Scheduling Data Retrieval for Unsynchronized Channels in Wireless Broadcast Environments

K.Vishal Kumar¹, Mrs.S.Nasrath ²*, Ms. K.Sai Priyanka ³*

¹ Student, Computer Science And Engineering, Gates Institute Of Technology, Andhra Pradesh, India
² Assistant Professor, Computer Science And Engineering, Gates Institute Of Technology, Andhra Pradesh, India
³ Assistant Professor, Computer Science And Engineering, Gates Institute Of Technology, Andhra Pradesh, India

vishalkumar0238@gmail.com
nasrath.shaik8@gmail.com
priyanka.kurnool@gmail.com

Abstract—In the mobile communication areas, wireless data transmission has been an extensively used technique of broadcasting data to users. It is particularly suitable for supplying users public information, such as traffic conditions, stock quotes and weather reports for the reason that of its flexibility and scalability. Usually, there are two classes of broadcast systems: pull based and push-based. In a pull-based system, the clients will formally send requests to the server and in return the server will supply well-timed broadcast based on the requests received. But, In a push-based system, the server will transmit a set of data items to the clients from time to time according to a predetermined schedule; as In both systems, clients have to pay attention to the channels, wait for the requested data items and download them while they reach your destination. This paper proposes a data scheduling method which is capable of solving the LNDR (largest number data retrieval) problem in the unsynchronized broadcast environments. Doing this will reduce the communication overhead and also reduces the congestion problem occurring while transmitting the data.

I. INTRODUCTION

Mobile wireless networks are an appealing and fast growing option to extend or provide means of communication where it is hard or impractical to use a fixed wired network. Mobility reduces installation time and long-term cost savings are some of the wireless networks’ benefits. Wireless mobile networks can be categorized as: Wireless Local Area Networks (WLANs), Wireless Metropolitan Area Networks (WMANs) and Wireless Wide Area Networks (WWANs). This classification is based on network size and geographic span. To add to the classification completeness it is essential to add one more network type, which is the Wireless Personal Area Network (WPAN). Wireless network types could be summarized with the following table:

<table>
<thead>
<tr>
<th>Network Type</th>
<th>Technology Standard</th>
<th>Commercial Name</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPAN</td>
<td>IEEE 802.15</td>
<td>ZigBee, Bluetooth</td>
<td>Room size</td>
</tr>
<tr>
<td>WLAN</td>
<td>IEEE 802.11</td>
<td>Wi-Fi</td>
<td>Building</td>
</tr>
<tr>
<td>WMAN</td>
<td>IEEE 802.16</td>
<td>WiMAX</td>
<td>City size</td>
</tr>
<tr>
<td>WWAN</td>
<td>UMTS,GSM, and IEEE 802.20</td>
<td>MBWA</td>
<td>Earth size</td>
</tr>
</tbody>
</table>

Wireless PAN (WPAN) targets short-range communication of a person or a device forming a piconet. This is a network of users connected in a master slave fashion, where each piconet has one master and several slaves.

Wireless LANs (WLANs) are further classified by the IEEE 802.11 standard into two operational modes: infrastructure-based and ad hoc as depicted in Figure 1. The former type of networks incorporates access points that facilitate wireless connection from and to network users.

![Figure 1: wireless local area networks (a): infrastructure based (b) Ad Hoc based](image)

Mobile Ad hoc Networks (MANETs) are autonomous systems consisting of a set of mobile stations, (called also nodes) that are free to move...
without the need for a wired backbone or a fixed base station. A node is “any device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium”. MANET’s mobile nodes can be arbitrarily located and are free to roam at any given time. Moreover, node mobility can vary from almost stationary to constantly moving nodes. Consequently, network topology and interconnections between nodes can change rapidly and unpredictably. Additionally, there are no dedicated routers: each node in a MANET acts as a router and is responsible for discovering and maintaining routes to other nodes.

Wireless Sensor Networks (WSNs) are an example of MANETs. WSNs are MANETs with some of the following differences: mobility; a sensor networks node is mostly stationary through its life time, whereas a mobile network node, as the name implies, is mostly mobile all the time. Energy, since mobile networks’ nodes are expected to be devices held and operated by humans, it is likely for their batteries to be recharged or replaced; this is much less of an option with sensors’ batteries. Knowing that energy is more of a concern with sensors than with mobile network nodes, caution is needed in designing and developing sensor applications. An aggregation of WSNs would form a mesh network that is more immune to single point failure and nodes’ disabilities.

The IEEE 802.11 (1997) was one of the first standards devoted to facing the challenge of organizing a systematic standardized approach for WLANs. This standard formalizes the physical and MAC layers only as the upper layers (layer 3 and above) of the Open Systems Interconnection (OSI) model are independent of the network architecture.

Wireless MAN (WMAN) basic arrangement comprises one or more base stations, multiple subscriber stations and sometimes a repeater station or router to provide more network connectivity. Examples of WiMAX networks are Mobilin in Saudi Arabia and Urban Wimax in the United Kingdom.

Wireless WAN (WWAN) cellular systems use satellites and divide the network area into hexagonal cells that use multiple low-power transmitters and are served by its base station. Additionally IEEE 802.20 Mobile Broadband Wireless Access (MBWA) has some advantages over WiMAX: it provides full mobility up to 250 km/h which is vehicular speed.

II. RELATED WORK

Mobile ad hoc networks, owing to their quick and economically less demanding deployment, find applications in many areas. Examples of MANET applications are ad hoc wireless networks between mobile laptop devices, military applications, collaborative and distributed computing, emergency operations, inter-vehicle communications and hybrid wireless network architectures. There follows a brief description of some MANET applications.

Military applications: mainly military environments need autonomous and adaptive communication with self-configuring ability. Thus, wireless ad hoc networks are excellent candidates for military networks [2]. The military community is redefining the way wars will be fought in the future, evolving towards a Network-Centric Warfare (NCW) paradigm [3]. Moreover, future tactical networks such as the army modernization Brigade Combat Team (BCT) [4] will depend heavily on the use of MANETs.

Collaborative and distributed computing: the requirement of a temporary communication infrastructure with minimal configuration among a group of people, in a conference, for example, necessitates the formation of an ad hoc wireless network. However, the design, development and deployment of collaborative services in MANET environments raise complex group management issues. Several research efforts are in progress to construct the kind of group management infrastructures required to support collaborative applications in MANETs [5]. All solutions share a common design principle to consider user location as the key grouping criterion: users can collaborate and are assumed to belong to the same group as long as they are co-located.

Emergency operations: ad hoc wireless networks are very useful in emergency operations of search and rescue, crowd control and in areas destroyed by war or natural disasters, such as earthquakes. An example of emergency application is the Smart project [6]: it aims to create a prototype of a mobile telemedicine system including hardware and software that can be rapidly deployed in rural areas or in disaster conditions. Smart project integrates MIPv6 and IEEE 802.11 MANET to provide telemedicine.

Inter-Vehicle Communications: aiming at improved driving comfort and safety, inter-vehicle communication is employed between vehicles in the same area. However, factors such as signal strength fluctuations, high mobility or channel load saturation should be taken into consideration when designing an inter-vehicle protocol. The IEEE 802.11p standard, also referred to as Wireless Access for the Vehicular Environment (WAVE), enhances the original 802.11 standard by the support for Intelligent Transportation Systems (ITS) [7]. Additionally, it is based on the Dedicated Short Range Communication (DSRC) spectrum as it addresses the needs for high node mobility and rapid topological changes. Several organizations are interested in the development and deployment of Vehicular Ad hoc NETworks (VANETs) with regards to both safety and traffic efficiency; Carlink [8], Car-to-car [9] are some examples of currently running VANET projects.
Hybrid wireless networks: one of the major applications in ad hoc wireless networks is in hybrid wireless architecture such as Multi-hop Cellular Networks (MCN) and integrated Cellular Ad hoc Relay (iCAR) networks. MCN combine the reliability and support of fixed base stations of cellular networks with flexibility and multi-hop reliance of ad hoc wireless networks.

III. PROPOSED SCHEDULING MODEL

The main aim of the proposed approach is to solve the scheduling LNDR Problem (congestion) [1] at a particular node. For this the proposed model employs a congestion control strategy based on deleting and transferring the message, as the congested node calculate the storage value of each packet according to the forwarding possibility and Time to Leave (TTL) value of packet, then deletes the packet with the smallest amount of storage value and transfers the packet with the lesser forwarding possibility to neighboring nodes. The nearest nodes calculate the receiving value of the packet according to the forwarding possibility and free buffer capacity of this packet. The congested node transfers the packet to the adjacent node with the highest receiving value. The packet will be deleted when there is no adjacent node to receive it.

3.1 Network Model:

- When congestion occurs, the congested node determines a set of messages for deletion and another set of messages for migration.
- Meanwhile, the neighboring nodes determine whether to receive the transferred message and give a response to the congested node.
- If the neighboring nodes refuse to receive the transferred message, it will be deleted.

3.2 Steps to detect Congested Node & Processing:

Step 1: The congested node measures the storage value of each packet and deletes the packet with the smallest amount of storage value.

Step 2: The congested node transfers the packet with the smallest amount of forwarding probability to its adjacent nodes.

Step 3: The congested node broadcasts transfer request message to its neighboring nodes and gets their receiving values of the message. If there is no response from any neighboring node, go to Step 5.

Step 4: The congested node selects the adjacent node with the maximum receiving value according to the responses and transfers the chosen message to this neighboring node.

Step 5: The congested node deletes this packet.
The figure 3 depicts the packets continuously dropping between the node 8 and node 12 leading that the 12 is incapable of handling the incoming traffic and the figure 4 depicts that the node 12 is detected as congested node.

3.3 Steps for Neighbor Node Analysis:
- The neighboring node judges whether its own buffer space can meet the requirements and calculates the storage value of the transferred message.
- If the storage value of the transferred message is smaller than the minimum storage value in the neighboring node, the process is over.
- Otherwise, the neighboring node will calculate the receiving value of the transferred message and return this value to the congested node.

IV. EXPERIMENTAL EVALUATION

The proposed scheduling technique is tested under various general metrics including:
- Packet Drops
- Error Rate
- Delay Ratio and
- Throughput

The results of the proposed scheme (red) in colour are compared with the traditional BitTorrent (green) in colour System and the Network coding (blue) in colour scheme and are represented.

Figure 5 depicts the packet drops for all the three schemes and the result clearly show that the proposed scheme has less number of packet drops compared to the existing two schemes.

- The Transmission Control Protocol (TCP) detects packet loss and performs retransmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and reduces throughput of the connection.
- In streaming media and online game applications, packet loss can affect the user experience.

The next metric to measure is the Error Rate and is depicted in the figure 6 where the rate of error is low for the proposed scheme.

- Error Rate

- In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors.

- The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage.

- The bit error probability \( p_e \) is the expectation value of the bit error ratio. The bit error ratio can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.
The delay ratio plays an important role in any network transmission where the delay indicates the time taken to deliver the packets. The proposed system outperforms both the traditional systems and the results can be observed in Figure 7.

*Figure 7: Delay Ratio*

- Delay Ratio
- **Network performance** refers to measures of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

- Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

- ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The final and most crucial metric is the throughput. This defines the efficiency of the complete network; the higher the throughput then the performance will be greater.

- **Throughput**
- This article is about the amount of processed data in communication networks. For hard disk data in particular, see Throughput (disk drive). For business management, see Throughput (business).
- In general terms, throughput is the rate of production or the rate at which something can be processed.
- When used in the context of communication networks, such as Ethernet or packet radio, throughput or **network throughput** is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s orpps) or data packets per time slot.
- The **system throughput** or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. Throughput is essentially synonymous to digital bandwidth consumption; it can be analyzed mathematically by applying the queuing theory, where the load in packets per time unit is denoted as the arrival rate (\(\lambda\)), and the throughput, in packets per time unit, is denoted as the departure rate (\(\mu\)).
- The throughput of a communication system may be affected by various factors, including the limitations of underlying analog physical medium, available processing power of the system components, and end-user behavior. When various protocol overheads are taken into account, useful rate of the transferred data can be significantly lower than the maximum achievable throughput; the useful part is usually referred to as good put.

Observing all the results depicted above the proposed scheme clearly outperforms the traditional file sharing systems.

V. CONCLUSION
This paper addressed an issue regarding the problems occurring in Mobile Ad Hoc Networks which is congestion. Basically congestion occurs if multiple requests are carried out at the same time. As the network is un-synchronized then the occurrence of congestion will be high. To avoid that congestion and to design an efficient scheduling routing this paper used congestion detection and elimination algorithm. The results also demonstrated that the proposed model performed well in every aspect.

REFERENCES


