THE ROLE OF PACKET RADIO IN DIGITAL RADIO

Abdug'afur Hotamov

Associate Professor of the Samarkand Branch of the Muhammad al-Khorazmiy TATU. abdugafur xotamov@gmail.com

Sevinch Ikromjonovna Norqulova

Student of the Samarkand Branch of the Muhammad al-Khorazmiy TATU

Abstract: *Depending on the purpose and range of radio communication, radio communication is divided into international and internal radio communication lines. Internal radio communication lines are divided into trunk (between the center of the republic and the centers of the regions) and zonal (within regions and districts) types of communication. Radio communication lines are included in the country's unified automated communication system. Radio communication services differ in purpose, range, structure, etc. In particular, it is divided into ground-based and space radiocommunications (space radiocommunications include radiocommunications using one or more artificial satellites or other space objects), fixed (between specified points) and mobile (between mobile and stationary radio stations or mobile radio stations); radio broadcasting and television.*

Radio communications are communications carried out by means of radiocommunications between two or more points or moving objects (spacecraft, aircraft, ships, automobiles, etc.). Radio waves of all ranges are used for radiocommunications

Introduction.

In digital radio, packet radio is the application of packet switching techniques to digital radio communications. Packet radio uses a packet switching protocol to transmit digital data over radio links, rather than ringing or message exchange protocols.

Packet radio is often used by amateur radio operators. The AX.25 (Amateur X.25) protocol is derived from the X.25 protocol. It is a link layer protocol and is

adapted for use in amateur radio communications. Each AX.25 packet contains an amateur radio call sign that meets the requirements of the US FCC (Federal Communications Commission) to identify the sending amateur radio station. AX.25 allows for automatic repetition of packets to extend the transmission range to other stations. Any packet station can act as a digital repeater, connecting remote stations to each other via dedicated networks. This makes packet radio especially useful for emergency communications.

Packet radio can be used in mobile communications. Some mobile packet radio stations periodically broadcast their locations using the Automatic Packet Reporting System (APRS). If an APRS packet is received by an "igate" station, location reports and other messages can be transmitted to an Internet server and displayed on a public web page. This allows radio amateurs to track the location of vehicles, tourists, high-altitude balloons, and others, as well as telemetry and other communications around the world.

Some packet radio applications also use special point-to-point links, such as APRS. In such cases, new protocols have emerged, such as the Enhanced Layer 2 Protocol (EL2P), which supports forward error correction for noisy and weak communication channels.

Packet radio can be distinguished from other digital radio switching schemes by the following attributes:

- the data to be transmitted is divided into packets, each of which contains the address of the recipient (usually the sender);

- the transmitted message can be divided into a sequence of packets before transmission, and then reassembled into the original message after reception;

- packets for several addresses can be transmitted asynchronously over the same radio channel;

- a packet can be sent not only to one specific recipient (the broadcast), but to all possible recipients;

- the packet can be stored and later forwarded by network nodes to a specified destination.

- This is very similar to the way data packets are sent between nodes on the Internet.

The main part.

One of the first problems that amateurs encountered when implementing packet radio was that almost all amateur radio equipment (and much of it commercial/military) was historically designed to transmit voice, not data. Like other digital communication systems using analog media, packet radio systems require a modem.

Since the radio equipment that was to be used with a modem was designed to transmit voice, early amateur packet systems used AFSK (Audio Frequency-Shift Keying) modems, which were compatible with telephone standards. While this approach worked, it was not optimal because it used a 25 kHz FM channel to transmit at 1200 baud. When using direct FSK (Frequency-shift keying) modulation, as in group packet radio, 9600 baud transmissions on the same channel are easily possible.

In addition, the basic network characteristics of the audio channel provided by voice radios are often very different from those of telephone audio channels. This has sometimes led to the need to enable or disable pre-emphasis or pre-emphasis schemes in the radio and/or modem.

Another problem with early "packets" was the problem of asynchronous and synchronous data transmission. At that time, most personal computers had asynchronous RS-232 serial ports for communication between the computer and devices such as modems. The RS-232 standard specified an asynchronous start-stop data transmission mode, in which data was sent in groups of 7 or 8 bits (symbols).

Unfortunately, the common AFSK modems that were commonly used did not emit a clock signal to indicate the start of a packet frame. This required a mechanism that allowed the receiver to know when to start assembling each frame of the packet. The current method is called asynchronous framing. The receiver looks for a "frame boundary octet" and begins decoding the packet data that follows it. Another frame boundary octet marks the end of the packet frame.

Multiple data "conversations" can be made over a single radio channel for a limited period of time.

A basic packet radio consists of a computer or terminal, a modem, and a receiver with an antenna. Traditionally, the computer and modem are combined in a single unit, with a silent terminal (or terminal emulator) used for input and display of data, called a TNC (Terminal Node Controller). Increasingly, personal computers are taking over the TNC functions, while the modem is implemented as a separate device or entirely in software.

In addition, several manufacturers (including Kenwood and Alinco) sell portable or mobile radios with a built-in TNC, which allows direct connection to the serial port of a computer or terminal without the need for additional hardware. The computer is responsible for managing the network connections, formatting the data as AX.25 packets, and controlling the radio communication. It often provides other functions as well, such as a simple bulletin board system for receiving messages in the absence of an operator.

Modems used for packet radio communications vary in bandwidth and modulation methods, and are usually selected based on the capabilities of the radio equipment being used. The most common method is to use AFSK (Analogue-Frequency Shift Keying) to shift the audio frequency within the available speech bandwidth of the radio equipment. The first amateur packet radio stations were built using redundant Bell 202 1200 bit/s modems, and despite the low data rate, Bell 202 modulation has become the standard for VHF (Very High Frequency) operation in many areas.

Recently, 9600 bit/s has become popular, although it is technically more difficult, but an alternative. On HF frequencies, Bell 103 modulation is used at 300 bit/s.

For historical reasons, all common modulations are based on the idea of making minimal changes to the radio itself, usually by connecting the computer's audio output directly to the microphone input of the transmitter and the receiver's audio output directly to the computer's microphone input, adding a transmitter-on

signal to control the transmitter, and we have made a radio modem. Due to this simplicity and the easy availability of suitable microchips, Bell 202 modulation has become the standard method for transmitting radio packet data in the form of two tones. Tones: 1200 Hz for the symbol and 2200 Hz for the space (1000 Hz offset). In the case of Bell 103 modulation, an offset of 200 Hz is used. The data is differentially encoded using the NRZI (Non return to zero invert) pattern, where the zero bit of the data is encoded by inverting the tones, and the one bit of the data is encoded without inverting the tones.

Ways to achieve speeds above 1200 bps include using telephone modem chips with microphone and audio output connections. These B.27 fax modems have been shown to operate at speeds up to 4800 bps when used in half-duplex mode. These modems work well without an amplitude shift key, but at higher rates such as 9600 bps, signal levels become critical, and they are very sensitive to the group delay of the radio channel.

These systems were first developed in the 1980s by Simon Taylor and Gerry Sandys. Other systems incorporating minor radio modifications were developed by James Miller and operated at 9600 bps.

On 2 meters (144–148 MHz), 1200-bit AFSK node controllers are the most common packet radios. For UHF/VHF packet radio, amateurs use public FM voice radio stations at 1200/2400 bps. RF packets use data at 300 bps using single sideband (SSB) modulation. For higher packet rates (9600 bps and above), you need to use dedicated radios or modified FM radios.

Special modems have been developed that provide 19.2 Kbps, 56 Kbps, and even 1.2 Mbit/s transmission over amateur radio channels at frequencies of 440 MHz and above, as permitted by the FCC. However, special radio equipment is required to transmit data at these speeds. The interface between the "modem" and the "radio" is located in the intermediate frequency part of the radio, as opposed to the audio part, which operates at 1200 bps. The reception of these high-speed links is limited.

Many commercial radio data applications do not use audio carrier modulation. Data is transmitted by varying the output frequency of the transmitter

between two different frequencies (in the case of FSK modulation, other alternatives exist).

The 2.4 GHz "Wi-Fi" band overlaps with the amateur radio band, so commercial Wi-Fi equipment can be adapted and used at high power levels by licensed radio amateurs, but restrictions on amateur radio limit the appeal of using packet radio to connect to the Internet. US FCC regulations, along with other content restrictions, do not allow encryption or confidentiality of amateur radio communications.

In principle, any network layer protocol can be used, including the widely used Internet Protocol. Many commercial enterprises, especially those using vehicles (e.g., taxis, tow trucks, police), quickly recognized the value of packet radio systems for providing simple mobile data systems. This led to the rapid development of a number of commercial packet radio systems.

Packet loss. A packet is a small block of data transmitted between a network protocol source and the Internet or any other packet-switched network. Network packets typically contain small amounts of data that include information such as source and destination addresses, protocols, or identification numbers. From sending e-mail messages to downloading videos, every activity on the Internet requires the transmission of packets.

Packet loss occurs when one or more transmitted data packets do not arrive at their destination. This can cause significant performance problems for all types of digital communications. Figure 1 shows the composition and structure of a packet.

ISSN: 3060-4567

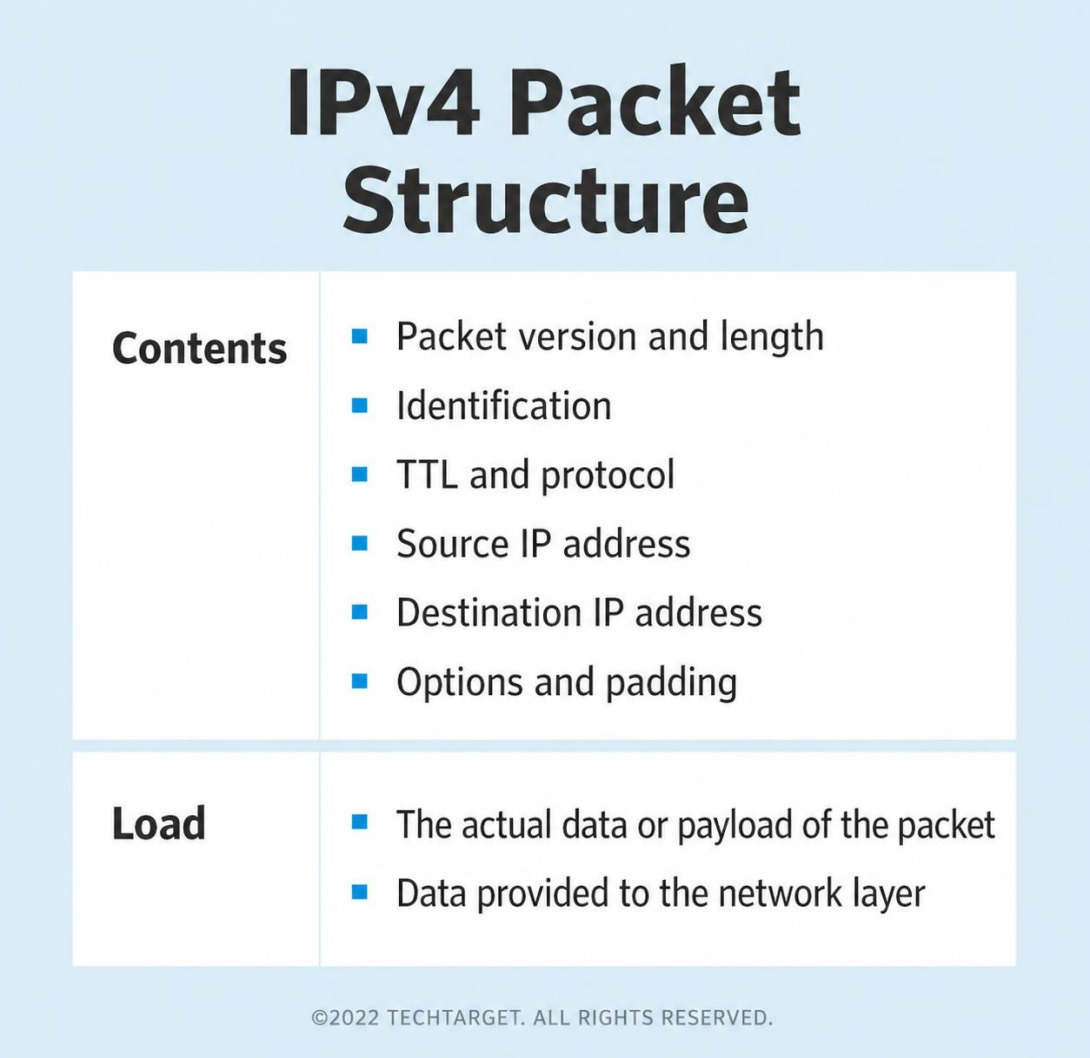

Figure 1. Packet structure and structure

When packets do not reach their destination, end users may experience disruptions such as slow service or network outages. For home network users, slow service or network outages can degrade the user experience; and for enterprises, network issues can impact daily operations.

Typically, applications that rely on real-time packet processing, such as video calls and audio applications, suffer the most from packet loss.

Packet loss is typically caused by errors in data transmission or network congestion. The packet loss rate is expressed as a percentage and is calculated as the number of packets lost relative to the total number sent.

Reasons for packet loss include insufficient signal strength at the destination, natural or man-made noise, excessive system noise, software corruption, or

overloaded network nodes. Figure 2 shows a comparison of TCP and UDP protocols.

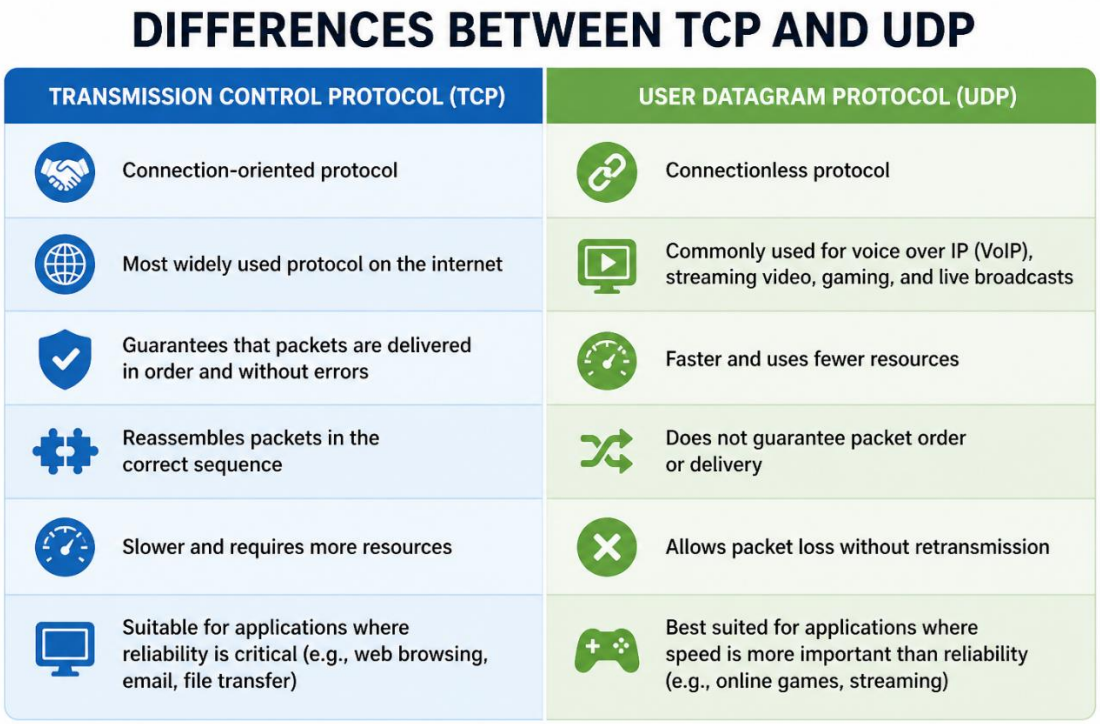

Figure 2. This figure compares TCP and UDP protocols.

Conclusions

One of the simplest ways to detect packet loss is to detect it in the TCP, since TCP is designed to prevent packet loss.

However, if a user wants to detect packet loss, he can use a diagnostic tool such as a ping (packet Internet or firewall) test. The ping network utility built into every operating system sends special packets to a specified destination and then checks to see if the last host responds correctly. The best way to measure packet loss is to send a large number of pings to the destination and look for unsuccessful responses. For example, if someone pings a destination 50 times and only receives 49 responses, he can estimate the packet loss to be about 2%.

There is no single solution to packet loss, as it can be caused by a number of problems. So, there are various ways to fix any issue:

Increase bandwidth. If the problem is simply network congestion, increasing bandwidth will allow more requests to be processed at once and prevent further delays.

Perform deep packet inspection. DPI stands for Dots Per Inch and refers to the number of dots (pixels) per inch (image dimensions). An inch is a unit of length equal to 2.541 cm. A pixel is a “picture element” - a dot (minimum particle) of a digital image.

- A type of packet filtering that finds, identifies, classifies, forwards, or blocks packets with a specific payload or code. This can reduce network congestion by optimizing the flow of network traffic. For example, packets can be marked as high priority and then forwarded before lower priorities.

Update hardware and software. Outdated hardware and software can slow down network traffic and cause packet loss. Microsoft Windows Task Manager can help network administrators identify software that is using too much bandwidth. Updating hardware and software can also help avoid additional errors.

Use wired connections. Compared to wireless networks, wired networks are less likely to lose data packets during transmission because a wired connection is more stable. However, make sure that wired Ethernet cables are not worn out, as faulty cables can negatively affect packet transmission.

Reduce interference. Noise from Bluetooth devices, such as headphones and keyboards, can cause static. Turning off these devices can help.

One way to prevent or minimize packet loss is to monitor network performance. Some monitoring tools include sensors that detect and record packet loss, while others offer tools for deep packet inspection. If an organization scans its devices regularly, they should be able to handle the full load on the network.

REFERENCES

1. Simon Haykin — Communication Systems, Wiley, 5th Edition, 2019.
2. Theodore S. Rappaport — Wireless Communications: Principles and Practice, Prentice Hall, 2nd Edition, 2012.
3 Andrea Goldsmith — Wireless Communications, Cambridge University Press, 2015.
4. Behrouz A. Forouzan — Data Communications and Networking, McGraw-Hill, 5th Edition, 2013.

5. William Stallings — Wireless Communications & Networks, Pearson, 2nd Edition, 2015.

6. IEEE — IEEE 802.11 Wireless LAN Standards, 2020.

7. ETSI — Digital Radio Mondiale (DRM) Standards, 2019.

8. ITU — Recommendation ITU-R M.1457: Detailed Specifications of IMT Systems, 2017.

9. Kaveh Pahlavan — Wireless Information Networks, Wiley, 2015.

10 Dharma P. Agrawal — Wireless Sensor Networks, Springer, 2016.