NTNU
Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Faglig kontakt under eksamen:

Navn: Bjarne E. Helvik
Tlf: 92667

EKSAMEN I EMNE SIE5025 PÅLITELIGHET SYSTEMER
(DEPENDABLE SYSTEMS)

Fredag 11. mai 2001
Kl. 0900 - 1300

Hjelpemidler:

B1- Typegodkjent kalkulator, med tomt minne, i henhold til utarbeidet liste.
Ingen trykte eller håndskrevne hjelpemidler.

Sensuren faller i 6 juni 2001.

The english version starts on (side) page 6.

- *In case of inconsistencies between the two languages, the Norwegian text is the prevailing.*
- *I tilfelle uoverensstemmelse mellom de to språkene er den norske teksten den gjeldende.*

Oppgave 1

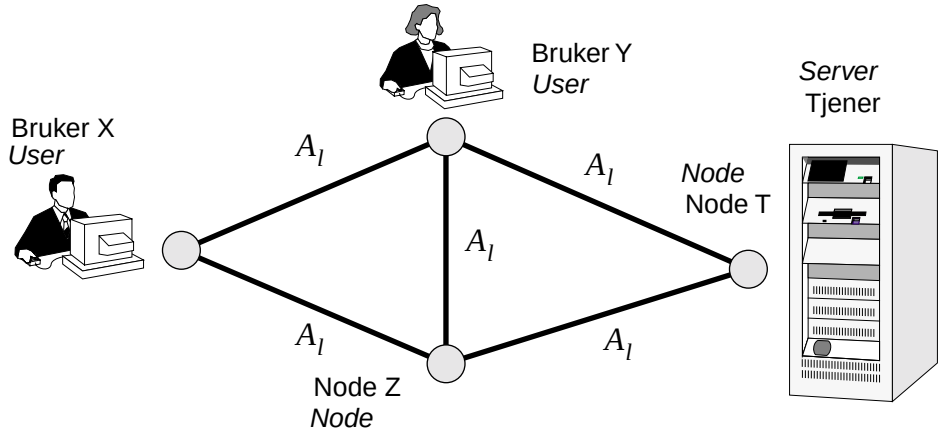
[Oppgaven tillegges 65% vekt]

Brukerne av en oppslagstjeneste som nås over nettet, setter som krav at forventningen til akkumulert tid de ikke kan benytte tjenesten i løpet av et år ikke skal overskride 10 minutt. Videre krever de at sannsynligheten for at en sesjon på en time skal avbrytes må være mindre enn 10^{-5} og at sannsynligheten for at en sesjon som varer i en uke (7 døgn) skal avbrytes må være mindre enn 10^{-3}.

a) Formuler kravene beskrevet ovenfor som krav til systemets pålitelighetsattributter. Benytt standard termer. Både norske og engelske godtas.

b) Anta at avbrudd i tjenesten (feilytringer) skjer ifølge en homogen Poisson prosess. Er det kravet til avbrudd pr. time eller kravet til avbrudd pr uke som er det strengeste? Begrunn svaret. Finn forventet tid mellom feil (MTBF) og forventet nedetid (MDT) dersom kravene skal imøtekommes.

Topologien i nettet er vist i Figur 1.1. Anta at nodene, brukerutstyret og tjeneren er feilfrie, og anta i første omgang at alle lenkene i nettet feiler og blir reparert uavhengig av hverandre. Alle lenkene har asymptotisk tilgjengelighet A_l. Midlere nedetid på alle lenker er m. Det er ingen begrensninger på hvordan trafikken kan rutes i nettet og reruting skjer øyeblikkelig ved feil.



Figur 1.1

c) Tegn opp pålitelighetsblokkskjema og finn et uttrykk for asymptotisk tilgjengelighet for konnektivitet både mellom bruker X og tjeneren og mellom bruker Y og tjeneren.

d) Vis hvordan vi kan finne et uttrykk for feilintensiteten som bruker Y erfarer mot tjeneren.

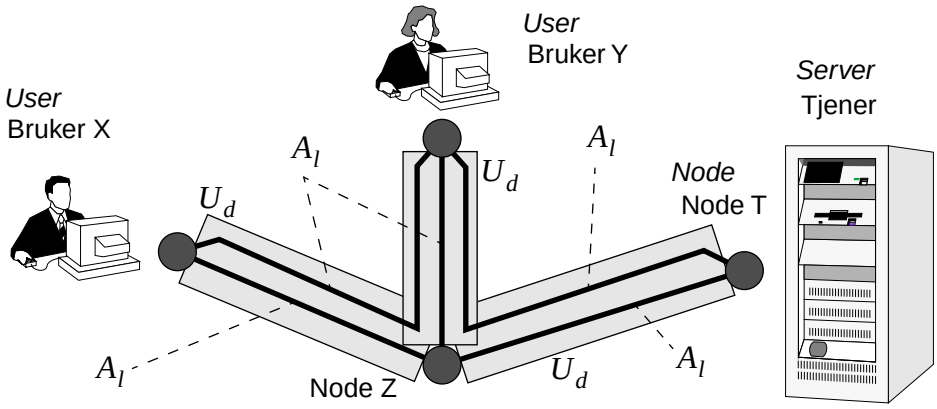
Bruker X og Y er tilsluttet nettet i hhv. node X og Y. Kapasiteten på de fem lenkene i nettet er $[X, Y] = [X, Z] = [Y, Z] = [Z, T] = C$ og $[Y, T] = 2C$. Tilbudt effektiv trafikk er $A_{XT}^* = A_{YT}^* = C$. (Både trafikk og kapasiteter er bidireksjonale.) Rutingen av trafikken når alle lenker i nettet fungerer er $\pi_{YT}(0) = \{Y, T\}$ og $\pi_{XT}(0) = \{X, Z, T\}$. Ved reruting etter feil har trafikken som benyttet en lenke før feilen, prioritet på å benytte denne også etter feilen. Nettet fungerer (er oppe) sett fra de to brukerne når det er tilstrekkelig kapasitet til å føre den tilbudte trafikken.

e) Vis og forklar kort hvordan vi kan finne en øvre og nedre grense for utilgjengeligheten mellom to noder i nettet når det kreves at tilbudt trafikk blir ført, uten å undersøke samtlige feilmodi/feiltilstander.

f) Finn øvre og nedre grenseverdier for utilgjengeligheten både mellom bruker X og tjeneren og mellom bruker Y og tjeneren i nettet beskrevet i Figur 1.1 når vi tar hensyn til maksimalt en feilet lenke i nettet.

g) Dersom vi kun har krav til konnektivitet i nettet finner vi at utilgjengeligheten for de to tilfellene er $U_{XT} \approx 2U_l^2$ og $U_{YT} \approx U_l^2$, hvor $U_l = (1 - A_l)$. Gi en fysikalsk forklaring på relasjonen mellom disse verdiene og resultatet i punkt f) over.

Lenkene i nettet i Figur 1.1 ligger i tre fysiske traseer som vist i Figur 1.2. Tilgjengeligheten av lenkene er A_l når en ikke tar hensyn til feil knyttet til traseen(e). I tillegg er det også en utilgjengelighet U_d knyttet til hver av traseene. En feil knyttet til en trase medfører at samtlige lenker i traseen feiler. Traseene feiler og repareres uavhengig av hverandre.



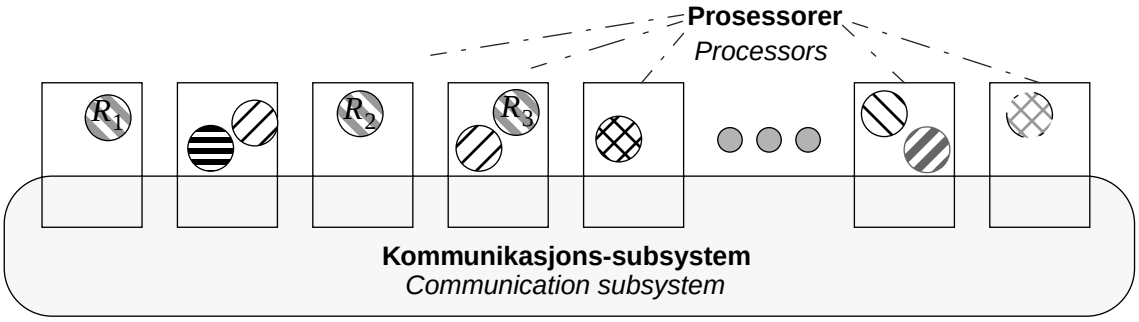
Figur 1.2

h) Utvid resultatet i punkt f) til også å ta hensyn til feil i traseene, dvs. finn øvre og nedre grenseverdier for utilgjengeligheten både mellom bruker X og tjeneren og mellom bruker Y og tjeneren i nettet beskrevet i Figur 1.2. Dersom ytterligere tilnærmelser benyttes, påpek og begrunn disse.

Oppgave 2

[Oppgaven tillegges 35% vekt]

Vi betrakter et distribuert system som illustrert på Figur 2.1. Systemet består av en rekke prosessorer knyttet sammen ved hjelp av et kommunikasjons-subsystem. I systemet er det tre replika av en tjenerprosess, R_i, $i = 1, 2, 3$ samt et antall prosesser som benytter den tjenesten disse leverer.



Figur 2.1

a) Beskriv hva som ligger i objektgruppe (object group) paradigmet innen gruppekommunikasjon.

b) Hvilke krav må settes til meldingsutveksling og eksekvering for at aktiv replikering skal kunne benyttes for å realisere feiltoleranse i et distribuert system?

En logisk feil i kommunikasjons-subsystemet medfører at det ikke alltid klarer å levere meldinger med total orden til de tre replikaene (R_i, $i = 1, 2, 3$,) av tjenerprosessen. La $N_1(t)$ være antall ganger meldinger er levert i en orden som er forskjellig til den ene av replikaene i løpet av tiden t. For eksempel: replika 2 mottar sekvensen m_5, m_6, m_8, m_7, m_9 mens replika 1 og 3 mottar m_5, m_6, m_7, m_8, m_9. Likeledes la $N_{\text{all}}(t)$ være antall ganger meldingene er levert i forskjellig orden til samtlige replika, og $N_{1/2}(t)$ antall ganger to bestemte replika mottar meldinger i ulik rekkefølge. La

$$\psi_i = \lim_{\Delta t \to 0} \frac{E(N_i(t + \Delta t) - N_i(t))}{\Delta t} \text{ for } i \in \{1, \text{all}, 1/2\}$$

Der som et av replikaene faller ut av synkronisme klarer systemet å introdusere et nytt replika som er i synkronisme med de øvrige i løpet av en negativt eksponensialfordelt tid med forventning δ^{-1}. Dersom alle replikane kommer ut av synkronisme vil tjenesten feile.

c) Etabler en tilstandsmodell og et ligningssett med sikte på å bestemme sannsynlighetstetthetsfordelingen av tiden til tjenesten feiler, $f(t)$, p.g.a. at kommunikasjonssubsystemet ikke klarer å levere ordnede meldinger. Se bort i fra alle andre feilårsaker. Initielt er alle replikaene synkrone.

Etter at likningssettet i punkt c) er etablert, ønsker vi å betrakte spesialtilfellet hvor $\psi_{1/2} = \psi_1 = \psi$ og $\psi_{\text{all}} = 0$. Løst gir dette følgende sannsynlighetstetthetsfordeling for tiden til tjenesten feiler.

$$f(t) = \frac{\psi^2}{\alpha}\left(e^{-\frac{(\delta + 2\psi - \alpha)}{2} \cdot t} - e^{-\frac{(\delta + 2\psi + \alpha)}{2} \cdot t}\right) \tag{2.1}$$

$$\alpha = \sqrt{\delta(\delta + 4\psi)}$$

d) Anta at tiden for å gjenopprette et synkront replika er vesentlig kortere enn forventet tid mellom hver gang meldinger kommer i ulik orden. Benytt dette til å forenkle uttrykket over. Begrunn de ulike steg i forenklingen og kommenter resultatet.

e) Finn forventet tid til tjenesten feiler på grunn av manglende total orden i leveransen av meldinger. Forenklingen funnet i punkt d) kan benyttes. Hvordan vil resultatet endres dersom $\psi_{all} \neq 0$? Hvor stor må ψ_{all} bli for at ulik ordning meldinger til samtlige replika skal dominere forventet tid til feil av tjenesten?

Gitt: Rekkeutvikling av kvadratroten $\sqrt{x + y}$ omkring x:

$$\sqrt{x + y} = \sqrt{x} + \frac{y}{2\sqrt{x}} - \frac{y^2}{8x\sqrt{x}} + o(y^2)$$

□

- In case of inconsistencies between the two languages, the Norwegian text is the prevailing.
- I tilfelle uoverensstemmelse mellom de to språkene er den norske teksten den gjeldende.

Problem 1

[This problem represents 65% of the exam]

The users of a look up service which is reached over the network, have the following requirements for the service. The expected accumulated time they can not use the service shall not exceed 10 minutes during one year. The probability that a one hour session is interrupted shall be less than 10^{-5} and the probability that a one week (7 days) session is interrupted shall be less than 10^{-3}.

a) Formulate the requirements presented above as requirements for the dependability attributes of the system. Use standard terminology. Both English and Norwegian terms are accepted.

b) Assume that interruptions of the service takes place according to a homogeneous Poisson process. Which requirement for interruptions are the strictest, the per hour requirement or the per week requirement? Motivate the answer. Obtain the mean time between failures (MTBF) and the mean down time (MDT) which meets the above requirements.

The topology of the network is shown in Figur 1.1 on page 2. Assume that the network nodes, the user equipment and the server are fault free, and assume for a start, that all the links fails and are repaired independent of each other. All the links have the asymptotic availability A_l. The mean down time of all links is m. It is no limitations on the routing of the traffic through the network, and rerouting takes place instantaneously.

c) Draw reliability block diagrams and find expressions for the asymptotic availability of the connectivity between both user X and the server and between user Y and the server.

d) Show how an expression of the failure intensity user Y experiences toward the server T may be obtained.

Users X and Y are connected to the network in nodes X and Y respectively. The capacity of the five links in the network are $[X, Y] = [X, Z] = [Y, Z] = [Z, T] = C$ and $[Y, T] = 2C$. Offered effective traffic are $A_{XT}{}^* = A_{YT}{}^* = C$. (Both traffic and capacities are bidirectional.) The routing of the traffic when all links are working are $\pi_{YT}(0) = \{Y, T\}$ and $\pi_{XT}(0) = \{X, Z, T\}$. By rerouting after a failure, the traffic which used the link before the failure has priority with respect to using this link after the failure. The network is working (up) seen from the two users when there is sufficient capacity to carry the offered effective traffic.

e) Demonstrate and explain shortly how we may obtain an upper and a lower bound of the unavailability between two nodes of the network when it is required that the offered traffic is carried, without having to investigate all failure modes/ states.

f) Obtain the upper and lower bounds of the unavailability between both user X and the server and user Y and the server in the network presented in Figur 1.1 on page 2 when we takes into account maximum one failed link in the network.

g) If we have only requirements for the connectivity of the network, we find that the unavailability in the two cases are $U_{XT} \approx 2U_l^2$ and $U_{YT} \approx U_l^2$, where $U_l = (1 - A_l)$. Give a physical explanation of the relation between these values and the result in item f) above.

The links of the network of Figur 1.1 on page 2 lay in three physical ditches as illustrated in Figur 1.2 on page 3. The unavailability of the links is A_l when failures related to the ditch(es) are not taken into account. In addition, there is also an unavailability U_d related to the ditches. A failure related to a ditch results in the failure of all links in the ditch. The ditches fail and are repaired independently of each other.

h) Extend the result of item f) to also take into account failures related to the ditches, i.e. find an upper and a lower bound on the unavailability between both user X and the server and user Y and the server in the network presented in Figur 1.2 on page 3. If additional approximations are used, identify and justify these.

Problem 2

[This problem represents 35% of the exam]

We regard a distributed system as illustrated in Figur 2.1 on page 4. The system consists of a number of processors interconnected with a communication subsystem. In the system, there are three replica of a server process R_i, $i = 1, 2, 3$, as well as a number of processes using the service that these provide.

a) Describe what is contained in the object group paradigm in group communication.

b) What are the requirements for message exchange and for execution if it shall be possible to use active replication to realize fault-tolerance in a distributed system?

A logical fault in the communication subsystem has as a consequence that it does not always deliver messages in total order to the three replicas (R_i, $i = 1, 2, 3$) of the server process. Let $N_1(t)$ be the number of times messages has been delivered in an order which is different for one of the replicas during the time t. For instance: replica 2 receives the sequence m_5, m_6, m_8, m_7, m_9 while replica 1 and 3 receive m_5, m_6, m_7, m_8, m_9. Likewise, let $N_{\text{all}}(t)$ be the number of times messages have been delivered in a different order to all replicas, and $N_{1/2}(t)$ the number of times two specific replicas receives messages out of order. Let

$$\psi_i = \lim_{\Delta t \to 0} \frac{E(N_i(t + \Delta t) - N_i(t))}{\Delta t} \text{ for } i \in \{1, \text{all}, 1/2\}$$

If one of the replicas falls out of synchronism, the system is able to establish a new replica, synchronous with the rest, in a negative exponentially distributed time with expectation δ^{-1}. If all replicas falls out of synchronism, the service will fail.

c) Establish a state model and a set of equations which may be used to find the probability density function (pdf) of the time until the service fails, $f(t)$, due to the inability of the communication subsystem to always deliver ordered messages. Failures due to other causes shall not be regarded. Initially, the replicas are synchronous.

After the set of equations in item c) is established, we would like to consider the special case where $\psi_{1/2} = \psi_1 = \psi$ and $\psi_{\text{all}} = 0$. Solved, this yields the following pdf for the time until the service fails:

$$f(t) = \frac{\psi^2}{\alpha}\left(e^{-\frac{(\delta + 2\psi - \alpha)}{2} \cdot t} - e^{-\frac{(\delta + 2\psi + \alpha)}{2} \cdot t}\right)$$

$$\alpha = \sqrt{\delta(\delta + 4\psi)}$$

d) Assume that the time needed to re-establish a synchronous replica is significantly shorter than the expected time between messages delivered out of order. Use this to simplify the expression above. Justify the various steps in the simplification and comment on the result.

e) Find the expected time until the service fails due to lack of total order in message delivery. The simplification obtained in item d) may be used. What is the effect on the result if $\psi_{all} \neq 0$? How large must ψ_{all} become before a different order in the delivery of messages to all replicas shall dominate the expected time until failure of the service?

Given: Series expansion of the square root $\sqrt{x+y}$ around x:

$$\sqrt{x+y} = \sqrt{x} + \frac{y}{2\sqrt{x}} - \frac{y^2}{8x\sqrt{x}} + o(y^2)$$

□