International Journal of Computer Science and Security (IJCSS)

ISSN : 1985-1553

VOLUME 2, ISSUE 3

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

Editor in Chief Dr. Haralambos Mouratidis

International Journal of Computer Science and Security (IJCSS)

Book: 2008 Volume 2, Issue 3
Publishing Date: 30 - 06 - 2008
Proceedings
ISSN (Online): 1985 -1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 2, Issue 3, June 2008.

Pages

Camera Ready of the Manuscript

Title:

TOWARD THE RECOGNITION OF USER ACTIVITY BASED ON USER LOCATION IN UBIQUITOUS COMPUTING ENVIRONMENTS

Accepted to

International Journal of Computer Science and Security
ISSN: 1985-1533 (Online-Open Access)

Date

3 August 2008

TOWARD THE RECOGNITION OF USER ACTIVITY BASED ON USER LOCATION IN UBIQUITOUS COMPUTING ENVIRONMENTS

Teddy Mantoro teddy.mantoro@anu.edu.au
Department of Computer Science
The Australian National University
ACT 0200, Australia

Media A. Ayu media@staff.gunadarma.ac.id
Department of Industrial Engineering
University of Gunadarma, Indonesia

Abstract

Human Activity is not a well defined concept in Ubiquitous Computing discipline because human activity is very complex and the computer environment is very limited in capturing user activity. However, user activity is an essential ingredient for the determination of appropriate response from Intelligent Environment in order to provide appropriate services with or without explicit commands. This paper describes an approach to the determination and recognition of user activity based on user location. The characterisation of user activities can be deduced from sensor activities based on the scalable distribution of context location information. This approach does not require users to label their activities.

Keywords: User Activity, User Location, Smart Sensors, Ubiquitous Computing, Intelligent Environment.

1. INTRODUCTION

Scientists in the Ubiquitous Computing area are researching ways to make embedded computing and Ubiquitous Computing work better for people by creating and equipping an Intelligent Environment, such as an active home or an active office, with technologies that can identify the user's needs and meet them speedily, efficiently and unobtrusively.

The goal of Ubiquitous Computing in general is to make user interaction with the computer easier in the Intelligent Environment where technology is spread throughout (pervasive), computers are everywhere at the same time (ubiquitous) and technology is embedded (ambient) in that environment. The context-aware application should reduce the load of the user and adapt to users seamlessly [1,2]. While a user is doing his daily activities, his access to the Intelligent Environment should not be difficult, tedious or need considerable learning on the part of the user. The interaction should be safe, easy, simple and enable new functionality without need to learn a new technology. As human activity is a central part of the user context [1], the context-aware system would provide relevant information and a simple way for a user to deal with the computing environment. Context information cannot be supplied by the user. It should be sensed automatically using sensors in the computing environment, in making these smart environments have the capability to assist people with a variety of activities by detecting a users' current state/context to determine what actions to take based on that context.

An important problem in an Intelligent Environment is how the system could characterise user situation based on user activity, where user activity is based on any objects (such as smart

sensors) being in action relating to a particular person's use. It could provide complex and rich information which is relevant to the situation/domain being examined.

This information is used to characterise the situation of user entity and environment entity. The user entity is a person being in the environment, and an environment entity is an indoor or outdoor space that is embedded/equipped with smart sensors. A set of user activities can be identified by reading and interpreting any association between a user (user entity) and smart sensors (in the environment entity).

In an indoor space such as home environment, the benefit of such technology might simply be convenience and enjoyment at home, for example, knowing when the occupant wakes up and what radio station they like to listen to without waking up the rest of the house. On the other hand, the active home could be life saving by detecting when an occupant collapses and needs medical help.

For an office environment, the benefit would be the capability in measuring user productivity. If user productivity is a goal of the use activity, then it can be measured by counting the number of tasks completed per unit of time, and can also convert these measurements to measurements of time per task. Our approach is to locate a person within an environment using wireless connections in devices that are normally carried for other purposes, for example, a mobile phone, PDA or a laptop computer. The location of these devices, and hence the person with them, is determined by a mixture of precise, proximate and predicted location sensors. The data from these sensors is turned into a predictor to precisely locate the device, and thus the person. Once a user is located, such services can be delivered based on the current situation from a resources manager.

User activity can be shown from sensor activity in capturing changes in state, time and location. To manage and respond to rapidly changing aggregated sensor data, DiCPA architecture [3] is used. This scalable distribution context processing architecture in the Intelligent Environment allows continued operation across changing circumstances for users, the collection of nearby people and objects, accessible devices and changes to those objects over time in the environment. The DiCPA architecture is implemented to recognise user location and user mobility. This could lead to the understanding of the concept of user activity. The context information of this user activity can be used to characterise the user situation.

This paper contributes mainly to 1. the study of user activity based on location in smart environment which proposes an approach to the determination and recognition of user activity based on user location. 2. propose the strategy in providing service to unregistered (guest) user as a unique perturbation situation in office environment, including how to estimate the location of this type of users (Section 5).

In the following section, a related work in user activity area is also discussed, followed by 1. the user activity concept, 2. Activity-Based processing model 3. the role of user location to user activity 4. Mobile Access Point concept and 5. monitoring user activity. The paper is closed by conclusion and closing remarks.

2. RELATED WORK IN USER ACTIVITY

In the current literature, researchers who work in the area of user activity fall into three categories, they: 1. develop equipment using wearable devices to be worn by the user to sense user activity and recognise user location, 2. study user behaviour in the workplace area and home, and 3. develop a system/device to equip the environment (Figure 1).

Firstly, in the area of wearable devices, it is possible to determine a user's location using a dead-reckoning method to detect the transition between pre-selected locations, and recognise and classify sitting, standing and walking behaviours, for instance in [4].

Secondly, in the study of user behaviour, user activity changes in work and society are impinging on the place where the user works and how the work gets done. For example, the increasingly international nature of work has led to a growing amount of travel despite the use of advanced collaboration technologies [5]. It has been argued that many more people are experiencing a blurring of the division between 'home' and 'work' domains as different forms of work become possible within the physical space of home.

While Koile proposes activity zones to construct an activity area, Crabtree introduces communication places. Activity zones have a physical form – e.g. wall, furniture – which partition places into zones of human activity and places of communication that are familiar at home as areas of production, management and consumption of communication. Activity zones were constructed by tracking systems to observe people's activities over time. Crabtree considers three different properties: ecological habitats, activity centers and coordinate displays. Activity centers are places where media are actively produced and consumed and where information is transformed [6,7].

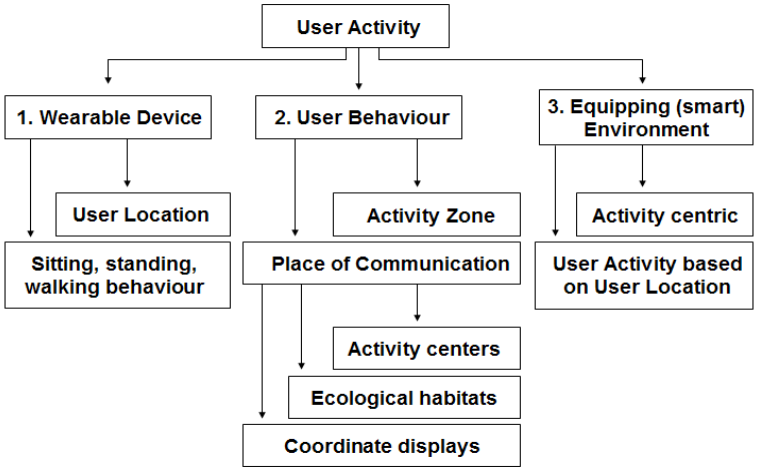

FIGURE 1: Research Categories in the Area of User Activity

Thirdly, in the area of developing a system/device to equip the environment, Prekop and Burnett [8] developed an Activity-Centric context, i.e. context-aware applications that are capable of supporting complex and cognitive user activities in a smart room. Mantoro studied user mobility based on user location leading to user activity in the Active Office [9]. As mentioned earlier, this work mainly proposes an approach to the determination and recognition of user activity based on user location in a smart environment.

Currently, there are a number of smart environments already in use in research organisations, for example, MIT's Intelligent Room [10], Stanford iRoom Project [11], NIST's Smart Space Lab [12], Georgia Tech's Aware Home project [13] and ANU's Active Office [3,9,14,15].

To provide a dynamic environment of located-objects, Schilit [16] proposed Active Map Geographic Information to manage information about the relationship that exists between locations. In people's daily lives, two kinds of spatial relationships are commonly used: containment and travel distance. In addition, Schilit also mentioned that Euclidian distance between positions within a coordinate system are not suitable for human activity.

Related study in user activity also considers the social aspect of the user. The user social aspect research area mostly studies in user dimensions, instead of environment dimensions or technological aspects, such as the study of the use-of-time [17]. Time use studies typically have a single focus: to study the frequency and duration of human activities.

According to Stinson [18], the use-of-time for Canada's telephone administration can be placed into two categories, i.e. firstly **in places**, such as a respondent's home, a workplace, at someone else's home, at another place (including park, neighbourhood); and secondly **in transit**, such as in a car (driver or passenger), walking, in a bus or subway, on a bicycle, others (airplane, train, motorcycle). Throughout the world, most of the currently used activity classification systems have evolved from the original structure developed by Alexander Szalai for the Multinational Time-Use Project of the 1960s. These activity codes are typically arranged into mutually exclusive behaviour groups that cover all aspects of human activity. These primary divisions of behaviour, which may be considered for the study of user activity in the Intelligent Environment, generally include:

- Personal care activities
- Employment related activities
- Education activities
- Domestic activities
- Child care activities
- Purchasing goods and services
- Voluntary work and care activities
- Social and community activities
- Recreation and leisure
- Travel time

However, the recent technically advanced studies in Active Badge/Bat (Cambridge), Wearable Computing (University of South Australia), Cricket (MIT), and Smart Floor are also enabling the creation of such Intelligent Environments in capturing and understanding user activity [19,20,21,22]. These advances in technology to equip the environment have demonstrated the potential to observe user activity, but have also shown that these kinds of systems are still extremely difficult to develop and maintain [3,23].

3. USER ACTIVITY CONCEPT

In the Context-Aware Computing or Ubiquitous Computing discipline, user activity is not a well defined concept, this may be because of:

- the transition between activities is sometimes not very clear,
- an activity can be seen as part of another activity,
- an activity can be in sequence mode (for example, open the door and followed by walking) or in parallel mode (for example, receiving phone call while walking) or both together,
- different views can be deduced from different activities.

For example, the difference between a running and walking activity; it needs clear variables to be defined, several variables which may involve, e.g., the length of the user's leg, the speed of movement, the number of steps taken in each minute, etc. When a user cleans his house, he needs to move or walk. Thus, it may not be clear whether the activity of the user is walking or cleaning the house. A different view and a different perspective can lead to the assumption of a different user activity.

User activity in the Intelligent Environment is divided into 4 categories:

a. activity as any association between a user and smart sensors in the environment
b. activity as a node in a work flow or job breakdown
c. activity as a physical movement mode or state
d. activity as a mode of state of human intent

In this study, user activity in an Intelligent Environment is defined as *a sequence of any association between a user and the smart sensors in the environment that can be determined and recognised as an activity.*

To recognise a user's activity while accessing resources, the context-aware application requires user identification. A user's identity can be captured from the user's mobile computing devices or user's image/voice recognition. Users can be characterised by several means, i.e., identification and authentication, user profile, user's terminal and user's access network characteristics, and service adaptation to user environment (the detail implementation is discussed in Section 7).

User characteristics can be recognised when any association exists between a user and smart sensors, and the association is recorded in a sensor database which contains information relating to user identity, sensor identity, location identity, time and state. The collection of this data, user activity history data, forms a pattern of the user's mobility and the regularity of a user's activity pattern also capable of being recognised. This pattern can predict a future user activity based on a user routine activity by querying the user activity pattern.

Many earlier projects acknowledge the need for the capability to capture user activity in the complex relationships between a user and the environment:

a. the activity as an essential ingredient for determining appropriate reactive behaviour as requirements for Response Offices at Xerox PARC [24].
b. the need for tracking activity such as EasyLiving at Microsoft acknowledges [25], or tracking activity of daily living to identify the short- and long-term changes in the health of elderly people [26].
c. the utilisation of the activity based approach such as in the second generation of iRoom at MIT [27]. This approach is similar to the activity-centric context model at DSTO, which have agents and activities as key components. The activity centric context model adopts a knowledge management approach to support the hand-over of artefacts from one individual or group to another. For example, to hand over a system design it is necessary to pass the formal artefacts of the design activity but it is also important to pass the tacit system design context, the mental models, assumptions and other factors that exist when the design was developed [28].

In our work, the capability to capture user activities outlined above was considered and followed the prediction of future user activity by the use of history data to form an activity pattern.

4. ACTIVITY-BASED PROCESSING MODEL

An activity-based approach uses the abstraction of the sensor data that is accessed by a user in the computing environment. In this part, the activity-based processing model will be discussed. The model has 5 stages as shown in Figure 2, i.e. Sensors, Smart Sensor, Resolver, Resources Manager, and Presentation.

Sensors

In recognising user activity, the principle questions are: How many sensors are needed to recognise a user activity and at what precision? Can activities be recognised using simple sensors that detect changes to the states of objects and devices in a complex office setting? The answer is sometimes simple, for a simple activity, a single simple sensor can often provide powerful clues to activity. For instance, a keyboard activity sensor can capture user typing activity and a pressure chair sensor can strongly suggest that a user is sitting on the chair, both types of sensors can show user location as well. However, these sensors cannot show other activity, such as that a user has a meeting activity. It also depends on the type, function and the capability of the sensor in capturing the user data.

An Active Office in this experiment has two types of sensors, i.e., proximate and fixed sensors. It uses proximate sensors, such as WiFi, Bluetooth, RFID and IrDA. These sensors have been used to sense user activity. The other sensors can be added as required by the room to capture user activity, such as UWB, eye-movement sensors, etc. For fixed sensors, magnetic phone sensors, pressure chair sensors, magnetic door sensors, keyboard activity sensors, mouse

activity sensors and swipe cards are used. Fixed sensors can also be extended to other sensors such as biometric/finger print sensor, iButton sensor, etc.

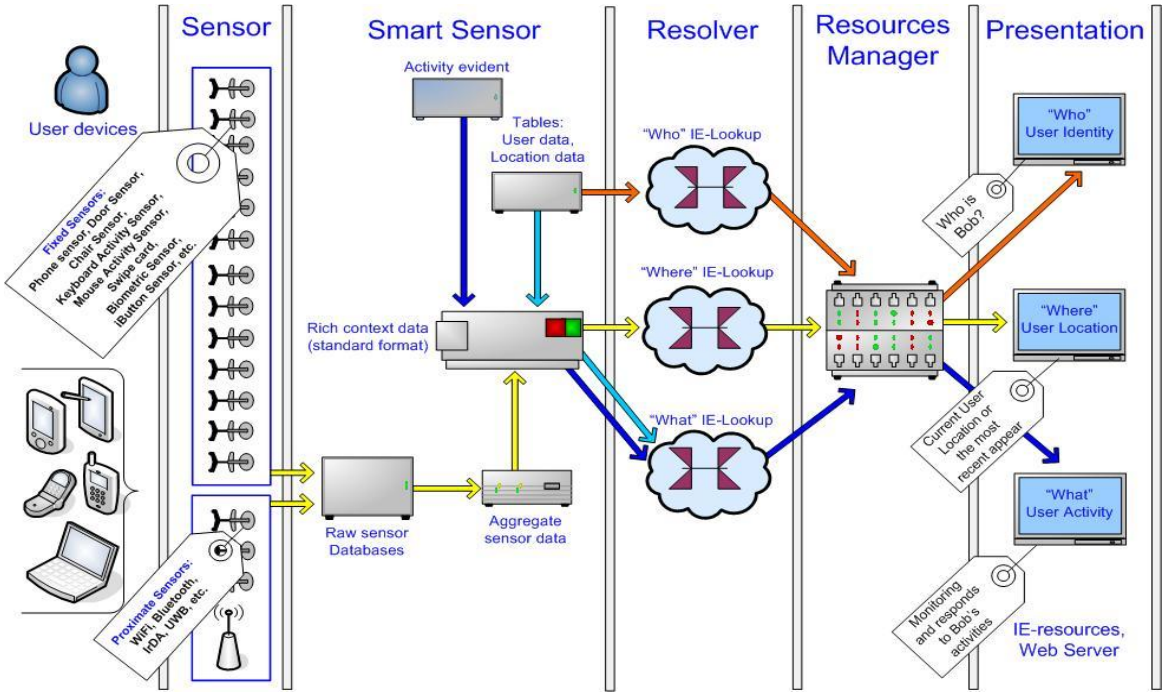

FIGURE 2 User Activity Processing Model

Smart Sensors

A smart sensor is one or more sensors (array sensors) with the integrated application that has the capability to make decisions for certain purposes including recognised user activity. Aggregation of sensor data is the only one of the processes in the sensor application to characterise user activity. The smart sensor is based on three kinds of data, i.e., raw sensor data, activity-evident data, and data-tables, such as user data-table, location data-table, etc. The raw sensor data which is recorded in a spatio-temporal database is a key entity for the smart sensor to deduce what kind of user context information is. Aggregate sensor data is the extracted data from a raw sensor database. The spatio-temporal database in this model can be used for two purposes, i.e.: speeding the process query and showing the scalability of the query.

Resolver

Resolver is the procedure for looking-up user identity, location and activity. This approach is similar to the DNS server lookup host table. DNS server can resolve host name to ip-address and vice versa. In our model, the resolver uses the DNS idea more widely, it resolves three variables i.e., User Id, Device Id and MAC address. It covers for a user to have several devices and the possibility for each device to have several MAC addresses, and hence possible for a user to have many identities in the environment. There are three functions of the resolver in this work that have been designed for Active Office purposes, i.e. 1. for user identity purposes, it uses user identity lookup tables; 2. for location purposes, it uses scalability of location lookup tables and 3. for user activity purposes, it uses several entities (databases) to deduce user activity.

Resource Manager

In Active Office's network management, a resource manager acts as the coordinator. It maps available resources. It contains agents such as resolution agent, inter-domain agent, ICMP agent, SNMP agent, Content Routing agent, etc. For user activity purposes, some of the resources manager's functions may not be used much, such as accepting the object's global name from the resolution server or the use as persistent mapping to request persistent location

from the resolution server. In this part, the resource manager's function is to coordinate the resources based on the status of the sensor data including the aggregate sensor data to provide a complete set of context-aware information which contains user identity, location and activity information.

Presentation

The presentation is in the form of response or action from IE. The pesentation is based on data processing from the resource manager. User activity can be shown whether virtually, in a web page, in computer monitoring (see Section 7), or in direct action to the user.

5. THE ROLE OF LOCATION TO USER ACTIVITY

When smart sensors sense a user and recognise a user location, the possible activity of the user can be estimated based on the user location itself. For example, in Table 1, when a user is found in his office (N235), the possible activities in his room are working on the computer, working on his table, using the telephone, or having a meeting. The user activity is not reported by the user while he is on the move. In this section, how to recognise user activity based on sensor data will be discussed. This approach does not need the subject to label his activities such as in [28, 29], where it could be difficult to adapt to individual patterns of activities.

To clarify the tree of the user activity, some parts of user activity can be formed in a tree structured as follows:

- Working on the computer
  - Office Application
    - Word processing
    - Spreadsheet
    - Presentation software
  - Mail agent
    - Read email
    - Forward and write email
    - New email and write email
  - Web application
    - Download paper/image
    - Searching information
    - Web email
      - Read email
      - Forward and write email
      - New email and write email
    - Monitoring equipment
- Working on the table
  - Read a paper
  - Make a note
  - writing a paper
- On the phone
  - Internal call
  - Local call
  - Inter-local call
  - International call
- Meeting
  - Meeting with staff
  - Have a guest
  - Meeting with supervisor

When a user is working on the computer, the mouse and keyboard activity sensors can be used to detect in which windows and with which applications the user is engaged. Hence, when the location sensor finds his location is in room N235, the mouse and keyboard sensor can then

report an activity such as user id, windows and application. These could then be used to deduce the type of user activity.

In the case of a user working with email, there are many ways to access email, such as remote access and open mail agent, create a pop email script and convert to special word format, etc. This is not recommended in the Active Office, because it will lead to difficulties in recognising user activity. In the Active Office, working with email is only recognised when a user makes common use of a regular mail agent (such as Microsoft Outlook, Mozilla Thunderbird, Eudora, Pine, etc.) or web-mail (such as mail.google.com, mail.yahoo.com, etc.).

Recognising user activity when the user may be working on his table is not simple, so far in the Active Office only user location data have been recognised from WiFi signals, and chair sensor data using a pressure sensor that is embedded in the chair, but as yet no sensor has been embedded in the table. Once the Active Office has a pressure sensor covering the whole surface of the table, the Active Office will be able to deduce when the user is working on his table. However, the situation where a user works on his table is a different situation from that where the user is on the phone, since, as the Active Office has a phone sensor, it can be easily recognised when the user is having a phone call.

In the case where the user has a meeting, when it is found that other users are also in the same location (room) for a certain period, it can be deduced that the user has a meeting with other people. If the other user status is recognised as student then it is a meeting with a student, the same thing can happen when the user identity is found to be his supervisor. The context-aware application will deduce the activity based on the recognition of the user's identity. However, when there is a user/guest and his location is recognised but no identity is available, then the Active Office needs to find a way to recognise the existence of that user/guest, one option is by identifying his mobile device using resolver.

When a user leaves his office, user activity status will be undetectable. This status will be the same when the user does not allow the Active Office to detect his location. When a user's location is found to be in a seminar room, and it also matches with the seminar schedule, it can be deduced that joining the seminar is his user activity status.

Room	Visit (times)	Duration (minutes)	Possible Activities
N235	7	337	Working on the computer. Reading a paper. Make a note or writing a paper. Telephone. Meeting.
Undetectable	1	56	Out of office. Not allowed to detect.
Seminar	1	53	Join DCS seminar.
DCS café	1	16	Afternoon tea. Morning tea.
Corridor	9	9	Walk through.
Toilet	2	7	Toileting.
Stair Level 1	6	6	Walk through.
Resources Room	1	3	Picking up print out. Check mail. Fax. Binding. Pick up stationery/paper. Pick up reading material. Photocopy.

TABLE 1: Summary of a Staff Member's Activities on a One Day Observation.

A similar deduction may be made when a user is found in the DCS café; if he has stayed for more than 5 minutes and the time is in the morning about 11am, then it can be deduced that he has a morning tea activity. This applies also for afternoon tea activity.

When a user's location is found to be in a corridor or on the stairs, and his location changes at a reasonable speed, it can be deduced that he walks in a corridor/on stair activity. When a user's location is found in toilet for more than 3 minutes, it also can deduce that he may be so engaged.

Table 1 shows the summary of the duration of a staff member's activities on a one day observation, sorted by the duration of visits to rooms. The measurements are based on data collection using various fixed and proximate sensors. If proximate sensors reported user location, it used nk-Nearest Neighbour algorithm to estimate symbolic user location [30]. This table also shows that the user spent 69% of his office hours on that day in his office which may relate to the measurement of user productivity. This approach proposes the tagging of each room with the function of the room and how often the users have activities in a particular room.

To have a better understanding of the recognition of user activity based on location, activity zones can be created, as explained in [7]. Activity zones can be mapped by including observed location features in regions corresponding to activities or sets of activities. In this study, a 3-D pattern of user locations is not further explored, instead short-range sensors, such as an RFID sensor, which can be embedded in any Active Office object used to allow recognition of user activity. 3-D location of users or an RFID sensor is useful but alone is insufficient as context information. In this experiment, the raw RFID sensor data is combined with raw WiFi data.

The partition of space/zone is based on simple proximity or relies on user specified maps of regions. Location regions can be learned from observed activities, including user changes to location/motion. Each zone corresponds to a region in which a person is likely to be engaged in similar activities. Activity zones can overlap in space, since motion can indicate a different activity. This activity map can be used at run time to contextualise user preferences, such as allowing "location-notification" settings of messaging, environmental control and multi-media delivery [7].

For example in the case of a resources room in our department, as shown in Figure 3, if a user's location is found by WiFi sensors to be in the resources room, and RFID sensors in front of the Reading Material zone sense that a book has just been moved from the shelf, the Active Office can deduce that the user is picking up a book.

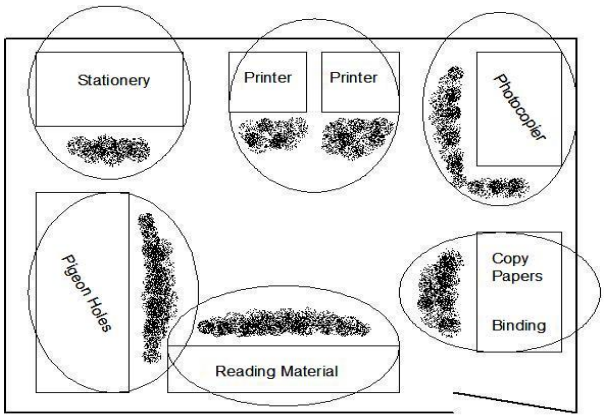

FIGURE 3 Access Zone in the Resources Room

A more complex application allows the recognition of a complex user activity by the addition of the semantic of an object (knowledge of objects such as chair, desk, and computer) and the semantics of human behaviour (such as people who come to the office around 9 am, read and write at a desk). In an Active Office, user activity depends on the type of organisation and the location/position. In the case of the University organisation, especially in the head of department room at department level, the most frequent activities are working on the computer, talking on the phone, having a guest, a staff meeting, or meeting with a student.

Some activities in the Active Office, such as in the University, could easily be detected, for example working on the computer or talking on the phone. However, recognising the difference between when the Head of Department is having a guest, and the Head of Department is meeting with a staff member or a student, is a still problem, since at the moment not all people have an identity that can be recognised by the Active Office. If user productivity is a goal of the Active Office, it can be measured by counting the number of tasks completed per unit of time, and can also convert these measurements to measurements of time per task [31].

The most complex activity occurs when a group of people share their activities. The social exchange and actions within a group of people have direct impact on group activity. A working group is situated in a rich context of organizational strategies and objectives, job roles and responsibilities, interpersonal relationships, task assignments and interdependencies and tool-handling and material resources [32] and makes the group's activities harder to understand than that of a single user's activity. This context is in the domain of user activities.

Group activity implies knowledge of how task components are identified, coordinated and carried out. Task components must be understood and pursued in the context of the overall purpose of a shared activity, the goals and requirements for completing it, and how individual tasks fit into the group's overall plan. When collaborative activity is carried out and the collaborators are in different time zones or cultures, it will not include face-to-face interaction and many interaction resources will be disrupted i.e., field of view is reduced, the possibility of gesture use is limited, facial expressions are eliminated/constrained, auditory cues are diminished, tools and artefacts cannot be as easily shared, deixis and spatial co-references are difficult to resolve [33,34]. It is also difficult to repair miscommunication.

6. MOBILE ACCESS POINT

Mobile Access point is an access point that is capable to follow a user or the user follows the access point, and to establish a connection to the network for that user and deliver service while the user is on the move. The purpose of the development of the mobile access point is to monitor user activity based on user location of "unregistered but legal" user or unknown device in the Active Office.

This will not only have implications for the context-aware application in providing service to the unregistered user, if it is allowed, but also to the development of the social policy of the environment as well, as a unique perturbation situation in an Active Office. The generic social scenario for this situation is when a staff member has a guest. A guest user, a user without enough knowledge of the local network, gains access to the Active Office and in the view of the guest user, Active Office is unfamiliar domain for the user. This is a unique situation in a social model in ubiquitous computing environment.

In an Active Office, a guest is a different user category from that of a visitor, such as visiting fellow, a guest may visit only for a couple of hours but a visitor may stay for several days and as a consequence of this situation, a visiting fellow may register in a local server, but a guest clearly may not.

"Having a Guest" Scenario

How Active Office provides support for a guest user to office resources is a common problem. Generally when a guest user/colleague comes to the office, he is under the responsibility of the staff member, especially if the guest has limited access to office resources.
For that purpose, the policy of the office needs to be developed, how confident the office administrator is of the network's security when it is accessed by an external user, such as a guest user, or other guest user categories (every guest user has his own characteristics and needs).
The social policies designed for "having a guest" in our Active Office follow the requirements below:

- A user (staff member) who is employed in an Active Office is allowed to have a guest.
- A guest user is under the responsibility of the staff member.
- Active Office provides support for a guest user to gain access to limited general resources but, for security reason, a guest cannot directly use his workstation.
- Mobile computing equipment (Notebook or PDA) of a staff member can be used as a Mobile Access Point for his guest user in accessing Active Office resources.
- A mobile access point can be used by the staff member and his guest user while they are on the move in an Active Office.
- At the same time, an Intelligent Environment application can locate a Mobile Access Point that turns to approximate guest user location.

In the implementation, a staff mobile device is set up as a mobile access point. This mobile access point is an access point for a guest user device to access the network. Staff members and their user guests can access the resources in the four buildings and the surroundings which have several fixed sensors and are covered by the wireless network. While they are on the move in the Active Office, these resources can be accessed anytime, anywhere.

The following is an example scenario of "having guests" in an Active Office.

> *John Blog has a smart personal assistant (SPA), a laptop with Linux Fedore, that uses wireless connection (WiFi and Bluetooth capable device) to the networks in his Active Office. When Adrian, Mick and Walter come to John's office and they bring their own SPA: Adrian brings his Phone PDA with Windows CE, Mick brings his PDA with Linux Familiar and Walter has a smart phone with Symbian operating system, all with Bluetooth capability. When they have a meeting and need connections to the net, they are able to create an ad hoc network through John's SPA using Bluetooth network. The different types of devices and operating system platforms are not the barrier.*
>
> *John's SPA is set as a mobile access point using Bluetooth network for his guests, but it remains as a client of the Active Office server using WiFi network.*
>
> *When Adrian device is connected to the Active Office network, the MAC address of his device is caught up by the resolution server to find his profile including his identity from his local server in his university office (outside John's office). The Active Office can then deliver a welcome message to Adrian. The same way happens to Mick from his industry server and Walter from his government server out there and the meeting begins.*

The Active Office provides the mobile access point through John's laptop, calculating the guests' incoming and outgoing data which is stored as John's responsibility. The handling systems or Persistent-URL systems is used for a resolution server to recognise the guest identity, if his device is not registered in Active Office. Moreover, the Active Office server can deliver information relating to John's location to his laptop which can lead to the location of their guests. The proximate location of a guest user measured by finding the proximate location of the mobile access point and turned to a proximate guest user location by using the symbolic or coordinate user location algorithm mentioned in [30].

Guest User Location Based On Mobile Access Point Connectivity

Communication between small embedded devices and sensing devices are an integral service of the Active Office. The existing communication technologies use wired and wireless local area networks to form the communication network. The wired local area network uses fibre optic, RJ45 or USB networking and the wireless local area network uses WiFi, or wireless personal area networks (Bluetooth or IrDA). In an Active Office, the use of mobile phone network (GSM/GPRS) by the guest is allowed but not supported, since the access to mobile phone network is not under control of the Active Office infrastructure and the cost of connection also needs to be considered by the guest user. However, the guest has an option to connect to the network through 3G telecommunication service, for example, without any interference of Active Office systems.

Category	SPA Client	Mobile AP	AP/Server
1	Fixed/Precise Location	Fixed/Precise Location	Fixed/Precis e Location
2	Mobile/Proximat e Location	Mobile/Proximat e Location	Fixed/Precis e Location
3	Mobile/Proximat e Location	Fixed/Precise Location	Fixed/Precis e Location
4	Mobile/Proximat e Location	Mobile/Proximat e Location	Fixed/Precis e Location

FIGURE 4 The Possible Connectivity of a Mobile Access Point to File Server.

In our implementation, several access points of Bluetooth and WiFi are used to cover the three buildings and their surroundings. The users are attached to the Active Office servers through the WiFi Access Points using Virtual Private Network (secure mode), and the server provides authoritative dynamic IP address service by registering the user's MAC address devices for security and zero-configuration purposes. It is possible for an SPA user to connect to a WiFi server using wired or wireless LAN. When a user uses WiFi in an Active Office, his mobile device will be set up as a secure client to the WiFi's server to provide a connection for his guest, and his mobile device also needs to be set up as a Network Access Point (NAP) especially when his guest needs to connect using Bluetooth networking (Figure 4). When a guest brings his PDA with Bluetooth or USB capability, a scattered Bluetooth network or USB network is available to access the Active Office resources.

In this experiment, three PDAs (WinCE and Linux Familiar) and a Smart Phone are used as clients and a laptop (Linux Fedora) is used to build USB networking or Bluetooth networking. While using Bluetooth Networking, the laptop was set up as a Bluetooth NAP and the PDAs and a Smart Phone were set up as a Bluetooth Personal Access Network User clients (PANU).

To develop an application on the mobile access point to send user location data to clients, the Bluetooth, WiFi, USB and RJ45 connection can be considered as a regular connection in the Active Office. The four situations in which the connection to the Active Office can be formed are as follows (Figure 4):

From the study of the situation above, it is obvious that the user location for the SPA client depends on the location of the mobile access point. If the mobile access point moves, then the SPA client will also move. Table 2 shows only five possible situations (grey shading) which can occur when the SPA client comes to the proximate user location, while the rests are in fixed/precise user location. This happens when a mobile access point or an SPA client is using a wireless connection (Bluetooth/WiFi). The guest activities in accessing the resources while the guest user is on the move were monitored using network monitoring application.

An Active Office provides full support to any resource movement (user mobility devices), in the sense of the availability of the independent resources. In the case of a mobile access point, it is possible for the staff member to change his connection from wired to wireless connection, but his

guest continues to access the service transparently through his mobile access point, which is also his mobile device.

7. SYSTEM MONITORING USER ACTIVITY IN AN ACTIVE OFFICE

As mentioned earlier in Section 4 – Resources Manager, in Active Office's network management, a resource manager acts as the coordinator. It maps available resources. This section presents a sample map in Active Office for a user.

When a user has an activity in an Active Office, which is recognised by any sensors being in active use by a user or where any transaction occurs between a user and smart sensors in the environment, the user activity can be detected and monitored. The user activity information can be used to understand the user situation.

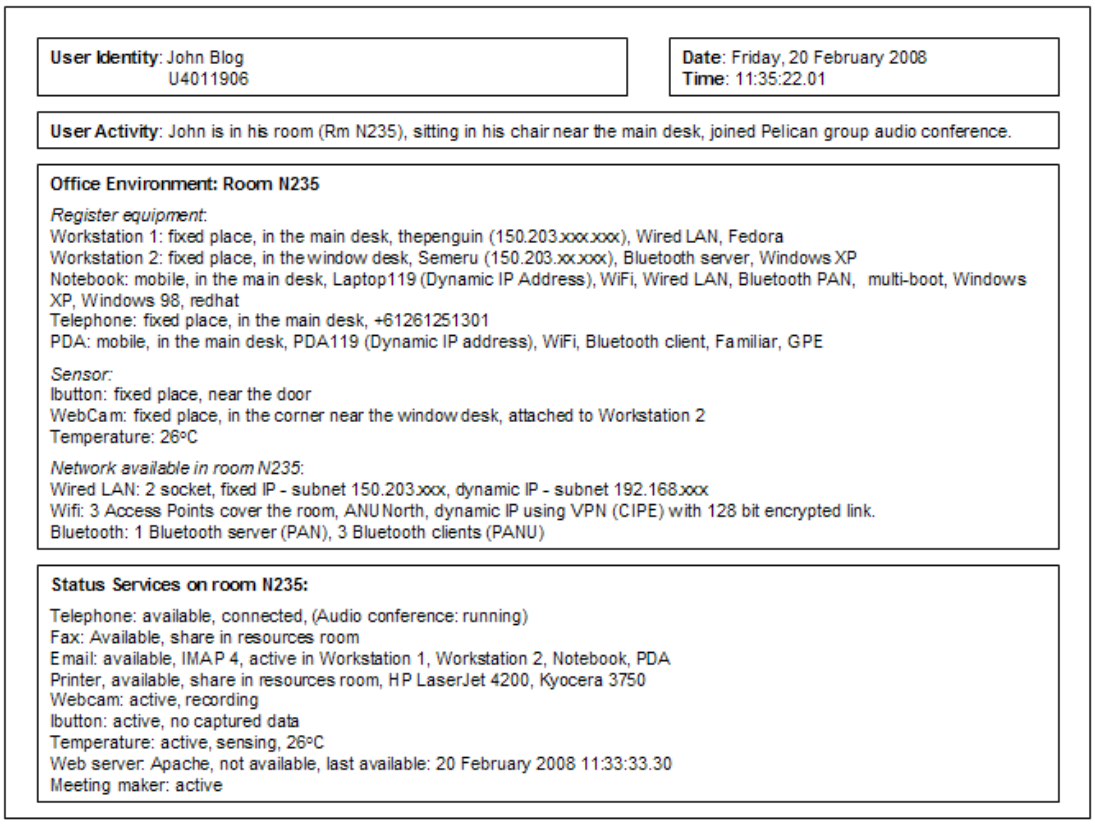

FIGURE 5 A Sample Snapshot of a User's Current Location and a User's Activity Recognition Window

To monitor user activities, several important variables need to be considered, for example:

- user identification,
- user location,
- register of fixed devices/sensors,
- network availability (WLAN: Bluetooth, WiFi),
- service status of the room in the Active Office.

All objects, such as user identity, devices/sensors and network availability, have:

- object identification,
- an object name,
- other characteristics.

Once a relationship exists between user identification and objects such as user location or register devices, this relationship will be registered and stored in the Intelligent Environment repository as a transaction of a user model.

User location can be recognised by WiFi or Bluetooth. A proximity location sensor is used in the Active Office. In the case when the user has two devices with two connectivity capabilities, using WiFi and Bluetooth for instance, the Active Office environment will check both devices, then use the latest user location and store it in the Intelligent Environment repository as the current location.

Service status captured directly from the resources manager, which accesses the Intelligent Environment repository and the user model. The Intelligent Environment repository and the user model holds the information from all sensors/devices and the relationship between user identification and sensors/devices.

The snapshot in Figure 5 is an example of monitoring of user activity. John Blog is in his room (room N235), sitting on his chair, near the main desk, and joins a teleconference with Pelican Group. John is monitored logging onto his computer (John is in room N234 and room N234 belongs to John), he sits on his chair (the iButton/RFID in the chair and keyboard activity is in active mode as John continues typing) and he registers onto the conference with Pelican Group (based on John's schedule, he is having a teleconference with the Pelican group and at the same time his phone status is in audio conference).

The user activity process (Figure 5) has the similar process as the other smart sensors, the deduction is concerned to user-id and the transaction between user-id and the objects i.e., sensors, devices, services.

The deduction from the context information above shows John's activity is a teleconference situation.

8. CONCLUSION

This paper discussed an approach towards the determination and recognition of user activity in Ubiquitous Computing Environments. This approach is relied on location information. One of the motivations of this work is that user activity is not well defined in the Ubiquitous Computing discipline. This may occur because the transition between activities is sometimes not very clear. An activity can be seen as a part of other activity, it can be in sequence mode or in parallel mode or both together, and different views can be deduced from different activities.

User activity in the Intelligent Environment can be defined as any association between a user and smart sensors in the environment, or any sensors being in active use to access the resources. It is divided into 4 categories, i.e., 1. as association between a user and smart sensors in the environment, 2. as a node in a work flow or job breakdown, 3. as a physical movement mode or state, or 4. as a mode of state of human intent.

This paper also presented a system monitoring user activity, based on the user activity processing model. The user activity processing is based on DiCPA architecture which is implemented in a smart office (Active Office). In an Active Office, a Mobile Access Point is developed and analyses the gathering of the guest user location which leads to guest activity.

For office environment, our user activity approach can be used to measure a user productivity based on time and location, depending on the variable that is measured, for example by measuring the use of time of the user. For home environment, this approach can measure the enjoyment and relaxing activities of the occupants.

However, as the computing environment changes over time, monitoring user activity becomes progressively more difficult.

9. REFERENCES

[1] Kern, N., B. Schiele, et al. (2003). *"Multi-sensor Activity Context Detection for Wearable Computing."* EUSAI 2003, Springer-Verlag Berlin Heidelberg, LNCS 2875. pp. 220-232.

[2] Lukowicz, P., J. A. Ward, et al. (2004). *"Recognizing Workshop Activity Using Body Worn Microphones and Accelerometers."* Pervasive 2004, Springer-Verlag Berlin Heidelberg, LNCS 3001. pp. 18-32.

[3] Mantoro, T. and C. W. Johnson (2004). "*DiCPA: Distributed Context Processing Architecture for an Intelligent Environment."* The Communication Networks and Distributed Systems Modelling Conference (CNDS'04), San Diego, California.

[4] Lee, S.-W. and K. Mase (2002). "*Activity and Location Recognition using Wearable Sensors."* IEEE Pervasive Computing(July-Sept 2002): pp. 24-31.

[5] Churchill, E. F. and A. J. Munro (2001). "WORK/PLACE: Mobile Technologies and Arenas of Activities." SIGGROUP Bullettin Vol. 22(3): pp. 3-9.

[6] Crabtree, A., T. Rodden, et al. (2003). *"Finding a Place for Ubicomp in the Home."* Proceedings of The fifth International Conference on Ubiquitous Computing (Ubicomp'03), LCNS 2864, Seattle, USA, Springer Verlag. pp. 208-226.

[7] Koile, K., K. Toolman, et al. (2003). "*Activity Zones for Context-Aware Computing."* Proceedings of The 5th International Conference on Ubiquitous Computing (Ubicomp'03), LNCS 2864, Seatle, USA, Springer-Verlag. pp. 90-103.

[8] Prekop, P. and M. Burnett (2002). *"Activities, Context and Ubiquitous Computing."* Computer Communications 26(11): pp. 1168-1176.

[9] Mantoro, T. and C. W. Johnson (2003). "User Location and Mobility for Distributed Intelligent Environment." Adjunct Proceedings, The Fifth International Conference on Ubiquitous Computing (UbiComp'03), Seattle, Washington, USA. pp. 12-15.

[10] Benerecetti, M., O. P. Bouquet, et al. (2000). *"Contextual Reasoning Distilled."* Journal of Experimental and Theoretical Artificial Intelligence (JETAI) 12(2000): pp. 279-305.

[11] Brown, P. J., J. D. Bovey, et al. (1997). "*Context Aware applications: From the laboratory to the marketplace."* IEEE Personal Communication 4(5): pp. 58-64. 1070-9916.

[12] Budzik, J. and K. J. Hammod (2000). *"User Interactions with Everyday Applications as Context for Just-in-time Information Access."* Proceedings of the International Conference on Intelligent User Interfaces, New Orleans, Louisiana, USA. pp. 44-51. 1-58113-134-8.

[13] Kidd, C. D., R. Orr, et al. (1999). "*The Aware Home: A living Laboratory for Ubiquitous Computing Research."* Proceedings of The 2nd International Workshop on Cooperative Building (CoBuild'99), LNCS 1670, Pittsburgh, PA, Springer Verlag. pp. 191-198.

[14] Mantoro, T., and C. W. Johnson (2003). *"User Mobility Model in an Active Office."* LNCS 2875, European Symposium on Ambient Intelligence (EUSAI'03), Eindhoven, The Netherlands.

[15] Mantoro, T. and C. W. Johnson (2003). "*Location History in a Low-cost Context Awareness Environment."* Workshop on Wearable, Invisible, Context-Aware, Ambient, Pervasive and Ubiquitous Computing, ACSW 2003, Adelaide, Australia, Australian Computer Science Communications Vol. 25 (6). pp. 153-158.

[16] Schilit, W. N. (1995). *A System Architecture for Context-Aware Mobile Computing.* PhD thesis. The Graduate School of Arts and Sciences. Colombia, Colombia University, PhD thesis: 144 pages.

[17] Szalai, A. (1972). *The Use of Time: Daily Activities of Urban and Suburban Populations in Twelve Countries.* Paris, The Hague, Mouton.

[18] Stinson, L. L. (1999). *"Measuring How People Spend Their Time: a Time-Use Survey Design."* Monthly Labor Review (August 1999): pp. 12-19.

[19] Thomas, B. H., V. Demczuk, et al. (1998). "*A Wearable Computer System with Augmented Reality to Support Terrestrial Navigation."* Proceedings of The 2nd International Symposium on Wearable Computers (ISWC 1998), Pittsburgh, Pennsylvannia, USA, IEEE Computer Society. pp. 168-171.

[20] Orr, R. J. and G. D. Abowd (2000). "*The Smart Floor: A mechanism for Natural User Identification and Tracking."* Proceedings of the Conference on Human Factors in Computing Systems (CHI '00), The Hague, Netherlands, ACM Press. pp. 275-276.
[21] Priyantha, N. B., A. Chakraborty, et al. (2000). "*The Cricket Location-Support System."* Proceeding of The 6th ACM international Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, MA, ACM. pp. 32-43.
[22] Harter, A., A. Hopper, et al. (2001). *"The Anatomy of a Context-Aware Application.*" Wireless Networks 1: pp. 1-16.
[23] Hong, J. I. and J. A. Landay (2001). "*An Infrastructure Approach to Context-Aware Computing."* Human-Computer Interaction (HCI) Journal 16(2,3,4): pp. 287-303.
[24] Elrod, S., G. Hall, et al. (1993). "Response Office Environments." Communications of the ACM 36(7): pp. 84-85. 0001-0782.
[25] Brumit, B. L., B. Meyer, et al. (2000). "*EasyLiving: Technologies for Intelligent Environments.*" 2nd International Symposium on Handheld and Ubiquitous Computing (HUC 2000), Bristol, UK. pp. 12-27.
[26] Patterson, D. J., D. Fox, et al. (2003). "*Expressive, Tractable and Scalable Technique for Modelling Activities of Daily Living."* UbiHealth 2003: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Seattle, WA.
[27] Kulkarni, A. (2002). A *Reactive Behavioural System for the Intelligent Room.* Master Thesis. Computer Science. Cambridge, MA, Massachusetts Institute of Technology: pp. 63.
[28] Tapia, E. M., S. S. Intille, et al. (2004). "*Activity Recognition in the Home Using Simple and Ubiquitous Sensors."* Pervasive 2004, LNCS 3001, Berlin Heidelberg: Springer-Verlag. pp. 158-175.
[29] Lin L., D. Fox, et. al. (2005). "Location-Based Activity Recognition using Relational Markov Networks." Proceedings of the Nineteenth International Joint Conference on Artificial Intelligence, Edinburgh, Scotland.
[30] Mantoro, T., C. W. Johnson (2005). *nk-Nearest Neighbour algorithm for Estimation of Symbolic User Location in Pervasive Computing Environments.* Proceeding of The IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Taormina, Italy, June 13-16, 2005.
[31] Nielsen, J. and J. Levy (1994). "*Measuring Usability: Preference vs. Performance*." Communications of the ACM 37(4): pp. 67-76.
[32] Carroll, J. J., D. C. Neale, et al. (2003). "Notification and awareness: synchronizing task-oriented collaborative activity." International Journal of Human-Computer Studies 58: pp. 605-632.
[33] Tang, T. J. (1991). "*Finding from observational studies of collaborator.*" International Journal of Man-Machine Studies 34: pp. 143-160.
[34] Gutwin, C. and S. Greenberg (1996). "*Workspaces awareness for groupware.*" The proceeding of the ACM HCI'96 Conference on Human Factors in Computing Systems, New York, Association of Computing Machinery. pp. 208-209.

A Review of Current Routing Attacks in Mobile Ad Hoc Networks

Rashid Hafeez Khokhar rkhokhar@gmail.com
Faculty of Computer Science and Information System
Department of Computer System & Communication
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Md Asri Ngadi dr.asri@utm.my
Faculty of Computer Science and Information System
Department of Computer System & Communication
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Satria Mandala satriamandala@hotmail.com
Faculty of Computer Science and Information System
Department of Computer System & Communication
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Abstract

A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, the current security issues in MANET are investigated. Particularly, we have examined different routing attacks, such as flooding, blackhole, link spoofing, wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols.

Keywords: MANET security, Routing protocols, Cryptography, Communications and data security, Shared wireless channel.

1. INTRODUCTION

A MANET is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other

security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET [6] such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. Currently, the routing, power management, bandwidth management, radio interface, and security are hot topics in MANET research. Although in this paper we only focus on the routing protocols and security issues in MANET. The routing protocols in MANET may generally be categorized as: table-driven/proactive and source-initiated (demand-driven)/reactive. In proactive routing protocols, such as the optimized link state routing (OLSR) [4], nodes obtain routes by periodic exchange of topology information. In reactive routing protocols, such as the ad hoc on demand distance vector (AODV) protocol [19, 20], nodes find routes only when required.

The overall goal of the security solutions for MANET is to provide security services including authentication, confidentiality, integrity, anonymity, and availability to the mobile users. In order to achieve to this goal, the security solution should provide complete protection spanning the entire protocol stack. We can categories MANET security in 5 layers, such as *Application layer, Transport layer, Network layer, Link layer,* and *Physical layer.* However, we only focus on the network layer, which is related to security issues to protect the ad hoc routing and forwarding protocols. From the security design perspective, the MANETs have no clear line of defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols, such as (AODV) [19, 20], (DSR) [11], and wireless MAC protocols, such as 802.11 [14], typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications.

Recently, several research efforts [8, 9, 13, 23, 26] introduced to counter against these malicious attacks. Most of the previous work has focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy traffic load to exchange and verify keys, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. The MANET protocols are facing different routing attacks, such as flooding, blackhole, link withholding, link spoofing, replay, wormhole, and colluding misrelay attack. A comprehensive study of these routing attacks and countermeasures against these attacks in MANET can be found in [7]

The rest of this paper is organized as follows. In next section, we discuss routing protocols in MANET. Section 3 discusses current routing attacks as well as countermeasures against such attacks in existing MANET protocols. Finally, we summarize the paper.

2. ROUTING PROTOCOLS IN MANET

MANET routing protocols can be categorized into 2 classes as: table-driven/proactive and source-initiated (demand-driven)/reactive. In the following sections, we present the overview of these protocols.

2.1 Table-driven routing protocols

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by

propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1.1 Destination-sequenced distance-vector (DSDV)

The Destination-Sequenced Distance-Vector (DSDV) routing protocol [18] is a table-driven algorithm based on Bellman-Ford routing mechanism [2]. The improvements made by [18] to the Bellman-Ford algorithm include freedom from loops in routing tables. In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. To help alleviate the potentially large amount of network traffic that such updates can generate, route updates can employ two possible types of packets: full *dump* and *s*maller *incremental* packets. Each of these broadcasts should fit into a standard-size of network protocol data unit (NPDU), thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packets.

New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast [18]. The route labeled with the most recent sequence number is always used. In the event that two updates have the same sequence number, the route with the smaller metric is used in order to optimize (shorten) the path. Mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received (see [18]*).* By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future.

2.1.2 Optimized link state routing (OLSR) protocol

Optimized link state routing (OLSR) protocol [4] is a proactive routing protocol and based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. Generally, two types of routing messages are used in the OLSR protocol, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbor sensing and MPR selection.

In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network. For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

2.1.3 Wireless routing protocol (WRP)

Wireless routing protocols (WRP) [12, 24] is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. WRP is a loop free routing protocol. Each node maintains 4 tables: distance table, routing table, linkcost table & message retransmission list table. Link changes are propagated using update messages sent between neighboring nodes. Hello messages are periodically exchanged between neighbors. This protocol avoids count-to-infinity problem by forcing each node to check predecessor information.

2.1.4 Clusterhead gateway switch routing (CGSR) protocol

Clusterhead gateway switch routing (CGSR) protocol is based on a cluster multihop mobile wireless network with several heuristic routing schemes [3]. The authors state that by having a cluster head controlling a group of ad hoc nodes, a framework for code separation (among clusters), channel access, routing, and bandwidth allocation can be achieved. A cluster head selection algorithm is utilized to elect a node as the cluster head using a distributed algorithm within the cluster. However, frequent cluster head changes can adversely affect routing protocol performance since nodes are busy in cluster head selection rather than packet relaying. Hence, instead of invoking cluster head reselection every time the cluster membership changes, a Least Cluster Change (LCC) clustering algorithm is introduced. Using LCC, cluster heads only change when two cluster heads come into contact, or when a node moves out of contact of all other cluster heads.

CGSR uses DSDV as the underlying routing scheme, and hence has much of the same overhead as DSDV. However, it modifies DSDV by using a hierarchical cluster-head-to-gate-way routing approach to route traffic from source to destination. Gateway nodes are nodes that are within communication range of two or more cluster heads. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination.

2.2 On demand-driven reactive protocols

On demand protocols create routes only when desired by source nodes [19, 11, 17 24]. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired.

2.2.1 Ad hoc on-demand distance vector (AODV)

AODV [19, 20] is an improvement of DSDV algorithm previously described. It is typically minimizes the number of required broadcasts by creating routes on a demand basis, while DSDV algorithm maintain a complete list of routes. The authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing acquisition or participate in routing table exchanges. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with

destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

2.2.2 Dynamic source routing (DSR)

Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing [11]. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broad- casting a *route request* packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the *route record* of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. A *route reply* is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

2.2.3 Temporary-ordered routing algorithm (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive loop-free distributed routing algorithm based on the concept of link reversal [17]. TORA is proposed to operate in a highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any desired source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes. The protocol performs three basic functions: route creation, route maintenance, and route erasure.

2.2.4 Relative distance micro diversity routing (RDMAR)

Relative Distance Micro diversity Routing (RDMAR) protocol estimates the distance between two nodes using the relative distance estimation algorithm in radio loops. RDMAR is a source initiated and having features similar to associativity based routing (ABR) protocol. RDMAR [19, 20, 17, 24] limits the range of route searching in order to save the cost of flooding a route request message into the entire wireless area. It is assumed in RDMAR that all ad hoc mobile hosts are migrating at the same fixed speed. This assumption can make good practical estimation of relative distance very difficult.

3. ROUTING ATTACKS IN MANET

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.

3.1 Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious

node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

A simple mechanism proposed to prevent the flooding attack in the AODV protocol [25]. In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. In [5], the authors show that a flooding attack can decrease throughput by 84 percent. The authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to [25], in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [25], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

3.2 Blackhole attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure 4 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

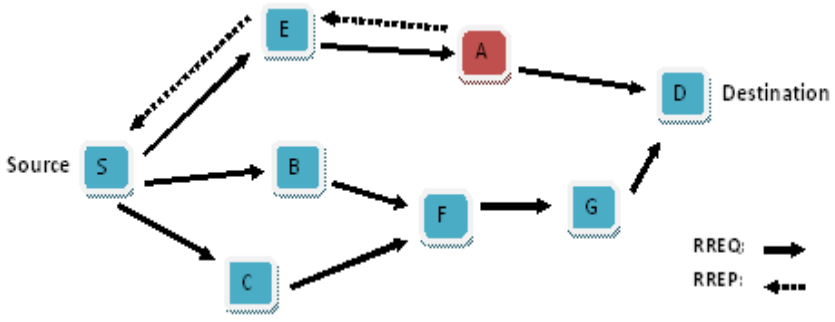

Figure 1: Blackhole attack on AODV

The route confirmation request (CREQ) and route confirmation reply (CREP) is introduced in [15] to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After

receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In [1], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main draw back of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive. In another attempt [10], the authors analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

3.3 Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. Figure 2 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and E are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

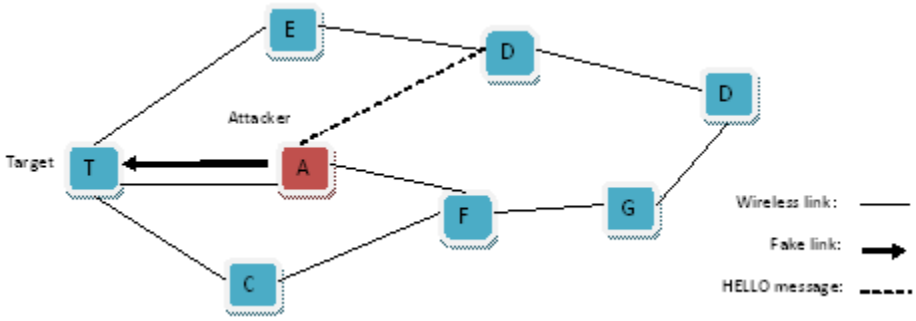

Figure 2: Link spoofing attack

A location information-based detection method is proposed [22] to detect link spoofing attack by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work

in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack.

In [8], the authors show that a malicious node that advertises fake links with a target's two-hop neighbors can successfully make the target choose it as the only MPR. Through simulations, the authors show that link spoofing can have a devastating impact on the target node. Then, the authors present a technique to detect the link spoofing attack by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

3.4 Wormhole attack

A wormhole attack [13] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node

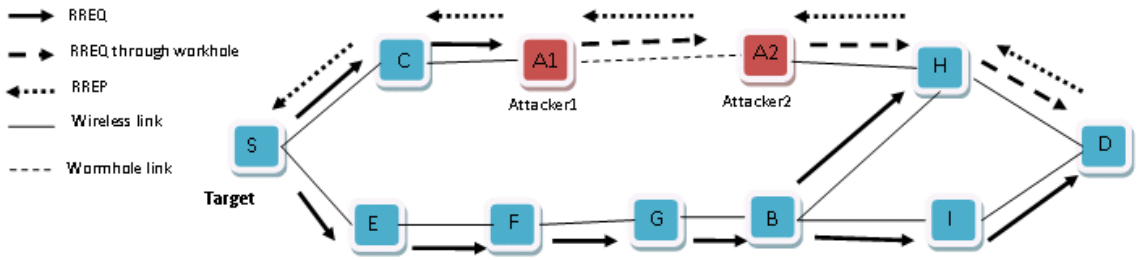

Figure 3: Wormhole attack on reactive routing

D, its neighbors C and E forward the RREQ as usual. However, node A1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-H-D that indeed passed through A1 and A2 to send its data.

In [13], packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, t_e, based on the speed of light c and includes the expiration time, t_e, in its packet to prevent the packet from traveling further than a specific distance, L. The receiver of the packet checks whether or not the packet expires by comparing its current time and the t_e in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks. For the geographical leash, each node must know its

own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization needs not to be highly tight.

In [22], the authors offer protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of a public key infrastructure and time-stamp synchronization between all nodes that is similar to the geographic leashes proposed in [13]. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack. In [21], the authors propose a statistical analysis of multipath (SAM), which is an approach to detect the wormhole attack by using multipath routing. This approach determines the attack by calculating the relative frequency of each ink that appears in all of the obtained routes from one route discovery. In this solution, a link that has the highest relative frequency is identified as the wormhole link. The advantage of this approach is that it introduces limited overhead when applied in multipath routing. However, it might not work in a non-multipath routing protocol, such as a pure AODV protocol.

3.5 Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and *pathrater* [16]. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [8] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

Figure 4: Colluding misrealy attack

A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient. In [9], the author proposes a method to detect an attack in which multiple malicious nodes attempt to drop packets by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main draw back of this approach is that even if we require each node to increase transmission power to be K times, we still cannot detect the attack in which K + 1 attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

4. SUMMARY

A MANET is a promising network technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Although, we have only discussed the security issues in this paper, particularly routing attacks and its existing countermeasures. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks and countermeasures against MANET protocols. Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol.

Because of the characteristic of dynamic wireless network, MANET presents the following set of unique challenges to secure. *Dynamic network:* the topology of MANETs is highly dynamic as mobile nodes freely roam in network, join or leave the network on their own will, and fail occasionally. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Mobile users roaming in the network may request for anytime, anywhere security services. *Resource constraints:* the wireless channel is bandwidth constrained and shared among multiple networking entities. The computation and energy resources of a mobile node are also constrained. *No clear line of defense:* MANET has not offer a clear line of defense. Moreover, the wireless channel is accessible to both legitimate users and malicious attackers. The boundary that separate the inside network from the outside world becomes blurred. *Device with weak protection:* portable devices, as well as the system security information they store, are vulnerable to compromises.

Security solutions are important issues for MANET, especially for those selecting-sensitive applications, have to meet the following design goals while addressing the above challenges. *Availability:* ensures the survivability of the network services despite Denial of Service (DoS) attacks. A DoS attack could be launched at any layer of ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. The security service is highly available on the network layer at anytime and at anywhere. On the higher layers, an adversary could bring down high-level services. *Efficiency:* the solution should be efficient in terms of communication overhead, energy consumption and computationally affordable by a portable device. *Authentication:* enables a mobile node to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. *Integrity:* guarantees that a message being transmitted is never corrupted. A message could be corrupted because of being failures, such as radio propagation impairment, or because of malicious attacks on the network. *Confidentiality:* ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. *Non-repudiation:* ensures that the original message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised mobile nodes.

5. REFERENCES

[1] M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.

[2] L. R. Ford Jr. and D. R. Fulkerson, Flows in Networks, Princeton Univ. Press, 1962.

[3] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SICON '97, Apr. 1997, pp. 197-21 1.

[4] Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.

[5] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[6] C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Ad-hoc Networks. 19th International Conference on *Advanced Information Networking and Applications, 2005. AINA 2005, Volume: 1, On page(s): 72- 77 vol.1*.

[7] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[8] B. Kannhavong et al., “A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks,” IEEE GLOBECOM ’06.

[9] Z. Karakehayov, “Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks,” Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[10] S. Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Proc. Int’l. J. Network Sec., 2006.

[11] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[12] Jyoti Raju and J.J. Garcia-Luna-Aceves, “ A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks’,” in Proceeding of IEEE ICC, June 2000.

[13] Y-C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[14] IEEE Std. 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 1997.

[15] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[16] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th MobiCom, Boston, MA, Aug. 2000.

[17] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. INFOCOM '97, Apr. 1997.

[18] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Com- mun. Rev., Oct. 1994, pp. 234-44.

[19] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[20] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[21] L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path,” IEEE Wireless Commun. and Networking Conf. ’05.

[22] D. Raffo et al., “Securing OLSR Using Node Locations,” Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13, 2005.

[23] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002.

[24] C.K.Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems,” Prentice Hall Publications, 2002.

[25] P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.

[26] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

Toward Coexistence and Sharing between IMT-Advanced and Existing Fixed Systems

Zaid Ahmed Shamsan shamsan22@yahoo.com
Wireless communication center (WCC)
Faculty of Electrical Engineering
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Sharifah Kamilah Syed-Yusof kamilah@fke.utm.my
Wireless communication center (WCC)
Faculty of Electrical Engineering
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Tharek Abd. Rahman tharek@fke.utm.my
Wireless communication center (WCC)
Faculty of Electrical Engineering
Universiti Teknologi Malaysia (UTM)
Skudai, 81310, Johor Bahru, Malaysia

Abstract

In this paper coexistence and spectrum sharing between systems as a recently critical issue due to emerging new wireless technologies and spectrum scarcity are investigated. At *World Radiocommunication Conferences 2007* (WRC-07), *International Telecommunication Union - Radiocommunications* (ITU-R) allocated 3400-3600 MHz band for the coming fourth generation (4G) or IMT-Advanced on a co-primary basis along with existing Fixed Wireless Access (FWA) systems. Therefore, coexistence and sharing requirements like separation distance and frequency separation coordination must be achieved in terms of both co-channel and adjacent channel frequencies. Co-sited the two base stations antennas and non co-sited coexistence of the two systems are analyzed. The interference analysis models, Adjacent Channel Interference Ratio (ACIR) and spectrum emission mask are applied in the 3.5 GHz band to extract the additional isolation needed to protect adjacent channel interference. Also interference to noise ratio as a standard interference criteria is introduced. Finally, possible intersystem interference mitigation techniques are suggested and explained.

Keywords: ACIR, Additional isolation, Spectral emission mask, FWA systems, IMT-Advanced system,

1. INTRODUCTION

In wireless communication, Interference between two systems occurs when these systems operate at overlapping frequencies, sharing the same physical environment, at the same time with overlapping antenna patterns. ITU-R recommends expressing the level of interference in terms of the probability that reception capability of the receiver under consideration is impaired by

the presence of an interferer. Concerning the different systems of International Mobile Telecommunication (IMT-Advanced) and Fixed Wireless Access (FWA) systems, it is natural to conclude that those technologies will work in the same environment that leads to occurrence of performance degradation. Main mechanisms of coexistence are: co-sited (co-located) and non co-sited (non co-located). FWA system and Fixed Satellite Service (FSS) downlink part use 3400-4200 MHz band. Meanwhile, the 3400-3600 MHz frequency band is identified at WRC-07 for IMT-Advanced in several countries in Asia with regulatory and technical constraints [1], which mean that frequency sharing between these systems is bound to happen. A few studies were done between terrestrial systems in the said band because this band did not use for mobile as the bands lower than 3 GHz as in WCDMA up to 2690 MHz.

The studies which carried out in this band (3.5 GHz) are in [2], [3]. In [2] the study implemented by using Advanced Minimum Coupling Loss (A-MCL) between beyond 3G systems and fixed microwave services to get the minimum separation distance and frequency between the two systems. Whereas in the [3], BWA system represented by FWA is studied to share the same band with point-to-point fixed link system also to determined the minimum separation distance and frequency separation. In our study the concept of spectral emission mask, adjacent channel leakage ratio and adjacent channel selectivity is presented such that the effect of both of transmitter and receiver are taking into account.

The reminder of this paper is organized as follows. In Sections 2 and 3 a vision for IMT-Advanced and its allocated spectrum are presented. Sections 3 to 7 describe in detail interference models used, systems parameters, protection criteria and propagation models. Sections 8 and 9 are devoted to describing the coexistence scenarios, results, analysis and compatibility between systems. Suggested intersystem interference mitigation methods are presented in Section 10. Finally, the conclusions are presented in Section 11.

2. IMT-ADVANCED SYSTEM CONCEPT

It is expected that the development of International Mobile Telecommunications -2000 (IMT-2000) will reach a limit of around 30Mbps [4]. IMT-Advanced is a concept from the ITU for mobile communication systems with capabilities which go further than that of IMT-2000. IMT-Advanced was previously known as “systems beyond IMT-2000” [5]. In the vision of the ITU, IMT-Advanced as a new wireless access technology may be developed around the year 2010 capable of supporting even higher data rates with high mobility, which could be widely deployed about 7 years (from now) in some countries. The new capabilities of these IMT-Advanced systems are envisioned to handle a wide range of supported carrier bandwidth: 20 MHz up to 100 MHz and data rates with target peak data rates of up to approximately 100 Mbps for high mobility such as mobile access and up to say 1 Gbps for low mobility such as nomadic/local wireless access [5].
IMT-Advanced will support connectivity, with increased system performance for a variety of low mobility environments, such as: Stationary (fixed or nomadic terminals); Pedestrian (pedestrian speeds up to 3 km/h); Typical vehicular (Vehicular speeds up to 120 km/h); High speed vehicular (high-speed trains up to 350 km/h).

Furthermore, IMT-Advanced shall support seamless application connectivity to other mobile networks and IP networks (global roaming capabilities), will deliver improved unicast and multicast broadcast services, and provide network support of multiple radio interfaces, with seamless handover, addressing both the cellular layer and the hot spot layer (and possibly the personal network layer) per ITU-R Rec. M.1645 [4]. Further, as technical requirements, IMT-Advanced systems shall support multiple input-multiple output (MIMO) and beamforming, including features to support multi-antenna capabilities at both the base station (BS) and at the mobile terminal, including MIMO operation. Also, IMT-Advanced shall support the use of coverage enhancing technologies according to [4], [6]. For the cell coverage, Table 1 records the IMT-Advanced deployment scenarios in which the deployment scenarios require availability for

mobile access for nomadic users (short-range), for ad-hoc network users, for outdoor users (wide and metropolitan range), and for moving users (in a car or a high-speed train).

Cell Range	Performance Target
Up to 100 m	Nomadic Performance, up to 1 Gbit/s
Up to 5 km	Performance Targets for at Least 100Mbps
5-30 km	Graceful Degradation in System/Edge Spectrum Efficiency
30-100 km	System Should be Functional (Thermal Noise Limited Scenario)

Table 1: IMT-Advanced Deployment Scenarios [6]

3. WRC-07 OUTCOMES FOR IMT-ADVANCED BANDS

At WRC-07 in Geneva, concerning item 1.4, the candidate bands for IMT systems have been discussed [1] and the results of this item in the conference can be summarized in Figure 1. The NO sign indicates that WRC-07 decided not to change the table of allocation regarding the candidate bands 410-430 MHz, 2700- 2900 MHz and 4400- 4900 MHz.

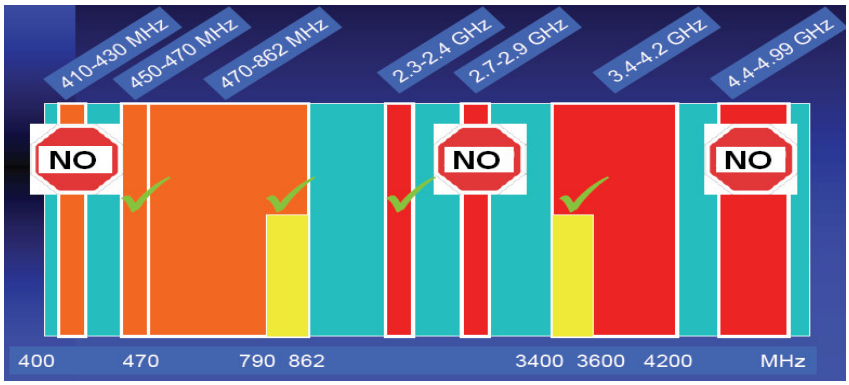

FIGURE 1: WRC-07 outcome for IMT system bands [7]

3.1 Globally Allocation

The frequency bands 450-470 MHz and 2300-2400 MHz are now identified for IMT and globally harmonized. However, the use of this band is dependant on every administration.

3.2 Region 1 Allocation (Europe, Africa & Arab countries)

The band 790-862 MHz that was only allocated for broadcasting systems is now equally allocated Mobile Service and identified for IMT in Europe/Africa and Arab countries with equal rights (co-primary basis). Mobile Service, and by that IMT, can now also use the band 3 400- 3 600 MHz on a co-primary basis with other services sharing this band (Fixed and Fixed Satellite Services), under regulatory and technical conditions, in 83 countries in Region 1, including most of the European countries.

3.3 Region 2 Allocation (Americas)

The band 698-806 MHz has now a Mobile allocation on a co-primary basis in this region (noting that 806-862 MHz was already co-primary for Mobile) except in Brazil where this band is secondary basis (operational restrictions compared with broadcasting services). This band is also identified for IMT. The band 3400-3500 MHz is now allocated for Mobile on co-primary basis with FS and FSS but without IMT identification in a number of countries in Latin America.

3.4 Region 3 Allocation (Asia)

The band 470-862 MHz was already allocated to the Mobile service on co-primary basis. The part 698-790 MHz is now identified for IMT in some countries but the part 790-862 MHz is identified for IMT in the whole Asia. The band 3400-3500 MHz is now allocated for Mobile on co-primary basis with FS and FSS and identified for IMT in several countries with regulatory and technical constraints. The band 3500- 3600 MHz that was already allocated to Mobile on co-primary basis is now identified for IMT under regulatory and technical constraints in several countries. With the outcome of WRC-07, the utilization of the new bands, can be classified into the global ones (450-470 MHz and 2300-2400) and regional ones (790-862 MHz and 3400- 3600 MHz). The amount of spectrum for Mobile Service and identified for IMT at WRC-07 could be generalized to 120 MHz globally and 392 MHz (120 + 72 + 200) in many areas. For our focusing on the band 3400-3600 MHz in all three Regions can be depicted in Figure 2, 3400-3600 MHz are allocated to the mobile service on a primary basis or identified for use by administrations wishing to implement IMT as in Figure 2.

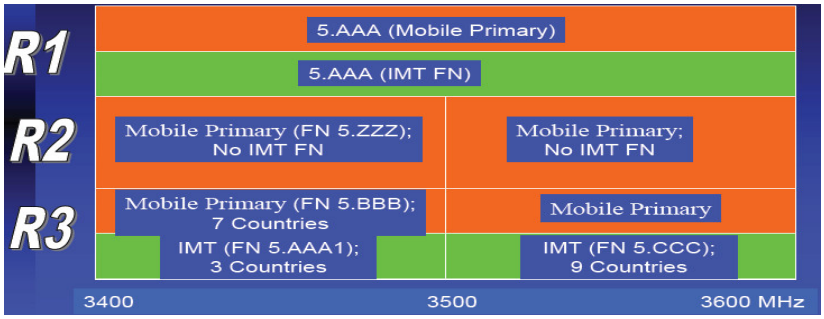

FIGURE 2: WRC-07 Outcome on IMT Band 3.4-3.6 GHz Item 1.4 [9], 5.BBB: Different category of service: in Bangladesh, China, India, Iran (Islamic Republic of), New Zealand, Singapore and French Overseas Communities Countries, 5.AAA1: In Korea (Rep. of), Japan and Pakistan, 5.CCC: In Bangladesh, China, Korea (Rep. of), India, Iran (Islamic Republic of), Japan, New Zealand, Pakistan and French Overseas Communities.

4. INTERFERENCE MODELS

When a system IMT-Advanced of other is considered, main type of interference is intrasystem interference, including interference coming from given cell, adjacent cell, and thermal noise. Whereas two systems coexist in the same geographic area, the interference includes not only intrasystem interference, but also intersystem interference which is considered in this paper.
The forms of interference modeled in this paper are spectral emission mask of FWA system and ACI of IMT-Advanced system that arises from the ACLR from BS transmissions in the IMT-Advanced and Adjacent Channel Selectivity (ACS) of the BS receivers in FWA systems and the ability of this receiver to reject power legitimately transmitted in the adjacent channel.

4.1 Spectral Emission Mask

The spectral emission mask is a graphical representation of a set of rules that apply to the spectral emissions of radio transmitters. Such rules are set forward by regulatory bodies such as FCC and ETSI. It is defined as the spectral power density mask, within ± 250 % of the relevant channel separation (ChS), which is not exceeded under any combination of service types and any loading. The masks vary with the type of radio equipment, their frequency band of operation and the channel spacing for which they are to be authorized. FWA 7 MHz channel bandwidth mask according to [8], [9] is tabulated in Table 2. The spectral emission mask is considered in this study because it may be used to generate a “worst case” power spectral density for worst case interference analysis purposes, where the coexistence study can be applied by spectrum emission mask as an essential parameter for adjacent frequency sharing analysis to evaluate the attenuation of interference signal power in the band of the victim receiver.

Freq./Ch. Separation (Normalized (MHz)	**0**	**0.5**	**0.5**	**0.71**	**1.06**	**2**	**2.5**
Ch. Spacing (MHz)	**dB**	**dB**	**dB**	**dB**	**dB**	**dB**	**dB**
	0	0	-8	-27	-32	-50	-50
7	0	3.5	3.5	4.97	7.42	14	17.5

Table 2: Reference Frequencies Points for Spectrum Masks of Type-F ETSI- EN301021 (FWA)

4.2 Adjacent Channel Interference

The level of interference received depends on the spectral 'leakage' of the interferer's transmitter and the adjacent channel blocking performance of the receiver. For the transmitter, the spectral leakage is characterized by the ACLR, which is defined as the ratio of the transmitted power to the power measured in the adjacent radio frequency (RF) channel at the output of a receiver filter. Similarly, the adjacent channel performance of the receiver is characterized by the ACS, which is the ratio of the power level of unwanted ACI to the power level of co-channel interference that produces the same bit error ratio (BER) performance in the receiver. In order to determine the composite effect of the transmitter and receiver imperfections, the ACLR and ACS values are combined to give a single Adjacent Channel Interference Ratio (ACIR) value using the following equation [10],

$$ACIR = \frac{1}{\frac{1}{ACLR} + \frac{1}{ACS}} \qquad (1)$$

5. IMT-ADVANCED & FIXED WIRELESS ACCESS SERVICES PARAMETERS

In order to examine coexisting and sharing issues, it is necessary to clarify the parameters of IMT-Advanced and FWA systems that will affect the interference level and criterion as clarified in a next section.

5.1 IMT-Advanced Parameters

Now, the term IMT means IMT-2000 and IMT-Advanced [11]. As stated, IMT-Advanced target peak data rates are 100 Mbps for high mobility systems and 1 Gbps for low mobility of fixed and nomadic systems. The required channel bandwidths is ranging between 20-100 MHz where 50 MHz for suburban and 100 MHz for urban coverage [12]. Table 3 contains the IMT-Advanced parameters assumed for the comparison of the different studies. Where 5 MHz, 10 MHz and 15 MHz are offsets of 1st adjacent channel, 2nd adjacent channel and 3rd adjacent channel separation from center frequency, respectively.

5.2 FWA System Parameters

In Malaysia the frequency range 3.4-3.7 GHz is allocated for FWA systems, it is divided into sub-bands for duplex use (non duplex systems can still be used in this band), 3400-3500 MHz paired with 3500-3600 MHz as well as 3600-3650 MHz paired with 3650-3700 MHz. These FWA bands are to be used for direct radio connection in the last mile between a fixed radio central station and subscriber terminal stations in a point-to-point and/or point-to-multipoint configuration. Countries have various frequency channel spacing within the 3.5 GHz bands 1.25, 1.75, 3.5, 7, 8.75, 10, 14,

and 28 MHz can be used according to capacity needs [13]. FWA parameters are shown in Table 3.

Parameter		Value	
		IMT-Advanced	FWA
Center Frequency of Operation (MHz)		3500	3500
Base Station Transmitted Power (dBm)		43	36
Minimum Coupling Loss (dB)		30	30
Base Station Antenna Gain (dBi)		18	17
Base Station Antenna Height (m)		30	30
Interference Limit Power (dBm)		-109	-109
Channel Bandwidth (MHz)		20, 50, 100	7
ACLR (dB)	Offset @ 5 MHz	45	53.5
	Offset @ 10 MHz	50	66
	Offset @ 15 MHz	66	-----
ACS (dB)	Offset @ 5 MHz	45	70
	Offset @ 10 MHz	50	70
	Offset @ 15 MHz	66	70

Table 3: IMT-Advanced and FWA Systems Parameters (Macro Cell)

6. PROTECTION CRITERION

The interference threshold, in the deterministic analysis, of -109 dBm is used as the maximum interference limits that can be tolerated by both of the IMT-Advanced and FWA equipment. This threshold is specified in Report ITU-R [12] and the RF parameters specified by the WiMAX Forum [14] for the IMT-Advanced and FWA equipment, respectively. For discussion of various sharing scenarios, it is necessary to develop appropriate rules for sharing. Intersystem interference can be described as short term or long-term. It is referred to as “long term” interference for percentage of time of greater than 20% While a small percentage of the time in range of 0.001% to 1.0% is referred to “short-term” interference which is rarely evaluated in the coordination literature as it is very much statistical in nature and not found for many services and will be specific to the cases considered [15] [16]. In this paper we consider long term interference only.
The interference protection criteria can be defined as an absolute interference power level *I*, interference-to-noise power ratio *I/N*, or carrier-to-interfering signal power ratio *C/I* [16]. ITU-R Recommendation F.758-2 details two generally accepted values for the interference–to–thermal-noise ratio for long-term interference into fixed service receivers. When considering interference from other services, it identifies an *I/N* value of –6 dB or –10 dB matched to specific requirements of individual systems.

This approach provides a method for defining a tolerable limit that is independent of most characteristics of the victim receiver, apart from noise figure. Each fixed service accepts a 1 dB degradation (i.e., the difference in decibels between carrier-to-noise ratio *(C/N)* and carrier to

noise plus interference ratio *C/(N + I)* in receiver sensitivity. In some regard, an *I/N* of –6 dB becomes the fundamental criterion for coexistence [17], so it should be that [18]:

$$I - N \geq \alpha \qquad (2)$$

Where I is the interference level in dBm, N is the thermal noise floor of receiver in dBm and α is the protection ratio in dB and here has a value of -6 dB.

7. PROPAGATION MODELS

Particularly, there is no single propagation model used for different sharing studies because the particular deployment of the systems requires using specific propagation model relevant to the specific system.

7.1 Co-sited Macrocellular Base Stations Model

For co-sited BSs, a coupling loss value of 30 dB is assumed between co-sited antennas for all frequency bands, 30 dB was also a value measured by [19] for all frequency bands, horizontally separated antennas of the order of 1 meter [20].

7.2 Not Co-sited Macrocellular Base Stations Model

The standard model agreed upon in CEPT and ITU for a terrestrial interference assessment at microwave frequencies is clearly marked in [21]. This is model includes the attenuation due to clutter in different environments.

$$L(d) = 92.5 + 20\log d + 20\log f + Ah \qquad (3)$$

Where d is the distance between interferer and victim receiver in kilometers, f is the carrier frequency in GHz, and Ah is loss due to protection from local clutter or called clutter loss, it is given by the expression:

$$Ah = 10.25e^{-d_k}\left[1 - \tanh\left[6\left(\frac{h}{h_a} - 0.625\right)\right]\right] - 0.33 \qquad (4)$$

Where d_k is the distance (km) from nominal clutter point to the antenna, h is the antenna height (m) above local ground level, and h_a is the nominal clutter height (m) above local ground level. In [21], clutter losses are evaluated for different categories: trees, rural, suburban, urban, and dense urban, etc. The geographical area considered for sharing studies is urban area [22]. Increasing of antenna height up to the clutter height leads to decrease the clutter loss, as shown in Table 5 and Figure 3 which contain the urban and suburban categories.

Clutter Category	Clutter Height h_a (m)	Nominal Distance d_k (km)
Suburban Area	9	0.025
Urban Area	20	0.02

Table 5: Nominal clutter heights and distances

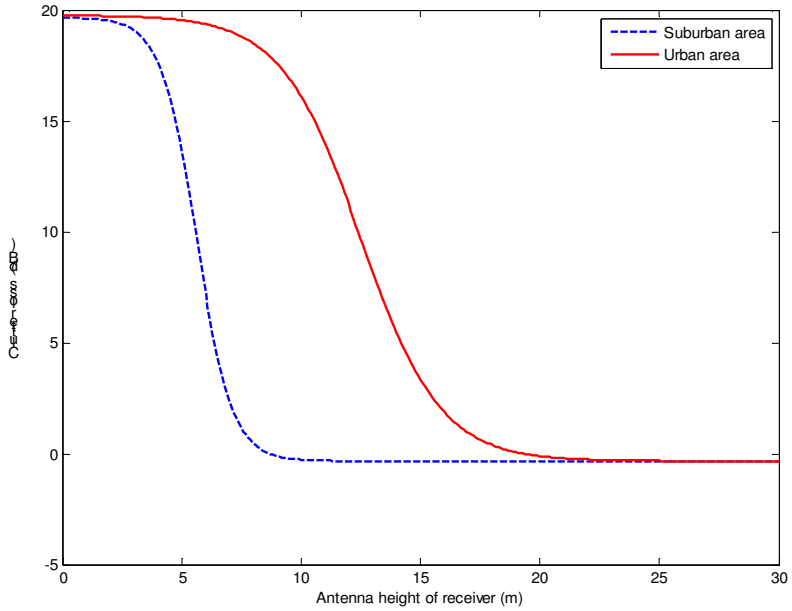

FIGURE 3: Clutter loss for suburban and urban areas

8. COEXISTENCE SCENARIOS & RESULTS

The coexistence scenarios which can occur between IMT-Advanced and FWA systems are BS-BS, BS-subscriber station, subscriber station-BS, subscriber station-subscriber station interference. As mentioned by [23], [24], [25], [26], BS-subscriber station, subscriber station-BS, subscriber station - subscriber station interference will have a small or negligible impact on the system performance when averaged over the system. Therefore, the BS-BS interference is the most critical interference path between IMT-Advanced and FWA will be analysis as a main coexistence challenge case for two systems. IMT-Advanced has no spectrum mask up to now, therefore, in case interference from IMT-Advanced toward FWA, The only form of interference modeled in this case is ACI that arises from the ACLR from BS transmissions in the IMT-Advanced system and the ACS of the BS receiver FWA system. Spectral emission mask of FWA systems in Table 2 will be used for the interference fall into IMT-Advanced system form FWA systems.

8.1 Co-sited Macrocellular Base Stations Analysis

In order to get additional isolation which is required to prevent adjacent channel interference for a collocated systems the following formula should be calculated.

$$\mathrm{A}_{addiso} = Pt - ACL - ACIR - I_{\lim it} \qquad (5)$$

Where A_{addiso} is additional Isolation (dB) required to prevent adjacent channel interference, Pt is the transmitter power, and I_{limit} is the Interference Limit. ACL is the antenna coupling loss which has practical values for macro, micro, and pico cell types, for BS-to-BS macro interference the antenna coupling loss is 30 dB [19], [20]. The additional isolation needed when the interference is generated from an IMT-Advanced BS to a FWA BS is shown in Table 6. Similarity, the additional isolation needed when the interference is generated from a FWA BS to an IMT-Advanced is tabulated in Table 7.

Parameter	Frequency Offset	
	5 MHz	10 MHz
Transmit Power (dBm)	43	43
Coupling Loss (dB)	30	30
ACIR (dB)	44.98	49.96
Interference Power at Receiver Input (dBm)	–32	–37
Allowed Interference Power (dBm)	–109.0	–109.0
Additional Isolation Needed (dB)	77	72

Table 6: Analysis For Co-Sited Macrocellular BS, Where the FWA is the Interference Victim

Parameter	Frequency Offset	
	5 MHz	10 MHz
Transmit Power (dBm)	36	36
Coupling Loss (dB)	30	30
ACIR (dB)	44.43	49.89
Interference Power at Receiver Input (dBm)	–39	– 44
Allowed Interference Power (dBm)	–109.0	–109.0
Additional Isolation Needed (dB)	70	65

Table 7: Analysis For Co-Sited Macrocellular BS, Where the IMT-Advanced is The Interference Victim

8.2 Not Co-sited Macrocellular Base Stations Analysis

8.2.1 FWA BS Interference on IMT-Advanced BS

As seen from Figures 4, 5, and 6, the interference from FWA BS (as an interferer) into IMT-Advanced BS (as a victim receiver) is applied, where the minimum separation distance and frequency separation for the minimum I/N ratio of -6 dB are analyzed according to the three selected bandwidths of IMT-Advanced channels in the urban area. It can be observed that the minimum separation distance between the two base stations must be greater than 10m, 6.5m and 4.5m for frequency offset of 14MHz to achieve the adjacent channel coexistence of FWA with 20MHz, 50MHz, and 100MHz channel bandwidth, respectively. The guard band between systems is 0.5MHz for 20MHz only while there is no guard band for 50 and 100MHz channel bandwidth. The zero guard band is represented by a vertical line in the graphs and equals to:

$$Z.G.B = 0.5(BW_{IMT-Advanced} - BW_{FWA}) \quad (6)$$

Where $BW_{IMT\text{-}Advanced}$ and BW_{FWA} are bandwidths of IMT-Advanced and FWA, respectively. Sharing the same channel (co-channel) is feasible between two systems only in case of separation distances are of the order of 3.25km, 2km, and 1.4km for 20MHz, 50MHz and 100MHz IMT-Advanced channel bandwidth, respectively, because at these distances or more the interference is always 6 dB or more below the thermal noise floor as the Figures show.

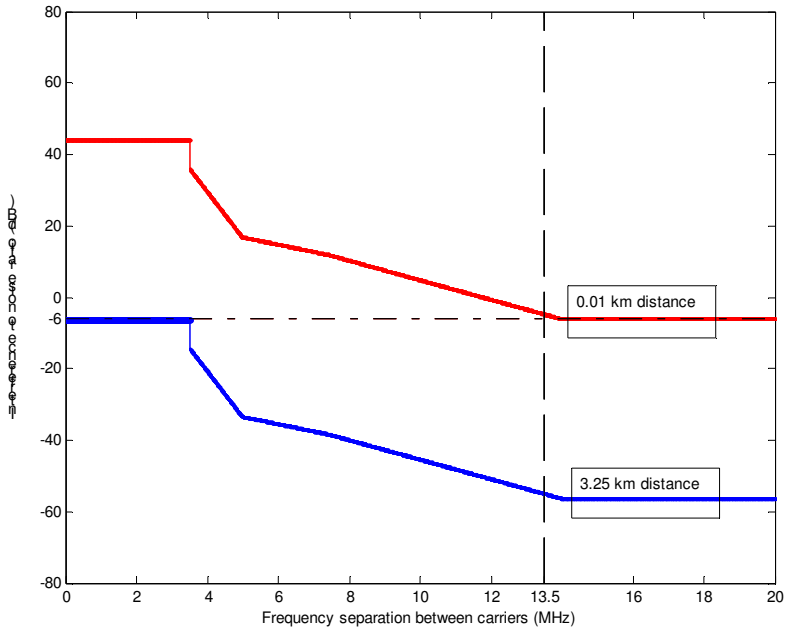

FIGURE 4: Interference from FWA into IMT-Advanced (20MHz)

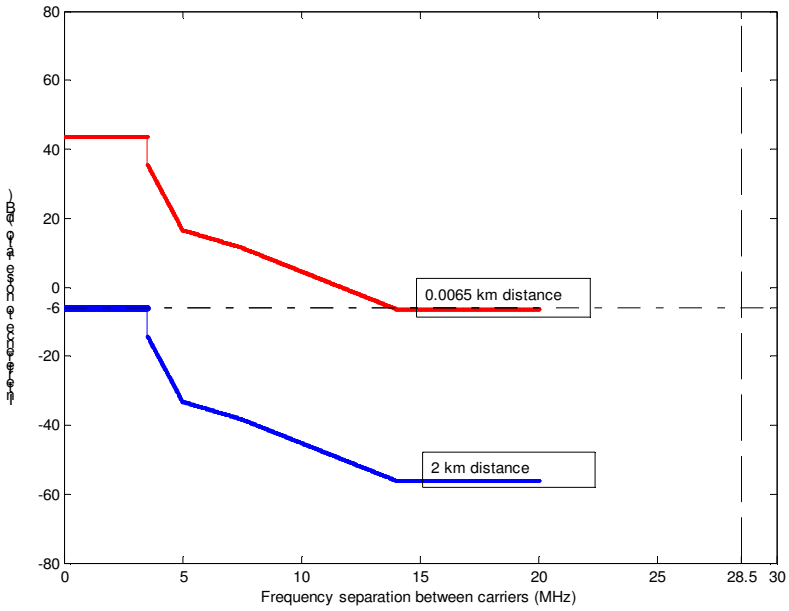

FIGURE 5: Interference from FWA into IMT-Advanced (50MHz)

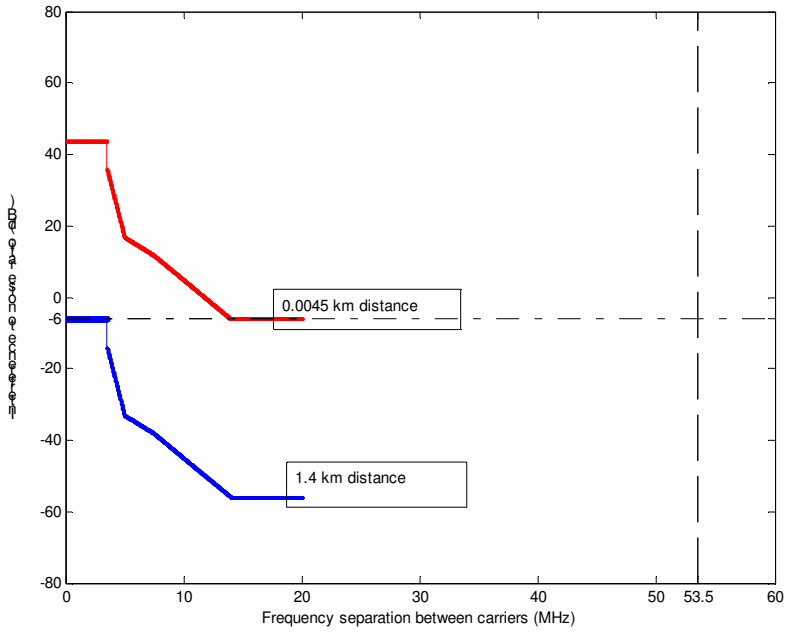

FIGURE 6: Interference from FWA into IMT-Advanced (100MHz)

8.2.2 IMT-Advanced BS Interference on FWA BS

As mentioned earlier, adjacent channel interference is used in this section, therefore the Additional isolation needed for certain distances can be extracted and expressed by

$$A_{addiso} = Pt + G_t + G_r - L_p - ACIR - I_{limit} \quad (7)$$

Where G_t is transmitter antenna gain, G_r is victim receiver antenna gain, L_p is propagation path loss, and I_{limit} is Interference Limit. The equation (7) can be represented by the following expression.

$$A_{addiso} = ACI - I_{limit} \quad (8)$$

Where ACI is adjacent channel interference which it should be minimum as much as possible. Figure 7 clarifies the high values of the additional isolation needed against separation distance for coexisting and sharing the same frequency band (3500MHz) when interference from IMT-Advanced BS on FWA BS is applied. The co-channel interference produces high additional isolation values ranging from 55dB (100MHz) to 62dB (20MHz) which are required for coexisting at a distance of 8km. In case of adjacent frequency bands, these additional isolation values are decreased to be 0dB at 5.5km, 3.5km, and 2.5km for 20MHz, 50MHz and 100MHz IMT-Advanced channel bandwidth, respectively, as shown in the Figures 8, 9 and 10. A negative value in the Figures signifies that the isolation provided by the standard equipment is sufficient to limit the interference in that particular case to acceptable levels and the absolute value indicates the size of the 'margin' available in the adjacent channel protection. As mentioned earlier, the interference to noise ratio is the considered protection criteria here, it is shown in the Figures11, 12 and 13 the amounts of interference noise ratio versus separation distance between BSs in case co-channel and adjacent channel frequencies. These Figures indicate that there is no communication possibility for the assumed scenarios between the two BSs except in the case of the third

adjacent channel frequency and above provided achievement the required separation distances as in the Figures below.

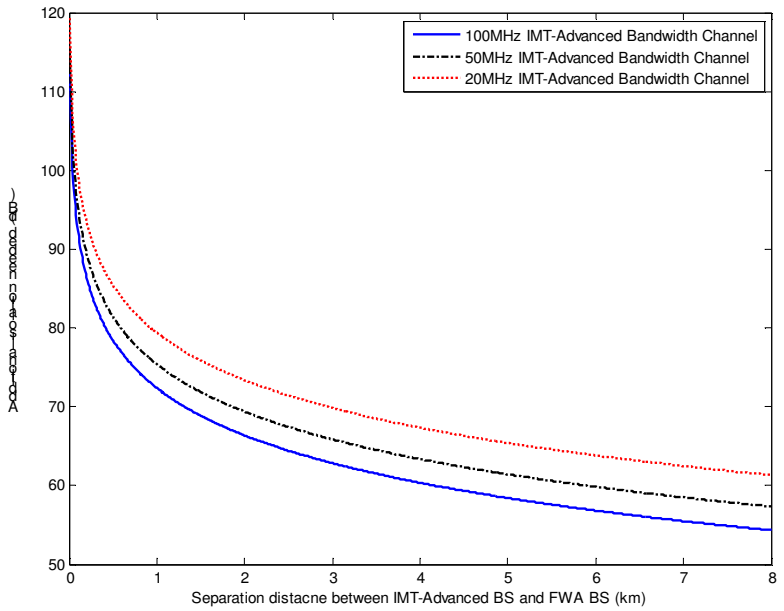

FIGURE 7: Required Additional Isolation When FWA is Victim (Co-Channel Frequency Sharing)

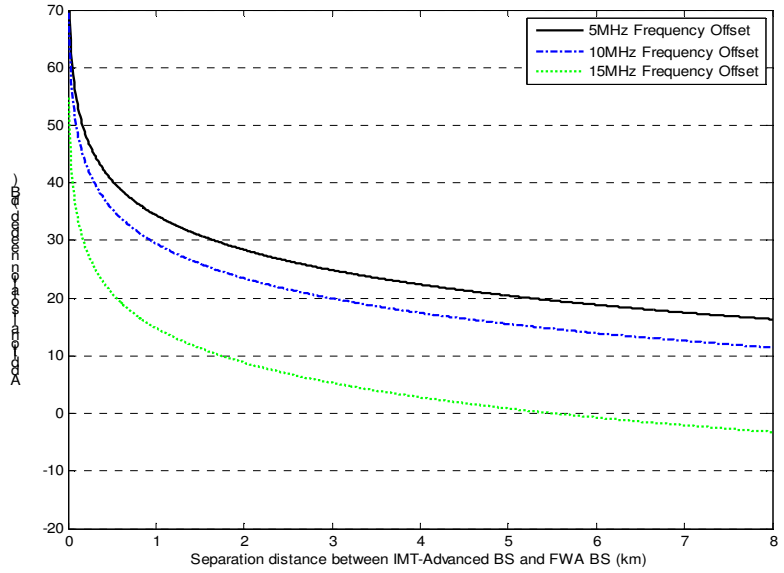

FIGURE 8: Required Additional Isolation When FWA is Victim (IMT-Advanced 20MHz)

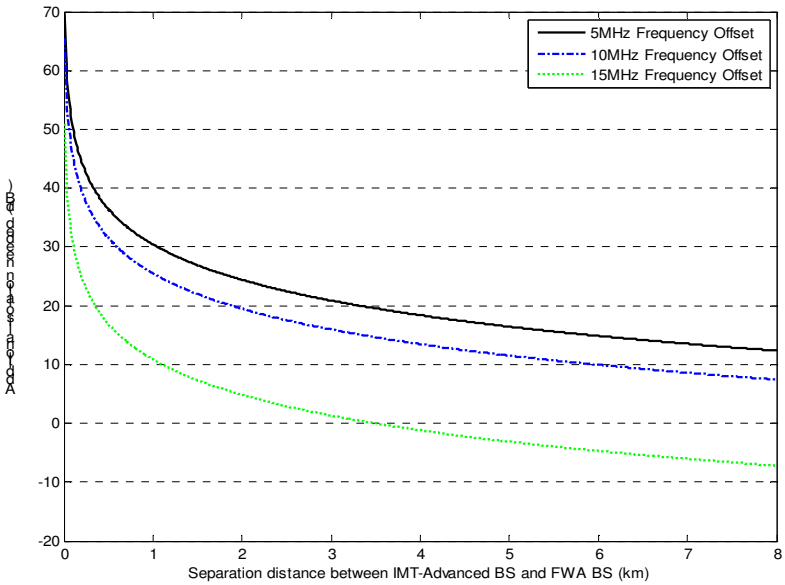

FIGURE 9: Required Additional Isolation When FWA is Victim (IMT-Advanced 50MHz)

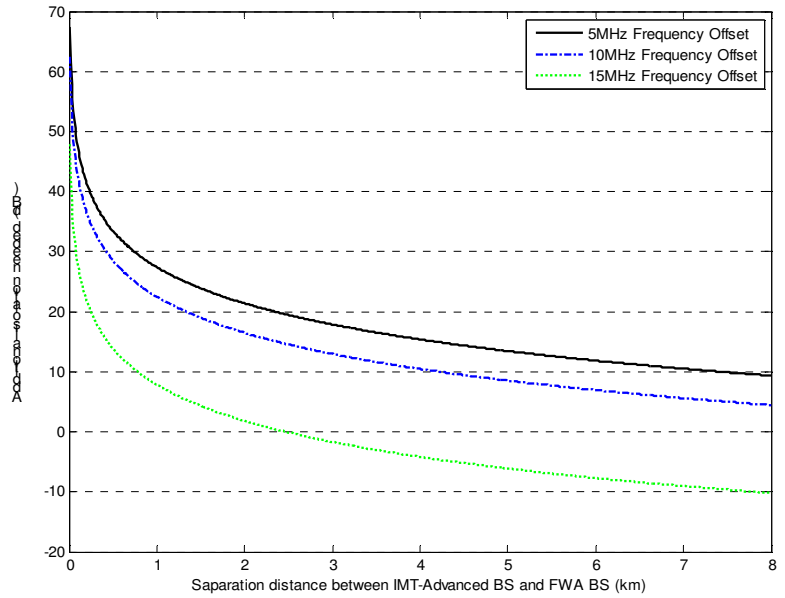

FIGURE 10: Required Additional Isolation When FWA is Victim (IMT-Advanced 100MHz)

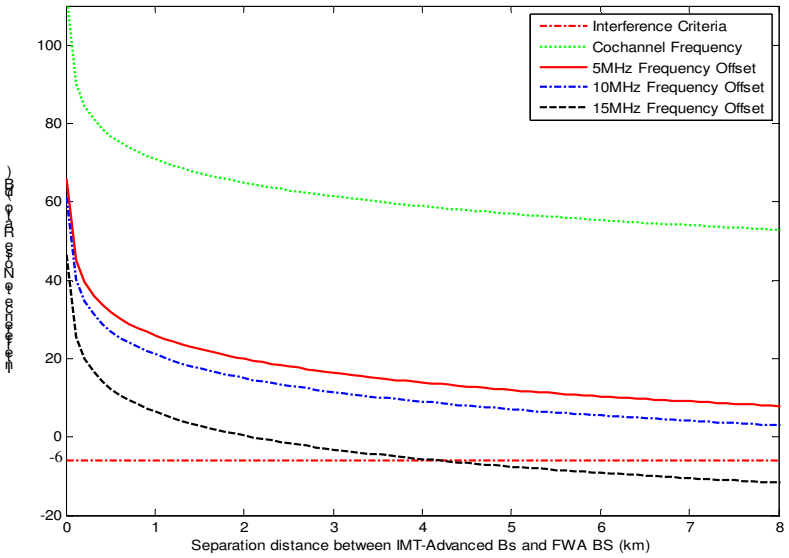

FIGURE 11: Interference from IMT-Advanced (20MHz) into FWA (7MHz)

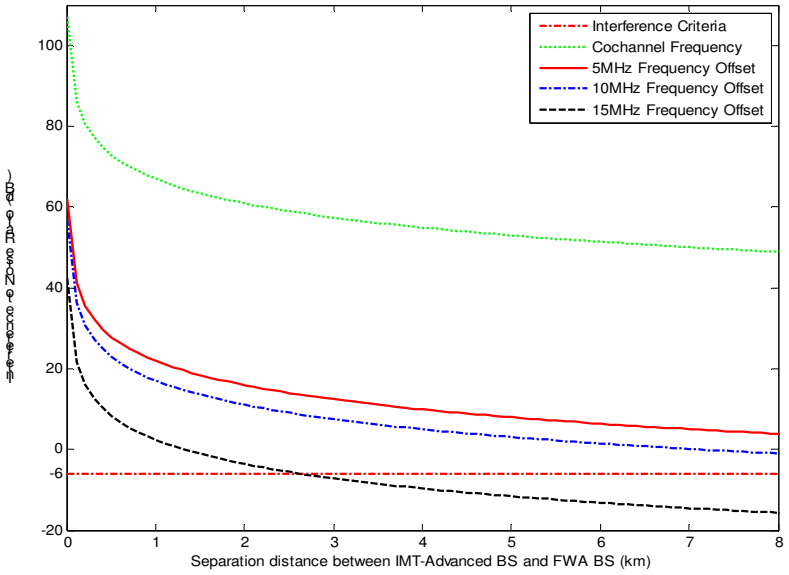

FIGURE 12: Interference from IMT-Advanced (50MHz) into FWA (7MHz)

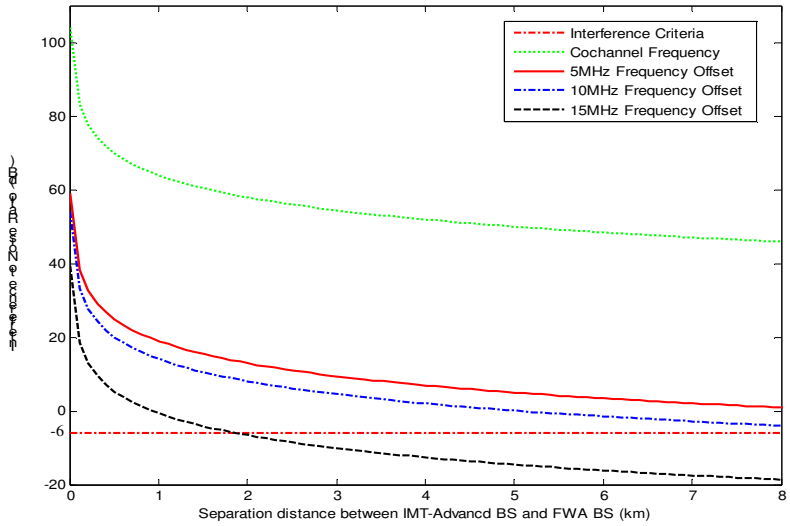

FIGURE 13: Interference from IMT-Advanced (100MHz) into FWA (7MHz)

9. ANALYSIS & COMPATIBILITY

With equipment that just conforms to the standards, it is unlikely to be possible to use a macrocellular IMT-Advanced BS in the same area as a macrocellular FWA BS if LOS path exists between the two antennas and each site is in the main beam of the other site's antenna (i.e., a worst case scenario) without mitigation techniques. As shown in Table 9, by taking ACIR into account, if the BSs operate on the same radio channels they can not coexist for a distance of 8 km or less, because the additional isolation values are 55 dB as aforementioned from the figures. However, coexistence the two BSs in co-channel frequency can be achieved for different separation distances when spectral emission mask of FWA BS is applied as in Table 8. Using ACIR, it makes 1st and 2nd Adjacent channels offsets useless even up to 8 km separation, while 14 MHz adjacent channels may be used for the separation distances in Table 8.

The results indicate that interference impacts form IMT-Advanced on FWA is more worst than the interference from FWA into IMT-Advanced, This is because of the effect of ACIR is more strict than spectral mask of FWA system, high power and high antenna gain of IMT-Advanced system. For coexistence reliability, either or both large separation distance and more frequency separation should be achieved. Therefore, the minimum separation distance and frequency separation in Table 9 should be taken into account for deploying the two systems without an interference mitigation technique because it represents the worst case scenario between them. This means that (when FWA is a victim) the coexistence is feasible only for the 3rd adjacent channel frequency (15MHz) at separation distances of 4km, 2.3km, and 1.8km for IMT-Advanced bandwidths of 20MHz, 50MHz and 100MHz, respectively.

IMT-Advanced Bandwidth	Co-channel Frequency		Adjacent Channel Frequency		Required Guard Band	
	km	MHz	km	MHz	km	MHz
100 MHz	1.4	0.0	0.0045	14	------	NO
50 MHz	2	0.0	0.0065	14	------	NO
20 MHz	3.25	0.0	0.01	14	0.01	0.5

Table 8: The Possible Minimum Separation Distance and Frequency Offset To Achieve Coexistence When IMT-Advanced BS is Victim (Using Spectral Emission Mask)

IMT-Advanced Bandwidth	Co-Channel Frequency	Adjacent Channel Frequency		
		offset @ 5MHz	offset @ 10MHz	offset @ 15MHz
100 MHz	NO	NO	NO	1.8km
50 MHz	NO	NO	NO	2.3km
20 MHz	NO	NO	NO	4km

Table 9: Possible Minimum Separation Distance (Less Than 8 Km) to Achieve Coexistence When FWA BS is Victim (Using ACIR)

10. ADDITIONAL ISOLATION BALANCE & INTERFERENCE MITIGATION

There are many intersystem interference mitigation techniques which may be applied to reduce interference and increase isolation between systems. The suggested mitigation techniques which are able to compensate additional isolation and get *I/N* ratio high are as follows.

10.1 Site Engineering Techniques

The techniques mentioned in [27] and [28] aim to improve antenna coupling and isolation, they can be categories into co-sited antennas techniques like, vertical separation (vertical end-to-end), horizontal separation (side-by-side) and horizontal separation (back-to-back). Also non co-sited antennas techniques using down tilt the antennas and mounting the antennas at different heights.

10.2 Transmitter & Receiver Equipments Enhancement

Improving of ACLR of transmitter, ACS of receiver and thus improving net filter discrimination lead to reduce interference between systems. Strict spectral emission mask may be provide a coexistence environment as well [25], [26].

10.3 Additional Filtering

In order to reduce the interference between systems operating in adjacent frequency bands an additional filtering is included to improve the transmitter ACLR and /or the receiver ACS. Filtering can add 9 to15dB improvements at 5MHz offset, 68dB at 10MHz offset [28], while, power amplifier linearization techniques can achieve 18dB at 5MHz offset and 13dB at 10MHz offset 60dB attenuation with minimal insertion loss is achievable with readily available low cost technology [29].

10.4 Antenna Adjustment

This scheme includes antenna polarization, antenna azimuth and antenna discrimination, it may be used to lower interference impacts [24], [28].

10.5 Transmission Power Reducing

The automatic power control is being used in the most existing cellular systems. To achieve the same coverage with less power more base stations may be required. Alternatively reducing propagation losses can be employed by moving of the base stations to be closer to the system users. This mechanism provides 0 to 15dB isolation for all interference modes [23], [25].

10.6 Smart (Adaptive) Antenna

Smart antenna [20] systems employ digital signal processing and introduce the concept of beam agility (beam forming), null steering and represent an evolutionary step in BS implementation. With this capability, smart antennas can ‘track’ users and, by dynamically adapting the composite beam pattern, realize significant Signal to Interference Ration (SIR) gains that, in turn, can be used to improve coverage and/or capacity and reduce interference caused to and received from other networks operating in the vicinity especially in mobile. Smart antennas provide a little impact on ‘peak’ interference but do significantly reduce the probability of interference. They can also substantially reduce the system sensitivity to incoming interference, particularly in the case

of the more advanced MIMO systems, which are a core feature of IMT-Advanced, and mobile WiMAX systems [30].

11. CONCLUSION

The additional isolation, separation distance and frequency separation required to protect interference are calculated and simulated. From above analysis and results, the most severity interference appears at co-located BSs scenario and the effect of ACIR is stricter than spectral emission mask for adjacent channel coexistence. Methods for enabling the coexistence of both systems would be inevitable especially at small geographical offset between two systems and at co-channel, 1st and 2nd adjacent channels frequencies. In general, the BSs which are either co-sited or non co-sited may be require antenna adjustment, additional filtering and site engineering to facilitate coexistence and sharing between the two terrestrial systems. Therefore, in order to help and ease both systems to operate together at either co-channel or adjacent channel mitigation techniques must be deployed and developed.

12. REFERENCES

1. IST-4-027756 WINNER II D 5.10.1. "*The WINNER role in the ITU process towards IMT-Advanced and newly identified spectrum*". Vo1.0, Nov. 2007.

2. J. H-Shin, Y. H-Goo, L. Jaewoo, C. Woo-Ghee, Y. Jong-Gwan, P. Han-Kyu. "*The coexistence of OFDM-based systems beyond 3G with Fixed service microwave system".* Journal of Communications and Networks, 8(2):187-193, 2006.

3. CEPT ECC Report 100. "*Compatibility Studies in the Band 3400- 3800 MHz between broadband wireless access (BWA) systems and other services*". 2007.

4. ITU-R M.1645. "*Framework and overall objectives of the future development of IMT 2000 and systems beyond IMT 2000*. 2003.

5. A. Mihovska, R. Prasad. "*Secure personal networks for IMT-Advanced connectivity*". Springer Science+Business Media, LLC. 2008.

6. ITU-R IMT.TECH, 18-07-0026-00-0000_ IMT_ Advanced.doc.

7. P. Scheele. "*WINNER-final meeting on WRC-07 outcome (on IMT)*". BNetzA, Munich, 2007.

8. ETSI EN 302 326-2 (V1.2.2). "*Fixed radio systems; multipoint equipment and antennas; part 2: harmonized EN covering the essential requirements of article 3.2 of the R&TTE directive for digital multipoint radio equipment*". 2007.

9. ETSI EN 301 021 (V1.6.1). "*Fixed radio systems; point-to-multipoint equipment; time division multiple access (TDMA); point-to-multipoint digital radio systems in frequency bands in the range 3 GHz to 11 GHz*". 2003.

10. 3GPP. "*Radio frequency system scenarios*, 3GPP TS 25.942 Version 6.4.0, March 2005.

11. I. Ferdo. "*4 GHz for 4G: Why, How and When?".* IEEE Conference, pp. 831-834, 2006.

12. ITU-R Document 8F/1015-E. "*Sharing Studies between FSS and IMT-Advanced systems in the 3400-4200 and 4500-4800 MHz bands*". 2006.

13. MCMC SRSP – 507a. "*Requirements for FWA systems operating in the frequency band from 3400 MHz to 3700 MHz*". No.1, 2001.

14. Report ITU-R M. [LMS.CHAR.BWA]. "*Characteristics of broadband wireless access systems operating in the mobile service for frequency sharing and interference analyses"*. 2006.

15. P. Gardenenier, M. Shafi, B. Vernall, and M. Milner. "*Sharing issues between FPLMTS and fixed services*". IEEE Comm. Mag., 32(6): 74-78, 1994.

16. NTIA Report 05-432. "*Interference protection criteria phase1- compilation from existing sources*". 2005. Available: http://www.ntia.doc.gov/osmhome/reports/ntia05-432/ipc_ phase_ 1 _ report.pdf.

17. IEEE Std. 802.16.2-2004. "*IEEE recommended practice for local and metropolitan area networks coexistence of fixed broadband wireless access systems*". 2004.

18. ITU-R Recommendation F.1402. "*Frequency sharing criteria between a land mobile wireless access system and a fixed wireless access system using the same equipment type as the mobile wireless access system*". 1999.

19. Engineering Services Group (Qualcomm incorporated). "*Interference analysis and guidelines for coexistence".* The 3rd Meeting of the APT Wireless Forum, 2006.

20. Allgon. "Antenna to antenna isolation measurements". 3GPP TSG RAN WG4 Meeting No.8, TDOC 631/99, 1999.

21. ITU-R P.452-12. "*Prediction procedure for the evaluation of microwave interference between stations on the surface of the earth at frequencies above about 0.7 GHz*". 2005.

22. ITU-R Document 8F/1015-E. "*Sharing studies between FSS and IMT-Advanced systems in the 3400-4200 and 4500-4800 MHz bands*". 2006.

23. Ofcom. " *Digital dividend–mobile voice and data* (IMT) issues". Mason Communic. Ltd., 2007.

24. WiMAX Forum. "*Service recommendations to support technology neutral allocations FDD/TDD coexistence".* 2007.

25. Ofcom. "*2500-2690MHZ, 2010-2025MHz, 2290-2302MHz Spectrum Awards Engineering Study (Phase 2)"*. Mason Communications Ltd., 2006.

26. ITU-R Document (ITU-R M. 2113). "*Draft new report on sharing studies in the 2 500-2 690 MHz band between IMT-2000 and fixed broadband wireless access (BWA) systems including nomadic applications in the same geographical area"*. 2007.

27. 3GPP. "User equipment (UE) radio transmission and reception (TDD)". 3GPP TS 25.102 Version 5.1.0.

28. Draft Report for ITU-R M.2045. "Mitigating techniques to address coexistence between IMT-2000 TDD and FDD radio interface technologies within the frequency range 2 500-2 690 MHz operating in adjacent bands and in the same geographical area". 2004.

29. T. Wilkinson, and P. Howard. "The Practical realities of 3GPP TDD and FDD co-existence and their impact on the future spectrum allocation". In Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Barcelona, Spain, 1: 22- 26, 2004.

30. Rscom07-69. "Radio spectrum committee final report, from CEPT in response to the EC mandate on the digital dividend". Part B, 2007.

Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad Hoc Networks

R.Asokan

asokece@yahoo.com
Assistant Professor
Electronics and Communication Engineering Department,
Kongu Engineering College, Perundurai, Erode 638052, Tamilnadu, India

A.M.Natarajan
Chief Executive and Professor
Bannari Amman Institute of Technology
Sathiyamangalam, Tamilnadu, India

C.Venkatesh

Professor
Electronics and Communication Engineering Department,
Kongu Engineering College, Perundurai, Erode 638052, Tamilnadu, India

Abstract

Quality of Service (QoS) support for Mobile Ad hoc Networks (MANETs) is an exigent task due to dynamic topology and limited resource. To support QoS, the link state information such as delay, bandwidth, jitter, cost, error rate and node energy in the network should be available and manageable. The focus of this paper is extending the scope to QoS routing procedure, to inform the source about QoS available to any destination in the wireless network. However, existing QoS routing solutions were dealt with only one or two of the QoS parameters. It is important that MANETs should provide QoS support routing, such as acceptable delay, jitter and energy in the case of multimedia and real time applications. This paper proposes a QoS Dynamic Source Routing **(**DSR) protocol using Ant Colony Optimization (ACO) called Ant DSR (ADSR).The performance of DSR and ADSR are analyzed using network simulator-2. ADSR produces better results than the existing DSR in terms of delay, energy, jitter and throughput.

Keywords: Ad Hoc Networks, Quality of Service, Dynamic Source Routing, ACO and ADSR

1. INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile devices, which form a communication network with no pre-existing wiring or infrastructure. Routing in mobile ad hoc networks is challenging since there is no central coordinator, such as base station, or fixed routers as in other wireless networks that manage routing decisions. All nodes in MANETs cooperate in a distributed

manner to make routing decisions. Multiple routing protocols have been developed for MANETs. In proactive protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

The Destination Sequenced Distance Vector (DSDV) routing protocol, Wireless Routing Protocol (WRP), and Cluster-head Gateway Switch Routing (CGSR) protocol are some examples for the protocols that belong to this category. Protocols that fall under reactive protocols category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence, these protocols do not exchange routing information periodically. The Dynamic Source Routing (DSR) protocol, Ad hoc On-demand Distance Vector (AODV) routing protocol, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR) are some examples for the protocols that belong to this category [1].

Quality of Service (QoS) is usually defined as a set of service requirements that need to be met by the network while transporting a packet stream from source to destination. With the increasing needs of QoS provisioning for evolving applications such as real-time audio/video, it is desirable to support these services in ad hoc networking environments. The network is expected to guarantee a set of measurable specified service attributes to the user in terms of end-to-end delay, bandwidth, probability of packet loss, energy and delay variance (jitter).

The QoS metrics can be classified as additive metrics, concave metrics, and multiplicative metrics. Bandwidth and energy are concave metrics, while cost, delay, and jitter are additive metrics. Bandwidth and energy are concave in the sense that end-to-end bandwidth and energy are the minimum among all the links along the path. The end-to-end delay is an additive constraint because it is the accumulation of all delays of the links along the path. The reliability or availability of a link based on some criteria such as link break probability is a multiplicative metric. Finding the best path subject to two or more additive/concave metrics is a complex problem. A possible solution to route dealing with additive and non-additive metrics is to use an optimization technique.

Ant Colony Optimization (ACO) is a subset of Swarm Intelligence. The basic idea of the ant colony optimization is taken from the food searching behavior of real ants [2]. When ants are on the way to search for food, they start from their nest and walk toward the food. When an ant reaches an intersection, it has to decide which branch to take next. While walking, ants deposit a pheromone, which ants are able to smell, which marks the route taken. The concentration of pheromone on a certain path is an indication of its usage. With time, the concentration of pheromone decreases due to diffusion effects. This property is important because it is integrating dynamic into the path searching process.

The rest of the paper is organized as follows. In section two, the previous work related to QoS routing protocols is briefly reviewed. In section three, enhanced version of DSR based on Ant Colony Optimization (ACO) called Ant Dynamic Source Routing (ADSR) is described. In section four, the major simulation results are shown. In section five, the result of the work done is summarized.

2. RELATED WORK

QoS support in MANETs includes QoS models, QoS resource reservation signaling, QoS Medium Access Control (MAC), and QoS routing [3]. This paper discusses some key design considerations in providing QoS routing support, and presents a review of previous work addressing the issue of route selection subject to QoS constraints.

Core-Extraction Distributed Ad hoc Routing (CEDAR) algorithm is designed to select routes with sufficient bandwidth resources. CEDAR dynamically manages a core network, on which the state information of those stable high bandwidth links is incrementally propagated. CEDAR selects QoS routes upon request [4].

A number of successful ant-based routing algorithms exist for wired networks, and are based on the pheromone trail laying-following behavior of real ants and the related framework of Ant Colony Optimization (ACO). Ant based routing algorithms exhibit a number of desirable properties for MANET routing: they work in a distributed way, are highly adaptive, robust and provide automatic load balancing. AntNet is an algorithm conceived for wired networks, which derives features from parallel replicated Monte Carlo systems, previous work on artificial ant colonies techniques and telephone network routing [5]. The idea in AntNet is to use two different network exploration agents (forward and backward ants), which collect information about delay, congestion status and the followed path in the network.

Ant based Control (ABC) is another ant based algorithm designed for telephone networks. It shares many similarities with AntNet, but also incorporates certain differences [6]. The basic principle relies on mobile routing agents, which randomly explore the network and update the routing tables according to the current network state. The routing table stores probabilities instead of pheromone concentrations.

Ant Colony Based Routing Algorithm (ARA) works in an on-demand way, with ants setting up multiple paths between source and destination at the start of a data session [7]. Probabilistic Emergent Routing Algorithm (PERA) works in an on-demand way, with ants being broadcast towards the destination at the start of a data session. Multiple paths are set up, but only the one with the highest pheromone value is used by data and the other paths are available for backup [8].

AntHocNet is based on ideas from Ant Colony Optimization [9]. AntHocNet uses end-to-end delay as a metric to calculate congestion at a node, which may not yield accurate results as end-to-end is affected by both congestion as well as the length of the route from source to destination. ANSI (Ad hoc Networking with Swarm Intelligence) is a congestion-aware routing protocol, which, owing to the self-configuring mechanisms of Swarm Intelligence, is able to collect more information about the local network and make more effective routing decisions than traditional MANET protocols. ANSI is thus more responsive to topological fluctuations [10].

A unicast on-demand routing protocol Swarm-based Distance Vector Routing (SDVR) is proposed to optimize three parameters delay, jitter, and energy[11].Ant-like agents are used in this algorithm to discover and maintain paths with the specified QoS requirements in Ad hoc On demand Distance Vector routing (AODV) protocol. SDVR produces better performance than AODV in terms of packet delivery ratio, end-to-end delay, energy, and jitter.

3. ANT DYNAMIC SOURCE ROUTING (ADSR)

This paper proposes an enhanced version of DSR based on Ant Colony Optimization (ACO) called Ant Dynamic Source Routing (ADSR) and it takes into consideration of three QoS parameters delay, jitter and energy.

3.1 Ant Colony Optimization (ACO)

Two of the most successful swarm intelligence techniques are Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO). ACO is a meta-heuristic optimization algorithm that can be used to find approximate solutions to difficult combinatorial optimization problems. In ACO artificial ants build solutions by moving on the problem graph and they, mimicking real ants,

deposit artificial pheromone on the graph in such a way that future artificial ants can build better solutions. ACO has been applied successfully to an impressive number of optimization problems. PSO is a global minimization technique for dealing with problems in which a best solution can be represented as a point or surface in an n-dimensional space.
ACO is application of ant's behavior to complex computational optimization problems. ACO is inspired by the foraging behavior of ant colonies, wherein they are able to find shortest path between two points through collective learning. Learning is achieved by deposition of a chemical called pheromone. ACO is based on real ant's behavior in finding a route to food nest. It has been observed that of available routes, ants find shortest route to food nest. To achieve this, ant communicates through deposition of chemical substance called pheromone along the route. Shortest path has highest concentration leading to more and more ants using this route.

Basic Ant Algorithm
The basic idea of the ant colony optimization Meta heuristic is taken from the food searching behavior of real ants. Figure 1 shows a scenario with two routes from the nest to the food place. At the intersection, the first ants randomly select the next branch. Since the route below is shorter than the upper one, the ants that take this path will reach the food place first.

FIGURE 1: Ants take the shortest path after an initial searching time

On their way back to the nest, the ants again have to select a path. After a short time the pheromone concentration on the shorter path will be higher than on the longer path, because the ants using the shorter path will increase the pheromone concentration faster. The shortest path will thus be identified and eventually all ants will only use this one. This behavior of the ants can be used to find the shortest path in networks. Especially, the dynamic component of this method allows a high adaptation to changes in mobile ad hoc network topology, since in these networks the existence of links are not guaranteed and link changes occur very often.

3.2 Ant Dynamic Source Routing (ADSR)
Dynamic Source Routing (DSR) protocol is an on-demand routing protocol that is based on the idea of source routing [12]. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learnt. The protocol consists of two major phases: route discovery and route maintenance.

Route Request
When a mobile node has a packet to send to the destination, it first consults its route cache to determine whether it previously has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record.

Route Reply

A route reply is generated when the route request either reaches the destination itself, or reaches an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator. If it has a route to the initiator in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record. If symmetric links are not supported, the node may initiate its own route discovery and piggyback the route reply on the new route request.

Route maintenance

Route maintenance is accomplished through the use of route error packets and acknowledgments. Route error packets are generated at a node when the data link layer encounters a transmission problem. When a route error packet is received, the hop in error is removed from the node's route cache and all routes containing the hop are truncated at that point. In addition to route error messages, acknowledgments are used to verify the correct operation of the route links. Such acknowledgments include passive acknowledgments, where a mobile is able to hear the next hop forwarding the packet along the route.

In Ant DSR (ADSR) the Forward ant (FANT) and backward ant (BANT) packets are added in the route request and route reply of DSR respectively as shown in figure 2 and 3. FANT and BANT packets are used in this route discovery process.

IP Header	DSR Fixed Header	Source Address	Sequence Number	Destination Number	Delay Energy Jitter	Route Record	Hop Count	Route Address Add1, Add2 -- Addn

FIGURE 2: ADSR Route Request Packet format

IP Header	DSR Fixed Header	Source Address	Destination Address	Delay Energy Jitter	Dynamic Route Record	Sequence Number	Reply Address Address source Add1, Add2 --Addr dest

FIGURE 3: ADSR Route Reply Packet format

Forward ants are used to explore new paths in the network. Ants measure the current network state for instance by trip times, hop count or Euclidean distance traveled. Backward ants serve the purpose of informing the originating node about the information collected by the forward ant. The ant routing has two types of feedback: positive feedback increases the pheromone levels on routes actively carrying ant packets and negative feedback periodically decreases pheromone values to limit the effects of stale information. Routing decisions tend to support paths with higher pheromone levels and, when allowed to converge, shortest end-to-end paths are empirically observed to be favored. Modified ant mechanism algorithm that uses energy, delay and jitter metrics to perform updates of pheromone levels is proposed. Assuming a control packet containing energy, delay and jitter metrics, a separate pheromone level will be maintained for each metric [11].

In the algorithm, ant packet headers have fields that:

1. track the minimum residual energy of the nodes that relay them and
2. track the cumulative delay and jitter based on backlog information of queued packets destined to the packet's source.

Thus, energy, delay and jitter pheromone levels will be maintained at each node.

4. PERFORMANCE EVALUATION

The performance of DSR and ADSR protocol is evaluated using the ns-2 simulator [13]. Throughput, end-to-end delay, routing overhead, jitter and residual node energy are used as metrics to compare the performance of DSR with ADSR. Table 1 lists the simulation parameters and environments used.

Simulation Parameters	
Simulation area (Grid size)	500m x 500m
Number of nodes	100
Node communication range	50 m
Protocol	DSR and ADSR
Medium access mechanism	IEEE 802.11b
Traffic source model	Constant bit rate
Packet size	1024 Bytes
Mobility model	Random waypoint
Initial Node Energy	100 J

TABLE 1: Simulation parameters

4.1 End-to-end Delay

Figure 4 shows effect of pause time on end-to-end delay of the two protocols. End-to-end delay tends to increase as the pause time increases in both protocols. The end-to-end delay is reduced by applying ADSR. This is mainly due to adding of delay pheromone in the RREQ and RREP packets. The reduction in delay is maximum (15 %) when the pause time reaches 300 seconds. Both protocols have same delay for higher pause time.

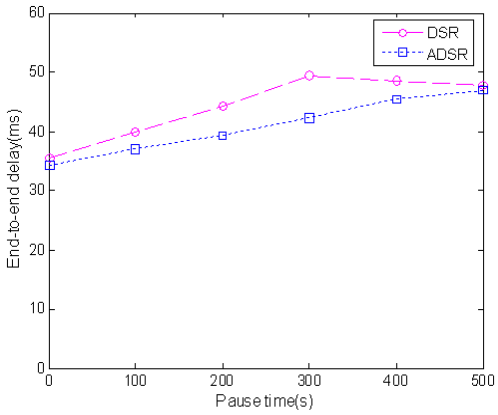

FIGURE 4: Effect of pause time on end-to-end delay

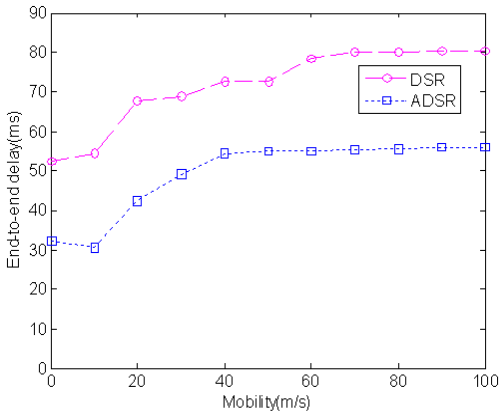

FIGURE 5: Effect of mobility on end-to-end delay

Figure 5 shows the effect of mobility on end-to-end delay. The end-to-end delay increases as the mobility increases. Higher mobility causes more link breaks and frequent re-routing, thus causing larger end-to-end delay. ADSR shows better performance in all the mobility conditions and the improvement over DSR is around 44%.

4.2 Energy

Figure 6 shows the effect of pause time on energy. The remaining energy of ADSR is 11% higher than DSR, since the energy pheromone is added in the route request and route reply of DSR packets. Figure 7 shows the effect of mobility on residual node energy. Residual node energy decreases with the increase in mobile speed, due to more link failures. The residual energy is high in ADSR than DSR because of energy pheromone is added in the route request and the route reply of DSR. The improvement over DSR is varies from of 6 to 26%.

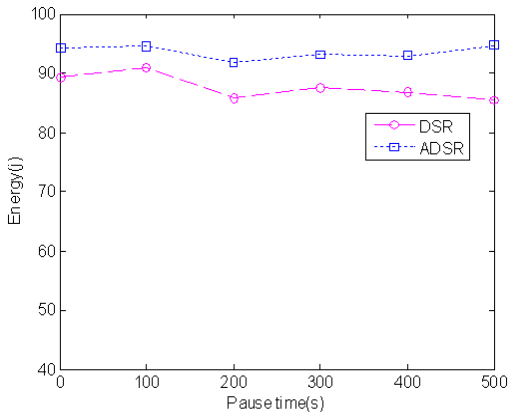

FIGURE 6: Effect of pause time on energy

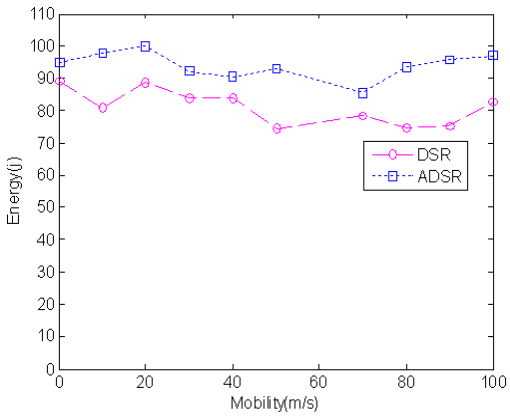

FIGURE 7: Effect of mobility on energy

4.3 Jitter

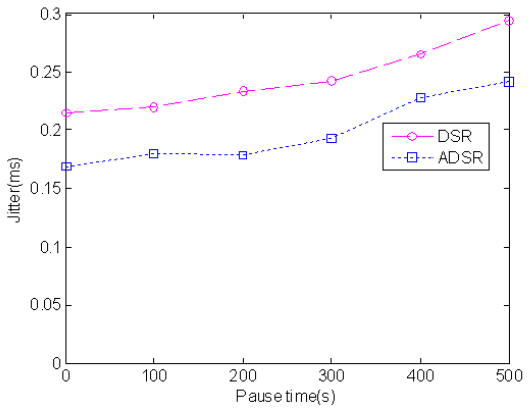

FIGURE 8: Effect of pause time on jitter

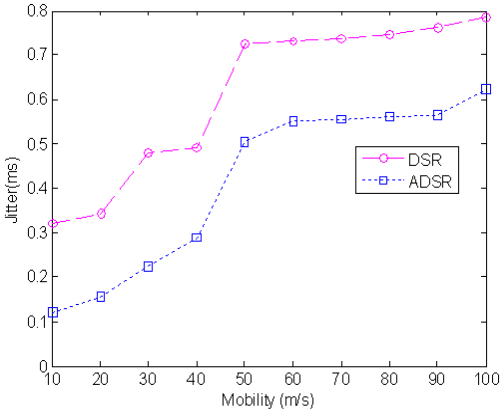

FIGURE 9: Effect of mobility on jitter

Figure 8 shows effect of pause time on jitter. The jitter is reduced in ADSR by 14 to 25%. This is due to addition of jitter pheromone in the route request and route reply. The variations in jitter under different mobility conditions are shown in Figure 9. The jitter is increased at higher mobility due to breaking of more links and frequent re-routing. The reduction in jitter varies from 24 to 30%. This is due to jitter pheromone included in the route request and route reply. ADSR gives better performance than DSR in all the mobility conditions.

4.4 Throughput

Figure 10 shows the effect of pause time on throughput. Number of packets received in the destination is calculated and taken as throughput. The improvement over DSR is high for low pause time. The throughput under different mobility values is shown in Fig. 11. It can be seen that increase in node speed results in significant decrease in throughput in both the protocols. This is due to more link breaks. ADSR shows around 5% improvement in throughput over DSR.

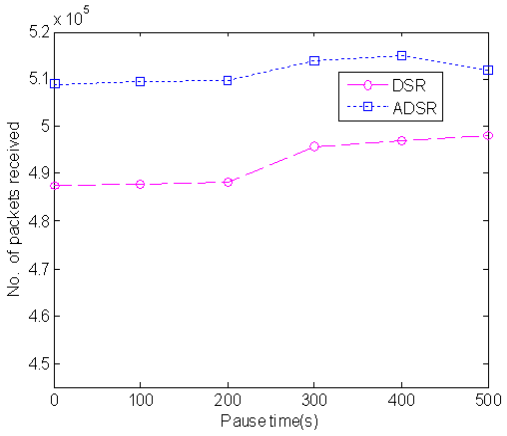

FIGURE 10: Effect of pause time on throughput

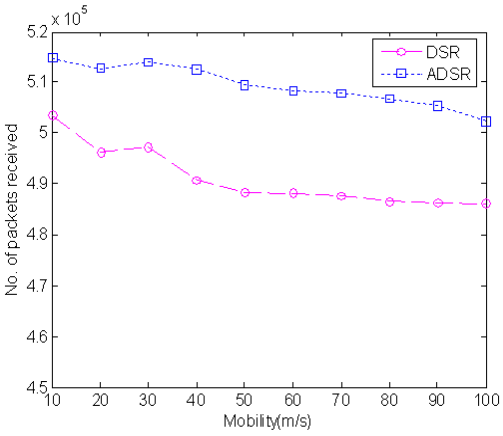

FIGURE 11: Effect of mobility on throughput

4.5 Routing Overhead

The effect of pause time on routing overhead is shown in Fig.12. Since more control packets are required at the route discovery phase and extra control packets are required periodically to monitor the condition of the paths, the routing overhead of ADSR is slightly higher than that of other protocol. The overhead for path monitoring can be reduced by piggybacking the pheromone information on data packets if appropriate traffic exists in opposite direction.

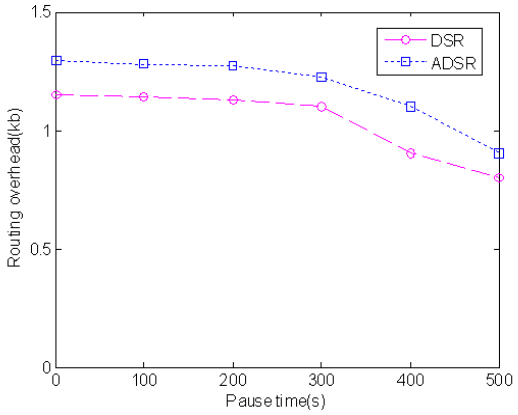

FIGURE 12: Effect of Pause Time on Routing Overhead

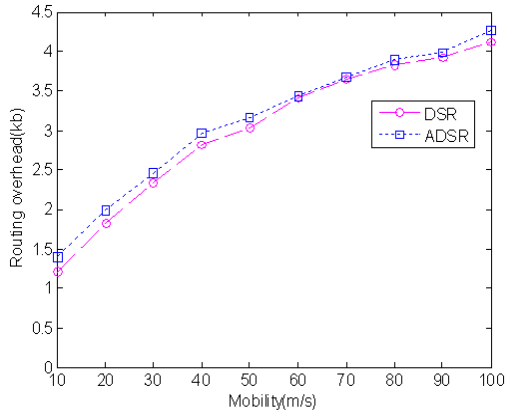

FIGURE 13: Effect of Mobility on Routing Overhead

The effect of mobility on routing overhead is shown in Fig.13. Higher mobility causes more links broken and frequent re-routing and thus causes larger routing overhead. Because of the periodic updates, ADSR requires certain amount of routing overhead constantly. The routing overhead due to mobility is slightly higher than that of DSR due to the use of FANTs and BANTs control packets.

5. CONCLUSION AND FUTURE WORK

In this paper, DSR based on-demand routing algorithm ADSR is proposed to optimize three QoS parameters delay, jitter and energy using Ant Colony Optimization (ACO). This avoids the overhead of having three independent routing algorithms, one for each QoS metric. The mechanism was based on the Forward ant (FANT) and backward ant (BANT) packets added in the route request and route reply. The proposed protocol selects a minimum delay path with the maximum residual energy at nodes. Furthermore, the selection of QoS routes should also take into consideration the jitter metric in order to keep the minimum and maximum delay values approximate to the average delay. ADSR produced better results than the existing DSR in terms of packet delivery ratio, end-to-end delay and residual energy at node. Even though ADSR results in a slightly high routing overhead than DSR, it performs well in route discovery with dynamic changes in the network topology and produces much better throughput with very low variance in the delay. Further, this can be implemented on the other reactive and hybrid routing protocols.

6. REFERENCES

1. E.M.Royer and C.K. Toh*, " A review of current routing protocols for ad hoc mobile wireless networks*" IEEE Personal Communications , 6(2): 46-55 , 1999

2. Z.Liu , M. Z. Kwiatkowska and C. Constantinou , "*A biologically inspired QoS routing algorithm for ad hoc networks"*, International Conference on Advanced Information Networking and Applications, AINA 2005 1: 426-431, 2005

3. Z.Baoxian , T. M. Hussain, "*QoS routing for wireless ad hoc networks: Problems, algorithms, and protocols,* IEEE Comm. Magazine , 43(10): 110-117, 2005

4. P.Sivakumar , P.Sinha and V.Bharghavan, "*CEDAR: A core-extraction distributed ad hoc routing algorithm*" Special Issue on Wireless Ad hoc networks, 17(8): 1454–65 ,1999

5. G.Di Caro, and M. Dorigo, "*AntNet: Distributed stigmergetic control for communications networks".* Journal of Artificial Intelligence Research, 9:317–365 , 1988

6. R.Schoonderwoerd , O. E. Holland, J. L.Bruten, and L.J.Rothkrantz, "*Ant-based load balancing in telecommunications networks"*, Adaptive Behavior, 5 :169–207 ,1996

7. M.Gunes, U. Sorges and I. Bouazizi, "*ARA: Ant-Colony based routing algorithm for MANETs"*, In Proc. of ICPPW, Vancouver, B.C., Canada. 18-21. 2002

8. J.S.Baras and H.Mehta, "*PERA:A probabilistic emergent routing algorithm for mobile Ad hoc Networks"* in WiOpt'03 Sophia-Antipolis, France ,2003

9. G.Di Caro, F. Ducatelle and L. M. Gambardella, "*AntHocNet: An ant-based hybrid routing algorithm for mobile Ad hoc networks",* in Proc. of PPSN VIII.LNCS. Springer-Verlag ,2004

10. S.Rajagopalan, C.C.Shen, "*ANSI: A unicast routing protocol for mobile networks using Swarm Intelligence",* Proc. of Intl. Conference on Artificial Intelligence, 24-27. 2005

11. R.Asokan, A.M.Natarajan and A.Nivetha "*A Swarm-based Distance Vector Routing to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad hoc Networks"* Journal of Computer Science 3(9):700-707 ,2007

12. D.B.Johnson and D.A Maltz . "*Dynamic source routing in ad hoc wireless networks*," in Mobile Computing, Kluwer Academic Publishers, 353(5):153–181 , 1996

13. The network simulator - Ns-2. http://www.isi.edu/nsnam/ns.

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA