International Journal of Thesis Projects and Dissertations (IJTPD)
Vol. 2, Issue 3, pp: (1-25), Month: July - September 2014, Available at: www.researchpublish.com

Bandwidth Estimation For IEEE 802.11 Based Ad Hoc Networks

Dr. Ashok Koujalagi

Abstract: **The concept of bandwidth is central to digital communications, specifically to packet networks, as it relates to the amount of data a link or network path can deliver per unit of time IEEE 802.11-based networks have been able to provide acertain level of quality of service (QoS) by the means of service differentiation, due to the IEEE 802.11e amendment. However, no mechanism or method has been standardized to accurately evaluate the amount of resources remaining on a given channel. Such an evaluation would, however, be a good asset for bandwidth-constrained applications. It is reduce the collision and we want to improve the Throughput value and finally we find the Bandwidth.**

In multihop ad hoc networks, such evaluation becomes even more difficult. Consequently, despite the various contributions around this research topic, the estimation of the available bandwidth still represents one of the main issues in this field. We propose an improved mechanism to estimate the available bandwidth in IEEE 802.11-based ad hoc networks. Through simulations, we compare the accuracy of the estimation we propose to the estimation performed by other state-of-the-art QoS protocols.

Keywords: **Digital Communications, Ad Hoc Networks, Quality Of Service (Qos).**

1. INTRODUCTION

1.1. PURPOSE

Bandwidth Estimation for IEEE 802.11-Based Ad Hoc Networks main idea is to provide quality of service and improve the performance of Ad Hoc Network packet transmission and reduce delay in packet transmission. Ad hoc networks works don't need any fixed infrastructure like base stations for its operation. In this technology packet transmission and receiving are addressed by nodes. Ad hoc system works on IEEE 802.11 wireless network standards which is not designed for ad hoc networks but it is used for wireless systems so this standards are not accurately suited to for this system.

AD hoc networks are autonomous, self-organized, wireless, and mobile networks. They do not require setting up any fixed infrastructure such as access points, as the nodes organize themselves automatically to transfer data packets and manage topology changes due to mobility. Many of the current contributions in the ad hoc networking community assume that the underlying wireless technology is the IEEE 802.11 standard due to the broad availability of interface cards and simulation models. This standard provides an ad hoc mode, allowing mobiles to communicate directly. As the communication range is limited by regulations, a distributed routing protocol is required to allow long distance communications. However, this standard has not been targeted especially for multihop ad hoc operation, and it is therefore not perfectly suited to this type of networks. Nowadays, several applications generate multimedia data flows or rely on the proper and efficient transmission of sensitive control traffic. These applications may benefit from a quality of service (QoS) support in the network. That is why this domain has been extensively studied and more and more QoS solutions are proposed for ad hoc networks. However, the term QoS is vague and gathers several concepts. Some protocols intend to offer strong guarantees to the applications on the transmission characteristics, for instance bandwidth, delay, packet loss, or network load. Other solutions, which seem more suited to a mobile environment, only select the best route among all possible choices regarding the same criteria. In both cases, an accurate evaluation of the capabilities of the routes is necessary. Most of the current QoS proposals leave this problem aside, relying on the assumption that the link layer protocols are able to perform such an evaluation. However, they are not. The resource evaluation problem is far from being trivial as it must take into account several phenomena related to the wireless environment but also dependent on less measurable parameters such as the node mobility.

The IEEE 802.11-based networks have been able to provide a certain level of quality of service (QoS) by the means of service differentiation, due to the IEEE 802.11e amendment. Such an evaluation would, however, be a good asset for bandwidth-constrained applications. In multi hop ad hoc networks, such evaluation becomes even more difficult. Consequently, despite the various contributions around this research topic, the estimation of the available bandwidth still represents one of the main issues in this field.

IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable for building mobile ad-hoc networks prototype.

An ad hoc network is a collection of nodes that communicate via wireless links in a multi hop fashion without any fixed infrastructure or centralized servers. An ad hoc network has many practical applications including emergency military operations and personal area networking a new method to evaluate the available bandwidth in ad hoc networks based on the IEEE 802.11 MAC layer.

Existing System:

1. The ad hoc networking community assumes that the underlying wireless technology is the IEEE 802.11 standard due to the broad availability of interface cards and simulation models.
2. This standard has not been targeted especially for multihop ad hoc operation, and it is therefore not perfectly suited to this type.
3. An accurate evaluation of the capabilities of the routes is necessary. Most of the current QoS proposals leave this problem aside, relying on the assumption that the link layer protocols are able to perform such an evaluation.

Proposed System:

1. In this system they are using 802.11 MAC layer to evaluate the correct bandwidth.
2. This method combines channel monitoring to estimate each node’s medium occupancy.
3. Probabilistic combination of the values is to account for synchronization between nodes, estimation of the collision probability between each couple of nodes, and variable overhead’s impact estimation.
4. This mechanism only requires one-hop information communication and may be applied without generating a too high additional overhead.
5. We show the accuracy of the available bandwidth measurement through NS-2 simulations.
6. These results show that single-hop flows and multihop flows are admitted more accurately, resulting in a better stability and overall performance.

2. LITERATURE SURVEY

2.1 Ad Hoc Network

AD-HOC network is a collection of nodes forming an ad-hoc network without the assistance of any centralized structures.These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective

Ad hoc networks, employing the IEEE 802.11 protocol in Distributed Co-ordination
Function (DCF) mode, are becoming increasingly popular. In DCF mode, the 802.11 protocol does not require any centralized entity to coordinate user’s transmissions. Nodes are free to move around, join and leave the network as needed. As this happens, new links form as nodes come within range of each other, and existing links break as two nodes move out of range of each other. These constant changes in topology impose a significant challenge for the communication protocols to continue to provide multi-hop communication between nodes.

FIG.1: AD HOC (CLIENT TO CLIENT)

Ad hoc networks, employing the IEEE 802.11 protocol in Distributed Co-ordination Function (DCF) mode, are becoming increasingly popular. In DCF mode, the 802.11 protocol does not require any centralized entity to coordinate user's transmissions. Nodes are free to move around, join and leave the network as needed. As this happens, new links form as nodes come within range of each other, and existing links break as two nodes move out of range of each other. These constant changes in topology impose a significant challenge for the communication protocols to continue to provide multi-hop communication between nodes.

Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available.

The whole life-cycle of ad-hoc networks could be categorized into the first, second, and the third generation ad-hoc networks systems. Present ad-hoc networks systems are considered the third generation.

The first generation goes back to 1972. At the time, they were called PRNET (Packet Radio Networks). In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad-hoc networks emerged in 1980s, program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

FIG 2 MOBILE AD-HOC NETWORK (MANET)

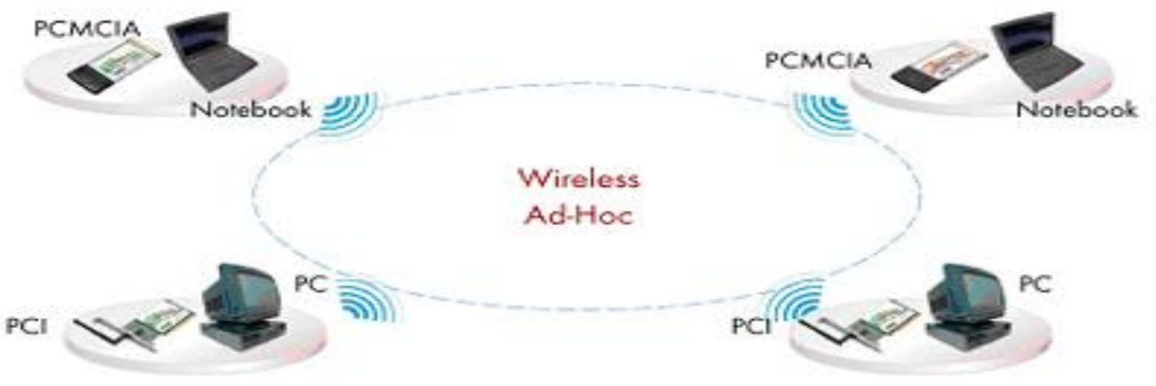
Wireless Networks

WIRELESS technologies have revolutionized the world of communications. It started with the use of radio receivers or transceivers for use in wireless telegraphy early on; and now the term wireless is used to describe technologies such as the cellular networks and wireless broadband Internet. Although the wireless medium has limited spectrum along with a few other constraints as compared to the guided media, it provides the only means of mobile communication. Wireless ad hoc networking is used for random and rapid deployment of a large number of nodes, which is a technology with a wide range of applications such as tactical communications, disaster relief operations, health care and temporary networking in areas that are not densely populated.

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are not within the transmission range in ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. The use of wireless ad hoc networks also introduces additional security challenges that have to be dealt with.

The infrastructure networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A “Hand-off” occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone.

The other type of wireless network, infrastructure less networks, is knows as Mobile Ad-hoc Networks (MANET) and is shown in Fig 1.1.These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner.



.

FIG.3: WIRELESS ADHOC

Characters and Fundamental Challenges Of Wireless Ad-Hoc Networks

Since Wireless Ad-hoc Networks are inherently different from the well-known wired networks, it is an absolutely new architecture. Thus some challenges raise from the two key aspects: **self-organization** and **wireless** transport of information. First of all, since the nodes in a Wireless Ad-hoc Network are free to move arbitrarily at any time. So the networks topology of MANET may change randomly and rapidly at unpredictable times.

This makes routing difficult because the topology is constantly changing and nodes cannot be assumed to have persistent data storage. **Bandwidth constrained** is also a big challenge. Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have **low throughput** with **energy constrains**. Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation. Mobile networks are generally more prone to physical **security threats** than are fixed cable networks. There are increased possibility eavesdropping, spoofing and denial-of-service attacks in these networks.

Routing Protocol in Wireless Networks

Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge. Lots of researchers did tremendous work on the Wireless Ad-hoc Routing Protocols. There are two main kinds of Routing Protocols

- **Table-driven protocols** (including distance vector and link state).
  In table driven routing protocols, the protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host.
- **On demand Routing protocols**
  "On demand" means that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.

Packet Radio (PR) represents the digital communications that use radio channels allocated to the amateur services. The name comes from the format in which the data are send, called packets.

This technology can be used to create inexpensive experimental radio networks. This paper presents the techniques utilized in packet-radio networks and the ways in which these techniques are used in commercial communications by wires and wireless. The main problem is that the network is not homogenous and even more it has an unpredictable character, that why the most used type of architecture is the "Mesh". The "Point to Point" type of networks could be encountered at the high-speed links that work at frequency higher than 432MHz.

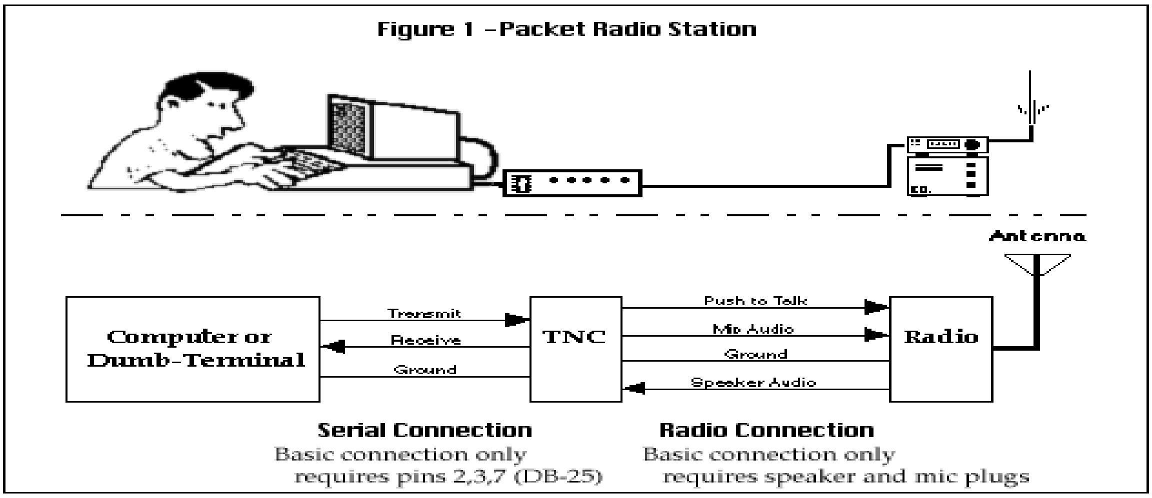
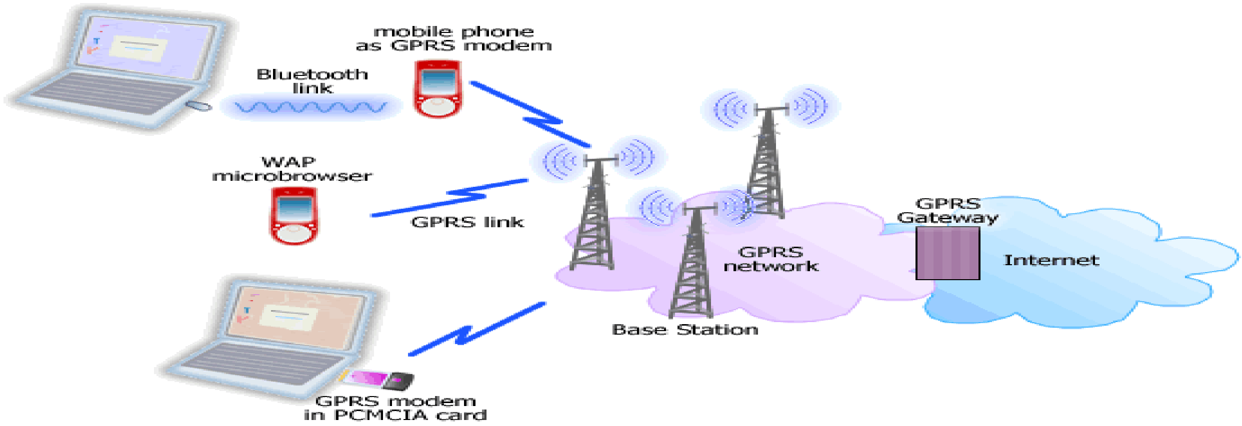


FIG.4: PACKET RADIO STATION

Only in the last period, the "Point to multi-point" architecture becomes widely used, mostly on links between Internet and packet-radio. This lead to the need of changing the medium access method, how will be reveled later in this document. GMSK system, the bit stream to be transmitted is passed through a Gaussian low pass filter. A Gaussian filter is a filter which, when excited by an impulse, outputs a Gaussian shaped output pulse. This type of modulation is used in GSM system, and offers the best ratio performance complexity.

Packet-radio networks use the AX25 protocol at the data link layer. This protocol conforms to the International Standards Organization (ISO) Information Standards (IS) 3309, 4335 and 7809 High-level Data Link Control (HDLC) and uses terminology found in these documents. It also follows the principles of the International Telegraph and Telephone Consultative Committee (CCITT) Recommendation Q.920 and Q.921 (LAP-D) in using of multiple links, distinguished bythe address field, on a single shared channel. Parameter negotiation was extracted from ISO IS. The data-link service definitions were extracted from ISO

ALOHA is the oldest access methods used in data radio networks. The very small efficiency, above 18%, forced the users to avoid it. The working principle is very simple: the users could send data any time they wish to. The collisions will destroy the data packets. Tanks to the confirmation of reception mechanism, the lost packets are retransmitted.



ALOHA is manly used in satellite networks, but even here, other medium access methods are preferred (like DAMA). CSMA (Carrier Sense Multiple Access) is the most used medium access protocol. When a station needs to send data it will listen the channel first to see if is not busy. If the channel is free, it sends a data packet. After a collision, the involved stations wait a random time interval before starting all over again. Is obvious that CSMA works only on half-duplex links. Because of the propagation time and the time needed to switch from reception to transmission there is a non-negligible chance that a collision could occur. If the signal from the first station has not reached yet the second station, it will consider that the channel is free and will transmit, so a collision will occur. By increasing the delays times, the probability of collision increases and the efficiency of CSMA decreases.

Establishing the Advanced Research Projects Agency (ARPA) was signed on February 7, 1958. The directive gave ARPA the responsibility “for the direction or performance of such advanced projects in the field of research and development as the Secretary of Defense shall, from time to time, designate by individual project or by category.”

DARPA - On March 23, 1972, by DoD Directive, the name was changed to the Defense Advanced Research Projects Agency (DARPA). DARPA was established as a separate defense agency under the Office of the Secretary of Defense.

ARPA - On February 22, 1993, DARPA was redesignated the Advanced Research Projects Agency (ARPA) - as the agency was known before 1972. The change was outlined in President Bill Clinton’s strategy paper, “Technology for America’s Economic Growth, A New Direction to Build Economic Strength.”

DARPA - On February 10, 1996, Public Law 104-106, under Title IX of the Fiscal Year 1996 Defense Authorization Act, directed an organizational name change to the Defense Advanced Research Projects Agency (DARPA).

ALOHA Current version allows the user to modify the persistence factor of the protocol. Another problem in radio networks comes from the distribution of radio coverage areas. For CSMA protocol to work properly all the stations on the network must hear when somebody transmits data.

Unfortunately, because of the uncontrollable way in which the network is build, not all the stations can listen each other, like in the next drawings. Station C can’t detect when station A is sending data, but could “hear” the B station. This phenomenon, called "hidden station problem", impose the network to act like pure ALOHA. There is an opposite problem as well, called "the exposed station problem", but his importance is smaller in our case.

DAMA (Demand Allocated Multiple Access) is used mainly because of the problems previously exposed. Only one station is a DAMA master, all others are DAMA slaves.

Once a connect request is recognized by the master, the connecting stations identification is added to the polling list and from this point on the master controls all connected stations. Permission to send data is granted by means of polls which might be included in ACK packets or even in transferred data frames. Therefore, in this case, a user will only be allowed to transmit after receiving "permission" in the form of a poll sent by the master station. Once permission is granted, several frames might be transmitted in a block. However, if the user does not respond within a given time frame then the master assumes that the poll got clobbered or the user never received it for some reason. The master then passes permission to transmit to all other active stations and, when completed, comes back to the first user and gives him another chance.

On the other hand, if the user (slave) actually receives the poll and replies with sent "I" (information) frames, the master will not acknowledge them until the next time around after serving all the other active stations. If when polled by the master, the user responds with an empty frame (Receive Ready/Final), then the master will reduce the user in polling priority and will skip him on the next time around.

As the activity on the frequency increases, the polling priority of inactive users might be further decreased, but when these stations respond with an I-frame they will again regain their original priority.

One advantage is the avoidance of system breakdown, which occurs with channel overload. Using DAMA, the throughput will increase continuously up to its maximum. The "Point to multipoint" network uses this type of medium access method, because the slave stations receive only the downlink channel and therefore they cannot know when the uplink channel is busy.

DAMA protocol is very new, so the implementations are rare at this time. One advantage of the DAMA method is that it does not require everybody to change everything all at once, the network with CSMA could use the same channel as a temporarily situation.

In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

The IEEE 802.11 subcommittee had adopted the term "ad-hoc networks" and the research community had started to look into the possibility of deploying ad-hoc networks in other areas of application.

Ad-hoc Networks are supposed to be used for disaster recovery, battlefield communications, and rescue operations when the wired network is not available. It can provide a feasible means for ground communications and information access.

Since Wireless Ad-hoc Networks are inherently different from the well-known wired networks, it is an absolutely new architecture. Thus some challenges raise from the two key aspects: self-organization and wireless transport of information.

First of all, since the nodes in a Wireless Ad-hoc Network are free to move arbitrarily at any time. So the networks topology of MANET may change randomly and rapidly at unpredictable times. This makes routing difficult because the topology is constantly changing and nodes cannot be assumed to have persistent data storage. In the worst case,we do not even know whether the node will still remain next minute, because the node will leave the network at any minute.

2.2 Manet (Mobile Ad Hoc Networks)

In fact, a key issue in MANETs is the necessity to establish an efficient and correct route between a pair of nodes so that messages may be delivered in a timely manner that what we calls the routing techniques. Several routing protocols have been developed. Such solutions must deal with the typical limitations of these networks, which include high power consumption, low bandwidth. However, most of theme considers the best effort data traffic and neglect connections with quality-of-service (QoS) requirements, such as voice channels with delay and bandwidth constraints.

There are quite a number of uses for ad-hoc networks. Wireless Ad Hoc Networks has been ongoing for decades. The wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DARPA) packet radio networks (PR Net), which evolved into the survivable adaptive radio networks (SURAD) program.

Applications of manet

There are many applications to ad hoc networks. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Web services are also possible in case any node in the network can serve as a gateway to the outside world. In this discussion, we need not emphasize the wide range of military applications possible with ad hoc networks. Not to mention, the technology was initially developed keeping in mind the military applications, such as battlefield in an unknown territory where an in frastructured network is almost impossible to have or maintain. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively. Advanced features of wireless mobile systems, including data rates compatible with multimedia applications, global roaming capabilities, and coordination with other network structures, are enabling new applications. Some well-known ad hoc network applications are:

1. Collaborative Work – For some business environments, the need for collaborative computing might be more important outside office environments than inside. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.

2. Crisis-management Applications – These arise, for example, as a result of natural disasters where the entire communications infrastructure is in disarray. Restoring communications quickly is essential. By using ad hoc networks, an infrastructure could be set up in hours instead of days/weeks required for wire-line communications.

3. Personal Area Networking and Bluetooth – A personal area network (PAN) is a short-range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary, illustrating the case where, for instance, people meet in real life. Bluetooth [Haarsten 1998], is a technology aimed at, among other things, supporting PANs by eliminating the need of wires between devices such as printers, PDAs, notebook computers, digital cameras, and so on, and is discussed later

FIG. 5: MOBILE ADHOC NETWORK

2.3 Security In Wireless Ad Hoc Network

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks.

Here, system constraints include low-power, small memory and bandwidth, and low battery power.

As for the networks attacks, there are several factors of security that we should consider. First, *Availability* ensures the survivability of network services despite denial of service attacks. *Confidentiality* ensures that certain information is never disclosed to unauthorized entities. *Integrity* guarantees that a message being transferred is never corrupted. *Authentication* enables a node to ensure the identity of the peer node it is communicating with. Yet, active attacks might allow the adversary to delete massages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Although that many security-related researches have been done to this problem, we could see that Mobile Ad hoc networks are inherently vulnerable to security attacks.

We designate by active approaches the techniques that rely on the emission of dedicated end-to-end probe packets to estimate the available bandwidth along a path. We designate by passive approaches the techniques that use only local information on the utilization of the bandwidth. A typical example of such approaches is a node monitoring the channel usage by sensing the radio medium. These mechanisms are usually transparent, but they may exchange information via one-hop broadcasts, as such information can be piggybacked in the Hello messages used by many routing protocols to discover the local topology

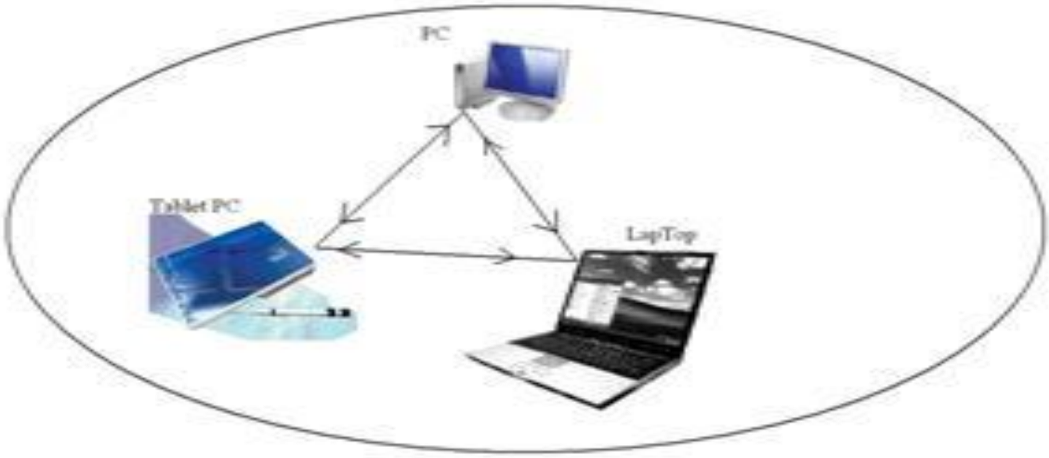
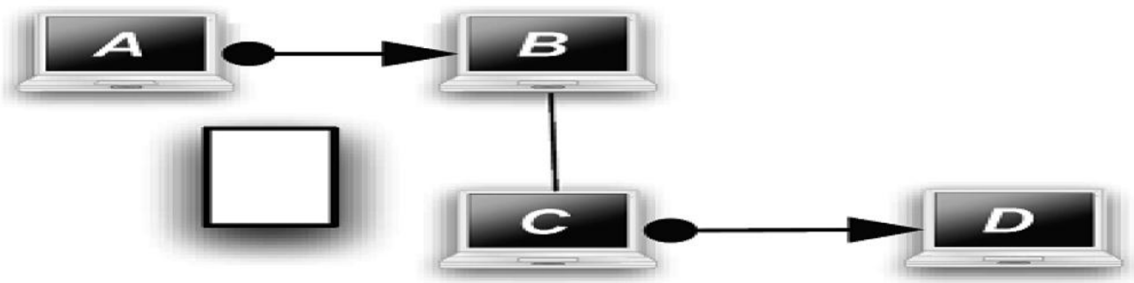


FIG. 6: SECURE ROUTING PROTOCOL WIRELESS NETWORK

2.4 Passive Bandwidth Estimation Techniques

A dynamic bandwidth management scheme for single-hop ad hoc networks is proposed in [6]. In this solution, one node in the network hosts the Bandwidth Manager process, which is responsible for evaluating the available bandwidth in the cell and for allocating the bandwidth to each peer.

Each node may ask the Bandwidth Manager for an exclusive access to the channel during a proportion of time using dedicated control messages. As the topology is reduced to a single cell, the available proportion time-share is computed by this entity considering that the total load is the sum of the individual loads. The available fraction of time may then be translated into an available bandwidth by considering the capacity of the wireless link, called total bandwidth, which is deduced from a measurement of the data packets' throughput. This approach can be considered as passive as very few control packets are exchanged, usually of small size. However, this solution is adapted to network topologies where all the nodes are within communication range but cannot be directly used in multihop ad hoc networks.



Even if the election, the synchronization, and the maintenance of several Bandwidth Managers may represent a significant cost in large distributed networks, similar measurements may be employed. When a node desires to estimate the bandwidth available in its vicinity, the intuitive approach consists in monitoring the channel over a given time period and to deduce from this observation the utilization ratio of the shared resource. The method proposed in uses such technique and adds a smoothing factor to hide transient effects. The QoS routing protocol esigned in this paper is based on a simple estimation of the available bandwidth by each node and does not consider any interfering nodes.QoS-AODV also performs such a per-node ABE. The evaluation mechanism constantly updates a value called Bandwidth Efficiency Ratio (BWER), which is the ratio between the numbers of transmitted and received packets. The available bandwidth is simply obtained by multiplying the BWER value by the channel capacity. This ratio is broadcasted among the one-hop neighbors of each node through Hello messages. The bandwidth available to a node is then inferred from these values as the minimum of the available bandwidths over a closed single-hop neigh borhood .QoS -AODV, therefore, considers not only the possibility to send a given amount of data but also the effect of the emissions of a node on its neighborhood .In Chaudet and Lassous proposed a bandwidthre servation protocol called Bandwidth Reservation underInTerferences influence (BRuIT). This protocol's ABE mechanism takes into account the fact that, with the IEEE 802.11 standard, the carrier sense radius is larger than the transmission range. In other words, emitters share the bandwidth with other nodes they cannot communicate with. Experimental studies have shown that this carrier sense radius is at least twice the communication radius. To address this issue, each node regularly broadcasts to all it simmediate neighbors information about the total bandwidth it uses to route and emit flows (deduced from applications and routing information) and its estimated available bandwidth. It also transmits similar information concerning all its one-hop neighbors, propagating such.

Information at a two-hop distance. Each node then performs admission control based on this two-hop neighborhood knowledge. When the carrier sense radius is equal to twice.

The communication radius, the authors have shown thattwo-hop communication represents the best compromise between estimation accuracy and cost .Making the same observation, Yalingand Kravets proposed the Contention Aware Admission Control Protocol (CACP). In this framework, each node first computes its local proportion of idle channel time by monitoring the radio medium. Then, the authors propose three different.

Techniques to propagate this information to the greatest number of nodes within the carrier sense area. First, similarly to BRuIT, they propose to include the information in Hello messages to reach the two-hop neighborhood .Second, they propose to increase the nodes' transmission power; however, this emission power is often limited by regulations and this technique may therefore only be applicable when power control is used for regular transmissions.

Finally, receiving nodes can also reduce the ire sensitivity in order to decode information coming from farther away, which depends on the quality of electronicsand on the signal modulation. Similarly to the authorsalso point out the existence of intra flow contention. When a flow takes a multihop route, successive routers contend for channel access for frames belonging to the same flow. It is thus important to take into account at least the route length when performing admission control. Ideally, the exactinte ractions between nodes along a path should be identified and considered. Finally, the AAC protocol, proposed in makes each node consider the set of potential contenders as a single node. It measures the activity period durations and considers that any such period can be seen as a frame emission of the corresponding length. With this mechanism, collisions and distant emissions are also considered when.

Computing the medium occupancy. Based on this measurement, each node is able to evaluate its available bandwidth. It exchanges this information with its neighbors to compute the bandwidth on each link, a link being defined as a pair of nodes. This value is defined as the minimum between the available bandwidths of both ends. AAC also takes into account the intra flow contention problem mentioned above.

2.5 AODV (AD HOC On-Demand Distance Vector)

AODV belongs to the class o f Distance Vector Routing Protocols (DV). In a DV every no de knows its neighbors' and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next h op to them. If a no de is no t reachable the distance to i t is set to infinity. Every no de sends its neighbors' periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as n ext ho p. When a link breaks a Count-To Infinity could happen.

AODV is an 'on demand routing protocol' with small delay. That means that routes are only established needed to reduce traffic overhead. AODV support s Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity an d loop problem is solved with sequence numbers and the of the costs. In AODV every hop has the const ant cost of one . The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very effectively. To characterize the AODV with the five criteria used by Keshav AODV is distributed, by-hop, deterministic, single path and state dependent.

AODV uses IP in a special way. It treats an IP ad dress just as an unique identifier. But also aggregated networks are supported. They are implemented as subnets. Only one router in each o f them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the net and to forward every package.

In AODV the routing table is expanded by a sequence number to every destination and by time to live for every entry. It is also expanded by routing flags, the interface, a list of precursors and for out dated routes the last hop count is stored **.**

2.6. Accurate Available Bandwidth Estimation

From the above literature study, some of characteristics that were identified for bandwidth estimation from one node to its neighbors and detailed evaluation are presented in these are following.

Carrier sense mechanism

The node is first needed to contend for medium access whenever it sends frame in network. If channel is free, it can send a frame.

Therefore, a sender needs to evaluate the proportion of time the medium is idle to determine the chance to gain access to the shared resource. So the carrier sense mechanism prevents two close emitters from transmitting simultaneously, unless they draw the same backoff counter value. Therefore, an emitter shares the channel bandwidth with all its close neighbors. The expected delay should be computed for accurate bandwidth estimation.

Channel's idle period synchronization

For a transmission to take place, the receiver needs that no interference occurs during the whole transmission. Therefore, the value of the available bandwidth on a link depends on both peer channel utilization ratios and also on the idle period synchronization. This synchronization needs to be evaluated.

Collision Probability

No collision detection is possible in a wireless environment.Therefore, whenever a collision happens; both colliding frames are completely emitted maximizing the bandwidth loss. The collision probability is needed to be estimated and integrated to Available bandwidth estimation.

Back off Time

When collisions happen on unicast frames, the IEEE 802.11 protocol automatically retries to emit the same frame, drawing the backoff counter in a double-sized contention window. The time lost in the additional overhead may also have an impact on the available bandwidth and has to be evaluated. Commonly resolving the collisions is handled by binary exponential backoff scheme in MAC Layer. Ignoring backoff account provides high inaccuracy in the estimated available bandwidth

2.7. Route Processing In Ad Hoc Network

The RREQ and RREP method is used to control the transmission requests and flow of data between sender and receiver node. The basic concept implemented here is before transmitting any data or file sender has to approval for his "Router Request" i.e. RREQ. This RREQ is sent to the server machine for route availability between source to the destination, after analyzing which path is available for the transmission, RREP is sent by the server machine to the source machine. This RREP contains the free path information and if no path is free then the server providing alert message that "No Path is Free, Please Try after Some Time", rejects the RREQ. RREQ and RREP are most needed before transmission of any data else if sender press send button without getting RREP from the server it would get the message of re-approach. So here we can say RREQ and RREP are the main functions here to provide the details whether bandwidth is available or not. If bandwidth is not available then the transmission is rejected, thus it helps in control the transmission flow.

Transmission Control Technique

In this transmission control mechanism we particularly depend upon the status of the availability of the bandwidth in the route. Here we represent the availability by zero and if any route is occupied by any of the transmission then it is represented by one. At first we set all the routes to free and assign zero to all the paths. Once if any sender request for any transmission and send RREQ to the sender it checks with the availability of the free route for transmission, if it gets zeros in any of the possible path for transmission, it sends the RREP after assigning one to all the required paths. If the server machine finds one in all the possible routes then simply it rejects the request by the source machine and shows message to the user. This method in conjunction with the RREQ and RREP controls the transmission of data in network

For unicast routing three control messages are used: RREQ (Route Reply), RR EP (Route RE Pl y), RE RR (Route Error). If a node wants to send a packet to a node for which no route is available it broadcasts a RREQ to fin d one. ARR EP includes a unique identifier, the destination IP address and sequence number, the source IP address and sequence number as well as a hop count initialized with zero and some flags. If a node receives a RREQ which it does not have seen before it sets up a reverse route to the sender.

If it does not know a route to the destination it rebroadcasts the up dated RREQ especially incrementing the hop count. If it knows a route to the destination it creates a RREP.

The RREP is unicasted to the origin node taking advantage of the reverse routes. A RREP contains the destination IP address and sequence number, the source IP address, a time to life, a hop count as well as a prefix only used for subnets and some flags. When a node receives a RREP it checks if the hop count in the RREP for the emitter of the message is lower than the one in its own routing table or the destination sequence number in the message is higher than the one in its own routing table . If none of them is true it just throws the package away. Otherwise it updates its routing table and if it is not the destination it reunicasts the RREP .

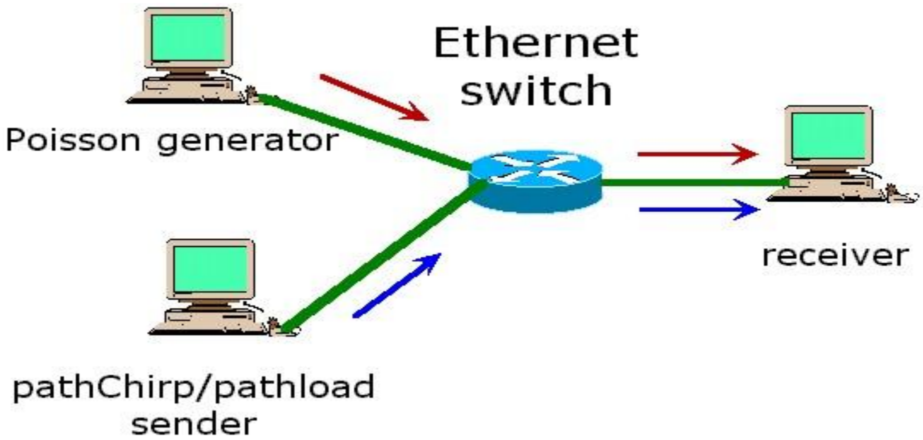


FIG.7: ETHERNET SWITCH

2.8 Bandwidth Estimation

The 802.11 protocol covers the MAC and Physical Layer. The basic access mechanism, called Distributed Coordination Function (DCF). In wireless networks the radio channel of each node is shared with all its neighbors. Because of the shared medium, a node can successfully use

the channel only when all its neighbors do not transmit and receive packets at the same time. Due to the shared nature of wireless network communication and MAC layer mechanisms, a node can estimate the channel occupancy by monitoring its environment. The radio medium is pervasive and a frame emission from a node has an impact on other nodes that located in common communication area. The term bandwidth refers to the information carrying capacity of a node in networks. It is measured by bits per second which refers to the speed of bit transmission in a channel or link. The bandwidth related metrics [1] are Capacity, Available Bandwidth and Bulk Transfer capacity (BTC). The first two are defined both for individual links and end-to-end paths, while the BTC is usually defined only for an end-to-end path. The maximum possible bandwidth that a link or path can deliver is called Capacity. The maximum unused bandwidth at a link or path is called available bandwidth. The achievable throughput of a bulktransfer TCP connection is called BTC. Here Available bandwidth is focused as QoS metric. Available bandwidth is the amount of bandwidth left over after the cross traffic. It can be determined by finding the time period for which the link is not utilized for transmitting data. Estimation of available bandwidth is difficult task in ad hoc networks. The general formula for estimating Available Bandwidth is given

BW available= BW physical – BW consumed

When the available bandwidth is estimated, the activities of the neighbors of nodes must be taken into account, since the wireless medium of a node is shared among neighboring nodes. Various tools and techniques are developed and proposed for estimating available bandwidth in networks. These are categorized into active and passive techniques.

Active techniques that are based on the end-to-end probe packets to estimate available bandwidth in wired networks. Numbers of techniques were developed to measure the end-to-end available bandwidth by sending packets of equal size from a source to receiver. Many available bandwidth estimation tools have emerged. These techniques that relay on the emission of dedicated end-to-end probe packets to estimate the available bandwidth along a path.

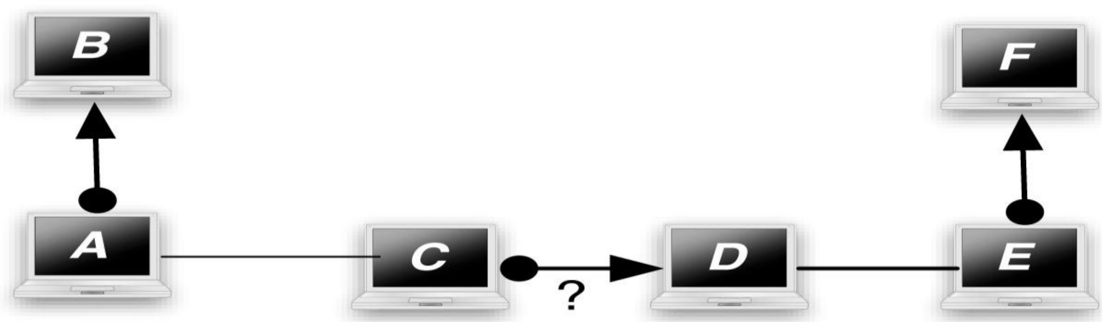
Cprobe was the first tool to attempt to measure endto-end available bandwidth. Cprobe measures the dispersion of a train of eight maximum-sized packets. In general the dispersion rate depends on all links in the path as well as on the train's initial rate. In contrast the available bandwidth only depends on the tight link of the path. Cprobe is described as a pioneering tool for estimating the available bandwidth using end-to-end measurements. Cprobe doesn't assume fair queuing. Instead of using a pair of packets, Cprobe sends a short train of ICMP packets and computes the available bandwidth as the probe traffic divided by the interval between the arrival of the last ICMP ECHO and the first ICMP ECHO in the train.

Passive techniques which are using only local information for the utilization of the bandwidth. A typical example of such approaches is a node monitoring the channel usage by sensing the radio medium. These mechanisms are usually transparent, but they may exchange information via one-hop broadcasts, as such information can be piggybacked in the Hello messages used by many routing protocols to discover the local topology. Bandwidth reservation protocol is proposed which is called Bandwidth Reservation under InTerferences (BRuIT) that takes into account the notion of carrier sensing area in the available bandwidth estimation. Indeed, with CSMA protocols (like in IEEE 802.11), two nodes within carrier sensing range share the medium and thus the bandwidth, even if they cannot directly communicate. Therefore, each node needs not only to know the channel occupancy in its communication range, but also in its carrier sensing range. BRuIT attempts to compute the channel usage in the carrier sensing area. In BRuIT, the carrier sensing area is approximated by the two-hop neighborhood. The drawback of this method is that the two-hop neighborhood may not correspond exactly to the carrier sensing area.

Available bandwidth estimation is a vital component of admission control for quality-of-service (QoS) in both wireline as well as wireless networks. In wireless networks, the available bandwidth undergoes fast time-scale variations due to channel fading and error from physical obstacles. These effects are not present in wireline networks, and make estimation of available bandwidth in wireless networks a challenging task. Furthermore, the wireless channel is also a shared-access medium, and the available bandwidth also varies with the number of hosts contending for the channel.Wireless last-hop networks employing the IEEE 802.11 protocol in Distributed Co-ordination Function (DCF) mode are becoming increasingly popular. In DCF mode, the 802.11 protocol [1] does not require any centralized entity to co-ordinate users' transmissions.

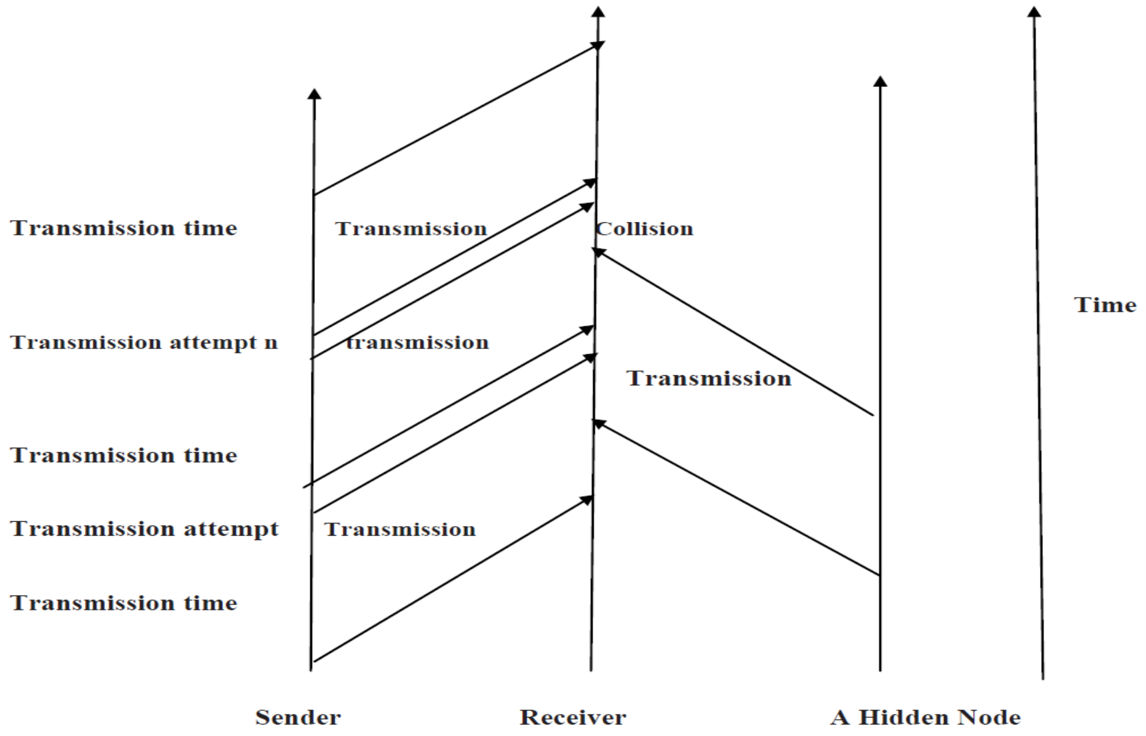
2.9 Ad Hoc Networks in Bandwidth Estimation

In ad hoc networks, due to the complex interactions between nodes, emitters and receivers are unlikely to be perfectly synchronized. Precisely evaluating the impact of his a synchronism requires the exchange of the exact medium utilization patterns of both peers and a fine clock synchronization mechanism, which represents a huge overhead, though. Therefore, we propose to use a probabilistic mechanism to estimate the effect of this phenomenon.



Let us examine the requirements for a successful frame transmission. First, for the communication to start, the medium has to be free during at least DIFS on the emitter's side so that this emitter gains access to the medium. Once the emission has started, the status of the medium at the emitter's side is irrelevant. On the receiver's side, the medium has to be free during the time required to transmit the whole data frame otherwise, a collision occurs. This value is not perfectly accurate, though. It makes the hypothesis that the level of signal that would provoke a collision is equal to the carrier sense threshold, regardless of the distance between the emitter and the receiver, for example. It also does not take into account the propagation time

The Communication model between wireless link to IEEE-802.11



Emitters can evaluate the collision probabilities toward certain receivers by counting the number of retransmission events at the MAC layer. However, such strategy is only applicable to nodes already emitting data frames. The evaluation mechanism should, however, be active even when no data traffic is emitted.

2.10 Mac Layer

The MAC layer uses a CSMA/CA algorithm for shared use of the medium. In this extended abstract, we present an available bandwidth estimation scheme for IEEE 802.11-based wireless networks. Our scheme does not modify the CSMA/CA MAC protocol in any manner, but gauges the effect of phenomena such as medium contention, channel fading and interference, which influence the available bandwidth, on it. Based on the effect of the phenomena on the working of the medium-access scheme, we estimate the available bandwidth of a wireless host to each of its neighbors

There are mainly two categories of MAC protocols in the literature. The first one is based on the bakeoff mechanism: the protocol uses the contention window to modify the behavior of the protocol. The use of the contention window can be a modification of the window size or of the way of increasing/decreasing it.

The choice of this protocol is justified according to two axes:

First of all, the medium radio, shared by all mobiles, is a very rare resource for networks Ad hoc. AODV, by his reactive nature, asks for a bandwidth less important for the service of the tables of routing than the protactive protocols. In fact, these last generate massive control traffic between useful periods of communication while the reactivity of AODV reduces the load of network in term of messages of control since paths towards destinations are established only at the request of the sources of traffic of data. Besides, the periodicity of emission of the control traffic, generated by a proactive protocol, can be useless and overload network knowing that there are paths which are constructed but not used by applications.

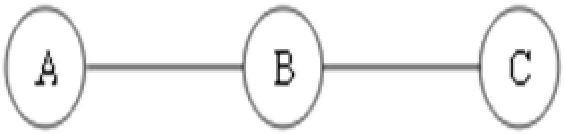
Besides, AODV is based on the most interesting notions since DSR and DSDV such as the concept of discovery of path by Route Request and maintenance by Route Error of DSR as well as the principle of sequecnce number and the mechanism of neighbourhood discovery since DSDV. Studies in this frame revealed that the protocol AODV assures a better success (especially in term of rate of the issued packets), by comparing it with other routing protocol

Medium Access Control (MAC) Protocols Issues

Maybe not as much as ad hoc routing protocols, but MAC protocols have also been receiving attention from the research community. There are still many issues that need to be addressed in order to design an efficient MAC protocol to be used in a wireless ad hoc network environment [Royer 2000]. There are several MAC protocols which can be employed for multi-hop ad hoc networking including IEEE 802.11 [Crow 1997], Bluetooth [Bluetooth] and Hiper LAN [Hiper LAN 1995]. Usually, the IEEE 802.11 standard is the platform employed to experiment multi-hop networking. However, it does not support multi-hop as is. In this section, we discuss some fundamental issues MAC protocols for wireless multi-hop ad hoc networks have to cope up with, along with their proposed solutions.

Hidden Terminal Problem:

In CSMA, every station senses the carrier before transmitting, and if it detects carrier then the transmission is deferred. Carrier sense attempts to avoid collisions by testing the signal strength in the vicinity of the transmitter. However, collisions occur at the receiver, not the transmitter; i.e., it is the presence of two or more interfering signals at the receiver that constitutes a collision. Since the receiver and the sender are typically not co-located, carrier sense does not provide the appropriate information for collision avoidance. Two examples illustrate this point in more detail. Consider the configuration depicted in . Station A can hear B but not C, and station C can hear station B but not A (and, by symmetry, we know that station B can hear both A and C). First, assume A is sending to B. When C is ready to transmit (perhaps to B or perhaps to some other station), it does not detect carrier and thus commences transmission; this produces a collision at B. Station C's carrier sense did not provide the necessary information since station A was "hidden" from it. This is the classic "hidden terminal" scenario.



Station B can hear both A and C, but A and C cannot hear each other.

An "exposed" terminal scenario results if now we assume that B is sending to A rather than A sending to B. Then, when C is ready to transmit, it does detect carrier and therefore defers transmission. However, there is no reason to defer transmission to a station other than B since station A is out of C's range. Station C's carrier sense did not provide the necessary information since it was exposed to station B even though it would not collide or interfere with B's transmission. The point to note here is that carrier sense provides information about potential collisions at the sender, but not at the receiver. This information can be misleading when the configuration is distributed so that not all stations are within range of each other.

The solution to the hidden terminal problem was proposed in [Karn 1990]. It consists of transmitting RTS (Request-to-Send) and CTS (Clear-to-Send) packets between nodes that wish to communicate. Among other things, these RTS and CTS packets carry the duration of the data transfer of the communicating parties. Stations in the neighborhood that do not participate in the communication but overhear either the RTS or CTS keep quiet for the duration of the transfer. Returning to our example of when node A wants to send a packet to node B, node A first sends a RTS packet to B. On receiving the RTS packet, node B responds by sending a CTS packet (provided node A is able to receive the packet). As a result of that, when node C overhears the CTS sent by B it keeps quiet for the duration of the transfer contained in the CTS packet. As for the exposed terminal problem, while in IEEE

802.11 MAC layer there is almost no scheme to deal with it, MACAW [Bharghavan 1994] solves this problem by having the source transmit a data sending (DS) control packet to alert exposed nodes of the impending arrival of an ACK packet.

FIG.8: MAC LAYER

2.11 Abe: (Available Bandwidth Estimation)

The different points mentioned above can be combined to estimate the available bandwidth on a wireless "link," i.e., between a given emitter and a given receiver. The whole mechanism, called ABE, leads to a lightweight protocol design, as it mainly relies on the perception that nodes have of their immediate environment**.**

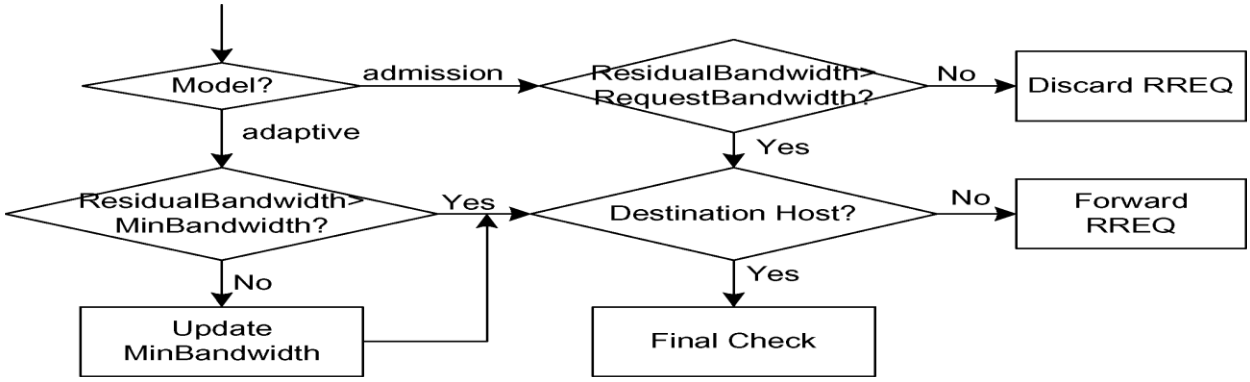


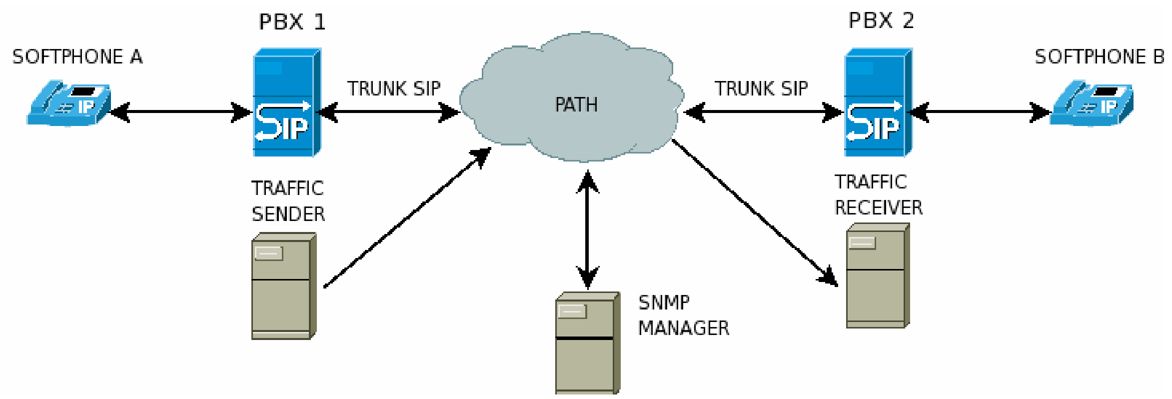
FIG.9: Working procedure for RREQ

2.12 Problem

1. Routing is a big problem. All the routing protocols for Wireless Ad hoc Networks are need patches. No suitable and stable routing protocols until now.
2. The topology of the network changed rapidly, which willlead to the loss of packets.
3. Second, we have tomodify every node's routing table that
4. Within the communication distance of the rapid-passing node, that will greatly improve the consumption of thebandwidth and the overhead of the networks.
5. Obviously there will be tremendous delay of the datasending to the rapid-moving node.
6. Transmission between two hosts over a wirelessnetwork does not necessarily work equally well inboth directions. Thus, some routes determined bysome routing protocols may not work in some environments.
7. Periodically sending routing tables will waste network bandwidth. When the topology changes slowly, sending routing messages will greatly waste the bandwidth of Wireless Ad-hoc Networks. Thiswill add additional burdens to the limited bandwidth of the Ad-hoc Networks.
8. Periodically sending routing tables also waste the battery power. Energy consumption is also a criticalfactor which prevents Wireless Ad-hoc Networks tobe a non-flowed architecture.
9. Bandwidth estimation may lead to inaccurate admission control because it is impossible to gauge beforehand the effect.

2.13 Deduction and Problem Solving

The carrier sense mechanism prevents two close emitters from transmitting simultaneously, unlessthey draw the same bakeoff counter value. Therefore,an emitter shares the channel bandwidth withall its close neighbors. The channel utilization has tobe monitored to evaluate the capacity of a node to emit a given traffic volume.



The receiver needs that no interference occurs during the whole transmission. Therefore, the value of the available bandwidth on a link depends on both peer channel utilization ratios and also on the idle period synchronization. This synchronization needs to be evaluated.

When collisions happen on unicast frames, the IEEE 802.11 protocol automatically retries to emit the same frame, drawing the backoff counter in a double-sized contention window. The time lost in the additional overhead may also have animpact on the available bandwidth and has to be evaluated.

Finally, when collisions happen on unicast frames the IEEE 802.11 protocol automatically retries to emit the same frame, drawing the backoff counterin a double-sized contention window. The timelost in the additional overhead may also have animpact on the available bandwidth and has to beevaluate.

Integration into AODV: Admission Control

We have slightly modified AODV in order to transform it into a QoS protocol based on ABE. It thus becomes across-layer routing protocol. The MAC layer estimates proactively and periodically the available bandwidth of the neighboring links, and the routing layer is in charge of discovering QoS routes complying to the application demands, basing its decisions on the MAC layer information.

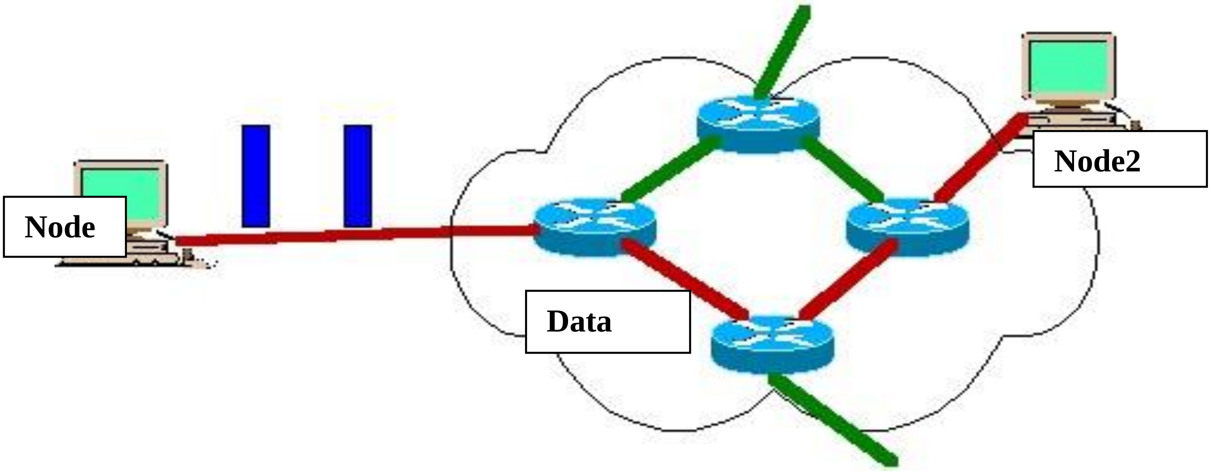
Route Discovery

The aim of the route discovery procedure is to find a route between the sender and the receiver that meets the constraints specified by the application level in terms of bandwidth. Therefore, two flows with the same source and destination can follow different routes depending on the network state. When a source node has data to send, it broadcasts a route request (RREQ) to its neighbors. The RREQ packet contains the address of the sender, the channel use, the requirements at the application level, the destination address, and a sequence number. Each mobile node that receives such an RREQ performs an admission control by simply comparing the bandwidth requirement carried in the RREQ packet to the estimated available bandwidth on the link it received the RREQ on. If this check is positive, the node adds its own address to the route and forwards the RREQ; otherwise, it silently discards the message. This step is different from the other tested protocols as the admission control is done at the receiver side and not at the sender side. This is explained by the fact that, in ABE, each node stores the available bandwidths of its ingoing links. Finally, if the destination receives a first RREQ, it sends a unicast route reply (RREP) to the initiator of the request along the reverse path. The resources are then reserved and the new QoS flow can be sent.

Intraflow Contention Problem:

Simply comparing the bandwidth application requirement and a link available bandwidth is not sufficient to decide about the network ability to convey a flow. Indeed, the intra flow contention problem has to be considered when performing multi hop admission control. Contention count (CC) of a node along a given path. This value is equal the number of nodes on the multi hop path that are located within the carrier sensing range of the considered node. To calculate the CC

of each node, the authors analyze the distribution of the signal power. ABE, we rather use a direct relationship between the end-to-end throughput and the number of hops. Hence, after consideration of the intra flow contention on an intermediate node j, which is located at H hops from the source and has received the
RREQ from a node.



Working Model

Bandwidth estimation techniques can be divided in two major categories:

1. We call intrusive approaches techniques that are based on end-to-end probe packets to estimate the available bandwidth along a path.

2. We call passive approaches techniques that use local information on the used bandwidth (like for instance the channel usage computed from the sensing of the radio medium) and that may eventually exchange this information via local broadcasts. Usually these local broadcasts are performed using Hello messages that are used in many routing protocols to discover local topology.

If these exchanges are not too frequent, this technique can be reasonably considered as non intrusive.

A. Intrusive bandwidth estimation techniques

Many active bandwidth estimation techniques have been proposed for wired networks. A detailed survey of the different techniques is proposed The Self-Loading Periodic Streams (SLoPS) technique measures the end-to-end available bandwidth by sending packets of equal size and by measuring the one-way delays of these probing packets. The source increases the sending frequency of the probing packets; as soon as there is a variation in the delay, the path is considered as saturated and the measurement point just before the variation indicates the available bandwidth. The Trains of Packet Pairs technique is based on the same principle. The main difference between these two methods concerns the rate increasing function: TOPP increases linearly the rate whereas SLoPS uses a binary search.

Based on TOPP method, the authors evaluated the accuracy of this type of techniques in wireless networks. This article showed that both probe packets size and volume of cross-traffic had a stronger impact on the measured bandwidth in wireless network than in wired networks. This advocates for the use of a different bandwidth probing mechanism in wireless networks and in wired networks and leaves the question of heterogeneous networks open.

The main idea presented is that a probe packet delay higher than the maximum theoretical delay can characterize the channel utilization. The authors propose such a method to compute the medium utilization from the delays and then to derive the available bandwidth from the channel utilization. All these techniques are active as they use end-to-end probe packets to characterize the channel. Such techniques, however present two major drawbacks. First, when every node in an ad hoc network needs to perform such an evaluation for several destinations, the number of probe packets introduced in the network can be important and interact on the traffic as well as on other probes. Second, in a mobile network that may present heterogeneous quality links, an end-to-end evaluation technique may not be as reactive as a local technique combined to a path-wide measurements combination mechanism, especially when it comes to local reconstruction of routes.

B. Passive bandwidth estimation techniques

When a node seeks to estimate the bandwidth available in its vicinity, the intuitive approach consists in monitoring the channel over a given time period and deduce from this observation the utilization ratio of the shared resource .uses this technique and adds a smoothing factor to mask transient effects. The QoS routing protocol designed in this article is only based on this estimation of the available bandwidth at each node and does not consider any possible distant interfering nodes.

QoS-AODV also performs such per-node available bandwidth estimation. The authors propose however to use a different metric, called BWER (Bandwidth Efficiency Ratio) that computes the ratio between the number of transmitted and received packets. This ratio is then locally broadcasted in Hello messages to propagate this value in the one-hop neighborhood of each node. The bandwidth available to a node is then computed as the minimum of the available bandwidths over a closed single-hop neighborhood. Chaudet and Gu´erin Lassous have proposed a bandwidth reservation protocol, called Bandwidth Reservation under InTerferences influence (BRuIT). This protocol's available bandwidth estimation mechanism takes into account the IEEE 802.11 increased carrier sense radius compared to the transmission radius. With this protocol, when performing carrier sense, nodes consider the medium as busy whenever the signal level on the medium is over a threshold defined to be much lower than the one required receiving a frame

correctly, extending the zone in which the medium is shared to at least twice the communication radius. In other words, medium may be shared with nodes that cannot be contacted directly. With BRuIT, each node regularly broadcasts to all its immediate neighbors information about the total bandwidth it uses information) and its estimated available bandwidth. It also includes in every such Hello packet similar information from all its one-hop neighbors, propagating this information at a two-hop distance. Each node gathers two-hop neighborhood knowledge that it may then use to perform admission control. In this article, the carrier sense zone is approximated by the two-hops neighborhood representing, with this technology, the best compromise between introduced overhead and estimation accuracy.

The Contention Aware Admission Control Protocol (CACP). First, each node computes the local idle channel time fraction by a permanent monitoring of the radio medium. Then, the authors propose three different techniques to propagate this information. First, like in BRuIT, to include it in Hello messages in order to broadcast it over the two-hop neighborhood. Nodes may also increase their transmission power of nodes so that all the nodes in the carrier sensing area could be reached. Finally, nodes may reduce their receivers' sensitivity in order to gather information on the bandwidth used in their carrier sensing area. The authors also raise the intra-flow contention problem as wireless links are not isolated, multiple routers on the path conveying a flow may contend for bandwidth at a single location. Therefore, it is important to take into account at least the route length, and better the exact interactions that may exist between each set of links on a single path. Each node considers the set of potential contenders as a single node. It measures the activity periods lengths and considers that any continuous busy period corresponds to a frame emission of the corresponding length, whether the frame can really be decoded or not. This way, collisions as well as distant emissions are also considered in the medium occupancy. Based on this measurement, each node is able to evaluate its available bandwidth and exchanges

This information with its neighbors to compute the bandwidth on each link, i.e. for each pair of nodes, as the minimum between the available bandwidths of both ends. AAC also estimates the contention count of nodes along a QoS path to solve the intra-flow contention problem mentioned before.

C. Motivation

The active techniques presented above are not satisfactory in this context, as they consume bandwidth and reduce the capacity of the network. They can also affect the on-going flows. Moreover, as the network mobility increases, they require frequent re-estimations of end-to-end paths and do not allow local routes reconstruction. The presented passive techniques do also not seem totally satisfactory, as most of them are based on estimations computed on the nodes and they do not provide an accurate evaluation of the available bandwidth on the links. They only consider the sender's side of the problem. Even though ensuring that the medium capacity is not overloaded anywhere in the network may be performed by only considering the emissions volumes, further accuracy could be added by considering the synchronization or lack of synchronization of parallel emitters.

If parallel emitters are badly synchronized, repetitive collisions can happen on a link and need to be taken into account in the evaluation. For example, let us consider the scenario depicted on Figure.

Let's consider that there is a constant bit-rate ongoing flow on the link (C,D). We intend on computing the available bandwidth on the link (A,B). In this case, the evaluations provided by BRuIT, CACP and AAC are identical and are represented in function of the throughput of the flow of the link (C,D) "estimated available bandwidth" .

For all these protocols, the available bandwidth on the link (A,B) corresponds to the available bandwidth value computed by node B (identical to the value computed by node C) and is equal to the capacity of the radio medium minus the bandwidth consumed by the flow on the link (C,D)

Accurate Available Bandwidth Estimation

1. Based on the previous literature study and considering how the IEEE 802.11 protocol operates, we can point out a few phenomena that may have an impact on the available bandwidth estimation mechanism:
2. Carrier sense mechanism prevents two emitters to transmit simultaneously. Therefore, an emitter shares the channel bandwidth with other emitters. There is a need to monitor the channel utilization to evaluate the capacity of a node to emit a given traffic volume.
3. For a transmission to take place, both emitter and receiver need to sense an idle medium during the whole transmission. Therefore, the bandwidth on a link, i.e. between an emitter and a receiver, is dependent on their respective channel utilization ratios but also on the idle periods synchronization. There is a need to evaluate this synchronization.
4. Whenever collisions happen, both colliding frames are fully transmitted, resulting in a bandwidth loss. As we have hinted in the previous section, only considering the two previous points is not enough to accurately estimate available bandwidth. There is a need to estimate and take into account the probability that a given frame collides.
5. When collisions happen on unicast frames, the IEEE 802.11 protocol retries a frame emission with a doubled contention window. Therefore, the time lost in additional overhead may have an impact on the available bandwidth and may have to be evaluated.

In this section, we will examine in turn all four points listed above and describe how we take these phenomena into account, or why we do not take some into account. Every point could, in theory, be evaluated by measuring some local metrics and exchanging information with close and far neighbors. However, in this article we seek a relatively lightweight and local mechanism to avoid consuming too much resource for network management and to allow a relatively fast reaction to mobility. We consider that no RTS/CTS mechanism is triggered. Local passive measurements combined to control packets locally broadcasted (with a single-hop MAC layer broadcast, i.e. one single frame emission) seems a reasonable overhead, especially considering that most routing protocols already use these packets (called Hello packets) to discover local topology. Resources evaluation information may therefore be piggybacked in such packets at a very light cost.

we designed a per-link available bandwidth estimation method that combines three measurements: a time-based channel utilization monitoring to estimate the bandwidth usage in the carrier sensing area, a probabilistic estimation of the overlap of the silence periods experienced by the two peers on a link and an estimation of the collision probability on a link.

The two last estimates require nodes to exchange bandwidth-related information. This exchange does not necessarily require dedicated control packets. This information can easily be appended to neighborhood discovery messages used by many routing protocols. Therefore our approach can be qualified as passive.

1. Estimating a node's available bandwidth

In order to evaluate the bandwidth it may use, every node shall monitor the radio medium and measure the total amount of time during which the medium remains free. As this method is solely based on a signal level measurement, it allows taking into account emissions happening in the carrier sensing area without identifying interfering emitters. In order to enhance the accuracy, we only consider silence periods long enough, i.e. lasting long enough (more than the DIFS timing) to allow a frame emission.

2. Estimating overlap of silence periods

We proposed a method to derive the available bandwidth on a link from the available bandwidth computed by the two nodes of the link. This evaluation uses a probabilistic estimation of the overlap of the silence periods and only requires the exchange of bandwidth usage information between neighbor nodes. We conclude that this method improves the evaluation but is still inaccurate, particularly when collisions decrease the available bandwidth, for instance with hidden nodes configurations. C. Collision probability estimation To enhance this estimation, we evaluate the collision probability by monitoring Hello packets. These control messages are sent periodically. Therefore, if we consider a given measurement period, it is possible to deduce the Hello collision rate using the number of actually received packets and the expected number of such packets. This estimation requires the Hello packets sending rate to be known by every node. This information can either be shared by all nodes, or included in Hello packets. It should be noted that Hello packets are sent in local broadcast, unlike data packets. Therefore, the collision rate experienced by Hello packets only reflects the probability that a data packet emission attempt fails. However, as collision detection is not possible in wireless systems, etransmissions performed by the MAC layer consume bandwidth as if they were different frames. The collision probability evaluated on broadcasted frames may thus be used to evaluate the bandwidth consumed by collisions. The main imprecision in this approach comes from the different frames sizes. Hello packets are expected to be rather small frames, unlike data packets. As the probability that a given frame collides with another is highly dependant on both frames' sizes, the performed measurement should be adapted. Actually, we deduce the collision probability on arbitrary frame size by using a Lagrange interpolating polynomial. This approach is static and performed offline. However, the simulations we performed show that this interpolation gives rather accurate results and allows an enhancement in the available bandwidth estimation method. Designing a dynamic mechanism may further enhance accuracy and is currently under investigation.

A. Carrier sense mechanism: estimating a node's emission capabilities

Whenever a node needs to send a frame, he first needs to contend for medium access and cannot emit its frame unless the medium is free. Therefore a potential sender needs to evaluate the load of the medium, i.e. the proportion of timethe medium is idle and would allow him to emit a frame.

Flow of nodes:

1. Send Message Pane*:* This pane includes options for sending the data to another node
2. Combo Box: To choose destination from the list of available nodes
3. File Chooser*:* For selecting the text files for file transmission
4. Text Area*:* Enables the user to write text or contains the selected file data to send
5. RREQ Button*:* For route request from current node to the destination
6. Send Button*:* For sending data to the destination node, it works only when the RREQ is confirmed
7. Clear Button*:* To clear the content of Text Area
8. Exit Button*:* To come out of the Application
9. Received Message Pane*:* This pane is used for displaying the text which arrives from other node.

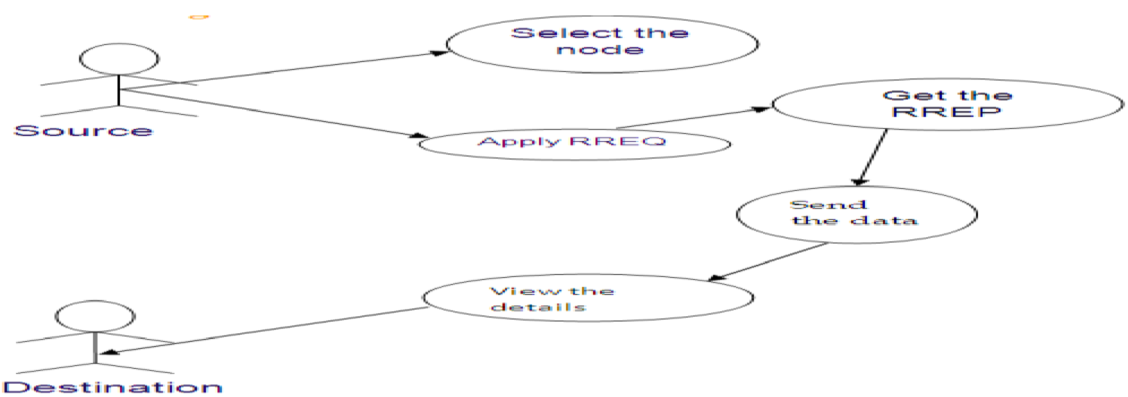


FIG.10: Flow of nodes

Limitations:

Limitations of this system are they work for short ranges mainly on radio communication range so in order to solve this problem in adhoc network distributed routing protocol is implemented for communication between out of range.

4. PROPOSAL

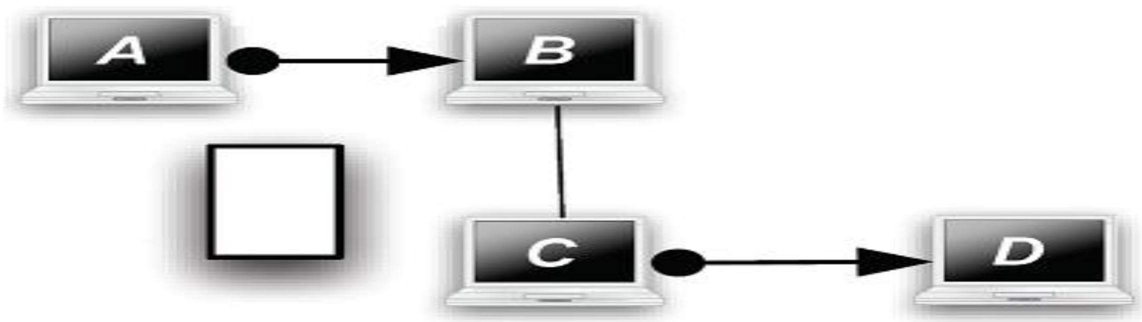
In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

It provides quality of service and improves the performance of Ad Hoc Network packet transmission and reduces delay in packet transmission. Ad hoc networks works don't need any fixed infrastructure like base stations for its operation. In this technology packet transmission and receiving are addressed by nodes. Ad hoc system works on IEEE 802.11 wireless network standards which is not designed for ad hoc networks but it is used for wireless systems so this standards are not accurately suited to for this system.

We have presented a new technique to compute the available bandwidth between two neighbor nodes and by extension along a path. This method combines channel monitoring to estimate each node's mediums occupancy including distant emissions, probabilistic combination of these values to account for synchronization between nodes, estimation of the collision probability between each couple of nodes, and variable overhead's impact estimation. This mechanism only requires one-hop information communication and may be applied without generating a too high additional overhead.

Let's consider that there is a constant bit-rate ongoing flow on the link (C,D). We intend on computing the available bandwidth on the link (A,B). In this case, the evaluations provided by BRuIT, CACP and AAC are identical and are represented in function of the throughput of the flow of the link (C, D) "estimated available bandwidth" .

For all these protocols, the available bandwidth on the link (A,B) corresponds to the available bandwidth value computed by node B (identical to the value computed by node C) and is equal to the capacity of the radio medium minus the bandwidth consumed by the flow on the link (C,D)



3.1 Algorithm

Simple approximation of maximum independent set

Input: A graph *G* defined based on one of the four graph Models.
Output: A maximal independent set *I*.

1: $I \leftarrow \emptyset$.

2: repeat

3: Finds the node, say *v*, with the smallest interference radius *rv*;

4: Adds it to the independent set, i.e., $I \leftarrow I$ _{*v*};

5: Removes this node and all its adjacent nodes from the graph *G*.

6: until *G* is empty

3.2 Module Diagram

1. Packet Creation

In this module we split the Data in to N number of fixed size packet with Maximum Length of 48 Characters.

2. Apply the RREQ and get RREP

The aim of the RREQ is to find a route between the sender and the receiver that meets the Constraints specified by the application level in terms of Bandwidth. When a source node has data to send, it broadcasts a route request (RREQ) to its neighbors. The RREQ packet contains the address of the sender, and the requirements at the application level, the destination address, and a sequence number.

3. Admission Control Mechanism

The Admission Control Mechanism is done in the receiver side. TheAdmission Control Mechanism has the all status of the node so if the nodes want to send RREP or discard the Message, the particular node check the status by using the Admission Control Mechanism.

4. Bandwidth Utilized

After the source nodes send the total message to the Destination Node finally we calculate the end to end delivery of the Bandwidth and Time delay. Processes for Web Based efficiency for IEEE802.11 Based Ad hoc Networks Apply the RREQ to Neighbor to Destination.

Dataflow diagram

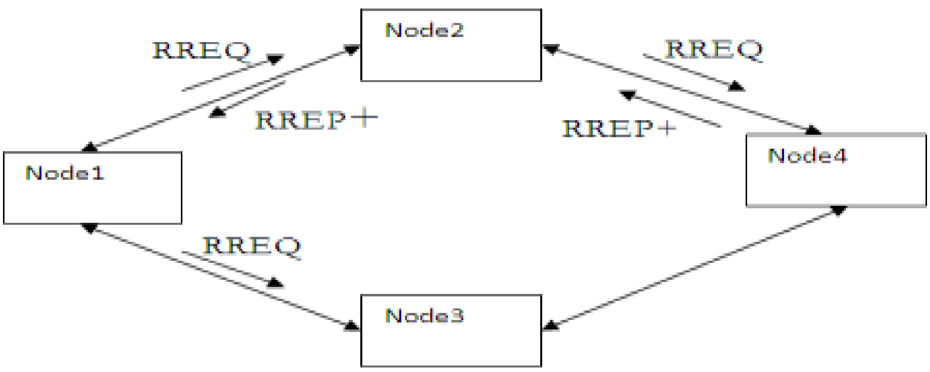


FIG.11: DATA FLOW DAIGRAM

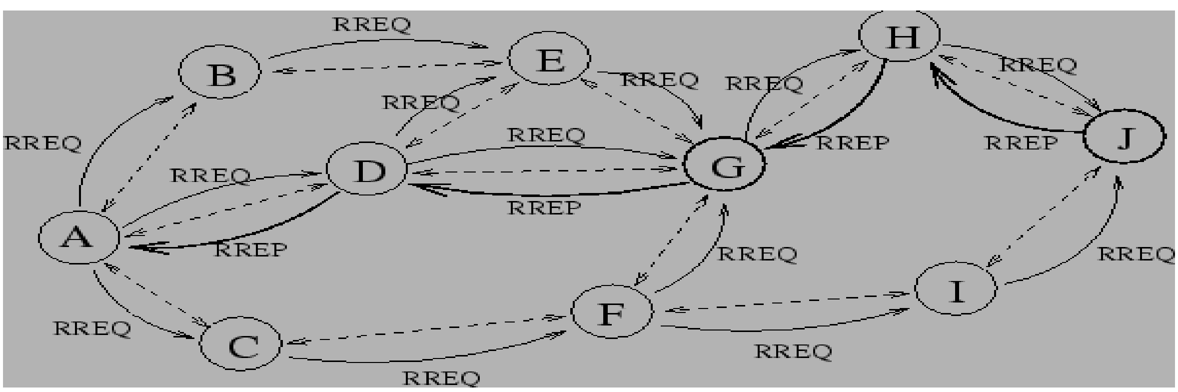


FIG.12: APPLY THE RREQ AND GET RREP

5. SYSTEM SPECIFICATION

System specification is a document that completely describes what the proposed software should do without describing how the software will do it.
It should be

a) Correct
b) Unambiguous
c) Complete
d) Consistent

There are many good definitions of System and Software Requirement Specification that will provide us a good basis upon which we can both define a great specification and help us entifydeficenceis in our past efforts .There is also a lot of great stuff on the web about writing good specification.

We have to keep in mind that the goal is not to create great specifications but to create great products and great software.

It is useful to- Establish the basis for agreement between the customer suppliers on what the software product is to do.

Reduce the development effort. Provide a basis for estimating costs and schedules. Provide a baseline for validation and verification facilitate transfer.It makes it easier to transfer the software product to new users or new serve as a basis for enhancement**.**

6. CONCLUSION

We have presented a new technique to compute the available bandwidth between two neighbor nodes and by extension along a path. This method combines channel monitoring to estimate each node's mediums occupancy including distant emissions, probabilistic combination of these values to account for synchronization between nodes, estimation of the collision probability between each couple of nodes, and variable overhead's impact estimation. This mechanism only requires one-hop information communication and may be applied without generating a too high additional overhead.

This technique has been integrated in AODV for comparison purposes. We show the accuracy of the available bandwidth measurements. These results show that single-hop flows and multi hop flows are admitted more accurately, resulting in a better stability and overall performance. Results are encouraging in fixed networks as well as in mobile networks From our point of view, these scenarios prove that the most difficult point when designing a QoS protocol is not the routing process but the estimation of available resources through the network.

As future works, we plan to focus on two issues. First, in our current evaluation, we make no difference between the bandwidth consumed by QoS flows and the bandwidth consumed by best effort flows. Therefore, it may be possible that a node considers its available bandwidth on a link as almost null whereas the whole bandwidth is consumed by best effort flows. Decreasing the rate of these flows may lead to a higher acceptance rate of QoS flows. Differentiating flow types may also result in a better utilization of the network resources. In parallel, we are investigating the delay metric, as preliminary studies indicate that some parts of the approach described in this may be use do converted to this other important parameter.

ACKNOWLEDGEMENT

I am faithful towards the Almighty who give me courage and help me courage and help me to take right decision and work towards the ultimate aim.

It is my pleasure to express with deep sense of gratitude to **Dr. M. JAYAPRAGASH,** project Guide, Department of Computer Science for his constant guidance, continual encouragement , understanding ; more than all ,continuous support.

I would like to express my gratitude to Prof. **Dr. J SEBASTIAN NIXON, HOD** Department of Computer Science , The Oxford College Of Science , for providing an environment to work in and for his inspiration during the tenure of the course.

In jubilant mood I express ingeniously my whole-hearted thanks to all teaching staff and members working as limbs of our computer science department for their timely encouragements, which prompted the acquirement of the requisite knowledge to finalize my course successfully.

Along I am faithful towards the Almighty who give me courage and health to take right decision and work towards the ultimate aim.

I would like to thank my parents for their endless support and encourage throughout my life. It is indeed a pleasure to thank my friends who persuaded and encouraged me to take up and complete this task me directly or indirectly towards the successful completion of this project, At last but not least, I express my gratitude and appreciation to all those who have helped me.

BIBLIOGRAPHY

[1] Chaudet , C., Chelius G., Lassous I.G., "Bandwidth Estimation for IEEE 802.11-Based Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol.7, Issue 10, 2008

[2] Bob Melander, Mats Bjorkman, Per Gunningberg, a New End-to-End Probing and Analysis Method for Estimating Bandwidth Bottlenecks, 2007

[3] Andreas Johnson, Bob Melander, and Mats Björkman (2010). "diettopp: A first Implementation and evaluation of a simplified bandwidth measurement method". Department of Computer Science and Engineering Mälardalen University, Sweden. International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.1, January 2011

[4] N. Ch. Sriman Narayana Iyengar, (2010) « An Efficient and secure routing protocol for Mobile Adhocnetworks », International Journal of Computer Networks & Communications (IJCNC)

[5] Cheikh Sarr, Claude Chaudet, Guillaume Chelius, and Isabelle Gue´ rin Lassous Bandwidth Estimation for IEEE 802.11-Based Ad Hoc Networks IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 10, OCTOBER 2008

[6] Cheikh Sarr, Claude Chaudet, Guillaume Chelius, Isabelle Guérin Lassous Available Bandwidth Estimation for IEEE 802.11-based Ad Hoc networks June 2007

[7] Bandwidth Estimation for IEEE 802.11-based adhoc networkscheikh Sarr†claudechaudet‡, Guillaume Chelius† and Isabelle Gu´erin Lassous_ IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. X, NO. X, APRIL 2007

[8] Heni KAANICHE1, Fatma LOUATI2 , Mounir FRIKHA3 and Farouk KAMOUNA QOS ROUTING PROTOCOL BASED ONAVAILABLE BANDWIDTH ESTIMATION FORWIRELESS AD HOC NETWORKS International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.1, January 2011 DOI :

[9] C. Sarr, C. Chaudet, G. Chelius, and I.G. Lassous, "A Node-basedavailable Bandwidth Evaluation in IEEE 802.11 Ad Hoc Networks,"Int'l J. Parallel, Emergent and Distributed Systems. 6, 2006.

[10] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," J. Selected Areas in Comm, Mar. 2000.

[11] L. Chen and W. Heinzelman, "qos-Aware Routing Based onbandwidth Estimation for Mobile Ad Hoc Networks," IEEE J. Selected Areas of Comm.

[12] Cheikh Sarr, Claude Chaudet, Guillaume Chelius, Isabelle Guérin Lassous (2005). "A node-Based available bandwidth evaluation in IEEE 802.11 ad hoc Networks". International Journal of Parallel ,Emergent and Distributed Systems.

[13] Dongyan Chen, Daqin Gu and Jinyun Zhang (2004). "Supporting Real-time Traffic with qos in IEEE 802.11e Based Home Networks". MERL – A Mitsubishi Electric Research Laboratory.

[14] Fedoua Didi, Houda Labiod, Guy Pujolle and Mohamed Feham (2009) "Mobility and qos of 802.11and 802.11e Wireless LAN Standards". The International Arab Journal of Information

[15] Andreas Johnsson, Bob Melander, and Mats Björkman (2010). "Diet To pp: A first Implementation and evaluation of a simplified bandwidth measurement method". Department of Computer Science and Engineering Mälardalen University, Sweden.International Journal of Computer Networks & Communications (IJCNC) , January 2011

[16] Anelise Munaretto, Mauro Fonseca (2007). "Routing and quality of service support for Mobile ad hoc networks", Computer Networks Elsevier