Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMEN I EMNE
TTM4120 PÅLITELIGE SYSTEMER

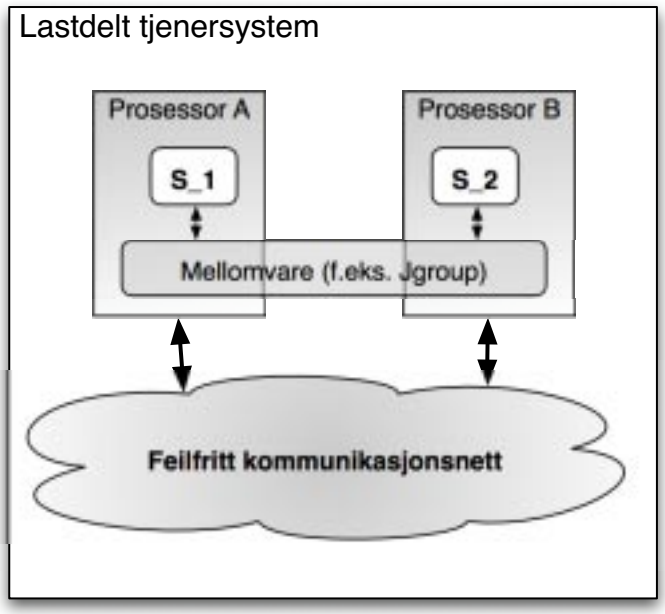
Faglig kontakt under eksamen: Bjarne E. Helvik
Tlf.: 92667

Eksamensdato:	24. mai 2005
Eksamenstid:	4 timer
Vekttall:	2,5 Vt
Tillatte hjelpemidler:	D
Språkform:	
Antall sider bokmål:	4
Antall sider nynorsk:	1
Antall sider engelsk:	0
Antall sider vedlegg:	0
Sensurdato[1]:	uke 24 - 2005

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.

BOKMÅLSUTGAVE

Vi har et lastdelt tjenersystem som vist i Figur 1 nedenfor. Tjenersystemet består av to prosessorer, A og B. På hver av disse kjører en tjenerprosess S. De to replikaene av tjenerprosessen, hhv. S_1 og S_2, kjører i lastdeling. Replikaene av tjenerprosessen bruker en mellomvare for synkronisering og er avhengige av denne for å fungere. Mellomvaren vil fungere selv om en prosessor feiler, og vil automatisk starte opp på den feilte prosessoren når den blir reparert.



Figur 1 Skisse av et lastdelt tjenersystem

Dette systemet er observert over en periode av varighet t_p. I løpet av denne perioden har systemet feilet og blitt "reparert" n ganger. Vi betegner oppetiden før i 'te feil for o_i, $i = 1, \ldots, n$ og den etterfølgende nedetiden d_i, $i = 1, \ldots, n$.

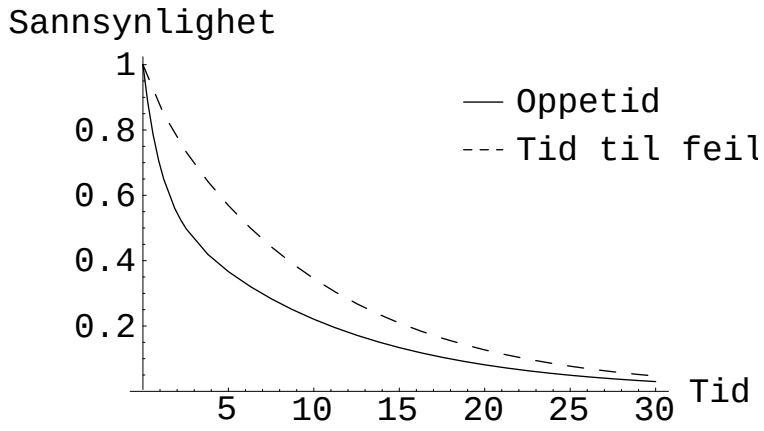
a) Etabler uttrykk for hvordan vi fra de observerte verdiene kan finne estimater for midlere tid mellom feil (MTBF), utilgjengeligheten (U) og den kumulative fordelingsfunksjon for oppetiden, $P(O \le o) = F_O(o)$.

Oppetidene antas å være uavhengige og identisk fordelte. Fordelingen kan beskrives ved funksjonen $F_O(t) = 1 - ge^{-\gamma t} - de^{-\delta t}$, hvor g og d kan interpreteres som sannsynlighetene for at oppetiden kommer fra en negativ eksponensialfordeling med forventning på hhv. γ^{-1} og δ^{-1}.

b) Finn et utrykk for midlere oppetid, MUT, gitt ved parametrene $\{g, d, \gamma, \delta\}$. Demonstrer at dersom vi starter å observere systemet på et tilfeldig tidspunkt mens det er oppe, så er sannsynligheten for tid til neste feil, T_F, gitt av

$$P(T_F > t) = R_r(t) = \frac{g\delta e^{-\gamma t} + d\gamma e^{-\delta t}}{d\gamma + g\delta} \qquad (1)$$

I Figur 2 er sannsynlighetene for at både oppetidene, T_U og tid til neste feil T_F plottet for parameterverdiene $\{g = 0.4, d = 0.6, \gamma = 1, \delta = 0.1\}$. Gi en forklaring på årsaken til forskjellen mellom de to kurvene.



Figur 2 Sannsynlighetene for at hhv. oppetid og tid til feil er lengre enn en gitt verdi.

Den observerte feilintensitet til systemet er for høy og en ønsker å bedre denne ved å endre driftsbetingelsene.

c) Hvilken lovmessighet antas det vanligvis å være mellom temperatur og maskinvarefeilintensitet/-rate. Kun hovedtrekkene i relasjonen kreves. Systemet er tidligere drevet ved to ulike temperaturer og det er observert prosessormaskinvarefeilintensiteter på hhv. α_1 og α_2. Begge disse er for høye. Finn den temperaturen systemet må drives ved for å bringe feilintensiteten ned til α_3. Nevn eventuelle usikkerhetsfaktorer knyttet til denne prediksjonen.

En prosessor (maskinvaren) har en konstant feilintensitet β. Et replika av tjenerprosessen har en konstant feilintensitet α, og mellomvaren har en konstant feilintensitet λ. Alle nevnte systemelementer feiler uavhengig av hverandre. Resterende systemelement, herunder kommunikasjonsystemet mellom replikaene antas feilfritt. Når mellomvaren eller en prosessor feiler, kreves en manuell aksjon, hhv. restart og reparasjon. Kun ett av disse systemelementene (mellomvaren og prosessorene) kan settes i drift ad gangen. Når en prosessor eller mellomvaren settes i drift startes tjenerprosessen som en del av dette. Tidene det tar å reparere og sette i drift en feilet prosessor er uavhengige og negativt eksponensialfordelt med forventning μ^{-1}. Tidene det tar å sette i drift mellomvaren etter den har feilet er uavhengige og negativt eksponensialfordelt med forventning ν^{-1}. Tjenerprosessene restartes automatisk dersom de feiler. Restarttidene er uavhengige og negativt eksponensialfordelt med forventning ξ^{-1}.

d) I første omgang betrakter vi kun maskinvaren i systemet og er interessert i å finne funksjonssannsynligheten for denne. Se bort fra feiling og restart av programvaren og sett opp en modell for maskinvaren og etabler ett fullstendig linkningssett for å bestemme $R(t)$.

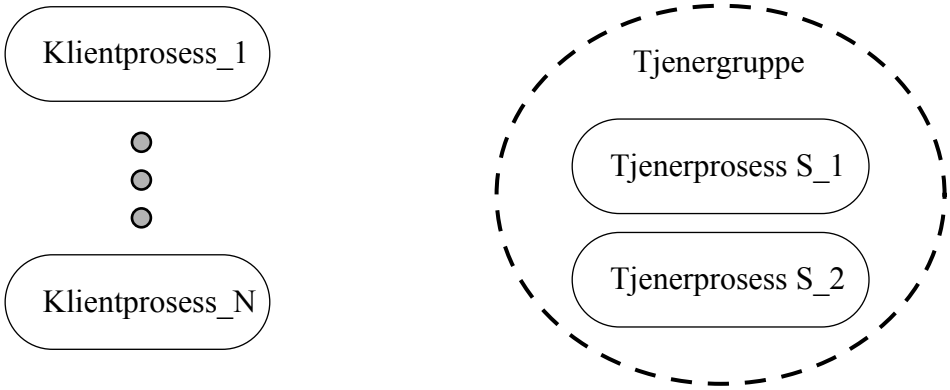
Løst gir ligningsettet $R(t) = (r_1 e^{r_2 t} - r_2 e^{r_1 t})/(r_1 - r_2)$ hvor

$r_1 = (-3\beta - \mu - \sqrt{\beta^2 + 6\beta\mu + \mu^2})/2$ og $r_2 = (-3\beta - \mu + \sqrt{\beta^2 + 6\beta\mu + \mu^2})/2$.

e) Vis at et eksakt uttrykk for midlere tid til første feil er $(3\beta + \mu)/(2\beta^2)$. Se på de tre spesialtilfellene, $\mu = 0$, $\mu \to \infty$ og $\beta \ll \mu$ og gi en fysikalsk forklaring på hvordan uttrykket for MTFF fremkommer i disse tre tilfellene.

f) Tegn et tilstandsdiagram for hele tjenersystemet. Det er ikke nødvendig å ekspandere tilstandsdiagrammet til mer enn at det to systemelement[1] som har feilet (ikke fungerer) samtidig. Utnytt symmetrier i systemet for å minimere antall tilstander. Angi tilstanden med hvilke elementer som har feilet, og indiker tydelig hvilke tilstander som er arbeidende og hvilke som er feiltilstander.

Anta at vi i tillegg til det som er vist i Figur 1 har et sett med klienter som kjører på prosessorer i tillegg til de som er vist på figuren. De to replikaene av tjenerprosessen S_1 og S_2 utgjør en gruppe tjener-objekter som vist i Figur 3 under. Klientene og tjenergruppen skal samarbeide ved hjelp av Jgroup. Anta at alle prosessene i figuren befinner seg på ulike prosessorer.



Figur 3 Hovedobjekter i klient-tjener systemet.

g) Introduser eventuelle elementer som er nødvendige (objekter som ivaretar funksjoner, maskiner/prosessorer, etc.) og angi kort og punktvis hvordan Jgroup settes opp for å klargjøre for kommunikasjon mellom klientene og tjenergruppen. (Vær tydelig på hvilke(n) prosessor(er) de ulike delene av mellomvaren befinner seg på.)

Tjenersystemet realiserer en offentlig nøkkel-infrastruktur (Public Key Infrastructure, PKI) og inneholder en database over alle gyldige offentlige nøkler. Anta her at databasen blir lagret i begge tjenerprosessene og at Jgroup brukes som mellomvare for å sikre at nøklene er tilgjengelige og at databasen er konsistent. En bruker som vil laste opp eller ned nøkler installerer et klientprogram på sin maskin.

Dersom en person ønsker å sende en epost til en annen person, og vil være sikker på at ingen andre enn mottakeren skal kunne lese innholdet, må senderen få tak i en gyldig kopi av mottakerens offentlige nøkkel (public key). Brukere gjør sin offentlige nøkkel tilgjen-

1. Systemelementene er: prosessorer, mellomvare, tjenerprosesser.

gelig for andre ved å publisere den vha. tjenersystemet. Dersom en nøkkel har blitt kompromittert, for eksempel fordi noen uvedkommende har fått tak i den private nøkkelen, må den kunne trekkes tilbake umiddelbart.

h) I Jgroup benyttes to typer metodekall (method invocation) på en gruppe, EGMI og IGMI. Forklar kort forskjellen på disse og hvorfor det er gunstig å skille mellom disse to typene metodekall. Hvilken type metodekall vil du bruke fra klient til tjenersystemet i ovennevnte eksempel? Beskriv med hvilken semantikk følgende metodekall fra klient til servergruppen utføres og gi en kort begrunnelse for valgene.
-Opplasting av egen offentlig nøkkel fra en klient til tjenergruppen.
-Nedlasting av offentlig nøkkel fra tjenergruppen.
-Tilbaketrekking (revocation) av nøkkel fra tjenergruppen.

NYNORSKUTGÅVE

For ikkje å få ulike semantikk i bokmål og nynorsk oppgåvetekst så er inga eige nynorsk oppgåvetekst laga. Sjå i staden bokmåloppgåve på side 2-5.

Ved problem ta kontakt med faglærar.