figure 4: BER performance of Classical OFDM Alamouti and the OFDM-OQAM proposal, both in a multiuser scenario.

It remains to confirm that our proposal outperforms the Alamouti one, and this can be accomplished if we prove that the sign of the phase effect is always positive. We do not concern about the phase distribution, but only about its sign distribution. Notice that the opportunistic selection in the OFDM/OQAM proposal will offer better performance as long as the user with best channel characteristics shows a positive value for the phase effect. The probability P to achieve such situation [28] can be easily formulated as

$$P = 1 - \left(\frac{1}{2}\right)^{V-1}, \tag{22}$$

where as expected, increasing the number of available users V will drive an improvement in the probability of better performance of the OFDM/OQAM proposal in comparison to the Alamouti scheme.

4. Simulations

To see the behaviour of the proposed scheme, extensive computer simulations are run on a wireless scenario with $n_t = 2$ transmitting antennas and a variable number of users each one equipped with a single antenna. The transmitter is implementing a spatial diversity scheme over OFDM-OQAM, where a total transmitted power $P_t = 1$ is assumed. A total system bandwidth of 1 MHz is considered in this scenario.

In a first comparison, we consider the BER performance of the proposed scheme in comparison to the standard OFDM Alamouti strategy, both operated in an opportunistic multiuser scenario with 10 users, where the BS carries out the scheduling of the user with the best channel conditions following the selection algorithms in Section 3.1. The results are shown in Figure 4 where both techniques present a very similar behaviour and slightly better for the OFDM-OQAM

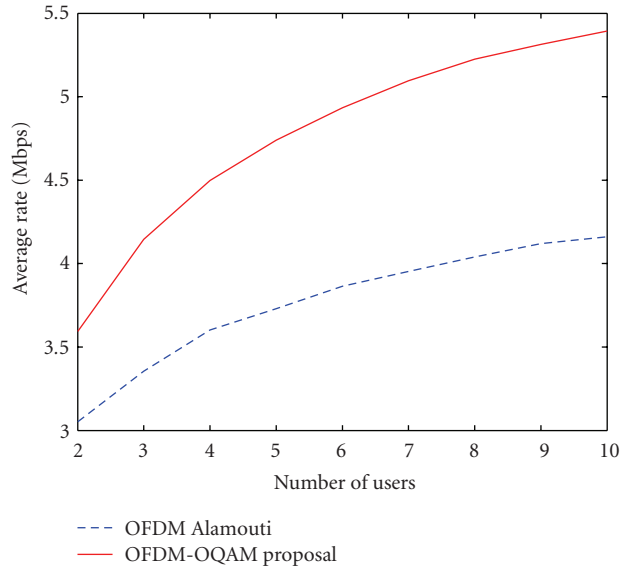

Figure 5: Rate performance of classical OFDM and OFDM-OQAM, both operated in the spatial diversity philosophy and within a multiuser scenario.

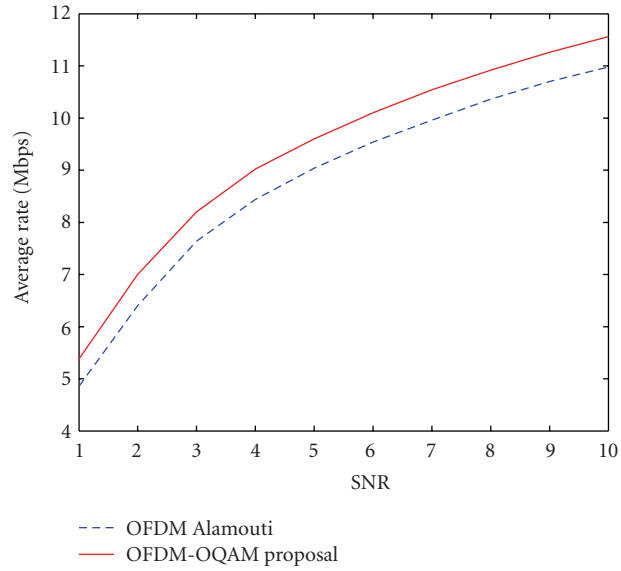

Figure 6: Rate performance of classical OFDM and OFDM-OQAM, both operated in the spatial diversity philosophy and with a variable SNR value.

proposal. This indicates that the reception quality is very close between the two schemes, which is an encouraging aspect, as all the benefits from the OFDM-OQAM system come at no cost on the reception quality.

One of these improvements is shown in Figure 5, where a scenario with a variable number of users is simulated. The comparison between the classical OFDM Alamouti scheme and the proposed OFDM-OQAM shows the better performance of our proposal, obtaining a higher benefit from the multiuser system capabilities. Obviously, this gain comes from the resource saving as the OFDM-OQAM proposal does not employ the CP, that is assumed to be 12.5% which is the most typical value within the in commercial standards [3]. But also, the multiuser gain is employed in a better approach by the OFDM-OQAM proposal, as shown in Section 3.1.

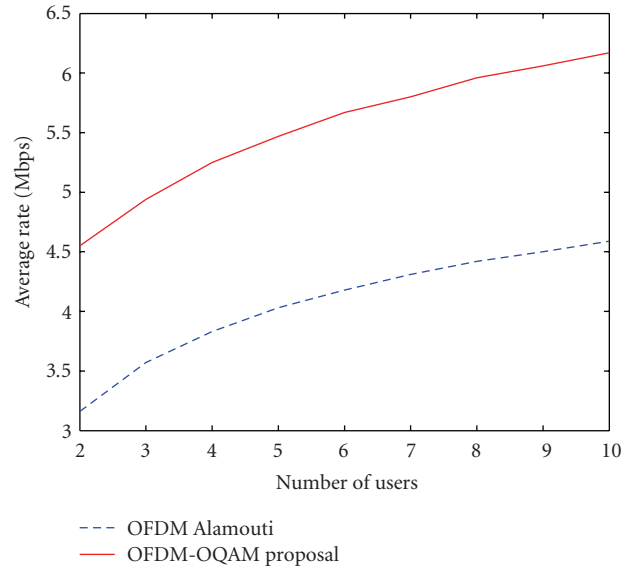

Figure 7: Rate performance of classical OFDM and OFDM-OQAM, both operated in the spatial diversity philosophy and within an Outdoor multiuser scenario.

To check for the system performance under different values of average SNR, we fix the number of users and vary in the SNR value to check for the proposal behaviour within different scenario conditions. Figure 6 shows a comparison between the proposed scheme and the standard Alamouti strategy applied over the same scenario for a fair comparison. The results show how both schemes have almost the same data rate enhancement for an increase in the SNR operating value, but all the time, being the OFDM-OQAM proposal larger than the standard Alamouti technique.

The last consideration for different scenarios to check for our proposal is in an outdoors channel, as both OFDM and the MIMO technologies have been also proposed for outdoor channels. The channel model for outdoor urban scenarios can be modeled as single or two cluster scenarios, where the channel is regarded as a large dominant component affected by multipath propagation, so that there exists a considerable angle spread at each receiving end. Moreover, the direction of arrival does not necessary match with the exact user position due to the reflections that each signal undergoes. The paper adapts a single-cluster outdoor channel model [29] with an angle spread value of $AS = 10$ degrees, and the results are shown in Figure 7. As we can see from the figure, the proposed OFDM-OQAM also outperforms the Alamouti scheme in outdoor scenarios, where the performance of both strategies are improved due to the more directionality that appears in the outdoors channels, and as the BS can select the user with best channel characteristics, then a better

directionality search is performed. From all the above figures, we realize that our OFDM-OQAM proposal outperforms the Alamouti strategy, and without the need of the CDMA spreading codes proposed in [12].

5. Conclusions

A spatial diversity scheme over OFDM-OQAM is presented along the paper to enable the implementation of OFD-OQAM in realistic systems. This is thanks to the required low-complexity processing at the receiver side that allows to totally cancel the OFDM-OQAM generated interference. In order to enhance the system data rate and BER performance, a selection of the user with best channel conditions at each transmitting instant is performed through an opportunistic scheduler at the transmitter side. To the authors' knowledge, no previous proposals have been presented in the literature to deal with such scenario setup.

The paper formulated the results of the proposed scheme in terms of data rate and BER and mathematically obtained the SNR expression. The results indicate that OFDM-OQAM proposal stands as a potential alternative to the classical OFDM for its consideration in realistic systems. Moreover, the proposed scheme does not employ the CP, which is a further increase in the system efficiency. Its advantages in terms of scalability and synchronization can be also attractive for the system. Therefore, OFDM-OQAM can be employed in certain scenarios upon the requirements and restrictions for the system designer.

Acknowledgment

This work was partially supported by the European ICT-2008-211887 project PHYDYAS, COST Action IC0902, Generalitat de Catalunya under grant 2009-SGR-940 and Jordan University project (DAR162). This work was partially presented at the International MobiLight conference, Athens, Greece, 2009.

References

[1] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems*, John Wiley & Sons, New York, NY, USA, 2003.

[2] K. Baum, B. Classon, and P. Sartori, *Principles of Broadband OFDM Cellular System Design*, Wiley-Blackwell, Hoboken, NJ, USA, 2009.

[3] IEEE 802.16e-2005, "IEEE Standard for Local and Metropolitan Area Networks Part 16," 3GPP, 2006.

[4] "Physical layer for dynamic access and cognitive radio," European Project ICT 211887, PHYDYAS, http://www.ict-phydyas.org.

[5] European COST Action IC0902, "Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks," January 2010, http://newyork.ing.uniroma1.it/IC0902.

[6] M. Bellanger, "Transmit diversity in multicarrier transmission using OQAM modulation," in *Proceedings of the 3rd International Symposium on Wireless Pervasive Computing (ISWPC '08)*, pp. 727–730, Santorini, Greece, May 2008.

[7] M. Bellanger, T. Ihalainen, and M. Renfors, "Filter bank based cognitive radio physical layer," in *Proceedings of the ICT Mobile and Wireless Communications Summit (ICT-Mobile Summit '09)*, Santander, Spain, June 2009.

[8] B. Hirosaki, "A maximum likelihood receiver for an orthogonally multiplexed QAM system," *IEEE Journal on Selected Areas in Communications*, vol. 2, no. 5, pp. 757–764, 1984.

[9] M. El Tabach, J.-P. Javaudin, and M. Hélard, "Spatial data multiplexing over OFDM/OQAM modulations," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 4201–4206, Glasgow, UK, June 2007.

[10] T. Fusco and M. Tanda, "Blind frequency-offset estimation for OFDM/OQAM systems," *IEEE Transactions on Signal Processing*, vol. 55, no. 5, pp. 1828–1838, 2007.

[11] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1277–1294, 2002.

[12] Ch. Lele, P. Siohan, and R. Legouable, "The Alamouti Scheme with CDMA-OFDM/OQAM," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, Article ID 703513, 2010.

[13] I. Estella, A. Pascual, and M. Payaro, "OFDM and FBMC performance comparison for multistream MIMO systems," in *Proceedings of the Future Networks Summit*, Florence, Italy, June 2010.

[14] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proceedings of the IEEE International Conference on Communications (ICC '95)*, pp. 331–335, Seattle, Wash, USA, June 1995.

[15] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[16] B. Farhang-Boroujeny and R. Kempter, "Multicarrier communication techniques for spectrum sensing and communication in cognitive radios," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 80–85, 2008.

[17] H. Zhang, D. Le Ruyet, D. Roviras, Y. Medjahdi, and H. Sun, "Spectral efficiency comparison of OFDM/FBMC for uplink cognitive radio networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, Article ID 621808, 2010.

[18] M. Shaat and F. Bader, "Low complexity power loading scheme in cognitive radio networks: FBMC capability," in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '09)*, Tokyo, Japan, September 2009.

[19] H. Zhang, D. L. Ruyet, and M. Terre, "Spectral efficiency analysis in OFDM and OFDM/OQAM based cognitive radio networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC '09)*, Barcelona, Spain, April 2009.

[20] P. Siohan, C. Siclet, and N. Lacaille, "Analysis and design of OFDM/OQAM systems based on filterbank theory," *IEEE Transactions on Signal Processing*, vol. 50, no. 5, pp. 1170–1183, 2002.

[21] M. Bellanger, *Filter Banks, Digital Processing and Signals: Theory and Practice*, chapter 11, John Wiley & Sons, New York, NY, USA, 3rd edition, 2000.

[22] A. Viholainen, T. Ihalainen, T. H. Stitz, M. Renfors, and M. Bellanger, "Prototype filter design for filter bank multicarrier transmission," in *Proceedings of the European Signal Processing Conference (EUSIPCO '09)*, Glasgow, UK, August 2009.

[23] M. G. Bellanger, "Specification and design of a prototype filter for filter bank based multicarrier transmission," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01)*, pp. 2417–2420, Salt Lake City, Utah, USA, May 2001.

[24] C. Lélé, J.-P. Javaudin, R. Legouable, A. Skrzypczak, and P. Siohan, "Channel estimation methods for preamble-based OFDM/OQAM modulations," in *Proceedings of the European Wireless Conference (EW '07)*, Paris, France, April 2007.

[25] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 528–541, 2006.

[26] 3GPP, "Practical aspects of multiple architectures for HSDPA," Tech. Rep. TSGR1#16 (00)1219, 2000.

[27] J. Akhtar and D. Gesbert, "Extending orthogonal block codes with partial feedback," *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 1959–1962, 2004.

[28] M. R. Spiegel, *Theory and Problems of Probability and Statistics*, McGraw-Hill, New York, NY, USA, 1992.

[29] D. Gesbert, L. Pittman, and M. Kountouris, "Transmit correlation-aided scheduling in multiuser MIMO networks," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '06)*, pp. 249–252, Toulouse, France, May 2006.