Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMENSOPPGAVE I SIE5025-PÅLITELIGE SYSTEMER

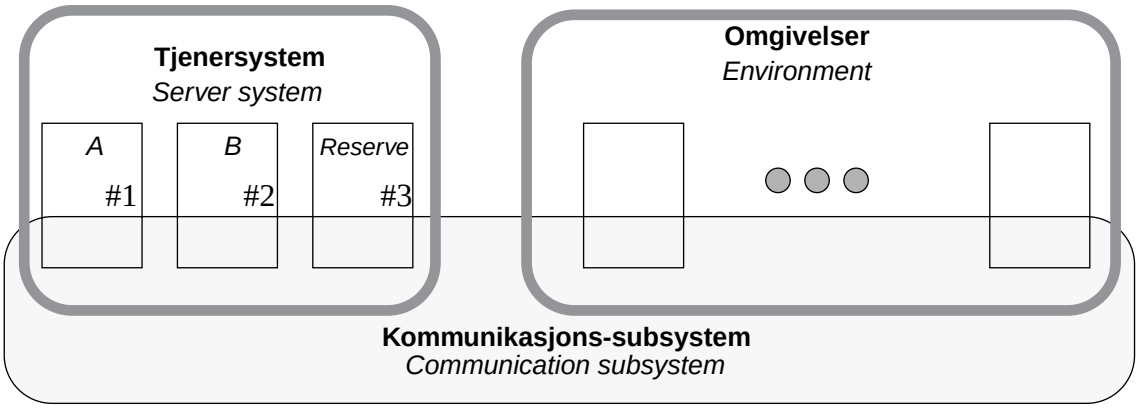
Faglig kontakt under eksamen:	Bjarne E. Helvik
Telefon.:	92667
Eksamensdato:	24. mai 2003
Eksamenstid:	4 timer
Vekttall:	2,5 Vt
Tillatte hjelpemidler:	D
Språkform:	
Antall sider bokmål:	6
Antall sider nynorsk:	
Antall sider engelsk:	
Antall sider vedlegg:	
Sensurdato[1]:	17 juni 2002

1. Merk! Studentene må primært gjøre seg kjent med sensur ved å oppsøke sensuroppslagene. Evt. telefoner om sensur må rettes til sensurtelefonene. Eksamenskontoret vil ikke kunne svare på slike telefoner.

Oppgave 1

[Oppgaven tillegges 50% vekt]

Vi betraker en tjeneste som leveres av et enkelt tjenersystem. Det består av tre tjenere som leverer to sett av funksjoner, A og B. Funksjonene A leveres av en tjener, funksjonene B leveres av en annen tjener og den tredje tjeneren er reserve for de to øvrige. Reserven kjører (er varm/"hot"), men utfører ikke funksjoner knyttet til tjenesten som systemet leverer. Mhp. feiling og feilavhjelping er de tre tjernerne identiske. Kommunikasjonssystemet antas å være feilfritt. Feilraten til en tjener er λ og tjenerne feiler uavhengig av hverandre. Tjenerne har feil-stopp ("crash failure") semantikk. Et eksempel på en systemkonfigurasjon er vist i Figur 1.1



Figur 1.1

a) Beskriv kort (ca. to linjer pr. moment) eventuelle fordeler og ulemper ved å ha en varm reserve i tjenersystemet fremfor kald (avslått/"not powered") reserve.

b) Hva menes med feilsemantikk generelt og feil-stopp semantikk spesielt? Nevn en måte å fremtvinge feil-stopp semantikk i en prosessor på.

Anta til å begynne med at systemet ikke er vedlikeholdt, dvs. en feilet tjener idriftsettes ikke igjen og at reserven alltid overtar for en feilet tjener uten avbrudd.

c) Tegn et pålitelighetsblokkskjema for tjenersystemet og finn et uttrykk for funksjonssannsynligheten. Hva er sannsynligheten (numerisk) for at tjenersystemet skal fungere lengre enn MTFF for en tjener?

Anta at en feil i en tjener avhjelpes i løpet av en negativt eksponensialfordelt tid med middelverdi μ^{-1}. Feil avhjelpes i kun en tjener ad gangen.

d) Vis hvordan en kan finne funksjonssannsynligheten for tjenersystemet i dette tilfellet. Det kreves at nødvendige ligninger etableres, men ikke at de løses. Begrunn kort valg av fremgangsmåte.

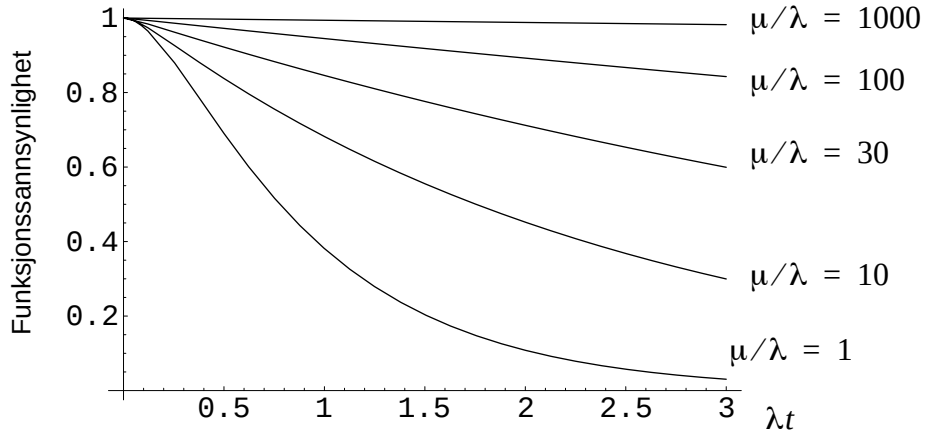
Løst gir ligningene følgende uttrykk for funksjonssannsynligheten

$$(r_1 e^{-r_2 t} - r_2 e^{-r_1 t})/\psi \tag{1.1}$$

hvor

$$r_1 = (5\lambda + \mu + \psi)/2$$
$$r_2 = (5\lambda + \mu - \psi)/2$$
$$\psi = \sqrt{\lambda^2 + 10\lambda\mu + \mu^2} = \mu + 5\lambda - 12\lambda^2/\mu + o(\lambda^2)$$

Grafisk fremstilt for noen parameterkombinasjoner gir dette Figur 1.2



Figur 1.2

e) Gi en fysikalsk forklaring på endringen i funksjonssannsynlighet når forholdet μ/λ øker. Som en del av dette:

- Forenkle (tilnærme) (1.1) ved å se på hvilke ledd og faktorer som får betydning når μ/λ blir stor. Gi en fysikalsk forklaring/interpretasjon av dette forenklede utrykket ut fra at μ/λ er meget stor og ut fra den modellen du brukte i punkt d).
- Jevnfør Figur 1.2 med det numeriske resultatet i punkt c) over og kommenter kort årsak til forskjell eller likhet.

Vi ønsker å ta hensyn til følgende i forbindelse med at reserven overtar funksjonene til en aktiv enhet som har feilet:

- Tiden fra en feil inntreffer til feilen er detektert, funksjonene til den feilte enheten er overført til reserven og denne er tilstandsmessig synkronisert med den andre utførende tjeneren, er en stokastisk variabel T_d. T_d er negativt eksponensialfordelt med forventning δ^{-1}, og påfølgende tider er uavhengig og identisk fordelte.
- Med en sannsynlighet $1 - c$ mislykkes prosedyren over selv om ingen nye feil inntreffer i denne perioden og systemet må startes på nytt. Tiden det tar å gjennomføre prosedyren er uavhengig av om den lykkes eller ikke. Å starte systemet på nytt tar en tid T_g som er negativt eksponensialfordelt med forventning γ^{-1}. Påfølgende tider er uavhengig og identisk fordelte.

Vi har at $\delta \gg \gamma > \mu \gg \lambda$ og $1 - c \ll 1$.

f) Vi ønsker å finne den asymptotiske utilgjengeligheten til systemet. Etabler et fullstendig tilstandsdiagram som kan benyttes til dette. Indiker hvilke tilstander som er arbeidende og hvilke som er feiltilstander.

Den asymptotiske utilgjengeligheten til systemet funnet ved hjelp av modellen i punkt f) kan uttrykkes som $U = s_1 / s_2$ hvor:

$$\begin{aligned} s_1 &= 12\gamma\delta\lambda^3 + 24\delta\lambda^4 + 6\gamma\delta\lambda^2\mu + 20\delta\lambda^3\mu - 8c\delta\lambda^3 + 4\delta\lambda^2\mu(1-c) \\ &\quad + 2\gamma\lambda\mu^3 + 2\delta\lambda\mu^3(1-c) + 4\lambda^2\mu^3 \\ s_2 &= 12\gamma\delta\lambda^3 + 24\delta\lambda^4 + 6\gamma\delta\lambda^2\mu + 20\delta\lambda^3\mu - 8c\delta\lambda^3 + 3\gamma\delta\lambda\mu^2 + 10\delta\lambda^2\mu^2 \\ &\quad + 4c\delta\lambda^2\mu^2 + \gamma\delta\mu^3 + 2\gamma\lambda\mu^3 + 2\delta\lambda\mu^3(2-c) + 4\lambda^2\mu^3 \end{aligned}$$

g) Vi ønsker å danne oss et bilde hva de enkelte parameterne betyr for utilgjengeligheten av systemet og finner fra ovenstående følgende tilnærmede sammenheng

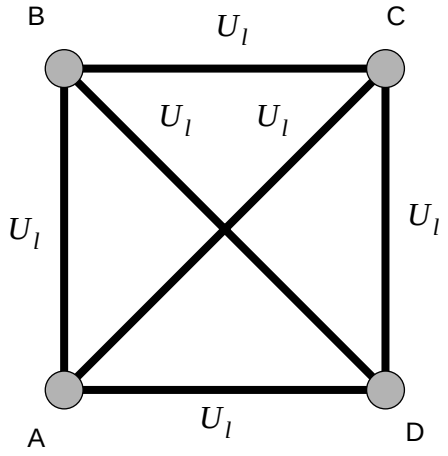
$$U \approx \frac{2\lambda}{\delta} + \frac{2\lambda(1-c)}{\gamma} + \frac{6\lambda^2}{\mu^2} \tag{1.2}$$

Vis hvordan (1.2) kan finnes fra det fullstendige uttrykket for U når vi tar hensyn til størrelsesforholdene mellom parameterne og at vi vil ha med de viktigeste bidragene hvor de ulike parametrene inngår. (Det ventes at dette vises ved en "formell" avledning.) Med utgangspunkt i (1.2) kommenter kort betydningen av de ulike parameterne kombinert med en fysikalsk fortolkning.

Oppgave 2

[Oppgaven tillegges 50% vekt]

I denne oppgaven betraktes et nett mellom fire steder A, B, C og D som illustrert i Figur 2.1. Vi antar i første omgang at alle lenkene har samme utilgjengelighet U_l og samme midlere tid mellom feil (MTBF), m, samt at de feiler og blir reparert uavhengig av hverandre. Nodene antas å være feilfrie.



Figur 2.1

Følgende pålitelighetskrav stilles til kommunikasjon (bæretjenesten) mellom to steder i nettet.

- I gjennomsnitt over et stort antall år skal det ikke være mer enn 100 minutt akkumulert nedetid per år.
- Gjennomsnittlig tid mellom feil skal ikke være mindre enn 4 måneder.
- Når kommunikasjonen mellom to steder feiler, skal feilen i gjennomsnitt være reparert (avhjulpet) i løpet av 3 timer.

a) Etabler uttrykk for og tegn et diagram som viser hvilke kombinasjoner av MTBF og MDT til bæretjenesten mellom to steder i nettet som imøtekommer pålitelighetskravene over. Anta at feilavhjelpingstiden er negativt eksponensial-fordelt. Hvor lang reparasjonstid må til for at 95% av feilene er korrigert?

b) Hva kalles den topologien som nettet i Figur 2.1 har? (Både norsk og engelsk term er akseptabel.) Angi kort (2-3 linjer) hvor i nettet denne topologien ofte anvendes?

c) Hva er utilgjengeligheten til bæretjensten mellom A og C når trafikken mellom disse to stedene kan rutes alle mulige veier gjennom nettet?

d) For å redusere kompleksiteten planlegges å benytte lenken AC som primærvei mellom A og C, og lenkene AD, DC som sekundær (reserve) vei. Hva blir nå utilgjeneligheten, MTBF og MDT til bæretjenesten mellom A og C?

Trafikkapasiten på lenkene og påtrykket trafikk mellom stedene A, B, C og D er som vist i Tabell 2.1.

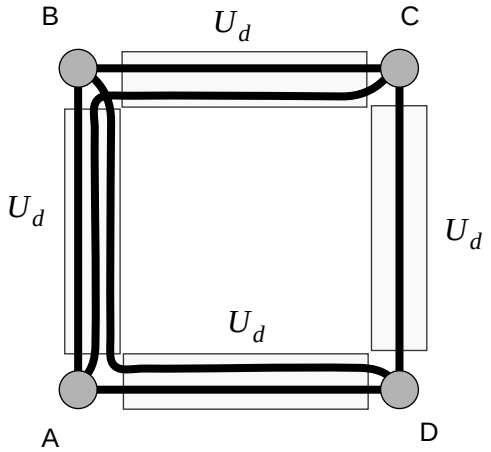
Tabell 2.1

Trafikk kapasitet på lenker [Gbit/s]					Tilbudt trafikk [Gbit/s]				
	A	B	C	D		A	B	C	D
A		10	10	10	A		2	8	2
B	10		10	10	B	2		2	8
C	10	10		10	C	8	1,5		8
D	10	10	10		D	2	8	8	

e) Vis hvordan en ved “back-up path” prinsippet kan definere veier (paths) i nettet slik at bæretjenesten kan opprettholdes mellom alle steder for alle enkeltlenkefeil i nettet. Hva er fordeler og utfordringer ved å benytte denne redundansstrategien i et nett?

f) Hva er sannsynligheten for at vi ikke har noen lenkefeil i nettet, en lenkefeil i nettet og mer enn en lenkefeil i nettet? Finn uttrykk for øvre og nedre grense for utilgjengeligheten av bæretjensten mellom A og C når en kun tar hensyn til den reduserte mengden feiltilstander hvor en har ingen eller en feil. Sammenlign med resultatene du fant i punktene c) og d), og kommenter.

Fysisk legges de seks lenkene i nettet Figur 2.1 langs fire traseer (kabelgrøfter) som vist i Figur 2.2. Utilgjengeligheten av lenkene er U_l som tidligere, men vi må i tillegg ta hensyn til feil assosiert med traseene som vil hindre trafikken på samtlige lenker som følger traseen. Traseene antas å feile og bli reparert uavhengig av hverandre.



Figur 2.2

g) Finn uttrykk for øvre og nedre grense for utilgjengeligheten av bæretjensten mellom A og C når vi tar hensyn til feil assosiert med kabeltrasene. Grensene bestemmes ut fra at betraker inntil en samtidig feil i systemet.