IQRA NATIONAL UNIVERSITY, PESHAWAR, PAKISTAN

NETWORKS MANAGEMENT

Program: MSCS/PhDCS **FINAL-TERM EXAM** **Semester: Spring 2020**

Maximum Marks: 50 **Time Allowed: 6 Hours**

Note : ***Write down the complete statements of Q1 otherwise just answers will lead to zero marks.***

The paper should be submitted in pdf form and plagiarism will be checked; ***2 students with the same plagiarism report and answers will lead to zero marks to both.***

Cc: ***to Vice Chancellor***

Controller of Examination

Head of Department

Q1. Select the correct answer of the given ones. (10)

1) Interactive transmission of data independent of a time sharing system may be best suited to
   (a) simplex lines (b) half-duplex lines (c) full-duplex lines (d) biflex lines
2) The loss in the signal power as of an Electromagnetic signal is called
   (a) attenuation (b) propagation (c) scattering (d) interruption
3) Early detection of packet losses improves ____________ acknowledgment performance.
   (a) odd (b) even (c) positive (d) negative
4) Additional signal introduced in the desired signal in producing hypes is called
   (a) fading (b) noise
   (c) scattering (d) dispersion
5) Token is a ________________ that rotates around the ring.
6) Ring may have up to ____________ (802.5) or ____________ (IBM) nodes.
7) FDDI can support a maximum of ____________ stations.
8) Error-correcting codes are _________________ enough to handle all errors.
9) ACK is a small ___________________ confirming reception of an earlier frame
10) Electronics are ________________ as compared to optics

Q2: Distinguish between error correction and error detection. Explain any two error detection techniques with mathematical examples other than given in slides, search from internet. (10)

Q3: What is encoding? Write down different types of encoding. Explain characteristics of AM, FM and PM with mathematical equations. (10)

Q4: Compare Ethernet and Token Ring concept of data networking with diagrams. Which one is better in your opinion and why? (10)

Q5. Explain the concept and review of Reliable Transmission with diagram (from a research paper of 2019 or 2020) and its functionality. The name and reference of paper should be given. (10)

Q1. Select the correct answer of the given ones.

1) Interactive transmission of data independent of a time sharing system may be best suited to
(a) simplex lines (b) half-duplex lines (c) full-duplex lines (d) biflex lines

2) The loss in the signal power as of an Electromagnetic signal is called
(a) attenuation (b) propagation (c) scattering (d) interruption

3) Early detection of packet losses improves _____________ acknowledgment performance.
(a) odd (b) even (c) positive (d) negative

4) Additional signal introduced in the desired signal in producing hypes is called
(a) fading (b) noise
(c) scattering (d) dispersion

5) Token is a **______logical ring____** that rotates around the ring.

6) Ring may have up to _800bit long fram_ (802.5) or __8_____ (IBM) nodes.

7) FDDI can support a maximum of ___500__ stations.

8) Error-correcting codes are __ **not advanced** ___ enough to handle all errors.

9) ACK is a small ___ Control frame____ confirming reception of an earlier frame

10) Electronics are __Slow_____ as compared to optics

Q2: Distinguish between error correction and error detection. Explain any two error detection techniques with mathematical examples other than given in slides, search from internet.

ANS: An error is when the output information does not match the input information. During transmission, digital signals

Suffering from noise, which may cause errors in binary bits transmitted from one system to another. Mean 0

Bits that can be changed to 1 or 1 can be changed to 0.

Error detection

Whenever a message is sent, it may be disturbed by noise or the data may be destroyed. To avoid this, we use error detection codes, which are additional data added to a given digital message, to help us detect whether an error has occurred during message transmission. Parity is a simple method of detecting errors. The parity bit is an additional bit sent with the data, it is just the sum of 1 bit of the data. The receiver adds the data bits and then compares the sum bit with the parity bit. If they do not match, the data (or the parity bit itself) has been corrupted on the way. A single parity bit is rarely used for content larger than bytes. For data blocks, different types of checksums are used. These can be just text sums of data bytes, which are usually truncated to 16 or 32 bits. However, this cannot detect errors such as transposed bytes or double-bit errors. A better solution is a cyclic redundancy check (CRC) algorithm, which uses a polynomial function to mix bits so that position information affects the result. Such a value is also called a hash or message digest. The longer the hash value, the less data can be destroyed, and always have the same hash value.

This concept is the core of digital signatures used in public key cryptosystems. The secure hash function (one-way) is used to generate the message digest of the document, which is then encrypted using the person's private key and attached to the document. The recipient uses the person's public key to decrypt the hash and compare it with the hash they generated from the same document. If they match, we know 1) the document has not changed since signing, and 2) the person's public key has successfully decrypted the file, and we know that the file comes from them.

Error correction

In addition to the error detection code, we can also transmit data to understand the original message from the damaged message received. This type of code is called an error correction code. Error correction codes also use the same strategy as error detection codes, but in addition, these codes can also detect the exact location of damaged bits.

In error correction codes, parity check has a simple method for detecting errors and a complex mechanism for determining the location of damaged bits. After finding the damaged bit, its value will be reversed (from 0 to 1 or 1 to 0) to get the original message. When transferring data (for example, via the Internet), it is usually necessary to retry the request to detect the error and correct it. But this method is impossible in many cases.

If the actual data provides enough redundant information, the damaged part can be reconstructed according to the degree of damage. For example, 4-bit redundant information (see Hamming code) is sufficient to correct single-bit errors in 16-bit blocks and detect (but not correct) double-bit errors. It is a scheme commonly used for highly reliable computer memory.

Music CDs contain a lot of redundant data (such as one-third of their content) to deal with damage caused by normal wear and tear, such as scratches and stains. You may have seen severely scratched discs still playing-you can thank the redundant data and error correction algorithms.The most popular Error Detecting Techniques are:

o Single parity

o Second parity check

o Checksum

o Cyclic Redundancy Check Single parity

o Simple parity is a simple and inexpensive mechanism for detecting errors.

In this technique, redundant bits are also called parity bits, and the parity bits are added to the end of the data unit, so the number of 1s becomes an even number. Therefore, the total number of bits transmitted will be 9 bits.

o If the number of bits 1s is odd, add the parity bit 1; if the number of bits 1s is even, add the parity bit 0 to the end of the data unit.

o During reception, calculate the parity bit based on the received data bits and compare it with the received parity bit.

o This technique generates a total of 1 pair, so it is called pair parity.

Error detection technology There are three main techniques for detecting frame errors: parity, checksum and cyclic redundancy check (CRC). Parity check

Parity is accomplished by adding an additional bit called parity to the data to make the number one, even in the case of parity or even parity. When creating a frame, the sender will count to 1 and add the parity bit as follows

• In the case of even parity: if the number 1 is even, the value of the parity bit is 0. If the number 1 is odd, the value of the parity bit is 1.

• In the case of odd parity: if the number 1 is odd, the value of the parity bit is 0. If the number 1 is an even number, the value of the parity bit is 1. When a frame is received, the receiver calculates the number of 1s it contains. In the case of even parity, if the number 1 is even, the frame is accepted, otherwise the frame is rejected. Parity check uses similar rules. Parity is only applicable to single-bit error detection.

Checksum

In this error detection scenario, the following procedure is applied

• The data is divided into fixed-size frames or segments.

• The sender uses complement arithmetic to add these segments to 1 to get the sum. Then, it completes the sum to obtain the checksum and sends it together with the data frame.

• The receiver uses 1's complement arithmetic to add the incoming segment to the checksum, get the sum, and then complete the summation.

• If the result is zero, the received frames are accepted; otherwise, they will be discarded.

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) involves the binary division of data bits sent by a predetermined divider agreed by the communication system. The divisor is generated using a polynomial.

• Here, the sender performs binary division on the data segment through the divider. Then, it adds the remaining data called CRC bits to the end of the data segment. This allows the resulting data unit to be completely divisible by the divisor.

• The receiver divides the input data unit by the divider. If there is no remaining, it is assumed that the data unit is correct and accepted. Otherwise, it is understandable that the data is corrupted and therefore rejected.

Error correction technology

Error correction techniques determine the exact number and location of damaged bits. There are two main methods

- Backward error correction (retransmission)-If the receiver detects an error in the incoming frame, it will request the sender to retransmit the frame. This is a relatively simple technique. However, it can be used effectively only when the retransmission is not expensive, such as in optical fiber, and the retransmission time is lower than the requirements of the application.

- Direct error correction-If the receiver detects an error in the incoming frame, it will execute the error correction code to generate the actual frame. This can save the bandwidth required for retransmission. This is inevitable in real-time systems. However, if there are too many errors, the frame must be resent.

The main four error correction codes are

- Hamming code

- Binary convolutional code

- Reed-Solomon code

- Low density parity check code

Q3: What is encoding? Write down different types of encoding. Explain characteristics of AM, FM and PM with mathematical equations.

ANS: Encoding is the process of converting data from one form to another. Although "encoding" can be used as a verb, it is usually used as a noun, referring to a specific type of encoded data. There are several types of encoding, including image encoding, audio and video encoding, and character encoding. Multimedia files are usually encoded to save disk space. By encoding digital audio, video and image files, you can save them in a more effective compression format. Encoded media files usually have similar quality to the original uncompressed copy, but the file size is much smaller. For example, the size of a WAVE audio file (.WAV) converted to an MP3 file (.MP3) can be 1/10 of the original WAVE file. Similarly, compared to raw digital video files (.DV), MPEG compressed video files (.MPG) may require only a small portion of disk space.

AM

The definition of amplitude modulation is that the amplitude of the carrier signal is proportional to the amplitude of the input modulation signal (based on). In AM, there is a modulated signal. This is also referred to as an input signal or baseband signal (such as speech). As mentioned earlier, this is a low frequency signal. There is another high-frequency signal called a carrier wave. The purpose of AM is to use carrier waves to convert low-frequency baseband signals to high-frequency signals. As mentioned earlier, high-frequency signals can travel longer distances than low-frequency signals. The derivative of amplitude modulation is as follows.

This happens when $m>1$

That is to say $(Vm / Vc)>1$. Therefore, $Vm> Vc$. In other words, the modulated signal is larger than the carrier signal.

The AM signal will generate new signals called sidebands at frequencies other than fc or fm.

We know that $VAM = (Vc + m\ Vm\ sin\omega mt)\ sin\omega ct$

We also know that $m = Vm / Vc$. So $Vm = m.Vc$

therefore,

Case 1: The input signal and carrier signal are sine waves.

$VAM = (Vc + m\ Vc\ sin\omega mt)\ sin\omega ct$

$= Vc\ sin\omega ct+ m\ Vc\ sin\omega mt$. Sine

Recall $SinA\ SinB = 1/2\ [cos\ (A-B)-cos\ (A + B)]$

Therefore $VAM = Vc\ sin\omega ct+ [mVc / 2\ cos(\omega c-wm)t]-[mVc / 2\ cos(\omega c+ wm)t]$

$Vc\ sin\omega ct$ is the carrier

$mVc / 2\ cos\ (\omega c-wm)\ t$ is the lower sideband

$mVc / 2\ cos\ (\omega c+ wm)\ t$ side dinner

Therefore, the AM signal has three frequency components: carrier, upper sideband, and lower sideband.

Case 2: The input signal and carrier signal are cos waves.

$VAM = (Vc + m\ Vc\ cos\omega mt)\ cos\omega ct$

= Vc cosωct+ mVc cosωmt. cosωct

Recall Cos A Cos B = 1/2 [cos (A—B) + cos (A + B)]

Therefore VAM = Vc cosωct+ [mVc / 2 cos(ωc-wm)t] + [mVc / 2 cos(ωc+ wm)t]

Vc cosωct

mVc / 2 cos (ωc-wm) t is the lower sideband

Sideband mVc / 2 cos (ωc + wm) t dinner

Therefore, the AM signal has three frequency components: carrier, upper sideband, and lower sideband.

FM

Frequency modulation uses the information signal Vm(t) to change the carrier frequency within a small range around its original value. These are three signals in mathematical form:

- Information: Vm (t)
- Carrier: Vc(t) = Vco sin(2 p fc t + f)
- FM: VFM(t)= Vco sin(2 p [fc +(Df / Vmo)Vm(t)] t + f)

We have replaced the term carrier frequency with time-varying frequency. We also introduced a new term: Df, peak frequency deviation. In this form, you should be able to see the carrier frequency term: fc + (Df / Vmo) Vm(t) now changes between the extreme values of fc-Df and fc + Df. The explanation of Df is clear: the FM signal is farthest from the original frequency. Sometimes it is called "swing" in frequency.

We can also define a modulation index similar to AM for FM:

b = Df / fm, where fm is the maximum modulation frequency used.

The simplest interpretation of the modulation index b is a measure of the peak frequency deviation Df. In other words, b represents a means of expressing the peak deflection frequency as a multiple of the maximum modulation frequency fm, that is, Df = bfm.

Example: Suppose the audio signal to be transmitted on the FM radio is between 20 and 15,000 Hz (in this case). If the maximum modulation index b used by the FM system is 5.0, the maximum “oscillation” of this frequency above and below the carrier frequency is 5 x 15 kHz = 75 kHz.

Here, the carrier frequency is 30 Hz, the modulation frequency is 5 Hz, and the modulation index is about 3, which makes the peak frequency difference about 15 Hz. The frequency will vary from 15 to 45 Hz. The speed of the completion cycle depends on the modulation frequency.

PM

Phase modulation (PM) is a modulation model used to adjust communication signals for transmission. It encodes the message signal in the form of an instantaneous phase change of the carrier. Phase modulation is one of the two main forms of angle modulation and frequency modulation.

The phase of the carrier signal is modulated to follow the changing signal level (amplitude) of the message signal. The peak amplitude and frequency of the carrier signal remain constant, but as the message signal amplitude changes, the carrier phase will also change accordingly.

Phase modulation is widely used for radio wave transmission and is an integral part of many digital transmission coding schemes that support a wide range of technologies such as Wi-Fi, GSM and satellite TV.

PM is used for signal and waveform generation in digital synthesizers (such as Yamaha DX7) to achieve FM synthesis. Casio CZ synthesizer uses a related sound synthesis method called phase distortion.

V = A sin [wct +Ø]

V = A sin [wct + mp sin wmt]

A = amplitude of PM signal

mp = PM modulation index

wm = 2πfm wc = 2πfc

V = A sin [2πfct + mpsin2πfmt]

The phase modulation diagram was explained above. If the amplitude of the input signal increases, the carrier phase difference will be greater, and vice versa. When the input amplitude increases (slope + ve), the carrier undergoes a phase lead. When the input amplitude decreases (-ve slope), the carrier phase shifts.

Therefore, as the input amplitude increases, the size of the phase conductor will continue to increase. For example, if the phase line is 30 degrees at t = 1 s, the phase line increases to 35 degrees at t = 1.1 s, and so on. The increase in phase line is equivalent to the increase in frequency.

Similarly, as the input amplitude decreases, the amplitude of the phase shift will continue to increase. For example, if the phase shift is 30 degrees at t = 1 second, then the phase shift will increase to 35 degrees at t = 1.1 seconds, and so on. An increase in phase shift is equivalent to a decrease in frequency.

Q4: Compare Ethernet and Token Ring concept of data networking with diagrams. Which one is better in your opinion and why?

ANS: A token ring is defined as a local area network that has the property to send a node only if it has certain coins continuously from other consecutive nodes. The token ring system is a region (LAN) in which all PCs are associated in a ring or star topology and at least one related token is transmitted from the host. Only the host with the token can send the message, and the token will be uninstalled after confirming the receipt of the message. The token ring system prevents data packets from blocking on a part of the network because the information must be sent by the token holder and certain accessible tokens must be controlled.

The token is an unusual coin design that rotates in a circle. To convey specific information, the PC obtains the token, adds a message to the token, and then provides it with the option to continue moving in the system. In addition, observe the passage of the token. It was introduced by IBM in 1984 and then institutionalized by the IEEE 802.5 convention. It is indeed convincing, especially in professional workplaces, but it is gradually covered up by the following form of Ethernet.

The sites on the Token Ring LAN are intelligently classified as a ring topology, starting from the ring site to transmit information in turn, and then using the control token to the next ring for cyclic transmission, the control token controls access around the ring. ARCNET, token transmission, 100VG-AnyLAN (802.12) and FDDI use comparative token delivery systems, which have the assumed favorable conditions on the original Ethernet CSMA/CD.

Ethernet is defined as a system for connecting various computers to form a local network, and has different protocols to ensure smooth transmission of information and simultaneous transmission does not occur. When Ethernet was first delivered in the 1980s, it maintained the highest data rate of 10 megabits per second (Mbps).

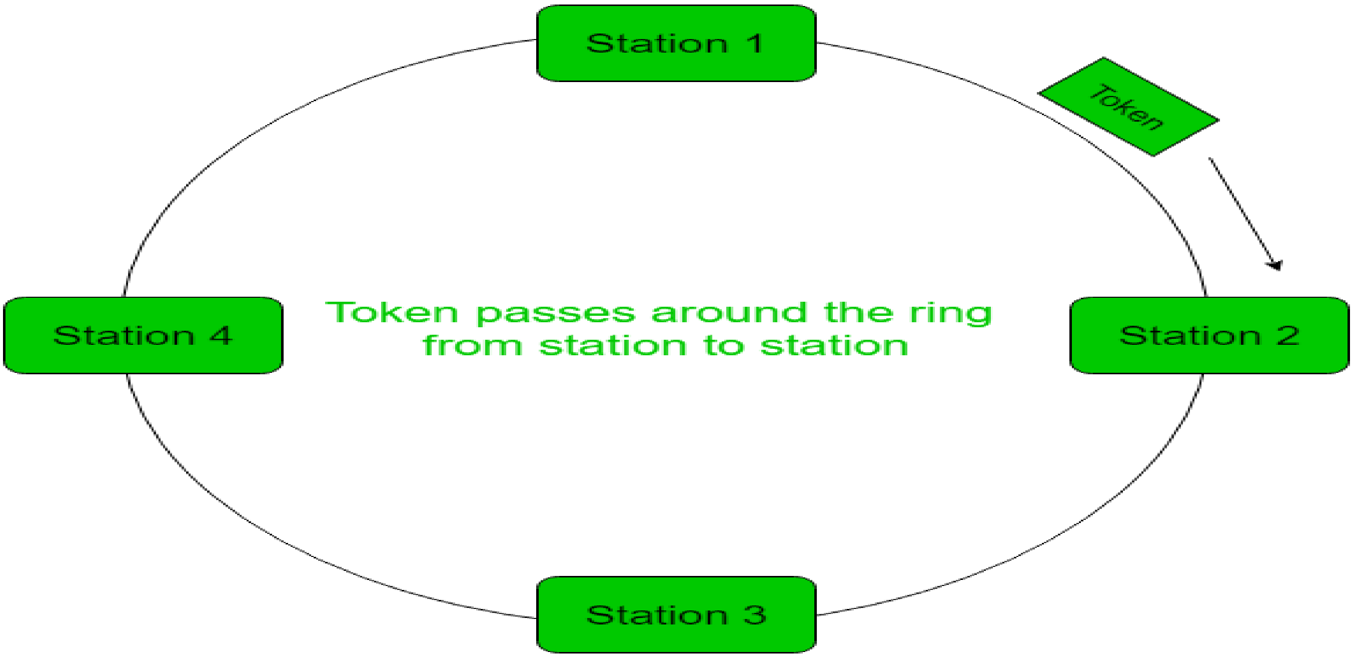
Subsequently, the so-called "Fast Ethernet" standard extended the most important information rate to 100 Mbps. Gigabit Ethernet innovation further extends peak performance to 1000 Mbps, and there are also 10 Gigabit Ethernet innovations.

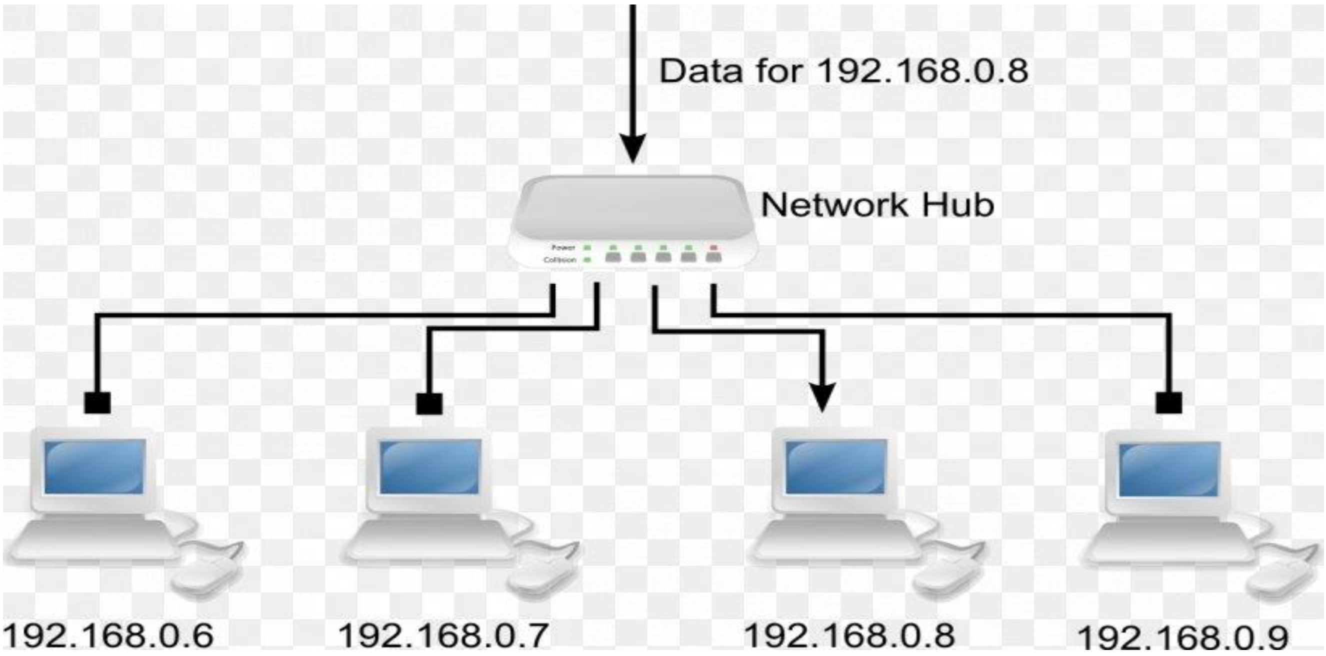
Ethernet is the most commonly used neighbor change (LAN). Ethernet is a connection layer convention in the TCP/IP stack that describes how organized gadgets organize information to transmit it to other system devices on similar system segments, and how to distribute this information across network associations. . It affects the layer 1 (physical layer) and layer 2 (data interface layer) in the OSI arrangement convention display.

The total length of a single Ethernet link is limited to approximately 100 meters; however, an Ethernet system can be effectively implemented using system connection gadgets to connect the entire school or office structure. Ethernet characterizes two transmission units, namely packaging box and box. The edge integrates the “payload” of the transmitted information and the physical “MAC” location that distinguishes the sender and the beneficiary, the VLAN tag and the nature of the management data, and the data trend of the data trend. Misadjusted to identify transmission problems.

The token ring station waits for permission to speak (token), but transmits all received traffic to the next member of the ring until the token is received. There are token management rules to ensure the maximum time limit before the workstation is allowed to speak. In a perfect world, it is very cool, but to ensure that all workstations collaborate will have a lot of complexity, and will deal with some special cases. This also means that even in a nominally inactive network, stations almost always have to wait for transmission.
(Conventional) The Ethernet station listens to the line and transmits only when it detects that the line is inactive. He thinks he has obtained permission. If two stations perform this operation at the same time, a "conflict" will occur and data will be lost. Each blocked site will wait for a random time to retry, and if there are consecutive conflicts, the time will multiply. There is no guaranteed upper latency limit, but statistical information is useful for this medium, especially when used with cooperative upper-layer protocols such as TCP.

Ethernet and Token Ring networking diagrams.





Q5. Explain the concept and review of Reliable Transmission with diagram (from a research paper of 2019 or 2020) and its functionality. The name and reference of paper should be given

ANS:-

Reliable Transmission of Short Packets Through Queues and Noisy Channels Under Latency and Peak-Age Violation Guarantees

Reference:-10.1109/ANTS47819.2019.9118022

Abstract- This paper studies the possibility of information delay and maximum information lifetime exceeding the required threshold in a point-to-point communication system with short information packets.The transmitter uses a variable-length variable-feedback coding system &#40;a general strategy that includes simple automatic repeat request (ARQ&#41; and more complex hybrid ARQ techniques as special cases) to send packets. The message is sent to other recipients. The numerical results reveal the dependence of delay and peak violation probabilities on system parameters (such as frame size and probability of undetected errors) and the selected packet management strategy.The guidelines provided by our analysis are particularly useful for designing ultra-reliable low-latency communication systems.

INTRODUCTION

Emerging wireless applications, automated automated transportation, industrial automation and control, and touch-screen Internet require the availability of mission-critical links that can deliver short packets with delays and delays. Strict reliability.
Manuscript received on June 21, 2018; revised on December 10, 2018; accepted on January 25, 2019. The release date is February 12, 2019; the latest date of the current version is March 15, 2019. This research was supported by the Swedish Research Council within the 2016-03293 grant framework. O's work. Simeone received funding from the European Research Council (ERC) within the framework of the European Union's Horizon 2020 research and innovation program under 725731. Uysal was supported by TÜB ITAK's 117E215 funding. Part of this paper was published at the IEEE International Information Theory Symposium (ISIT) in June 2018 [1]. (Corresponding author: Rahul Devassy) R Devassy and G. Durisi Department of Electrical Engineering at Chalmers University of Technology, Gothenburg, Sweden, 41296. (E-mail: devassy@chalmers.se; durisi@chalmers.se). . G. C. Ferrante taught at Chalmers University of Technology (412 96 Gothenburg) in Sweden. (Email: gcf@ieee.org). O. Simeone is part of the Department of Computer Science at King’s College London, WC2R 2LS, London, England (email: osvaldo.simeone@kcl.ac.uk). E. Uysal is in the Department of Electrical and Electronic Engineering, Middle East Technical University, Ankara, Turkey, address: 06800 (email: uelif@metu.edu.tr). Color versions of one or more graphics in this document are available online at http://ieeexplore.ieee.org. Digital Object Identifier 10.1109 / JSAC.2019.2898760 The Ultra Low Latency Communication (URLLC) defined by the International Telecommunication Union (ITU) [2] supports the introduction of URLLC services in next-generation (5G) wireless cellular systems. Considering the isolated transmission of a single data packet, due to its very high reliability capture constraints, short code data packets and payload, new non-asymptotic information tools are applied to the design of URLLC. Short messages and sporadic transmission. In particular, as recently shown in [3] and [4], the theory of information on finite block length provides an accurate tool for describing the trade-offs between delay, reliability, and bit rate when transmitting a single short data packet. . However, the latency of communication depends not only on the length of the block, but also on the contribution of the queuing delay embedded in the data stream. And understand that the delay of only control commands is not suitable for capturing the strict performance requirements of mission-critical applications for transmission, but the URLLC solution must ensure that the total delay is the total delay. The probability of falling below the tolerable threshold is high. In view of the critical role of queuing delay in ensuring URLLC delay performance, in this article, we will delay the overall steady state, and for a given reliability constraint, all information including queuing and transmission exceeds the expected level. . As discussed, in many cases where URLLC is used, global latency is a key indicator of concern. Delay is measured at the link layer, and it provides a useful quality of service metric for the upper layers of the protocol. However, some important applications (minimizing the delivery delay) may not meet the requirements of this layer. application. For example, in industrial automation, information packets exchanged on a wireless medium can remotely transmit the necessary sensor data to a given target, and the data must follow the process. Packets containing outdated sensor data are of no value to the target, so insisting on transmitting data with low latency is usually not the best option. A more

relevant performance indicator is the language of information, which measures the longest elapsed time since the destination received the last update (for example, see [5] and references here). Possibility that Figure. In the system model under consideration, a new packet arrives with probability λ in each channel usage. The data packets enter the first-come-first-served queue, and then use variable length stop feedback codes to transmit through the wireless channel.

For a given reliability constraint, the maximum steady-state life of the packet exceeds the expected level. Throughout the document, we consider a point-to-point communication system, in which packets arrive randomly according to channel usage, as shown in Figure 1. The analysis assumes that a single server queue and usage variable-length universal stop feedback (VLSF) codes are used for information transmission [4, equation. (ten)]. In the VLSF coding scheme, each codeword composed of any number of coding symbols is divided into frames of n symbols. After receiving the frame, the decoder will try to retrieve the packet. Then, it communicates the result of the decoding attempt to the encoder through the ACK/NACK bits transmitted on the feedback channel. If decoding fails, the next block is sent. If the decoding is successful, the transmission will stop and the packet will be deleted from the queue.In the VLSF coding scheme, each codeword including any number of coding symbols is divided into frames of n symbols. After receiving the frame, the decoder will try to retrieve the packet. Then, it communicates the result of the decoding attempt to the encoder through the ACK/NACK bits transmitted on the feedback channel. If decoding fails, the next block is sent. If the decoding is successful, the transmission is stopped and the packet is deleted from the queue. VLSF codes include strategies commonly used in current wireless systems under certain circumstances, such as Simple Automatic Repeat Request (ARQ), where all frames corresponding to the same packet contain the same coded bits, and ARQ incremental redundancy mix (HARQ), where each new frame contains other parity symbols.

Related Work

In addition to the work of Telatar and Gallager [6] using error exposure methods, most communication link queuing analysis is based on the abstraction of the bit pipe at the physical layer. Therefore, for a given shear probability, bits are reliably transmitted at a rate equal to the channel capacity, or in the case of a quasi-static fading channel, bits are reliably transmitted at a rate equal to the shear capacity. This work can be divided into three categories: (i) steady-state average delay analysis; (ii) the use of linked Chernoff to analyze the possibility of delay violations through network calculations or large deviation theory (see [7] , [8] and its references); (iii) Analyze the traffic delay trade-offs under time constraints [9], [10]. However, the bitstream abstraction is not suitable for URLLC traffic analysis because the delay limit prevents the use of channel codes with longer block lengths. Hamidi-Sepehretal [12] analyzed the queuing behavior when using BCH codes. They evaluated the probability distribution and average delay of the steady-state queue size. Their analysis takes into account undetected error events, that is, even if the decoded message is incorrect, an ACK event will be returned. More specifically, the author has shown how to use the erasure decoding rules proposed in [13] to mitigate the negative effects of these events.

CONCLUSION

The optimal design of URLLC should be based on non-asymptotic joint queue/coding analysis, not average. In this article, we explained how to arrive at i.i.d. Bernoulli packets, queue on a single server, and perform point-to-point communication on the dual AWGN channels through VLSF codes. We propose a method to evaluate the probability of delay violations and peak age violations, and analyze the two parameters for system parameters (such as frame length, probability of undetected errors and package management strategy. A new aspect of our method is that it also considers Undetected errors. Such errors may cause great harm to critical communication systems, and the specific design that minimizes them will be the subject of future work. Our analysis shows that the possibility of delay violations The value of the parameter is extremely sensitive. This can be seen in Figures 1 and 2. Figures 5 and 7 show the dependence of the maximum bit rate and the possibility of violation of the frame size delay violation for a simple ARQ with perfect error detection 6 and 6 show the probability of undetected errors for the probability of dependent delay violations. We also show that analysis based on average latency or based on random network calculations cannot achieve the optimal design, and for random network calculations , Its lack of versatility.

REFERENCES

[1] R. Devassy, G. Durisi, G.C. Ferrante, O. Simeone, and E. Uysal-Biyikoglu, “Delay and peak-age violation probability in short-packet transmission,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Vail, CO, USA, Jun. 2018, pp. 2471–2475.

[2] “IMT vision—Framework and overall objectives of the future development of IMT for 2020 and beyond,” ITU-R, Geneva, Switzerland, Tech. Rep. Rec. ITU-R M.2083-0, Sep. 2015.

[3] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2307–2359, May 2010.

[4] Y. Polyanskiy, H.V. Poor, and S.Verdú, “Feedback in the non-asymptotic regime,” IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4903–4925, Aug. 2011.

[5] M.Costa,M.Codreanu,andA.Ephremides,“Ontheageofinformationin status update systemswithpacket management,” IEEETrans.Inf.Theory, vol. 62, no. 4, pp. 1897–1910, Apr. 2016.

[6] I. E. Telatar and R. G. Gallager, “Combining queueing theory with information theory for multiaccess,” IEEE J. Sel. Areas Commun., vol. 13, no. 6, pp. 963–969, Aug. 1995.

[7] E. M.Yeh, “Fundamental performance limits in cross-layer wireless optimization: Throughput, delay, and energy,” in Foundations and Trends in Communications and Information Theory, vol. 9. Delft, The Netherlands: NOW, 2012.

[8] H. Al-Zubaidy, J. Liebeherr, and A. Burchard, “Network-layer performance analysis of multihop fading channels,” IEEE/ACM Trans. Netw., vol. 24, no. 1, pp. 204–217, Feb. 2016.

[9] M. Zafer and E. Modiano, “Minimum energy transmission over a wireless channel with deadline and power constraints,” IEEE Trans. Autom. Control, vol. 54, no. 12, pp. 2841–2852, Dec. 2009.

[10] R. Singh and P. R. Kumar, “Decentralized throughput maximizing policies for deadline-constrained wireless networks,” in Proc. IEEE 54th Annu. Conf. Decis. Control (CDC), Osaka, Japan, Dec. 2015, pp. 3759–3766.

[11] G. Durisi, T. Koch, and P. Popovski, “Toward massive, ultrareliable, and low-latency wireless communication with short packets,” Proc. IEEE, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[12] F. Hamidi-Sepehr, H. D. Pfister, and J. F. Chamberland, “Delay-sensitive communication over fading channels: Queueing behavior and code parameterselection,”IEEETrans.Veh.Technol.,vol.64,no.9,pp. 3957–3970, Sep. 2015.

[13] G. D. Forney, Jr., “Exponential error bounds for erasure, list, and decision feedback schemes,” IEEE Trans. Inf. Theory, vol. IT-14, no. 2, pp. 206–220, Mar. 1968.

RELIABLE AND SECURE TRANSMISSION FOR FUTURE NETWORKS

Reference: https://sci-hub.tw/https://ieeexplore.ieee.org/document/9053663

Abstract:-This article introduces a new physical layer encryption method called peer-to-peer random channel modulation (RRCM), which is used to reliably and securely transmit eavesdropping information (Eve) through any number of antennas and any level. noise. RRCM complicates Eve calculations to estimate user channel state information (CSI), which is used to disturb the information symbols transmitted between users. Since Eve cannot overcome the computational complexity of the physical layer, users can apply RRCM to achieve an almost constant (effective) bit/s/Hz unconditional secret-unconditional secret rate. Eve antenna, Eve noise level and CSI time coherence.

INTRODUCTION

Future wireless networks are expected to provide ultra-fast connections for people-to-people, device-to-device, person-to-person, and person-to-device communications around the world. However, there are many problems related to security, which hinders the development of ultra-fast networks that benefit humanity. The important security concern in this document is confidentiality. Like the current network, future networks will continue to rely on intermediate nodes (such as routers, base stations, servers, databases, etc.) to store and relay information transmitted from users. (Alice) to another (Bob), especially through social media. . Each such transmission leaves the original information somewhere on the track. Millions of personal accounts may be hacked, and their personal information may also be potentially abused. Therefore, there is a great need for end-to-end security on the Internet to meet the needs of personal, institutional and national security. To ensure end-to-end security, Alice and Bob must share secrets that no one knows. And such confidentiality should not be determined by third parties (including the "administrators" of the network). Alice and Bob can only establish this secret by themselves. The next question is: how do they do this without worrying about physical contact? Or how do they achieve when they are within each other's scope? The above is just one of many practical applications that require reliable and secure information transmission. Wireless secret transmission (no prior sharing required) This work was partially funded by the Army Research Office, with the authorization number W911NF-17-1-0581

Confidential) is the main goal to solve the security of the physical layer [1]-[17]. This field has developed rapidly, especially in the past decade. Many ideas, such as beamforming, artificial noise, cooperative junctions, etc. It has been proposed and extensively studied in the literature. Various assumptions have been used (for example, whether Alice/Bob knows or partially knows the monitor channel (Eve) and whether Alice/Bob knows or partially knows the location of Eve) to define the problem to be solved. However, for the case where Eve can have an unlimited number of antennas and is located anywhere that Alice/Bob does not know, people's attention is very limited. In order to improve security, regardless of the number of Eve antennas and the Eve signal-to-noise ratio (SNR), we hope to guarantee the affirmative confidentiality of Eve. This can be done by using mutual channel state information (CSI) between Alice and Bob. It is shown in [1] that for each cycle of CSI coherence, the theoretical and achievable secret (same as the state of the Eve channel (like the Eve antenna and SNR)) is not equal to the entropy H (S) from Alice and Bob shared CSI (discrete). We can designate H(S) as the strict unconditional confidentiality (UNS) (achievable) amount for each consistency period. However, H(S) is usually limited for each coherent period of length Kc, and as Kc increases, the strict bit rate of UNS (in bits/s/Hz) decreases to zero. In this article, we introduce a transmission scheme called random reciprocal channel modulation (RRCM) for the large Kc wireless channel. RRCM complicates the calculation, so the user's CSI can use the transmitter to scramble the information symbols (so it is necessary for the receiver to decode). Since Eve cannot overcome this complexity of the physical layer, RRCM can achieve an almost constant UNS rate for any effective Kc. RRCM is a physical layer encryption method intended for larger Kc, which is different from all other previous methods (eg [17]).