Global Journal of Embedded System in Engineering Research

Volume No. 12

Issue No. 1

January - April 2024

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

Global Journal of Embedded System in Engineering Research

Aims and Scope

The Global Journal of Embedded System in Engineering Research is published 3 times in a year by Enriched publications. Global Journal of Embedded System in Engineering Research is peer reviewed journal and monitored by a team of reputed editorial board members. This journal consists of research articles, reviews, and case studies on Electrical and Electronic Engineering. This journal mainly focuses on the latest and most common subjects of its domain.

Global Journal of Embedded System in Engineering Research

Global Journal of Embedded System in Engineering Research

(Volume No. 12, Issue No. 1, January - April 2024)

Contents

Non-Functional Requirements for Cloud Computing

Yahiya Gazi and Shahnawaz Ahmad
M. Tech. Scholar, Department of Computer Science and Engineering,
Al-Falah School of Engineering and Technology,
Dhauj, Faridabad, Haryana, India.
E-mail:yahiyaghazi@gmail.com
Shahnawaz98976@gmail.com

A B S T R A C T

In Cloud computing represents a solution with high reliability and performance through using non-functional requirements (NFRs) needs where usage patterns, and therefore resource requirements, may research on how functionality and Quality depend non exposure or trending. However, in order to take advantage of the cloud's benefits, software engineers need to be able to express the application's needs in Quality terms. Additionally, cloud computing providers have to understand such requirements in the terms of non-functional requirements and offer methods to acquire the necessary infrastructure to fulfill the users' expectations. In this paper, we discuss the design and implementation of non-functional requirements as a Quality of Service for cloud manager such that non-functional requirements determined during the requirements analysis phase can be mapped to properties for a group of Virtual Appliances running the the cloud computing . The discussed management system ensures that expected Quality of Service is maintained during execution and can be considered during different development phases.

I. INTRODUCTION

The emergence of cloud computing responds to a increasing trend in web application emergence and utilization. The wide adoption of Internet has resulted in systems that need to accommodate millions of users [1] and provide capabilities that until now were only required by critical, high availability or high throughput software. The practice of Software Engineering provides methodologies to ensure such characteristics are met, but it is necessary to review how they fit in this new paradigm. In this paper, we explore the applicability of traditional processes to the incipient field of cloud computing from the perspective of our research in an Infrastructure as a Service (IaaS) cloud manager. Internet has resulted in rapid cycles of software development, deployment and consumption by users. The rising numbers of subscribers, better network connectivity and band- width, and the growing connectedness between users

have created new dynamics where applications can be rapidly discovered and consumed. However, the benefits produced by these circumstances are hindered when expected requirements are not met. Nowadays, cloud computing is often employed as a solution to this problem. Capabilities such as pay-per- use, scalability or elastic provisioning of resources can help to overcome these new challenges. Nevertheless, application developers need to recognize how to apply Software Engineering methods to the cloud in order to successfully map their needs to fulfill service expectations. There are two interrelated points that we believe have to be considered to successfully make use of clouds to develop.

Applications that respond to the new demands generated in this field. First, developers must understand which non-functional requirements take renewed importance in cloud applications so that they can be accounted for during the requirements analysis phase. Second, cloud providers need to define better guarantees for their services, so developers can design their systems accordingly. We believe that providing a solution to these problems will result in a more dependable use of clouds to confront the new challenges of this era. In this paper we consider the concept of Distributed Ensembles of Virtual Appliances (DEVAs), introduced in [2], as a model to represent complex systems with Quality of Service (QoS) guarantees. We discuss how software architecture can be mapped to a DEVA, and how through the use of performance modelling and prediction we can make certain assurances about its behaviour in the cloud in order to address its non-functional requirements. We finally present a case study were we demonstrate the feasibility of our approach to model the expected number of requests per second and response time of a web application hosted in the cloud.

II. BACKGROUND

We define a cloud application as any software that runs on a distributed system that complies with the definition of a cloud. Such systems ([3], [4]) possess certain common capabilities such as on-demand provisioning, resource elasticity or pay- per-use billing model. Therefore, cloud applications can be deployed on remote resources with a minimal cost, and scaled dynamically when user demand grows. We consider three main actors in our scenario: application users, application providers, and cloud providers. In this proposed division, application providers also have the role of cloud users, even though in certain cases it would be possible that application and cloud providers are the same individual or organization. The cloud is usually divided in Software, Platform and Infrastructure as a Service—SaaS, PaaS and IaaS respectively. Application providers are in charge of implementing the SaaS layer, while the PaaS and IaaS layers are supplied by cloud providers. A DEVA is a group of Virtual Appliances and virtual network devices, where individual and composite policies can be defined for elements.

Machines with specific functions, usually containing a particular software and configuration; for simplicity, we'll use the more general term VM to refer to them. Figure 1 illustrates the architecture of the DEVA Manager. A user sends a specification for a list of VMs and their associated QoS requirements, which may consist of CPU, memory and required software for individual VMs, and network bandwidth and latency for the network links. Then, the Manager Instantiates the ensemble across heterogeneous resources, which may be located in different administrative domains. A group of agents monitors each VM's behaviour and provides the requested QoS and network isolation.

III. REQUIREMENT ANALYSIS AND ARCHITECTURAL DESIGN

In Software Engineering, the requirements analysis phase is in charge of determining the functional and non-functional requirements of the system based on the client's needs. In particular, non-functional requirements [6] describe the characteristics of the system not related to its functionality. These requirements shape the architecture of the system during the design phase. In this paper we target a class of applications that are specially suited to be hosted in the cloud and have a prevalent set of non-functional requirements. Identifying them allows developers to ensure that they are addressed during the requirement analysis phase, and establish a set of requisites that must be met by cloud providers in order to quantify their service and ascertain the application goals are met successfully. We enumerate the most salient ones next.

Response time

This requirement describes how much time it takes from the moment a user sends a request to the system, until a complete response is provided. In web applications, this com- pretends request transmission and processing, and response transmission. The factors that account for it are resource capabilities —processing power, memory, disk, network latency and bandwidth— and the load produced by other processes running in the server or the number of concurrent requests. For complex requests, this may also involve calls to external systems, or to other subsystems, in which case the host's internal network characteristics and other resources' load may be taken into account.

The total time the service is available. It may be expressed as a percentage. When considering this requirement, it is necessary to take into account the provider's own uptime. For example, if a provider has an uptime of 99.5%, it would be impossible to deploy an application with a higher uptime. Other factors involve the recoverability of the system (i.e., how much time it takes to restart the service after a failure happens).

Requests per unit of time

This requirement describes the number of requests the system can handle successfully per unit of time, and can also be referred to as the system's throughput. Resource allocation and usage has an impact in this parameter. Additionally, the number of requests can have an impact in the response time requirement (i.e., a high number of requests will result in a deterioration of the overall response time).

Fault tolerance

One of the system's properties is how it can withstand errors, either hardware or software-based. In the case of cloud, non-software errors can be generated either at the physical or the virtual machines hosting the service. While the first case is usually out of the developer's control, virtual machine faults can be handled by different means, for example by spawning new instances, or having backup VMs to respond to failures.

IV. SECURITY

Security is another requirement that can be applied to the cloud provider or to the developed system. In the first case, the application developer is under the provider's security measures such as physical infrastructure access policies or network isolation mechanisms. Alternatively, security in the instantiated VMs must be handled by the cloud user.

Operational cost

In traditional systems, hardware was determined based on the application's initial requirements. Changes in requirements would typically result in costly upgrades involving the acquisition of new physical machines and installation and configuration of the application to run on them. In cloud systems, resources can be upgraded almost instantaneously, meaning that cost can be considered a changing variable. This allows defining trade-offs to architectural (static) and operational (dynamic) behavior.

During the requirements analysis, it is the job of the soft- ware engineer to give appropriate values to each of the non- functional requirements according to the user's expectations. Each of these parameters needs to be reflected in one or more architectural decisions and tradeoffs.

V. MAPPING REQUIREMENTS TO DEVAS

The original implementation of the DEVA Manager accepts three types of parameters: nodes (VMs and virtual network devices), edges between nodes, and element annotations. Basic annotations describe node and edge characteristics such as VM processor power or memory size, and link bandwidth and latency, respectively. An application developer could map the assigned non- functional requirement values to any of the discussed DEVA parameters in order to ensure the application's operational guarantees. For example, the number of desired requests per second would influence the assigned

latency for the links between VMs; alternatively, the targeted response time could translate to a minimum processing power for the VMs in the ensemble. However, this process is complicated and error-prone: the relationship between non-functional requirements and low level values is in many cases difficult to determine, and many factors can take part in the fulfillment of one individual parameter. Thus, we propose an extension to our system where non-functional requirements can be directly mapped to the execution platform, not only during the deployment phase, but also along the whole design process. Our proposed approach in this paper extends DEVA an- notations with new high-level values that correspond to non- functional requirements. An underlying application-dependent model is in charge of translating high-level parameters to low- level ones, and performing the required operations on the appropriate elements. We describe our system design next, and discuss its implementation.

A. Processing annotations for DEVAs

Once the user defines a set of nodes, edges and annotations, a request is sent to the DEVA manager, which parses it and assigns the virtual resources to physical hosts that can comply with the requested QoS parameters. At each host, a number of VMs and virtual network links are created so that the ensemble appears as an isolated group of machines with dedicated resources. Additionally, a set of DEVA Agents are in charge of monitoring the infrastructure usage and ensuring global and individual QoS.

Requirements in the request are realized in two phases: first, the scheduling module of the manager chooses the target resources so that the ensemble requirements can be met. This implies selecting hosts with enough free memory and CPU for the VMs and ensuring the underlying physical network will be able to support the requested bandwidth and latency. Second, control measures are applied to constraint resource usage so that shared requests don't interfere among them. VM resources are adjusted by a Virtual Machine Monitor such as Xen or VMWare running in the target host, while network resources are controlled by a DEVA Agent. Agents apply shaping and monitoring to manage network QoS. In order to implement high-level annotations representing non-functional requirements, we need to extend the DEVA manager and agents so that the new parameters can be translated into the existing ones. Figure 2 shows the system architecture with the new components in a darker shade. First, the manager needs to translate non-functional requirements into values that can be considered as part of the scheduling process. We provide a non-functional requirement (NFR) Parser that is in charge of converting high-level values to low-level ones. For this, a Static Application Model is employed. Such model is dependent on the type of application, and can be defined either theoretically or empirically. We define a global annotation for the request, where the user can specify the application type. The value of this annotation will determine the model to use in the scheduler. The Non-Functional Requirements Parser

generates a set of requirements for nodes and connections based on the translated parameters, and these are fed to the scheduler, which takes them into account to generate a list of physical machine candidates. Each of the candidates is assigned a number of VMs to host. Finally, the Infrastructure manager, implemented in our system by Open Nebula, sends instantiation requests to Hypervisors and the DEVA Agents in charge of the dynamic behaviour of the application. After VMs are instantiated, DEVA Agents create a virtual network in the hosting machines. In our proposed architecture, we extend the system by adding three new components in the agents: First, we define an additional monitoring module with application dependent rules. While the basic component reads values such as CPU, memory and bandwidth usage, new values need to be contemplated in order to track non-functional requirements compliance. Examples of this are requests per second for a web server or database transactions for a database server. The application-dependent monitoring module can be extended based on different applications. All agents send the monitored data to the DEVA Manager, where the data is aggregated to determine high-level actions. The second change in the DEVA Agents consists in an Application Management module similar to the existing Network Management component. While the later one is in charge of determining low-level actions to maintain network QoS, the new subsystem needs to consider high-level requirements and send them as an input to the other module. The third modification of the agent, the Dynamic Application Model, provides the mapping based on a model of the application's behaviour. Contrarily to the Non-Functional Requirements Parser and the Static Application Model, the components in the agent can also consider the runtime state of the application.

B. Model-based translation of non-functional requirements

There are two modules with the task of translating non- functional —high level— to infrastructure or low-level requirements. As stated in the last section, the first one con- siders the static behaviour of the application and provides the necessary criteria to the scheduler, while the second one takes into account the dynamic state of the application. There are different approaches in the literature to modelling application performance which can be divided, into the categories of empirical, theoretical and on-line simulation models. The first category corresponds to those models created from the application's off-line execution. Requirements can be inferred by observing the behaviour of the system under different conditions and creating a model that can be later used to obtain approximate parameters to provide to the underlying management system. These models are usually measured by treating the application as a black-box (i.e., without employing any knowledge of the internal implementation or design). The second category consists of creating a mathematical model to relate the application's characteristics to its requirements. In this case, knowledge about the internal implementation is used to quantify the application's behaviour based on available resources. Finally, some models perform on-line (runtime) simulation of the application in order to find its behaviour for a certain input. Simulations can be either

event-based, for which an abstract model is created to approximate the behaviour under certain conditions, or real-time, where a part or the whole application is executed to predict how the real system would behave. Our system does not make any assumptions about the models used to map non-functional requirements to low-level ones. In fact, any of these could be employed either for the static or the dynamic modules in the manager and the agents. The basic prerequisite is that the used model understands the application's requirements and is able to determine a set of values that can be expressed via DEVA annotations. Some models may consider individual components of the system separately, while others contemplate complex relations between modules and how changes in one may affect others.

C. Non-functional requirements fulfillment

The modules added to the system allow the translation of non-functional requirements to low-level ones by using an application model. However, the DEVA Manager and agents need to perform the appropriate actions in order to fulfill the requested requirements. We classify these actions in two areas: resource allocation, and resource control. These categories also correspond to static and dynamic management, respectively.

The first type of actions is decided and enforced by the DEVA Manager based on the initial ensemble request and the model mapping. After parsing the user's input, non-functional requirements are translated into a set of low-level QoS values, which can be in turn used by the scheduler component to assign virtual elements to physical infrastructure. In our implementation in [2], the scheduler executes a met heuristic algorithm to iteratively choose a near optimal placement of the requested DEVA in the available resources. This mapping would ensure that non-functional requirements are met by employing the appropriate infrastructure. Additionally, the DEVA Manager sends a description of the requested network links to each agent. Agents perform traffic isolation and shaping operations on the physical links to multiplex their usage among ensemble members, and when needed, create tunnels between physical hosts in different domains to build a virtual overlay network. However, static allocation is not enough to respond to the runtime behaviour of the application. While some values can be applied during the instantiation phase, most of the non- functional requirements need to be considered in terms of the application's dynamic usage. The DEVA agent is in charge of monitoring the system's running state and executes the appropriate control mechanisms. In many cases, these actions have associated trade-offs which need to be considered. Examples of control mechanisms run by the agents are dynamic bandwidth or CPU adjustment, provisioning of additional VM instances or VM migration.

VI. EXPERIMENTAL VALIDATION

In order to validate the proposed architecture, we have implemented a prototype extending the original DEVA Manager and agent. There are two main goals for this section:

1) Demonstrate the feasibility of translating high-level, non-functional requirements into a deployed ensemble of VMs.

2) Show how high-level QoS requirements are met during a DEVA lifecycle. The experiment includes provisioning a test application through the DEVA Manager in order to determine how a set of non-functional requirements defined through the requirements analysis phase can be fulfilled during runtime. We have developed a three-tiered web application to illustrate the process.

A. The Chirper Application In our test scenario, an fictitious company wants to develop an internal messaging systems so that their employees can communicate without having to use third party applications. They decide to deploy this solution in their private cloud so that they can take advantage of their in-house resources. The application, which we call Chirper, stores profile information for users, and enables them to post short messages to a common virtual board and query others' messages. The application has two main components: the first one is a web server running the CherryPy1 python web server;

We focus on a subset of the typical non-functional requirements explained in Section III: after exploring their users' behaviour, our fictitious company estimates that the application should be able to respond to a peak of 40 requests per second, and that any request should be served in less than 500 milliseconds through the internal network. In the second step, we define the application's architecture and implement it. In our approach, we follow the Model-View- Controller (MVC) architecture: a front-end interface where the user can interact with the system, a controller to submit and request data to the database, and the database layer itself. Figure 3 shows a class diagram of the system.

B. Performance Modelling

Once the application complies with the specified functional requirements, a model is created to account for the expected performance. In this example, a simple black-box model is defined by benchmarking the application externally. We deploy both appliances in the private cloud, consisting of a cluster of machines with Pentium 4 processors and 1 GB of memory running the Xen 3.0 hypervisor, and a third VM to act as a user. Physical machines are interconnected with 1 Gbps Ethernet links and a dedicated

network switch. Initially, each VM is assigned a quota of 100% of the CPU, 1GB of disk, and 768 Mb of RAM. We run the Apache Benchmark tool to send 1000 requests with a level of concurrence of 10 to the service for each tested configuration. CherryPy is set up to spawn 10 serving threads without page caching mechanisms. We measure the request time and number of requests served per second for the operation of querying the last 50 messages in the database. We consider CPU and bandwidth as the VMs' configuration parameters. Memory allocation was discarded since the application doesn't require a high amount of main memory and consequently its performance doesn't depend on this parameter (our tests demonstrated 40 Mb were enough for the application to function at maximum capacity). In the first set of runs, we calculate the application's behaviour depending on the CPU quota. After running the tests, we determined that the Database appliance is not CPU bound, and therefore, there is no difference in performance with different values. Figure 4 shows the number of handled requests per second and the milliseconds taken for each request when the CPU allocation for the Web appliance is changed from 25% to 100% in intervals of 25%. As the figure shows, the number of served requests per second is directly proportional to the CPU allocation, while the time taken to respond to each request decreases with a higher CPU quota. As the second set of measurements, we explore the application's behaviour in relation to the allocated bandwidth. There are two links considered in this benchmark: the incoming connection to the Web appliance, and the private connection linking it to the database. Each of them can be constrained and isolated independently by the DEVA agents in the hosting ma- chines. By doing this, each DEVA can perform independently of the rest, and network traffic from different applications is separated so that different VMs can multiplex the physical channel. We test the application with symmetric network assignments —i.e. same incoming and outgoing rate— from 100 Kb/s to 500 Kb/s with increments of 100 Kb/s. Figure 5 shows the results in requests per seconds and milliseconds per request for the incoming link (in) and the private one connecting both Vms.

VII. CONCLUSIONS AND FUTURE WORK

As the cloud becomes more mainstream as a method to host applications, developers will need to consider how different providers —or in-house solutions— will be able to fulfill the final users' needs. Similarly, providers need to be able to give reliable guarantees for the Quality of Service of software deployed on their infrastructure. In this paper, we addressed this problem from both the developer's and cloud provider's perspectives. We showed how an example application with concrete requirements can be developed and deployed in a cloud manager that takes high-level non-functional requirements into consideration.

REFERENCES

- ***http://occi.googlecode.com/hg-history/e1decfed0420d3b8e98a324948b8613d6dac42e5/docs/occi-usecases_req-book.pdf***
- ***http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6842213&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A6842212%29***
- ***http://pire.fiu.edu/publications/SEKE-2011-Deva-Non-Funcational-Reqs.pdf***
- ***http://www.cloudbus.org/students/ResourceProvisioning_DIANABA.pdf***
- ***http://www.ibm.com/developerworks/cloud/library/cl-bluemix-nfr/index.html***
- ***http://globalsp.ts.fujitsu.com/dmsp/Publications/public/wp-Cloud-Adoption1.pdf***

Impact of Denial of Service attack in MANET

Ekata Gupta [1], Dr.S.K.Saxena [2]

[1] MCA Department ,GNIM, New Delhi and
Research Scholar, Mewar University
[2] CSE Department ,
Delhi Technological University(Formerly Delhi College of Engineering)
[1] ekata_2000@yahoo.com, [2] saxena58@gmail.com

A B S T R A C T

In the current era of wireless network Mobile ad hoc networks (Manets) are gaining a lot of concentration in research in recent times due to their importance in enabling mobile wireless nodes to communicate without any existing wired or predetermined infrastructures. Significant progress has been made towards making ad hoc networks secure and DoS resilient. In this paper, we design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause.

Keywords: MANET, ad-hoc networks, Denial of service ,Black-Hole

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication.

Some special characteristics of MANET like dynamic topology, fast deployment, robustness make this technology an interesting research area. The security of communication in ad hoc wireless networks is important, especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANET's more vulnerable to digital/cyber attacks than wired networks.

2. ATTACKS ON MANET

In MANET there is much more need for the security as each node is free to move in any direction and there is no centralized security provision in such networks. Attacks on MANET's are broadly divided into two major categories:

2.1 Active Attacks: Active attacks are those attacks whichtry to interrupt the proper functionality of the network.This can be done either through reading and changing the information on the data packets, denial of Services, altering the routing path by changing routing information, hop count etc. These attacks are easier to be detected as compare to their counterpart i.e. Passive attacks.

2.2 Passive Attacks: Passive attacks are those attacks which do not alter the normal functionality of network but silently try to listen or retrieve the vital information inside the data packets. These kinds of attacks are hard to detect. These attacks are further classified into four major categories described in Fig1 .Every routing protocol needs secure transmission of data. Security service requirements of MANET are similar to wired or any infrastructure wireless network.

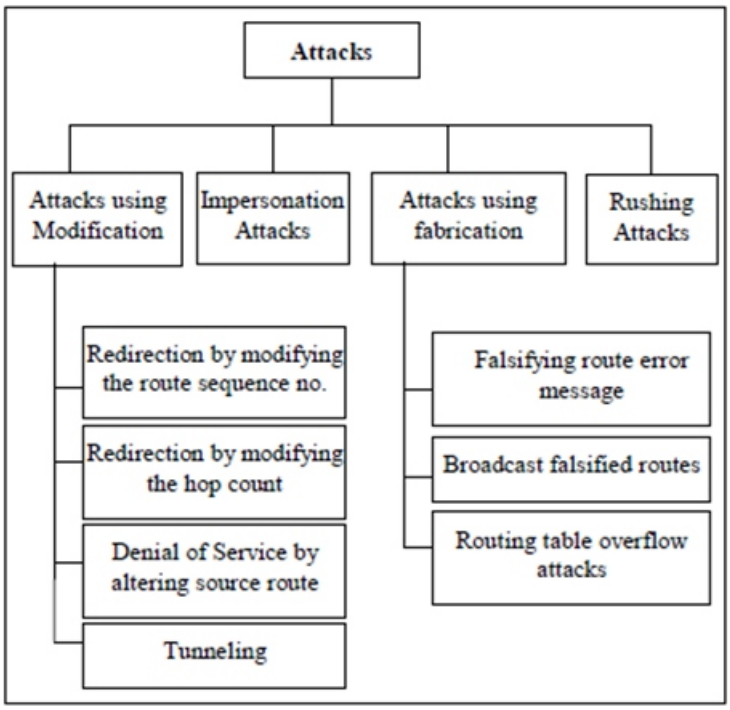


Figure 1: Attacks on Manet

3. SECURITY GOALS

Following are five major security goals which are needed for protecting the data and resources from attacks:

3.1 Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

3.2 Availability: Availability ensures the survivability of the services even in the presence of the attacks. Availability is concerned with the fact that the network services should be available whenever they are

needed. Systems ensuring the availability in MANET's should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehavior.

3.3 Confidentiality: Confidentiality ensures that information should be accessible only to the intended party. No other node except sender and receiver node can read the information. This can be possible through data encryption techniques.

3.4 Integrity: Integrity ensures that the transmitted data is not being modified by any other malicious node.

3.5 Non-Repudiation: Non-repudiation ensures that neither a sender nor a receiver can deny a transmitted message. Non-repudiation helps in detection and isolation of compromised node.Apart from the above stated issues some other issues need to be taken care of:

i. Cooperation and Fairness
ii. Confidentiality of location
iii. No Traffic diversion

4.BLACK HOLE ATTACK

In general, a packet can be dropped at either MAC or network layers due to the following reasons:

i. The transmission buffer at the MAC level is fixed so when the buffer is full any arriving packet is dropped
ii. A packet can be dropped if the RTS frame has reached a maximum value and thus collision can occur
iii A data packet may be dropped or lost if it is corrupted during transmission due to some phenomenon specific to radio transmissions such as interference, hidden nodes and high bit error rate.

Moreover a malicious node involved in a routing path may intentionally drop the packets at network layer in order to provoke a collapse in network performances.

In order to launch a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the routing/forwarding path of data/control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network.

Thus, any node can easily misbehave and provoke a severe harm to the network by targeting both data and control packets.

5. ROUTING PROTOCOL-SPECIFIC ATTACK

We first address black hole problem in the two routing protocols cited above.

5.1 Black hole attack in AODV: In order to discover a path source node broadcasts a route request (RREQ) message. The destination node on receiving the RREQ updates the sequence number and sends a route reply (RREQ) message. Any link broken due to mobility is also send to the source with route error message. In on-demand protocols a selfish node can drop the RREQ packet while a malicious node can drop a RERR packet to prolong the duration of use of broken routes and hence the network collapses.

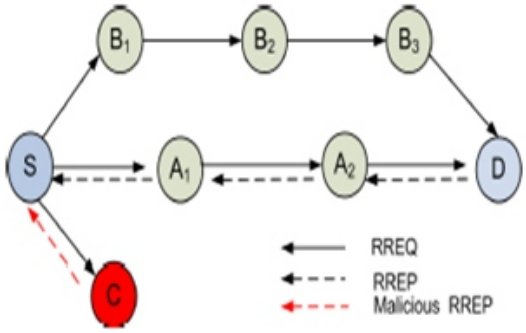


Figure : 2 black hole attack in ADODV

In Fig; 2 by breaking the rule node C gains confidence in S that it has the shortest path

5.2 Black hole attack in OLSR: The Optimized Link State Routing protocol (OLSR) is a proactive routing protocol designed for large and dense networks. The main optimization of this protocol is achieved through the use of MPRs (Multi Point Relays) which are a set of neighbor nodes that represent the unique responsible for spreading the local link state information to the whole network, thereby reducing the induced overhead.

The main functionality of OLSR is neighbor sensing and topology dissemination. Neighbor sensing is accomplished through the periodic exchange of Hello messages, in which every node advertises its neighbor set along with the state of the link connecting it to each neighbor. Notice that the local link state information is periodically advertised by the MPR nodes via the transmission of TC(Topology Control) messages. A malicious node may simply send a TC message claiming to be the MPR of nodes although it is not. Therefore, as the network depends on the MPRs for routing services, a malicious node that manages to become an MPR can easily launch a black hole attack on the network.

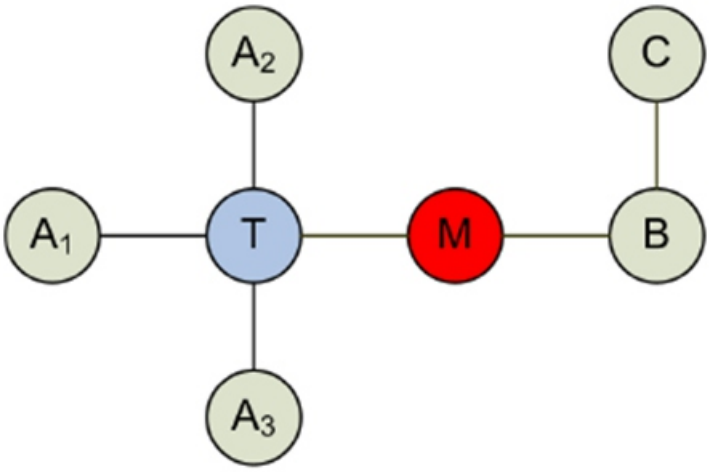


Figure 3: Black Hole attack in OLSR

In Fig 3 node M becomes the MPR's by constantly setting its willingness field to the highest allowed value regardless of its available resources.

6. SECURE MANETS AGAINST BLACK HOLE ATTACK

6.1 Security-aware ad hoc routing protocol (SAR): Some secure routing protocols, such as the security-aware ad hoc routing protocol (SAR), can be used to defend against black hole attacks. The security-aware ad hoc routing protocol is based on on-demand protocols, such as AODV or DSR. In SAR, a security metric is added into the RREQ packet, and a different route discovery procedure is used. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. At intermediate nodes, if the security metric or trust level is satisfied, the node will process the RREQ packet, and it will propagate to its neighbors using controlled flooding. Otherwise, the RREQ is dropped. If an end-to-end path with the required security attributes can be found, the destination will generate a RREP packet with the specific security metric.

If the destination node fails to find a route with the required security metric or trust level, it sends a notification to the sender and allows the sender to adjust the security level in order to find a route. To implement SAR, it is necessary to bind the identity of a user with an associated trust level. To prevent identity theft, stronger access control mechanisms such as authentication and authorization are required. In SAR, a simple shared secret is used to generate a symmetric encryption/decryption key per trust level. Packets are encrypted using the key associated with the trust level; nodes belonging to different levels cannot read the RREQ or RREP packets. It is assumed that an outsider cannot obtain the key.

In SAR, a malicious node that interrupts the flow of packets by altering the security metric to a higher or

lower level cannot cause serious damage because the legitimate intermediate or destination node is supposed to drop the packet,and the attacker is not able to decrypt the packet. SAR provides a suite of cryptographic techniques, such as digital signature and encryption, which can be incorporated on a need-to-use basis to prevent modification.

6.2 Requirements of ACK-based schemes:

All the nodes running a solution based on acknowledgment need to maintain a timeout (To) value. This timeout represents an upper bound of the time that the sender node has to wait for the ACK to arrive.
The timeout value should be greater than the Estimated threshold (Th) value which can be calculated as follows:

$$Th = T2 - T1 \quad (1)$$

where T1 and T2 are the sending (reception) time of the packet(ACK), respectively.

6.3 Reputation based schemes

The reputation is the art of using historic observation about the behavior of a node to determine whether it is trustworthy or not. Each node must form an opinion regarding the other nodes based on their observed past behaviors. Then the nodes with low reputation are punished or avoided while establishing routes.

7. CONCLUSION

As discussed, most of the proposed solutions are built on a number of assumptions which are hard to realize. Moreover; these solutions are generally unable to launch a global response system whenever a malicious node is identified. Due to these reasons, many challenges have to be carefully considered in order to design a robust solution to cope with the packet dropping attack. A simple way to secure MANETs against the increasing threat of the packet droppers without affecting their performance is to take into account the security metric at an earlier stage of the design process of routing protocols. Thus In this paper we have presented a survey of the state of the art on securing MANETs against packet dropping attack.

8. REFERENCES

[1] Marek hejmo, brian l. Mark, member, IEEE, charikleia zouridaki, student member, IEEE,And roshan k. Thomas design and analysis of a denial-of-service-resistant Quality-of-service signaling protocol for manets, in IEEE transactions on vehicular technology, vol. 55, no. 3, May 2006

[2] Soufiene djahel, farid -abdesselam, and zonghua zhang, mitigating packet dropping problem in mobile adhoc networks: proposals and challenges in IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011

[3]Imad aad, jean-pierre hubaux, senior member, IEEE, and edward w. Knightly, senior member, IEEE, impact of denial of service attacks on ad hoc networks, IEEE/ACM transactions on networking, vol. 16, no. 4, august 2008

[4] Mudhakar Srivatsa and ling liu, mitigating denial-of-service attacks on the chord overlay network: a location hiding approach at IEEE transactions on parallel and distributed systems, vol. 20, no. 4, April 2009

[5] Loay abusalah, ashfaq khokhar, and mohsen guizani, a survey of secure mobile ad hoc routing protocols in IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008

[6] Parul tomar, prof. P.k. Suri, Dr. M. K. Soni, a comparative study for secure routing in manet, international journal of computer applications (0975 – 8887)volume 4 – no.5, july 2010

[7]klara nahrstedt , wenbo he, ying huang , security in wireless ad hoc networks book chapter in guide to wireless ad hoc networks pages 391-425

[8] Praveen Joshi, Security issues in routing protocols in MANETs at network layer in Procedia Computer Science 3 (2011) 954–960

MIMO Technology for Future Wireless LAN

Sachin Garg
Department of Computer Science, Aggarwal College
Ballabgarh, Haryana. (M) +91-9968-322-785
E-mail-sgarg213@gmail.com

A B S T R A C T

Tremendous consumer interest in multimedia applications is fueling the need for successively higher data rates in wireless networks. Data rates in wireless wide area networks are limited by the need to address wide coverage, vehicular mobility, and the limitations of licensed spectrum. IEEE 802.11n takes the advantages of multi-path propagation to increase throughput to speeds above 100 Mbps, by using MIMO or in other words multiple transmitters and multiple receivers (MIMO) antennas. It uses spatial diversity to induce multi-path for the purpose of recombining the multiple signals to increase the signal gain and channel multiplexing to send multiple signals using multiple antennas therefore multiplying speeds, increases the range and enhances the performance.

Keywords: IEEE 802.11n,WLAN, MIMO, Spatial Diversity

I. INTRODUCTION

Wireless local area networks (WLANs) based on the IEEE 802.11 standard have crooked out to be a very booming technology with extensive acceptance, which has generated a whole communication sector. They provide cable-free access to high data rates for both indoor and outdoor environments. A WLAN offers the flexibility to relocate people and equipment or to reconfigure and add more nodes to the network. This flexibility is achieved without much planning effort and cost of re-cabling, thereby making future upgrades inexpensive and easy. Therefore, WLANs are becoming more popular and increasingly relied on. They can be found in public hotspots to home networks, are at the core of business models of many companies, even large ones and are interoperating with other key communication technologies. But, the real world is neither flat nor empty, however, and physical barriers have long been the opponents of WLAN performance. The natural and man made obstacles slow down wireless signals, resulting distortions, multi-path fading and retransmission as a consequences and ultimately effecting signal integrity and throughput. The IEEE 802.11a/g specifications provide up to 54 Mbps data rate, which is not sufficient to compensate these limitations. To overcome these limitations IEEE have revised

the standard. IEEE 802.11n standard is now taking advantages of diversity conditions to improve the throughput of WLAN. This latest standard is based on the multiple input and multiple output (MIMO) and the actual transmission rate is up to 600 Mbps by taking advantage of multi-path propagation [1]. The Multi-path propagation occurs when signal bounces building, walls and other obstacles and arrives at the receiver at different times and from different paths. If the time difference is large enough, the receiver gets confused and cannot interpret the signal causing retransmission and therefore reducing the speed and data rate of the 802.11 networks. But, IEEE 802.11n takes the advantages of multi-path propagation to increase the throughput.

The IEEE 802.11n based on OFDM (Orthogonal Frequency Division Multiplexing) have been extended to MIMO architectures using a space-time coding (STC) and space division multiplexing (SDM) [9]. STC system increases the error performance of the communication systems by coding over the different transmitting antennas, while SDM system provides very high data-rate communication over wireless channels without increasing the total transmitting power and bandwidth. A combination of MIMO signals processing with OFDM is regarded as a promising solution for enhancing the performance of next generation wireless communication.

IEEE 802.11n STANDARD

WLAN seeks to improve significantly upon the data rates experienced by end users of current WLAN systems, e.g., IEEE 802.11a, b, and g [3]. The data rate of IEEE 802.11g in its specification is 54 Mbps, but actually used data rate is just 20 Mbps. This data rate is not sufficient to satisfy the next generation applications, which demand large capacity and high data rate. That is why the IEEE 802.11n is necessary to acquire high data rate. IEEE 802.11n can support the data rate from 100 Mbps to 600 Mbps [4].

The one of main feature of IEEE 802.11n is fixed data rate in PHY layer. Then, we approach close to the PHY data rate. PHY layer use the MIMO system [5]. MIMO system can achieve the high data rate by using multiple antennas. The advantage of MIMO system is to raise efficiency of data rate. So, it can send the data without expanding bandwidth. 802.11n support the three physical layer modulation techniques used by the older standards; Direct Sequence Spread Spectrum (DSSS), Complementary code keying (CCK), Orthogonal Frequency Division Multiplexing (OFDM). IEEE 802.11n also incorporate many other features that improve throughput, range, reliability and efficiency. Comparison of the different features and the throughput of IEEE 802.11a/b/g/n are shown in Table1.

Table 1 IEEE 802.11 standards Comparisons

	802.11a	**802.11b**	**802.11g**	**802.11n**
Standard Approved	July 1999	July 1999	June 2003	Sept. 2009
Maximum data rate	54 Mbps	11Mbps	54 Mbps	600 Mbps
Modulation	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
RF Band	5 GHz	2.4 GHz	2.4 GHz	2.4 Ghz / 5Ghz
Number of spatial Streams	1	1	1	1,2,3, or 4
Channel Width	20 MHz	20 Mhz	20 Mhz	40 MHz

MIMO TECHNOLOGY

Multiple Input-Multiple Output (MIMO) is a wide set of multiple antenna technologies that can significantly increase the capacity of wireless networks, without additional bandwidth or increased transmission power. They are widely recognized as technologies essential for meeting, at relatively low cost, ever growing network requirements, such as higher data rate, high mobility, Quality of service (QOS) support, higher security, support for diversity and plurality of devices and services.etc [6].

HIERARCHY

Figure-1 illustrates different antenna configurations of a wireless link Single Input Single Output (SISO) corresponds to the traditional wireless link.

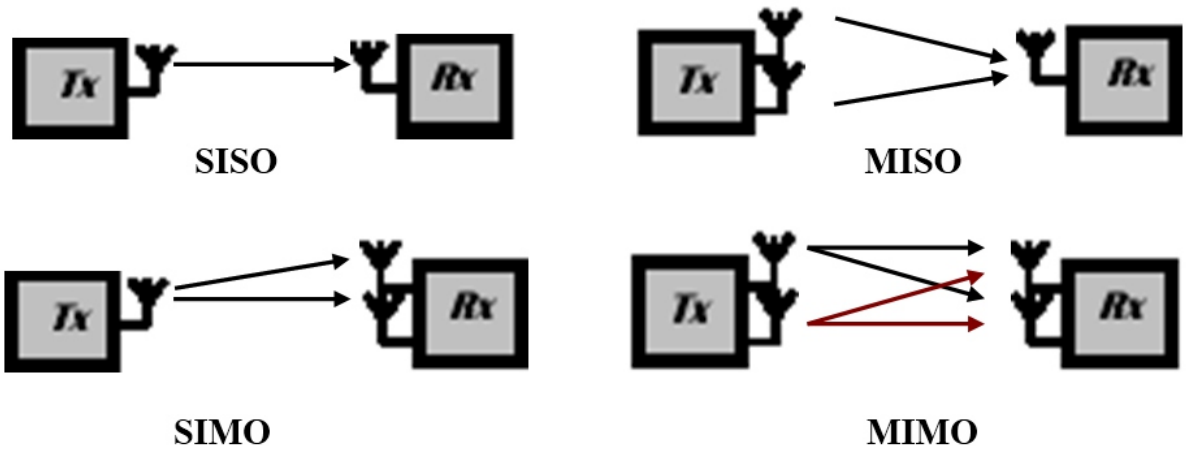


Figure-1 Overview of Single and Multiple Antenna Techniques

In Single Input - Multiple Output (SIMO) and in Multiple Input - Single Output (MISO) systems, multiple antennas are present only at one side: at the receiver or at the transmitter, whereas in MIMO systems both transmitter and receiver are equipped with multiple antennas. In another, more general view of MIMO systems, so called virtual MIMO, or cooperative MIMO, multiple antennas at the transmitter are not necessarily located at one station, multiple stations with coordinated transmissions appear to the receiver as one, and simulate a MIMO transmission.

HOW MIMO WORKS

MIMO takes advantage of multi-path. "Multi-Path" occurs when the different signals arrive at the receiver at various times. MIMO uses multiple antennas to send multiple parallel signals (from transmitter). In an urban environment, these signals will bounce off trees, buildings, etc. and continue on their way to their destination (the receiver) but in different directions. The receiving end uses an algorithm or special signal processing to sort out the multiple signals to produce one signal that has the originally transmitted data [6]. To understand the use of MIMO systems, we need to know the wireless channels limitations:

- Fading: Fading results in sudden drop of signal power in the receiver. Multi path fading results when the transmitted signal bounces off over an obstacle and creates multiple paths for the signal to reach the receiver at different times with different phases. The several incidences of the same signal with different phases and amplitudes may cancel each other, causing signal loss or drop of signal power as shown in figure-2.

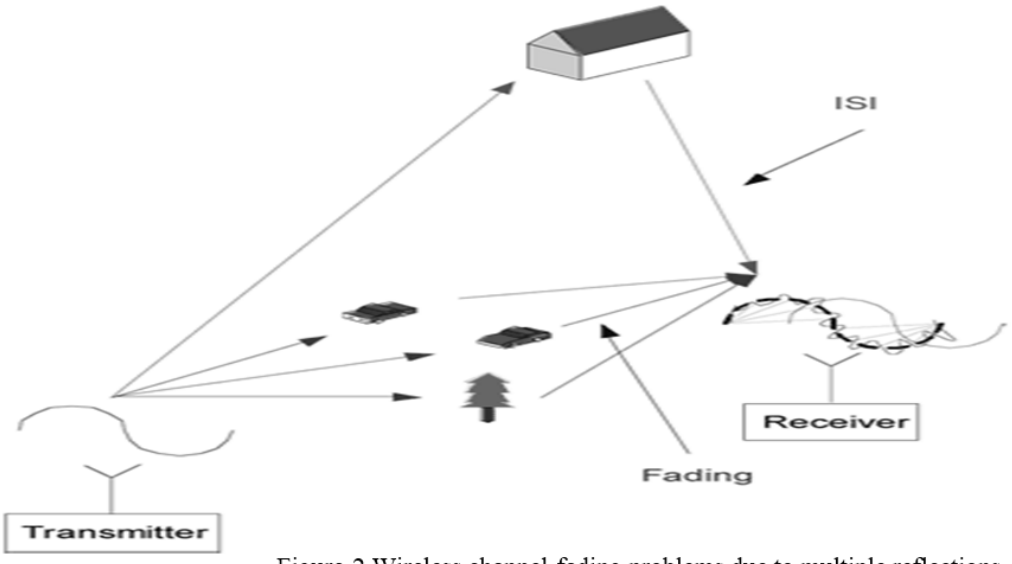


Figure-2 Wireless channel-fading problems due to multiple reflections

- Inter-symbol Interference: Multiple paths come with various delays, causing inter-symbol interference.
- Noise: Electronics suffer from thermal noise, limiting the SNR.

Considering the limitations above, the MIMO benefits can be summarized as follows:

- Capacity increased (with minimum number of base stations.)
- Better transmission quality
- Increased coverage.
- Improved user position estimation.

These benefits are gained due to the main aspects of MIMO.

MAIN ASPECTS TO UNDERSTAND MIMO

According to E.Biglieri, A. Goldsmith, B.Munquet and H.Sari [2], the basic features of MIMO technique are:

- Spatial Multiplexing Gain: Capacity gain at no additional power or bandwidth consumption obtained through the use of multiple antennas at both sides of a wireless link. MIMO channel offers a linear (in the minimum of the number of transmit and receive antennas) increase in capacity, compared to systems with single antenna at one or both sides of the link at no additional power or bandwidth expenditure. This gain, referred to as spatial multiplexing gain.
- Diversity Gain: Diversity gain is obtained by transmitting the same data signals over multiple independent fading dimensions. It makes the wireless link reliable and robust.
- Interference reduction: Multiple antennas at one or both sides of the wireless link can be used to cancel or reduce co-channel interference and hence improve the cellular capacity.

MAXIMIZING THROUGHPUT OF WLAN 802.11

IEEE 802.11n is the new international standard for wireless local area networks, incorporating new smart antenna technologies (MIMO) permitting a high performance and coverage improvement for WLANs. With multiple antennas both at transmitter and receiver not only rejects fading; better yet it actually control the fading itself in favor of increased throughput [8].

Consider the MIMO channel having multi-channel propagation between the transmitter and receiver is shown in figure-3:

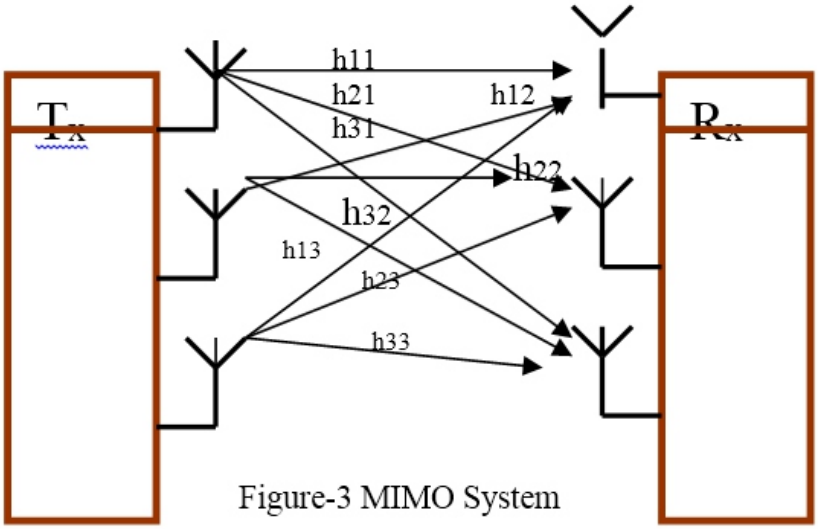


Figure-3 MIMO System

Let M_T and M_R be the number of transmit and receiving antennas, respectively.

The Channel Matrix H is:

$$\begin{pmatrix} h_{11}, h_{22}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots h1_m \\ h_{21}, h_{22}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots h2_m \\ h_{31}. h_{32}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots h3_m \\ . \\ . \\ h_{n1}, h_{n2}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots h_{nm} \end{pmatrix}$$

Where x1, x2, x3 ……..XN are the signals sent by the antenna MT and y1, y2, y3……..yN are the signals received by the antenna MR. The above wireless channel is modulated as:

$$y = H_x + n$$

Where H is the channel matrix and n is the channel noise.

The channel capacity is only a limit to error-free bit rate i.e. is the maximum throughput at which data can be sent over the channel. While maintaining the low probability of error, the capacity of a SISO channel [7] having one transmits and one receive antenna is:

$$C_{SISO} = \log 2 \left(1 + \frac{E}{N_0} \right) \quad \text{.....Eq. (1)}$$

From the above expression it is clear that the capacity of SISO system can be increased only if the transmission Energy (power) is increased. In case of Wireless MIMO (Larsson and Stoica, 2003], the channel capacity is:

$$C_{MIMO} = M \log 2 \left(1 + \frac{E}{N_0} \right) \quad \text{.....Eq. (2)}$$

From the Equation (1) and Equation (2) it is clear that the capacity of an orthogonal MIMO channel is M times the capacity of the SISO channel.

So, the multiplexing gain is;

$$\text{Multiplexing Gain} = \frac{C_{MIMO}}{C_{SISO}}$$

Thus, by using multiple antennas we can increase the throughput using MIMO architecture.

CONCLUSION

MIMO communications are globally seen as a key technology for the next generation wireless networks, because of their potential to dramatically increase the system performance without the additional power of bandwidth. 802.11n is an emerging IEEE wireless standard, which significantly improves throughput and range compared with older 802.11 standards. 802.11n is the only IEEE standard that operates in either the 2.4 GHz or 5 GHz frequency bands, and it is the first to standardize the use of MIMO architecture. 802.11n is backward compatible with 802.11a/b/g which means that an 802.1n device can communicate and; interoperate with legacy 802.11devices. 802.11n may eventually become the dominant enterprises LAN technology. It is understood that both MIMO technology and wider bandwidth channels will be required to reliably satisfy the higher throughput demands of next generation applications.

REFERENCES:

[1] Abdul Aziz, M.K., Fletcher, P.N. and Nix, A.R., 'Performance analysis of IEEE 802.11n solutions combining MIMO architectures with iterative decoding and sub-optimal ML detection via MMSE and Zero forcing GIS solutions', WCNC, March 2004.

[2] E. Biglieri, A. Goldsmith, B.Munquet and H. Sari (2007): 'Diversity, Interference Cancellation and Spatial Multiplexing in MIMO Mobile WiMax Systems'. Universitat Pompeu Fraba –Barcelona.

[3] Bing, B. ``Measured performance of the IEEE 802.11 wireless LAN, "IEEE Conf. LCN'2002. , pp. 34-42, October 2002.

[4] Broadcom, 802.11n: Next–Generation Wireless LAN Technology, White Paper dated April 2006

[5] IEEE P802.11n/D1.0 Draft Amendment to Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements Mar. 2006.

[6] Jacob Sharony (2006): 'Introduction to Wireless MIMO – Theory and Applications', IEEE Long Island (LI) & CEWIT, November 2006.

[7] Proakis, J. G. (2001). Digital Communications. Mc Grawn Hill. 9, 22, 28, 32

[8] Xiao, Y. (2005). IEEE 802.11n: enhancements for higher throughput in wireless LANs. Wireless Communications, IEEE, 12(6), 82-91, December 2005.

[9] Zelst, V.A., Nee, V.R., and Awater A. G., "Space division multiplexing (SDM) for OFDM systems," in Proc. IEEE Veh. Technol. Conf., May 2000, pp. 1070–1074.

Association Rule Mining with Sampling Algorithm

Amandeep Kaur Mehta[1], Dr Rajinder Singh [2]

[1]Department of Computer Science, SD College(Lahore),
Ambala Cantt , Haryana , India
[2]Department of Electronics ,SD College (Lahore),
Ambala Cantt, Haryana , India
1mehtaamandeep@yahoo.com, 2rsrana42@rediffmail.com

A B S T R A C T

The major area of research in Data Mining is discovery of Association rule from huge databases which is a very complex and time consuming process. The process of frequent item set mining requires multiple scans of large databases which is a computational process and IO overhead is very significant. Sampling is an effective technique to reduce the size of the dataset operated and speed up the whole process. Many sampling based approaches are designed to speed up the process of Association Rule Mining. Sampling is one of the important and popular data reduction techniques. In this technique a random sample is selected to frame the association rules and then verify results with the rest of the database. Sampling can speed up the mining of association rules. This paper gives an overview of existing sampling based association rule mining algorithms.

1. INTRODUCTION

There are basically two most important reasons that data mining has attracted a great deal of attention in the recent years. First, we are capable to collect and store the huge amount of data which is rapidly increasing day by day. As the cost of storage devices is decreasing and the processing power of computers is increasing so it has become possible now a days to store large volume of organizational data and process it. The second reason is the need to turn such data into useful information and knowledge. The knowledge that is acquired through the help of data mining can be applied into various applications like business management, market analysis etc.

Data mining or Knowledge discovery in databases (KDD) is the process of discovering previously unknown patterns from the huge amount of data stored in files, databases, data warehouses or any other type of information repository. Database mining deals with the large set of data stored in DBMS.

Organizations store huge amount of data and analyze this large data set to find out patterns which can help in decision support. But organizations are more interested in the interesting data rather than the heap of data. So they need a systematic, efficient and scientific approach to extract meaningful data out of heaps of the data and to find out the relations among these patterns. Association Rule mining introduced by Agarwal et al [1] is the technique to dig out interesting and frequent patterns from the spatial , transactional, temporal or other databases and to set relations or associations among those patterns (also known as item sets) in order to discover knowledge or to frame information. Association Rule is defined in Section 2 in detail. In this paper we have presented the Sampling technique for mining the association rule.

Sampling is the effective technique of mining association rule . It selects a random portion of database of predetermined size and then evaluate the frequency of item sets. The details of Sampling technique is given in Section 3.

2. ASSOCIATION RULE MINING

Association rule Mining is the popular method of finding relationships between various variable in a database. As defined in Wikipedia, It is intended to identify strong rules discovered in databases using different measures of interestingness. Association rules can be applied in various fields like network management, Basket data analysis, catalog design, clustering, marketing, classification etc. Association rules set the relationship between different variables to analyse the present situation. For e.g to find the relationship between the various items sold at a shopping mall, the association rule can be applied on the huge amount of data recorded by the Shopping mall. For e.g the rule {Computer, Speakers} {UPS} found in the sales data of a mall would indicate that if a customer buys Computer and Speakers together, he or she would definitely also buy UPS. This information can be used making the decision regarding keeping the stock of the products as well as to analyse the customer buying habbits and promotional activities for future.

Association rule works on the database of transactions where every transaction contain list of itemset (patterns). Measures of the rule are Support and Confidence. Support of rule is proportion of transaction in the data set that contains the item set to the total number of transactions. The Confidence of a rule is ratio of total number of transactions with all the items to the number of transaction with the A item set[2]. For e.g. if Dataset T is given and item set A has number of occurrences in it. An association rule is the relation ship between two item sets A and B . such as

A ⇨ B

means when A occurs B also occurs.

To illustrate and understand the basic terms we consider a small database of 6 transactions and 3 items. The rule is

{Computer, speakers} ⇨ {UPS}

Transaction Id	Itemset
1	{computer,speakers }
2	{computer,speakers ,Ups}
3	{computer}
4	{computer,speakers ,Ups}
5	{Ups}
6	{computer, speakers ,Ups}

Table : 1

This implies that if customer buy Computer and speakers, he tend to buy UPS also . Out of 6 transactions 3 transactions support this rule .In 3 rcords all the three items are brought together. So the Support of rule denoted as Supp (A) is proportion of transaction in the data set that contains the itemset to the total number of transactions. In the above example, the itemset {Computer, Printer, and UPS} has a support of 3/ 6 = 0.5 since it occurs in 50% of all transactions (3 out of 6 transactions).

The Confidence of a rule (denoted as conf (A ⇨ B)= Ratio of total number of transaction with all the items to the number of transaction with the A item set . for e.g Computer and speakers are purchased 4 times and out of 4 transactions UPS is purchased three times with Computer and speakers i.e A so the Conf (A, B) = ¾ =.75 i.e 75%.

So the association rule is the technique to set the relation between item sets to draw important conclusions. Agrawal and Srikant [3] present the Apriori algorithm for frequent itemset mining. Apriori algorithm is very efficiently used for framing association rules. It is basically used for the databases which contain huge volume of transactions. It is based on bottom up approach. It is used for mining frequent item set for association rules. But the main limitation of Apriori algorithm is that it involves lots of iterations leading to high scanning time. Another limitation is that If minimum threshold is not properly set , the results will be incorrect. Moreover the size of the data set plays an important role in data mining. As the size of data set increases we tend to get more reliable results. Association rule mining requires multiple scans of the databases thus the size of databases considerably increases the execution time of association rule mining algorithms. Disk I/O overhead also increases with the large volume of data sets. But as statistical analysis over a small random sample of a dataset is often considered to be as good as statistical analysis over the entire dataset so the same holds true for frequent item set mining also. Sampling is the technique to pick random sample S of size m by selecting m records randomly from the original dataset.

also. Sampling is the technique to pick random sample S of size m by selecting m records randomly from the original dataset.

The frequent item sets FS (and their supports) mined from the sample are a good representative of the frequent item sets F mined from the entire dataset DT. But still , there is always a small chance that important frequent item sets are missed out in the sample or their supports are wrongly represented. Therefore the user may be interested in the exact mining results.

3. SAMPLING TECHNIQUE

The importance of sampling for association rule mining has been recognized by several researchers. The usual approach is to take a portion of database randomly of a previously determined size and then calculate the frequency of item sets over the sample using a lower minimum support threshold σ' that is slightly smaller than the user – specified minimum support σ. Also the computational cost of association rule mining can be reduced in four ways:

- By reducing the number of scans over the data base
- By picking random samples from the database
- By adding extra constraints on the patterns
- Through parallelization.

The task of mining association rules is usually performed in transactional or relational databases, to derive a set of strong association rules may require repeated scans through the database. Therefore, it can result in huge amount of processing when working on a very large database. Many efficient algorithms can significantly improve the performance in both efficiency and accuracy of association rules .However; sampling can be a direct and easy approach to improve the efficiency when accuracy is not the soul concern. Simple Sampling algorithm [4] is shown below:

```
rs = Select_random_sample (DB);
// generate frequent itemsets for the sample drawn.
FS = generate_frequent_itemsets (rs, low_support);
// counting support for the itemsets and their negative border generated in the sample,
in the database DB.
F = {X € FS U NBD (FS) | X.count >= minsup};
// if NBD (FS) contains frequent itemsets, expand border
Repeat
FS = FS U NBD (FS);
Until FS does not grow;
```

// another scan of DB
F = {X € FS | X.count >= minsup};
Print F; // frequent item sets in the database DB

This algorithm can produce exact association rules in one full pass and two passes in the worse cases. The algorithm picks up a random sample form the database and then finds out frequent item sets in the sample using support that is less than the user specified minimum support for the database. These frequent item sets are denoted by FS. Then the algorithm finds out the negative border [10] of these item sets denoted by NBD (FS). The negative border is the set of item sets those are candidate item sets but did not satisfy minimum support. Simply NBD (Fk) = Ck - Fk. After that for each item set X in FS U NBd (FS) it checks whether X is frequent item set in entire database by scanning the database. [6, 7]

If NBD (FS) contains no frequent item sets then all the frequent item sets are found.

If NBD (FS) contains frequent item sets then the algorithm constructs a set of candidate item sets CG by expanding the negative border of FS U NBD (FS) until the negative border is empty. Now for each item set X in CG the algorithm scans the database for the second time. In the best case when all the frequent item sets are found in the sample this algorithm requires only one scan over the database. In the worst case it requires two scans over the database. [6, 7]

The performance of sampling algorithm relies on the quality of the sample chosen. If the sample chosen is a bad sample the number of candidates generates for second scan may be very large hence second scan can be inefficient. The sample can be a partition of the database. In that case the partition is treated just like a random sample chosen.

4. CONCLUSIONS

We have presented sampling techniques used for mining association rule in large database in this paper. The method adopted in sampling technique indicates that sampling can result in not only performance savings, but also good accuracy in practice. Sampling technique when used on large databases reduces the number of scans thus increasing efficiency in terms of Disk I/O and execution time.

5. REFERENCES

[1] R. Agrawal, T. Imielinski, and A. Swami. Mining association rules between sets of items in large databases. In SIGMOD Conference, pages 207–216, 1993.

[2] Ravindra Patel, D. K. Swami, K. R. Pardasani, "Lattice Based Algorithm for Incremental Mining of Association Rules," International Journal of Theoretical and Applied Computer Sciences, Vol- 1, pp. 119–128, 2006.

[3] Agarwal. R. Srikant.R: Fast algorithms for mining association rules. In proc Int'l Conf on VLDB (1994).

[4] H. Toivonen. Sampling Large Databases for Association Rules. In Proceedings of 22nd International conference on Very Large Databases 1996.

[5] A. Sarasere, E Omiecinsky and S. Navathe . An Efficient Algorithm for Mining Association Rules in Large Databases in 21st International Conference on Very Large Databases 1995,Zurich , Switzerland.

[6] J.Han and M.Kamber, Data Mining : Concepts and Techniques 2001: Morgan Kaufmann Publishers.

[7] J.L. Lin and M.H Dunham. Mining Association Rules : Anti-Skew Algorithm in 14th International Conference on Data Engineering Feb 1998.

Traffic Management over Wireless ATM Networks

Brijesh Kr. Gupta
Dept. of Computer Applications, College of Engineering & Technology,
Greater Noida, India
prof bkgupta@gmail.com

A B S T R A C T

The past few years have witnessed a tremendous growth of wireless LANs (WLANs) mainly due to their ease of deployment and maintenance. This is a practical fact that frequent handoff in Personal Communication Network (PCN) introduces the phenomena of congestion. Congestion Control is concerned with allocating the network resources such that the network can operate at an optimum performance level when the demand exceeds or it is near the capacity of the network resources. After studying the currently used schemes, it is clear that there is some room for improvement for conventional handoff ordering schemes. A new Hybrid Scheme [Gupta, B.K., et al., 2006] proposed by the authors to solve the hand off/ hand over problem in ATM-based PCN, which aims to give handover calls high priority over new calls. When reservation is applied on both radio and backbone channels, it leads to significant decrease in Forced Termination Probability (FTP) with acceptable increase in Call Blocking Probability (CBP).This is achieved by using queuing time rather than the norm of a queueing buffer.
Since the number of resources is limited (i.e. radio channels) as more channels are assigned to serve handover request, blocking probability will increase, which is obvious. Increase in CBP is always the price we have to pay for decrease in FTP.

KEYWORDS: Call blocking, congestion, force termination, handover, hybrid scheme, wireless ATM networks.

1. INTRODUCTION

The rapid worldwide growth in cellular telephone subscribers has demonstrated conclusively that wireless communication is a robust, viable voice and data transport mechanism. The widespread success of cellular has led to the development of newer wireless systems and standards for many other types of telecommunications traffic besides mobile voice telephone calls. As high speed wireless networks are expected to support multimedia applications (video, voice, and data), so it is important that these networks provide guarantees Quality – of – Service (QoS)[1], [2], [3], [4] and [5]. Provision of QoS in wireless networks become complex due to user mobility.

The problem becomes even more challenging as recent wireless networks have been implemented based on small – size cells to allow higher transmission capacity, and thus to achieve better performance. Small size cells increase the handoff rate, and result in rapid changes in the network traffic conditions, making QoS guarantees difficult. The unfair sharing of network resources, along with the growing exigency for effective support of the diverse requirements of emerging multimedia applications, prompted the development of mechanisms, algorithms, and QoS frameworks[10], [11], [13] and [15].

In wireless network congestion can occur when a number of Base Stations (BSs) can simultaneously send packets to the same switch in the network. Bursty communication requires dynamic bandwidth allocation, which may be difficult to allocate in practice. Bandwidth management is crucial for maintaining communication in the wireless networks. Hybrid mobile networks like those formed by wireless LANs and 3G cellular data networks require efficient handoff mechanisms to guarantee seamless connectivity [14].

To support network-wide handoff, new and handoff call requests will compete for connection resources in both the mobile and backbone networks. Handoff calls require a higher congestion related performance, i.e., blocking probability, relative to new calls because forced terminations of ongoing calls due to hand-off call blocking are generally more objectionable then new call blocking from the subscriber's perspective[5]. Handover initiated in PCN, a new channel has to be granted to handover request for successful handover.

To keep FTP to desired minimum values, handover algorithm should avoid blocking handover request due to lack of resources i.e. radio and wired links. We proposed a Hybrid Handover Scheme [6], this has been achieved by giving handover high priority over initiating calls. After applying proposed scheme it was proved that, there is a remarkable reduction in FTP at the cost of tolerable CBP. In the present paper performance analysis simulation study carried out to show how improvement is achieved by using our Hybrid Scheme in comparison to the other schemes like FIFO[7] and MBPS[8]. The improvement reflects remarkable reduced percentage of FTP due to handover failure, when we use our Hybrid Scheme.

Section 2 of this paper described Simulation Environment, and Section 3 presents Simulation Parameters. Results and Conclusion appears in Sections 4 and 5 respectively.

2. SIMULATION ENVIRONMENT:

In the simulation, we have simulated the traffic in six cells as a part of full network. From Fig.1, we consider the ATM switches 1, 2 and 3. Base Terminal Stations (BTS) 1 and BTS 2 form a cluster, and connected to ATM switch 1, BTS 3 and BTS 4 form a cluster and connected to ATM switch 2, similarly for ATM switch 3. ATM switches 1 with 2, and 2 with 3 are connected by backbone links; this configuration is illustrated in Fig.1. To eliminate the boundary effect, wraparound topology is used [12]. Traffic in the backbone link is from: calls between (BTS1 or BTS2), (BTS3 or BTS4) and (BTS5 or BTS6), and vice versa. Load from other parts of the network that may use this link in its communication. The number of channels available in this backbone network is relatively larger than that of each BTS radio channels.

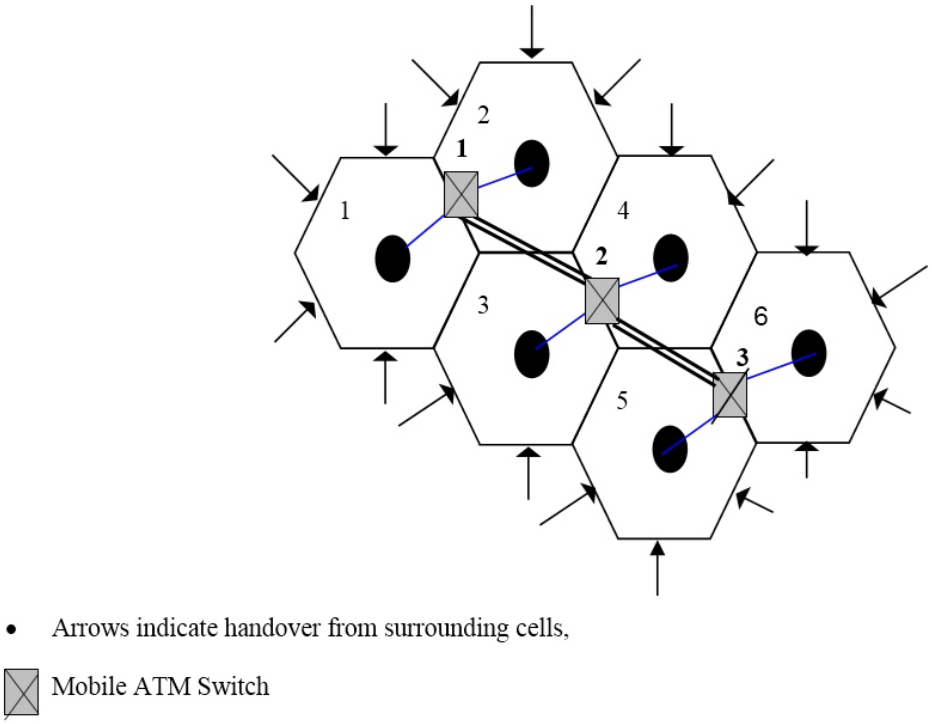


Fig. 1: Simulation Environment ATM-Based Cellular PCN

3. SIMULATION PARAMETERS:

The simulation parameters used for the purpose are as follows:

N_R: Number of radio channels in each cell.
N_{RG}: Number of radio guard channels in each cell.
λ_o: New call arrival rate.
λ_{hi}: Handover call arrival rate.
ρ : The offered load which is $\lambda_o + \lambda_{hi}$.
t_c: New call holding time.

t_h: Handover call holding time.
t_q: Maximum tolerable time in the queue.
N_L : Number of backbone channels in each backbone link.
N_{LG} : Number of backbone guard channels in each backbone link.
P_{cell} : Probability of in cell call.
$P_{cluster}$: Probability of in cluster call.
$P_{bacbone}$: Probability of out cluster call.

4. RESULTS:

In this section, simulation results are obtained to evaluate the proposed Hybrid Scheme. Simulation program was run using default values of simulation parameters to obtain the results. 10000 calls were sampled in one arbitrary cell of the simulation environment. Calls may require a fixed part of the network to complete their connections. The default values for the simulation parameter are defined as follows[9]:

N_R = 30 Radio channels in each cell,
N_{RG} = 3 Reserved Radio channels in each cell,
t_c = 60 seconds average of new call holding time,
t_h = 30 seconds average of handover call holding time,
t_q = 10 seconds average time in the handover queue.

Handover has 50% of the total traffic. The offered load varies from 4 calls/min to 60 calls/min, which is considered as an overload traffic to the system.

4.1 Improvement in FTP due to Reserving Channels at Backbone Link:

The improvement study carried out to show how much improvement is achieved by using the Hybrid Scheme in the comparison to the other schemes. The improvement reflects the reduced percentage of FTP due to handover failure. The improvement of scheme S1 over S2 is calculated as follows:

$$Improvement\ (S_1, S_2)\ \text{in}\ \% = \frac{\{f(S_2) - f(S_1)\}}{S_2} \times 100$$

Where f (S) is the FTP by using scheme S, substitute S1 and S2 for various schemes.

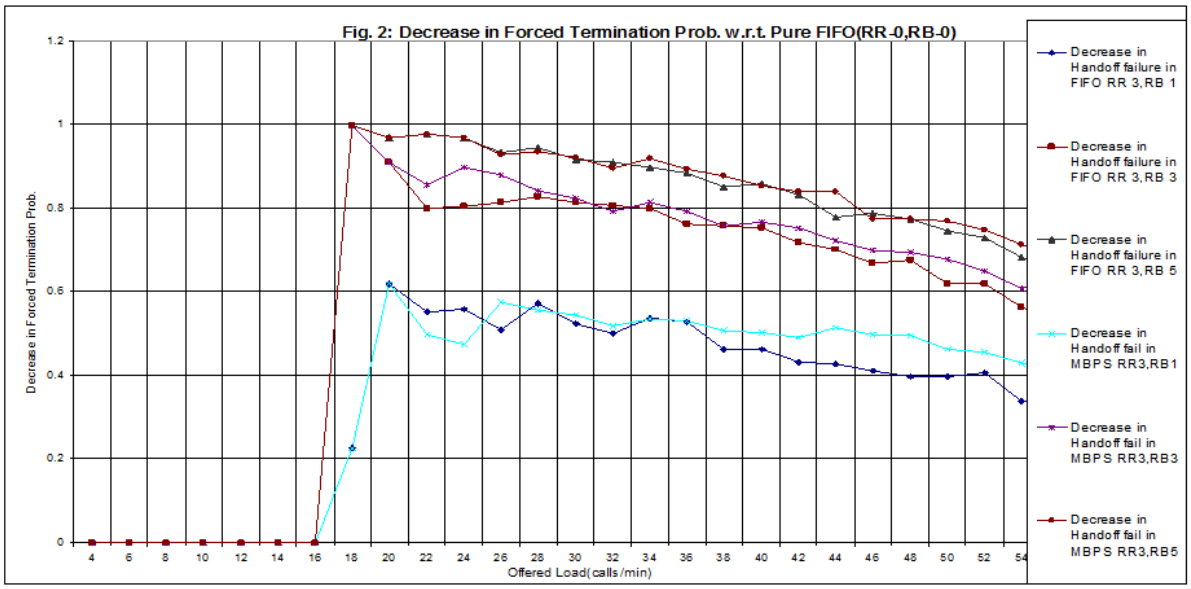
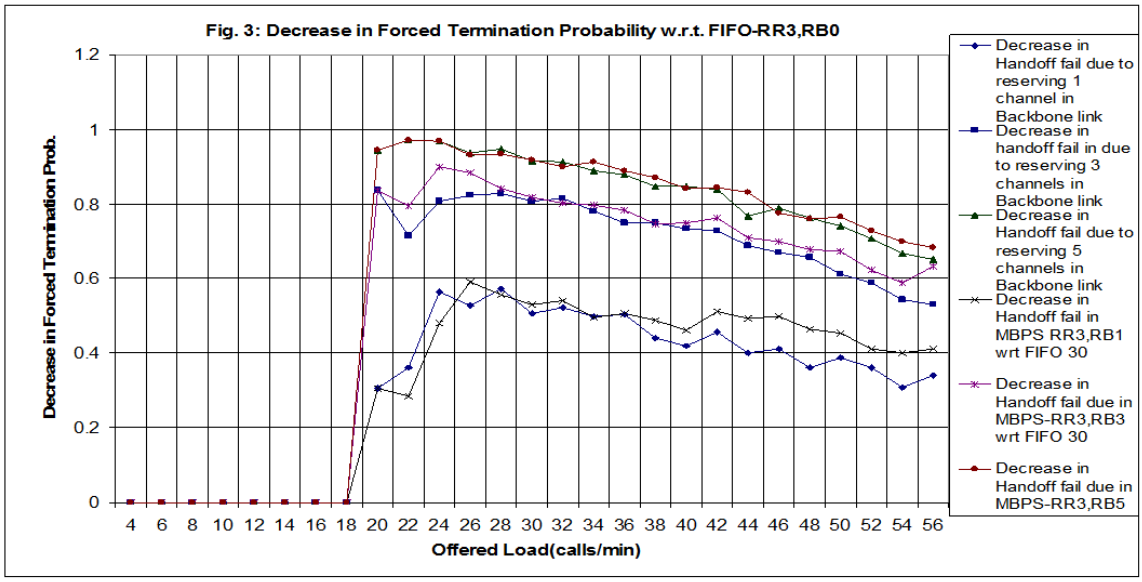


Fig.2 shows improvement of Hybrid Scheme (i.e. using reserved channels with MBPS and FIFO), with respect to pure FIFO(RR 0, RB 0). The figure shows a significant improvement when 3 or 5 channels are reserved in backbone link. The maximum improvement is achieved by the schemes FIFO (RR 3, RB 5) and MBPS (RR 3, RB 5), which is 100% - 80% at moderate offered load and 70% - 50% at higher load. At initial stage of the environment i.e. at low offered load the improvement in FTP is zero, which indicates that all the schemes have same performance. As the load increases the improvement is clear. The general tendency of the graph is towards reducing the FTP.

Fig.3 explores the improvement of Hybrid Scheme with respect to FIFO (RR 3, RB 0). The figure shows a significant improvement when 3 or 5 channels are reserved in backbone link. The maximum improvements are 95 % - 80 % for moderate loads and 80% - 60% at higher loads. The improvement percentage is positive for all points, which means applying reserved channels on backbone link always behaves better than non-reserved channels on backbone link. Applying reservation scheme on backbone link leads to less FTP. When only one backbone channel is kept reserved for FIFO and MBPS Hybrid Schemes, than maximum improvement is 60% at moderate load and 50% - 40% at higher load.



4.2 Increase in CBP due to Reserving Channels at Backbone Link:

As consequence of reduction in FTP, an increase in new CBP is introduced. The number of resources is limited (i.e. radio channels) as more channels are assigned to serve handover request, blocking probability will increase. We have studied how the Hybrid Scheme introduces increase in CBP, in comparison to other schemes. The increased blocking reflects the percentage increase in CBP due to non-availability of resources of scheme S_1 over scheme S_2, the increase in CBP is calculated as:

Blocking Increase (S_1,S_2) in % $\dfrac{\{b(S_1)-b(S_2)\}}{S_1}$ X 100

Where $b(S)$ is the CBP by using scheme S, substitute S_1 and S_2 for various schemes.

Reserving channels on backbone link leads to slight increase in CBP. Fig.4 explores the increase in CBP in Hybrid Scheme w.r.t. Pure FIFO(RR 0, RB 0). At low offered load(i.e. in initial stage) the increment in CBP is zero, which indicates that all the schemes have same performance. As the moderate load is offered to the network the increase in CBP suddenly raises up-to 100% for some duration, and than reduces to 30% gradually. The reason is that in the beginning of this duration no new calls get a channel all the channels are utilized by on going calls. As some channels get freed for new calls the increment in CBP starts reduces till 30% as mentioned above. For higher loads this range is 30% - 10%.

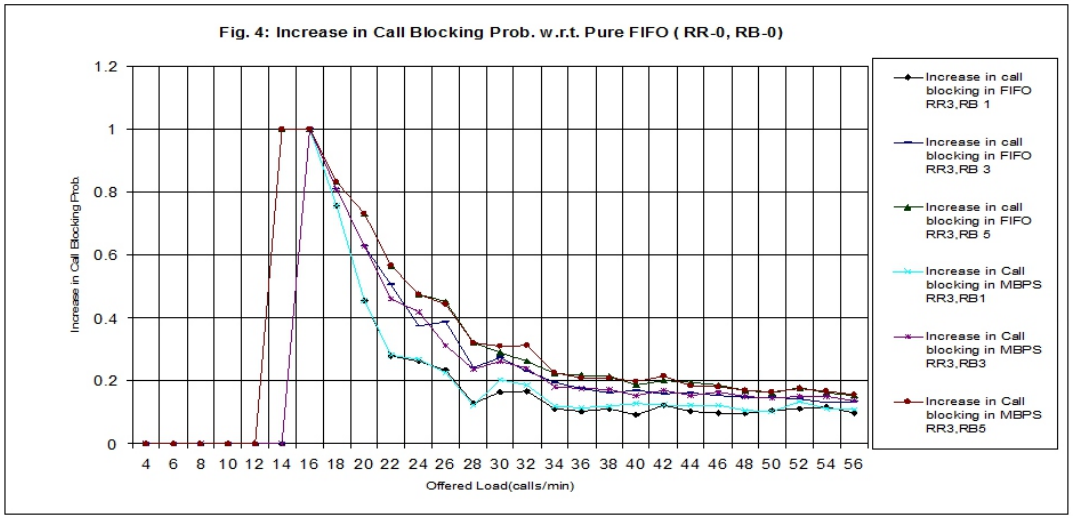
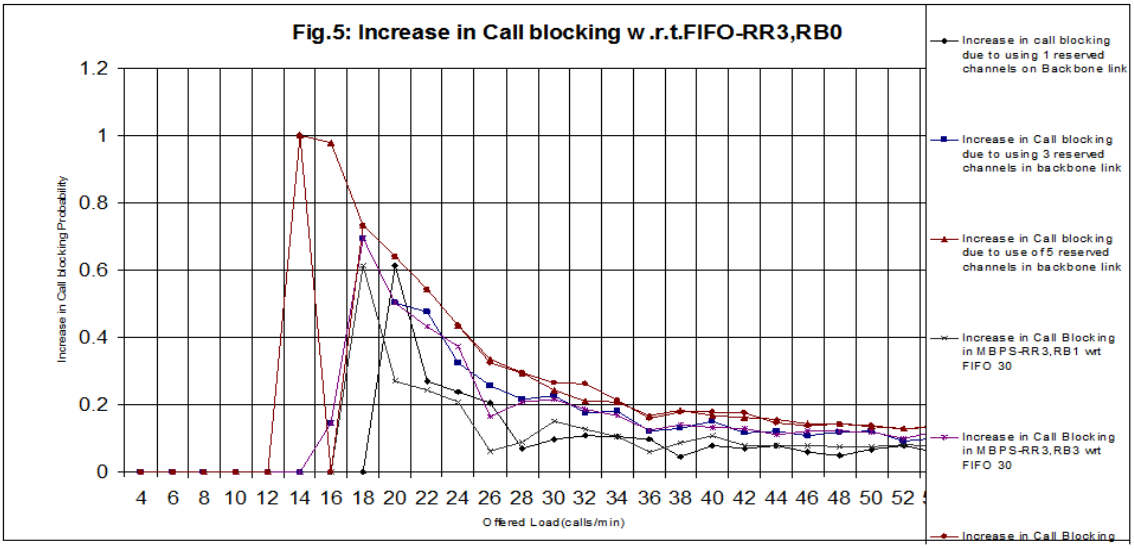


Fig. 5 represents the increase in CBP of Hybrid Scheme w.r.t. FIFO (RR 3, RB 0). The figure shows no increment in CBP at the initial stage. At moderate offered load for schemes FIFO(RR 3, RB 5) and MBPS (RR 3, RB 5) there is increment of 100% in CBP like previously, when 5 channels are reserved in backbone link. As this situation passed all the schemes shows similar characteristics. For moderate loads this range varies from 70% to 25% and 25% to 15% at higher loads.



5. CONCLUSIONS:

After studying the currently used congestion control schemes, it is clear that there is some room for improvement for conventional handoff ordering schemes. The performance analysis study carried out to show how much improvement is achieved by using the Hybrid Scheme in the comparison to the other schemes. Significant improvement achieved using Hybrid Scheme with respect to pure FIFO(RR 0, RB 0), when 3 or 5 channels are reserved in backbone link. The maximum improvement is achieved by the

schemes FIFO (RR 3, RB 5) and MBPS (RR 3, RB 5), which is 100% - 80% at moderate offered load and 70% - 50% at higher load. Applying reservation scheme on backbone link leads to less FTP. When only one backbone channel is kept reserved for FIFO and MBPS Hybrid Schemes, than maximum improvement is 60% at moderate load and 50% - 40% at higher load.

As consequence of reduction in FTP, an increase in new CBP is introduced. The number of resources is limited (i.e. radio channels) as more channels are assigned to serve handover request, blocking probability will increase. The price paid for using reserved channels is increase in Call Blocking Probability 75% to 25% approximately for moderate loads and 25% to 15% (approx.) for higher loads. This occurs because there is finite capacity for the network, and keeping more handoffs calls from being lost will result in more originating calls being lost because there are insufficient resources to handle them. Increase in CBP is always the price we have to pay for decrease in FTP. We obtained better results by using queuing time rather than the norm of a queueing buffer.

REFERENCES:

1. *Oliveira, C., et al., [Aug. 1998] : "An adaptive bandwidth reservation scheme for high-speed multimedia wireless networks," IEEE JSAC, vol. 16, no. 6, pp. 858-873.*
2. *Huang, Nen-Fu, and Wang, Rui-Chi, [1997] "An Efficient Algorithm for ATM-Based Personal Communication Network", Wireless Personal Communications, vol.4, pp. 257-275.*
3. *Acampora, A [Aug. 1996] "Wireless ATM: A perspective on issues and prospects," IEEE Personal Communications, vol. 3, no. 4, pp. 8-17.*
4. *Low, C.P.,[July 2000] "An Efficient Algorithm for Link Allocation Problem on ATM-Based Personal Communication Network", IEEE Journal on Selected Areas in Communications, vol. 18, no. 7, pp. 1279 – 1288.*
5. *Oliver, T. W., and Victor, C.M., [Sept. 1997] "Adaptive Resource Allocation for Prioritized Call Admission over an ATM-Based Wireless PCN," IEEE JSAC, vol.15, no. 7, pp. 1208-1225.*
6. *Gupta, B.K., Lal, M., and Sharma, S.C., [April 2006] : "A Hybrid Scheme for Handover in ATM - Based Personal Communication Network," Int'l Journal on Wireless and Optical Communications, Vol. 3, No. 1, pp. 69 – 81.*
7. *Lee, W.C.Y., [1989] "Mobile Cellular Telecommunication System," New York: McGraw – Hill, pp. 269- 282.*
8. *Tekinay, S.,and Jabbari, B. [Oct. 1992] "A Measurement-Based Prioritization Scheme for Handovers in Mobile Cellular Network," IEEE JSAC, Vol. 10 No. 8, 1343 – 1350.*
9. *Ebersman, H.G., and Tonguz, O.K., [Jan. 1999] "Handoff Ordering Using Signal Prediction Priority queuing in Personal Communication Systems," IEEE Transactions on Vehicular Technol., Vol. 48, no.1, pp. 20-35.*
10. *Tsigkas, O., and Pavlidou, Fotini-Niovi, [Feb. 2008] "Providing QoS Support at the Distributed Wireless MAC Layer: A Comprehensive Study," IEEE Wireless Communications, pp. 22-31.*
11. *Jiang, H., Zhuang, W., Shen, X., and Bi, Q., [Jan. 2006] "Quality of Service Provisioning and Efficient Resource Utilization in CDMA Cellular Communications," IEEE J. Selected Areas Communication, Vol. 24, no. 1, pp. 4-15.*
12. *Guerrero, L.O., and Aghvami, A.H.,[July 1999] " A Prioritized Handoff Dynamic Channel Allocation Strategy for PCS," IEEE Trans. on Veh. Technol., vol. 48, no. 4, pp. 1203-1215.*
13. *Li, Wei, and Chao, Xiuli, [February 2007] "Call Admission Control for an Adaptive Heterogeneous Multimedia Mobile Network," IEEE Transactions on Wireless Communications, Vol. 6, No. 2, pp.515 -525*
14. *Bernaschi, M., Cacace, P., Iannello, G., and Za, S., [June 2005] "Seamless Internetworking of WLANs and Cellular Networks: Architecture and Performance Issues in a Mobile Ipv6 Scenario," IEEE Wireless Communications , pp. 73-80.*
15. *Alasem, R., Hossain, Alamgir and Awan, I., [2011] "Adaptive Traffic Management Scheme for Wireless and Wired Networks" International Journal of Discrete Event Control Systems, 1 (2). pp. 151-158.*

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005