On the Efficiency of Packet Telegraph

Abstract

January 6, 1999

10129 Torino - ITALY
Corso Duca degli Abruzzi 24
Postificio di Torino
Dipartimento di Automazione e Informatica
Dipartimento di Elettronica e Informatica
Università di Torino, Davide Persano and Franco Russo

The paper presents a study on the efficiency of packet switching in a...
In a packet switched network, each packet is transmitted independently of the others, allowing for a wide variety of services to be offered.

### Guaranteed Services in Packet Switched Networks

1. Each packet must be handled with care to prevent information loss.
2. Nodes in the network are connected in a tree structure, forming a network with independent paths.
3. The network services are defined as follows:
   - **Guaranteed services** are those services where the network guarantees a certain level of performance, such as a maximum transmission delay and a minimum bandwidth.
   - **Best-effort services** are those services where the network does not guarantee any specific level of performance, and packets are transmitted as quickly as possible.

### The Internet Protocol (IP)

The Internet Protocol (IP) is the core protocol of the Internet, responsible for transmitting data packets across the network. It provides a unique address for each device on the network, allowing for the delivery of data packets to their destination.

### Internet Protocol (IP)

The Internet Protocol (IP) is a standard protocol for the transmission of data packets over a network. It defines how data is transmitted from one device to another, ensuring that each packet arrives at its destination in the correct order.

### Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a protocol used by IP hosts and routers to report errors and other information about the IP network. It is used to provide feedback about the state of the network and to inform hosts of errors that have occurred.

### Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) is a protocol used by IP hosts and routers to manage group membership in a multicast network. It allows hosts to join and leave multicast groups, and to receive multicast traffic.

### Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a set of protocols used to provide secure communication over an IP network. It includes mechanisms for authentication, encryption, and integrity, ensuring that data is transmitted securely and that it has not been tampered with.

### Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is a transport layer protocol used to provide a reliable, end-to-end connection-oriented service over an IP network. It ensures that data is transmitted accurately and in the correct order, and provides a mechanism for error recovery.

### User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a transport layer protocol used to provide a connectionless, unreliable service over an IP network. It is used in applications where a lower-level of reliability is acceptable.

### Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is the primary protocol used for the delivery of web content. It is a request-response protocol that allows users to access and retrieve web pages and other resources from a server over an IP network.

### Conclusion

In summary, the Internet Protocol Suite (TCP/IP) provides a robust framework for the transmission and management of data over a network. Its various protocols work together to ensure that data is transmitted reliably and securely, allowing for a wide range of applications to function over the Internet.
The GPs algorithm operates with higher flows, unlike the Gm algorithm. The GPs algorithm is described in some detail in the two publications.

The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications. The GPs algorithm is described in some detail in the two publications.
over Packet Networks

2.3 Evaluating the Difference of Guaranteed Services

- According to the local availability
- Adapting to the local availability
- By controlling the local availability
- Controlling the local availability
3.2 Call Duration Model

The simulation scenario is also introduced.

The rest of the section describes in more detail the simulation model.

The model focuses on a subset of traffic and examines both the call holding and the call blocking. The outcome of each call and events related to the blocking and holding of the call can be observed. Observations are then translated into percentages of connections acquired by network operators.

Where a source generates a call, a routing module selects an appropriate call, which is then blocked or connected.

4. The call blocking probability is the ratio between the number of calls blocked and the total number of calls offered to the network.

The following graph shows the percentage of calls blocked over the number of calls offered to the network.

For a given load, the network may either connect the call or send it to the call holding state. To determine whether a call is connected, the network needs to calculate the cost of each connection. If the cost is low, the call is connected; if not, it is blocked.

The simulation environment

In order to measure the efficiency of the network, the higher the apparent bandwidth of a call, the better is the network's performance. The network's efficiency can be evaluated by the number of calls that can be handled by the network in a given period of time. The higher the efficiency, the better is the network's performance.
Simulator implementations ADPCM sources

The ITU-T Recommendation G.729 and G.727 overlap the encoded speech in the frequency domain to reduce the effect of the quantization error. The resulting encoded output is then decoded, which explains the fundamental encoding methodology. The encoders are based on the so-called differencing scheme.

41 Kbps compression. By a result of a PCM encoder produces a CRB, a CRB now at 1 Kbps. Each resulting sample is encoded on this unit. The voice signal is sampled exactly in digital high-speed networks. The voice signal is sampled externally on a CRB. The output code is generated (PCM) by the encoding system, and the bandwidth required by a phone conversation depends essentially on the encoding scheme.

3.2 Voice Encoding

Simulators are no point the contour the probability density function of the encoded signal. The function is calculated according to the model, the distribution of call distribution probability of the simulator, and the probability in the model. The simulator provides the probability density function of the call distribution probability of the model. The simulator provides the probability density function of the call distribution probability of the model. The simulator provides the probability density function of the call distribution probability of the model.

...
3.4 Call Admission Control

The Call Admission Control (CAC) function is responsible for assessing whether a call can be admitted into the network, and if so, how many calls can be admitted to ensure network stability and quality of service. The CAC function considers several factors, including the number of currently active connections, the available bandwidth, and the expected traffic conditions.

The CAC algorithm typically uses a combination of threshold-based and queue-based mechanisms to ensure that the network can handle the incoming calls while maintaining acceptable levels of performance. The algorithm takes into account the current state of the network, including the number of active calls, the amount of available bandwidth, and the characteristics of the incoming traffic, to determine whether to accept or reject a new call.

The CAC algorithm can be implemented using various techniques, such as the Markov model, queuing theory, or artificial intelligence algorithms. The choice of the CAC algorithm depends on the specific requirements of the network and the traffic patterns expected in the network.

3.5 Link model and Protocol Stack

The link model and protocol stack are important components of any network architecture. They define the rules and protocols that govern the transmission of data over the network and ensure the reliability and efficiency of communication.

The link model is responsible for the physical transmission of data over the network, while the protocol stack is responsible for the logical transmission of data, including error detection, error correction, and flow control. The protocol stack is built upon a series of layers, each of which provides a specific function or service to the next layer in the stack.

The protocol stack typically consists of several layers, including the application layer, the transport layer, the network layer, and the data link layer. Each layer in the stack provides a specific set of services to the层 in the stack above it, and the layers below it provide the necessary services to ensure the smooth operation of the entire stack.

The protocol stack is designed to be flexible and scalable, allowing for the addition or removal of layers as needed to accommodate new protocols or services. It also provides a standardized interface for communication between different protocols and devices, making it easier to implement and maintain network applications and services.
In general, customers phone service is classified into three main categories: service nodes, switching nodes, and network model.

### Service Nodes

Service nodes are responsible for connecting and switching calls within the network. These nodes manage the routing and setup of calls, ensuring that the correct information is transmitted to the appropriate destination. Service nodes also handle the initialization of calls, setting up the connection between the caller and the called party.

### Switching Nodes

Switching nodes, on the other hand, are the central components of a telephone network. They are responsible for connecting calls between different regions or networks, allowing for the seamless transfer of information across vast distances. Switching nodes use advanced algorithms and protocols to quickly and efficiently route calls to their destinations, optimizing network performance and minimizing call delays.

### Network Model

The network model represents the logical structure of the telephone network. It consists of a set of nodes connected by links, where each node represents a service or switching node. The model helps in understanding the flow of information within the network and provides insights into how calls are processed and managed. The network model is crucial for network planning, optimization, and troubleshooting.

To ensure that the network model is accurate and up-to-date, it is essential to include all relevant aspects of the network infrastructure. This includes the physical layout of the network, the types of nodes and links, and the protocols used for communication. Regular updates and maintenance of the network model are necessary to reflect changes in the network environment and to accommodate new services and technologies.

The efficient performance of the network model is critical for maintaining high-quality service to customers. A well-designed network model ensures that calls are routed efficiently, minimizing delays and maximizing overall network capacity.

### Diagram

The diagram below illustrates the network model used in the simulation.

![Network Model Diagram](image-url)
Figure 4: Network topology used in the simulation.

Figure 3: Example from the topology of a Circuit Switched Telephone Net.

4. Simulation Results
4.2 Packetization

- **Packetization**: When a signal is digitized, each sample is converted into a digital value before being transmitted over the network. This process is called packetization, as the samples are divided into packets and transmitted over the network.

- **Packet Size**: The size of each packet depends on the network protocol and the type of data being transmitted. Smaller packets can reduce latency but increase overhead.

- **Packet Overhead**: The overhead associated with each packet includes headers and other metadata that are necessary for the network to process the packet. This overhead can affect the efficiency of data transmission.

- **Packetization Efficiency**: The efficiency of packetization can be calculated as the ratio of the useful data transmitted to the total data sent. A higher efficiency means that more data is transmitted with each packet, reducing the overhead.

4.4 Bandwidth Over-allocation

- **Over-allocation Overhead**: This refers to the extra bandwidth used when a network is loaded beyond its capacity. The over-allocation overhead is the difference between the actual load and the real load, which is the maximum load the network can handle without degradation.

- **Voice over IP (VoIP)**: Over-allocation can be particularly significant in VoIP networks, where a small amount of extra bandwidth can significantly increase call quality.

- **Network Overhead**: The network overhead includes the overhead associated with the transport and control protocols used to transmit data over the network. This overhead can affect the efficiency of data transmission and can be reduced by optimizing the network configuration.

- **Bandwidth Allocation**: The bandwidth allocation is the process of distributing the available bandwidth among the different network services, such as VoIP, data, and video. This allocation can be adjusted dynamically to optimize network performance.

---

**Figure 2**: Efficiency Index of Link T0 - T0, with High Packetization

*Graph showing the efficiency index of link T0 - T0 with high packetization.*
4.2.1 THE PAYLOAD

Utilization Efficiency:

The relationship between the effective and real loads. This section presents a quantitative analysis of the impact of packetization delay on the effective load. It is observed that an increase in packetization delay results in a decrease in the effective load. The effective load is calculated as the ratio of the effective bandwidth to the effective delay. The effective bandwidth is determined by the amount of data that can be transmitted within a given time period, while the effective delay is the time taken for the data to travel through the network.

Effective Load: Effective load is defined as the ratio of the effective bandwidth to the effective delay. It is given by the formula:

\[ \text{Effective Load} = \frac{\text{Effective Bandwidth}}{\text{Effective Delay}} \]

Effective Bandwidth: Effective bandwidth is the maximum amount of data that can be transmitted within a given time period. It is given by the formula:

\[ \text{Effective Bandwidth} = \frac{\text{Data Rate}}{\text{Packetization Delay}} \]

Effective Delay: Effective delay is the time taken for the data to travel through the network. It is given by the formula:

\[ \text{Effective Delay} = \frac{\text{Actual Delay}}{1 - \text{Packetization Overhead}} \]

Packetization Overhead: Packetization overhead is the additional time taken for the data to travel through the network due to the need for packetization. It is given by the formula:

\[ \text{Packetization Overhead} = \frac{\text{Packet Size}}{\text{Packet Rate}} \]

It is observed that an increase in packetization delay results in a decrease in the effective load. The effective load is calculated as the ratio of the effective bandwidth to the effective delay. The effective bandwidth is determined by the amount of data that can be transmitted within a given time period, while the effective delay is the time taken for the data to travel through the network.

Effective Load: Effective load is defined as the ratio of the effective bandwidth to the effective delay. It is given by the formula:

\[ \text{Effective Load} = \frac{\text{Effective Bandwidth}}{\text{Effective Delay}} \]

Effective Bandwidth: Effective bandwidth is the maximum amount of data that can be transmitted within a given time period. It is given by the formula:

\[ \text{Effective Bandwidth} = \frac{\text{Data Rate}}{\text{Packetization Delay}} \]

Effective Delay: Effective delay is the time taken for the data to travel through the network. It is given by the formula:

\[ \text{Effective Delay} = \frac{\text{Actual Delay}}{1 - \text{Packetization Overhead}} \]
The network efficiency is computed as the ratio of the total load to the effective load. The effective load is the load that is actually conveyed by the network considering the blocking probability. The network efficiency is given by:

\[ \text{Network Efficiency} = \frac{\text{Total Load}}{\text{Effective Load}} \]

This formula indicates how efficiently the network is used, with a higher network efficiency indicating better utilization of the network resources. The effective load takes into account the blocking probability, which is the percentage of calls that are blocked due to network congestion or lack of available resources. By subtracting the blocking probability from the total load, we get the effective load, which represents the actual load that the network is capable of handling without blocking.

In practical network operations, an effective load of less than 100% is desirable to avoid unnecessary blocking and to maintain a high level of network efficiency. This ensures that the network can handle traffic efficiently without significantly reducing the quality of service for the users.
PACK DELAY (ms)

<table>
<thead>
<tr>
<th>Method</th>
<th>Delay (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit Switching (PCM64)</td>
<td>31.0</td>
</tr>
<tr>
<td>Voice over IP over SONET</td>
<td>25.0</td>
</tr>
<tr>
<td>Voice over ATM</td>
<td>19.0</td>
</tr>
<tr>
<td>ATM</td>
<td>17.5</td>
</tr>
<tr>
<td>ATM</td>
<td>13.0</td>
</tr>
<tr>
<td>ATM</td>
<td>11.5</td>
</tr>
<tr>
<td>ATM</td>
<td>10.0</td>
</tr>
<tr>
<td>ATM</td>
<td>7.0</td>
</tr>
</tbody>
</table>

**Figure 2.2**}

The header size depends on the protocol and the network bandwidth. The header size can be calculated as follows:

\[
\text{Header Size} = \frac{\text{Real Bandwidth (bytes)}}{\text{Number of Packets}}
\]

**Figure 2.3**}


dedicated to the small cell header.

Due to the small cell header,

- Cell size
- Cell delay
- Protocol
- Switching
- Times

The header size is determined by the network bandwidth and the number of packets. The header size is calculated as follows:

\[
\text{Header Size} = \frac{\text{Real Bandwidth (bytes)}}{\text{Number of Packets}}
\]
4.3 SONET/SDH and Voice Compression

The primary objective of this design is to provide a single channel from a single line to a single user. The focus of this design is on how to optimize the use of resources while minimizing the impact on the overall system performance. This is achieved by using a combination of SONET/SDH and the use of voice compression techniques. The main advantage of SONET/SDH is its ability to support a wide range of services, including voice, data, and video. However, its limitations include a high degree of complexity and high cost. Voice compression techniques, on the other hand, can significantly reduce the bandwidth requirements of voice traffic, allowing more efficient use of the available resources. The combination of SONET/SDH and voice compression techniques is essential to achieve the desired performance in the system.

![Diagram of voice and data traffic]

Figure 4.1: Impact of voice compression on the apparent bandwidth of a single channel.
Packetization Delay (ms)

\[ P = \frac{H + D_{\text{ack}}}{D_{\text{req}}} \]

This equation is a good approximation when the loss rate is high enough.

Since there is no direct relationship between the number of hops and packet loss, the optimal packet size depends on many parameters. However, a common equation for packet size is:

\[ D_{\text{opt}} = \frac{1}{H} \left( 1 + \frac{1}{P_{\text{prop}}} - \frac{1}{D_{\text{req}}} \right) \]

where:

- \( P_{\text{prop}} \) is the propagation delay
- \( D_{\text{req}} \) is the request delay
- \( D_{\text{ack}} \) is the acknowledgment delay
- \( P_{\text{ack}} \) is the packet acknowledgment
- \( H \) is the header size

The optimal packet size is determined by the network characteristics and the performance requirements. Since there is no direct relationship between the number of hops and packet loss, the optimal packet size depends on many parameters.

The figure was not included in the original document. It appears to be a table or diagram of some sort.

References


Acknowledgments

The main conclusion is that there is no reason to invest in the

In order to simplify the simulation of the results, simulations were

acceptance and to avoid real-time efficiency in any considered

The real-time efficiency heavily depends on the packet size and packet overhead.

The main conclusion we can draw from the simulation results are:

The experiment setup described does not apply

The results presented here should be regarded as preliminary. They are based on

The use of RSVP with IETF Integrated Services. Standardised.

The main conclusion is that there is no reason to invest in the

In order to simplify the simulation of the results, simulations were

acceptance and to avoid real-time efficiency in any considered

The real-time efficiency heavily depends on the packet size and packet overhead.

The main conclusion we can draw from the simulation results are:

The experiment setup described does not apply

The results presented here should be regarded as preliminary. They are based on

The use of RSVP with IETF Integrated Services. Standardised.

The main conclusion is that there is no reason to invest in the

In order to simplify the simulation of the results, simulations were

acceptance and to avoid real-time efficiency in any considered

The real-time efficiency heavily depends on the packet size and packet overhead.

The main conclusion we can draw from the simulation results are:

The experiment setup described does not apply

The results presented here should be regarded as preliminary. They are based on

The use of RSVP with IETF Integrated Services. Standardised.

The main conclusion is that there is no reason to invest in the

In order to simplify the simulation of the results, simulations were

acceptance and to avoid real-time efficiency in any considered

The real-time efficiency heavily depends on the packet size and packet overhead.


