**Norwegian University of Science and Technology**
**Department of Telematics**



Contact during exam [Faglig kontakt under eksamen]:
Bjarne E. Helvik (92667)

EXAM IN COURSE [EKSAMEN I EMNE]
TTM4120 Dependable Systems [Pålitelige systemer]

Friday [Fredag] 2009-05-15
09:00 – 13:00

The English version starts on page 2.

Den norske bokmålsutgaven starter på side 8.

Hjelpemidler:
D - No printed or handwritten material is allowed. Predefined simple calculator [Ingen trykte eller håndskrevne hjelpemidler tillatt. Forhåndsbestemt enkel kalkulator]

Sensur 2009-06-09

## English version[1]

This exam deals with some dependability issues related to a simple peer-to-peer network, the nodes in the network and a service provided by the network. We focus on a service, which should be provided by $N$ nodes. The service is working (up) when at least $\lceil \frac{3}{4}N \rceil > 0^2$ nodes provide the service. If the service is provided by less than $N$ nodes, the network will install the service on a new node. This takes a negative exponentially distributed time with expectation $\theta^{-1}$. If more installations are needed, they take place one at a time. We may assume that there is always more than $N$ nodes in the network. A user of the service receives it from one of the nodes providing the service. If this node fails, the users will try to obtain the service from one of the other nodes providing the service. The nodes of the network have a churn, i.e., a node is switched off, or leaves the network, controlled by its operator/owner without failing, according to a Poisson process with intensity $\alpha$, and it is switched and/or or joins the network according to a Poisson process with intensity $\beta$. Note that a node may leave the network also when it is busy providing service to one or more users. When a node joins the network, the service must be reinstalled at the node if the node shall provide the service, irrespective of whether the node has provided the service before or not. Each node in the network fails according to a Poisson process with intensity $\lambda$ and is repaired independently with negative exponentially distributed repair times with expectation $\mu^{-1}$. When the repair of a node is finished, it is not immediately connected to the network.

**a)** The service is obtained from one specific node in the network. What is the probability that this service will continue uninterrupted for a time $\tau$? Motivate the answer. What is this property of the "system" denoted?

The node may stop providing service due to two simultaneously active Poisson processes, which yield a Poisson process with the compound rate $\alpha + \lambda$. Hence, the time to failure is n.e.d. and $\Pr(T > \tau) = \exp(-(\alpha + \lambda)t)$ where $T$ is the duration of uninterrupted service. The previous is denoted the *reliability function*and the ability to provide uninterrupted service is denoted *reliability*.

**b)** Establish an appropriate model of a node in the network, and find an *exact* expression for its asymptotic availability under the assumptions made above.

It is expected that the student understands that an Markov model is the appropriate for an exact solution. Model and solution in Figure1. Expected to be solved according to the standard methodology: 1) Balance equation or matrix combined with 2) normalization constant, yielding the result

$$\frac{\beta\mu}{(\alpha+\beta+\lambda)(\lambda+\mu)}$$

```
In[1]:= << "/Users/bjarne/Undervisning/ttm4120/tools/mma_state-diagrams/StateDiagrams.m"

In[2]:= Mtemp = {{, α, λ}, {β, xxx, λ}, {0, μ,}};

In[3]:= (Mx = SetDiagonal[Transpose[Mtemp]])//MatrixForm
```

Out[3]//MatrixForm=

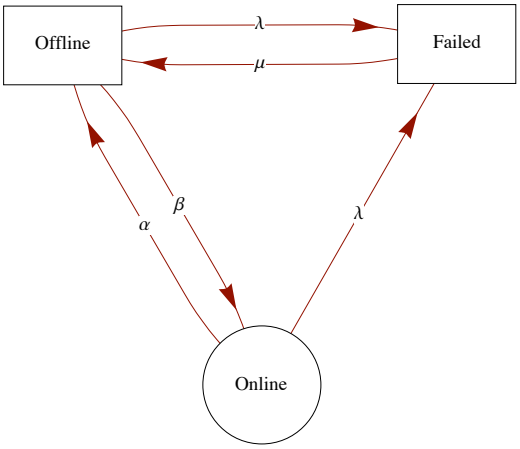
$$\begin{pmatrix} -\alpha-\lambda & \beta & 0 \\ \alpha & -\beta-\lambda & \mu \\ \lambda & \lambda & -\mu \end{pmatrix}$$

```
In[4]:= WorkingQ = {True, False, False};

In[5]:= Labels = {"Online", "Offline", "Failed"};

In[6]:= PlotDiagram[Mx, WorkingQ, Labels]
```

Out[6]=




```
In[10]:= A = ProbStationary[Mx][[1]] // Simplify
```

Out[10]=

$$\frac{\beta\,\mu}{(\alpha+\beta+\lambda)\;(\lambda+\mu)}$$

Figure 1: Mma solution of task b)

**c)** The nodes are assumed to have a crash failure semantic. Explain what is meant by this. Describe briefly the principles used in order to make the system providing the service tolerant to node failures. Is group or hierarchical switching used? Motivate the answer. Assume that the service relies on a common limited pool of resources, e.g. licences temporarily provided to the users of the service to download material from a scientific literature database. What is the main challenge in providing the service according to the principles you have described? Suggest briefly an approach to deal with this challenge.

*Crash failure semantic:*When it fails, it stops providing service. (No incorrect results provided, no untimely behaviour)

*Principle:*Load sharing with hierarchical failure switching.

*Hierarchical failure switching:* It is the user of the service that detects the failure and "selects" another server to get the service.

*Challenge:* To keep a consistent view of which resources that are available, to grant the various nodes providing the service permission to lease resources (licences) to its clients without performing multiple assignments and without creating unnecessarily high loads/delays in the system.

*Solution:* Using a group communication system (e.g. Jgroup or Spread/JaSoS) and a shared (dynamic) responsibility for subsets of the licences among the servers, similar to what was done in the Lab.

**d)** What is the minimum number of nodes $N$ that must provide the service in order to make it 1-fault tolerant, i.e. tolerant of a single node failure? Draw a Markov model (state diagram) that may be used to determine the availability of the service; annotate the diagram such that the configuration and whether the service is working (up) or not, is clearly shown. There is a certain probability that the service disappears from the network, i.e., no node provides the service. Describe *the procedure for* how we may find the distribution of the time, $T_{\text{Disappear}}$, until this happens.

To allow at least one node to fail without the service failing, we must have that $\lceil \frac{3}{4}N \rceil \leq N - 1 > 0$, and hence, $N = 4$.

The model is shown in Figure 2.

To determine the time to the service disappears from the system, the following steps is taken, similar to that of finding the Reliability function of the system (with at least one working server).

1. Referring to the model in Figure 2 of the system. Make the state where there is no provisioning of the service in the system absorbing, i.e., remove the "dashed transition" in the model.

[1] In case of divergence between the English and the Norwegian version, the English version prevails.
[2] Function giving the smallest integer larger than or equal to the argument.

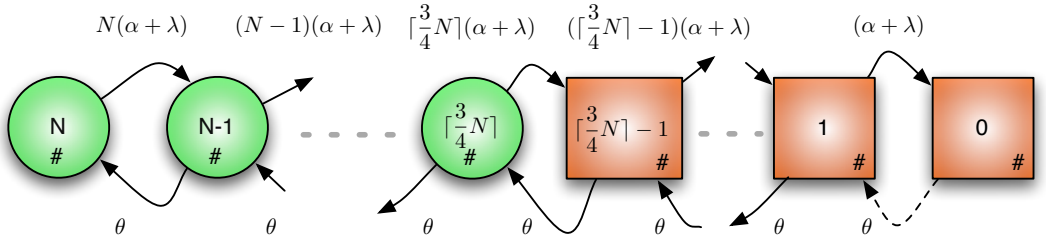



Figure 2: Model of a load shared group of nodes providing the service with failure, churn and activation of new servers in a P2P network.

2. Establish the transition matrix of the model, and the set of linear differential equations of the probabilities of being in the $N+1$ states.

3. Define the state with $N$ servers as the initial state, i.e., $p_n(0) = 1$. Solve the equations to find $p_i(t)$.

4. Then $\Pr(T_{\text{Disappear}} > t) = 1 - p_0(t)$.

The initial assumption was that the intensity of nodes leaving the system due to churn and failure was constant. However, it is suspected that this is not the case. Hence, the number of nodes that stops to provide service is recorded during 100 days. The accumulated number of nodes providing the service that have left the network at time $t$, is denoted $M(t)$. The result is shown in Figure 3, where $t$ is scaled in days. The first obervation is $M(1) = 6$ and the last is $M(100) = 147$.

**e)** Is the intensity of nodes stopping to give service increasing, constant or decreasing? Motivate the answer. If it is assumed that nodes leave according to an (in)homogeneous Poisson process, motivate and suggest a parametrised model for the intensity of this process. Make a rough, approximate estimation of the parameters of the model from the figure.

Decreasing. Dividing the observation interval into two, it is seen that there are approx. 100 "leaves" during the first 50 days and 50 during the next. This, combined with a monotone function, yields a decreasing rate.

It is seen that the observations form an almost straight line in a log-log plot. Hence, $\lg E[M(t)] = \lg Z[t] = a + b\lg(t)$ yielding $Z(t) = at^b$ may be an appropriate model for the cumulative failure intensity $Z(t)$. This model is called the *Duane model* (for reliability growth). The intensity is $z(t) = \frac{d}{dt}Z(t) = ab\,t^{b-1}$.

From the diagram we see that the straight line that may drawn through the observation points crosses the y-axes, i.e. at $\lg(t) = \lg(1) = 0$, at approximately $a = 10$. Similarly we see that $b = \frac{\lg(147)-\lg(10)}{\lg(100)-\lg(1)} = \frac{2.16-1}{2-0} = 0.58$[3].

[3]The data were generated with $b = 0.6$.

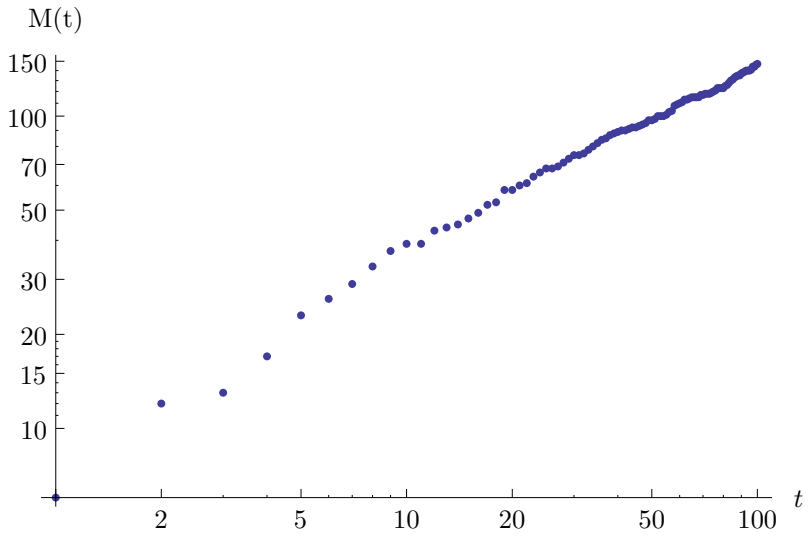



Figure 3: Plot of the accumulated number of node "failures" as a function of days of operation of the service. [Plott av akkumulert antall node"feil"som funksjon av antall døgn tjenesten har vært i drift.]

**f)** Maintain the assumption that nodes leave according to an (in)homogeneous Poisson process. Use the results found in e) to find the probability that no node stops to give the service during the 101'st day and the numerical value of the failure intensity in failures per hour at the start of the 101'st day.

The number of failures in $100 < t \leq 101$ is Poisson distributed. Hence the probability of no failures is $\exp(-Z(101) + Z(100)) = \exp(-10(101^{0.58} - 100^{0.58}) = 0.43$.

The failure intensity is derived in e). Hence, $z(100_+) = 10 \cdot 0.58 \cdot 100^{0.58-1}(\text{day})^{-1} = 0.84(\text{day})^{-1} = 0.034(\text{hour})^{-1}$.

There is a logical fault in a new version of the software providing the service which is introduced in the network. It does not influence the service given, but may cause the node to crash. Below we will investigate how this logical fault influences the dependability of the service. Figure 4 shows a simplified Markov model of a virtual node providing the service in the network. (After having "failed" a physical node will be replaced by another representing the same virtual node.)

**g)** Explain the following concepts: i) error latency, ii) error propagation (between nodes) and iii) fault dormancy. Assume that $\delta(s) = \delta_0$. What are the expected error latency and the expected fault dormancy related to the logical fault?

*i) error latency:* The time from a fault is activated and until it causes a failure, i.e. has propagated across the border of the node. If we let $\alpha + \lambda \to 0$, it is seen that the expected latency due to the error caused by the logical fault is $\phi^{-1}$.

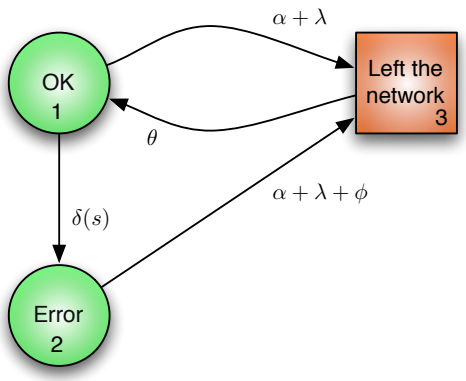



Figure 4: Markov model of a virtual node in the P2P network, subject to hardware and software failures as well as churn. [Markovmodell av en virtuell node i P2P nettet, med hensyntaken til maskinvare- og programvarefeil, såvel som "churn".]

*ii) error propagation (between nodes)* : An error is introduced into (transferred to) another node through interaction/co-operation (without the a fault in the receiving node being activated).

*iii) fault dormancy:*The time from a fault is introduced into the system and until it is activated and causes an error. In our case this is the time from the node commences to provide the service and until the "Ok -> Error" transition takes place, i.e. (if we let $\alpha + \lambda \rightarrow 0$) $\delta_0^{-1}$.

**h)** Suggest a model for $\delta(s)$, which also takes error propagation between nodes into account for a service provided by $N$ nodes. State the line of reasoning behind the model and define any notation that is used properly. For the case where $N = 2$ draw a complete Markov model of the service[4]. Make a proper annotation of the states and indicate whether the service is working (is up) or not.

$\delta(s) = \delta_0 + \delta_1 \cdot s$, where $0 \leq s \leq N$ is the number of nodes in the system that are in the Error state and have an error which may propagate. The intensity with which an error propagates from one node to another is $\delta_1$. It is assumed that there is at most one error in a node at a time.

See Figure 4 below for the model.

[4]Hint: The system consists of the virtual nodes providing the service.

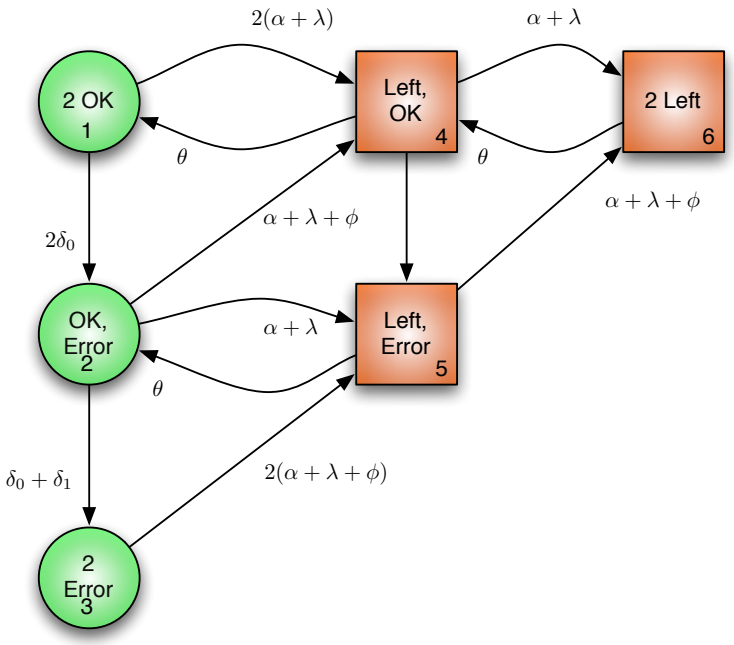



Figure 5: Markov model of the service provided by two nodes, logical fault and error propagation taken into account.

## Norsk bokmål utgave[5]

Denne eksamen omhandler noen pålitelighetsspørsmål knyttet til et enkelt peer-to-peer-nett, nodene i nettet, og en tjeneste som tilbys av nettet. Vi fokuserer på en tjeneste som skal tilbys av $N$ noder. Tjenesten fungerer (er oppe) når minst $\lceil \frac{3}{4}N \rceil > 0$[6] noder tilbyr tjenesten. Hvis tjenesten er levert av mindre enn $N$ noder, vil nettet installere tjenesten på en ny node. Dette tar en negativt eksponensialfordelt tid med forventning $\theta^{-1}$. Hvis flere installasjoner er nødvendig, foregår de én om gangen. Vi kan anta at det er alltid mer enn $N$ noder i nettet. En bruker av tjenesten får den levert fra en av nodene som tilbyr tjenesten. Hvis denne noden ikke leverers, vil brukerne prøve å få tjenesten fra en av de andre nodene som leverer tjenesten. Nodene på nettet har en "churn", dvs. en node blir slått av, eller forlater nettet, styrt av sin operatør/eier uten at noden feiler, ifølge en Poisson-prosess med intensitet $\alpha$, og det er slått og/eller kobles til nettet i henhold til en Poisson-prosess med intensitet $\beta$. Merk at en node kan bli koblet fra nettet også mens den leverer tjenester til en eller flere brukere. Når en node kobles til nettet, må tjenesten installeres på noden hvis den skal kunne tilby tjenesten uansett om noden har levert tjenesten tidligere eller ikke. Hver node i nettet svikter i henhold til en Poisson-prosess med intensitet $\lambda$ og blir reparert uavhengig av andre med en negativ eksponensial fordelt tid med forventning $\mu^{-1}$. Når reparasjonen av en node er ferdig, er den ikke umiddelbart

[5] I tilfelle uoverensstemmelse mellom den engelske og norske utgaven, er det den engelske som er gjeldende. Engelske betegnelser anvendes hvor ingen norsk oversettelse ble funnet.

[6] Funksjon som gir det minste heltallet større eller lik argumentet.

koblet til nettet.

**a)** Tjenesten hentes fra en spesifikk node i nettet. Hva er sannsynligheten for at denne tjenesten vil fortsette uavbrutt for en tid $\tau$? Begrunn svaret. Hva betegnes denne egenskapen til "systemet"?

**b)** Etabler en modell av en node i nettet som er hensiktsmessig mhp. å finne et eksakt uttrykk for dens asymptotiske tilgjengelighet, og finn dette eksakt uttrykket under forutsetningene gjort ovenfor.

**c)** Nodene antas å ha en krasjfeilsemantikk (Eng: crash failure semantic). Forklar hva som menes med dette. Beskriv kort prinsippene som brukes for å gjøre systemet som leverer tjenesten tolerant for nodefeil. Er gruppe eller hierarkisk svitsjing (Eng: group or hierarchical switching) benyttet? Begrunn svaret. Anta at tjenesten er avhengig av en felles begrenset pool av ressurser, f.eks. brukstillatelser midlertidig gitt til brukerne av tjenesten for å laste ned materiale fra en vitenskapelig litteraturdatabase. Hva er den viktigste utfordringen i å tilby tjenesten i henhold til de prinsipper du har beskrevet? Foreslå kort en måte å håndtere denne problemstillingen på.

**d)** Hva er det minste antall noder $N$ som må kunne tilby tjenesten for å få den 1-feiltolerant, dvs. kunne tolerere at en enkelt node feiler? Tegn en Markovmodell (et tilstandsdiagram) som kan brukes til å finne tilgjengeligheten til tjenesten; merk diagrammet slik at konfigurasjonen og om tjenesten fungerer (er oppe) eller ikke fremkommer tydelig. Det er en viss sannsynlighet for at tjenesten forsvinner fra nettet, dvs. ingen node tilbyr tjenesten. Beskriv *fremgangsmåten* for hvordan vi kan finne fordelingen av tiden $T_{\text{Disappear}}$, til dette skjer.

Den opprinnelige antakelsen var at intensiteten av noder som forlater systemet på grunn av "churn" og feil var konstant. Det er imidlertid mistanke om at dette ikke er tilfelle. Derfor er antall noder som slutter å gi tjenesten registrert i løpet av 100 dager. Akkumulert antall noder som tilbyr tjenesten som har forlatt nettverket ved tid $t$, betegnes$M(t)$. Resultatet er vist i figur 3, hvor $t$ er skalert i døgn. Den første obervasjonen er $M(1) = 6$ og den siste er $M(100) = 147$.

**e)** Er intensiteten av noder som slutter å levere tjenesten økende, konstant eller synkende? Begrunn svaret. Hvis det antas at noder forlater nettet i henhold til en (in)homogen Poissonprosess, motiver og foreslå en parametrisert modell for intensiteten i denne prosessen. Foreta et grovt, omtrentlig estimat av parametrene i modellen fra figuren.

**f)** Oppretthold at noder forlater nettet i henhold til en (in)homogen Poissonprosess. Bruk resultatene funnet i punkt e) til å finne sannsynligheten for at ingen node slutter å levere tjenesten det 101'ste døgnet, og den numeriske verdien av feilintensiteten i feil per time ved starten på det 101'ste døgnet.

Det er en logisk feil i en ny versjon av programvaren som leverer tjenesten, som er innført i nettet. Det påvirker ikke tjenesten som blir levert, men kan føre til at noder krasjer. Nedenfor vil vi undersøke hvordan denne logiske feilen påvirker påliteligheten av tjenesten. Figur 4 viser en forenklet Markovmodell av en virtuell node som tilbyr tjenesten i nettet. (Etter å ha "feilet", vil en fysisk node bli erstattet av en annen som representerer den samme virtuelle node.)

**g)** Forklar følgende begrep: i) "error latency", ii) "error propagation" (no: feil forplantning) (mellom noder) og iii) "fault dormancy". Anta at $\delta(s) = \delta_0$. Hva er de forventet "error latency" og forventet "fault dormancy" knyttet til den logiske feilen?

**h)** Foreslå en modell for $\delta(s)$ som også tar hensyn til feilforplantning mellom noder, for en tjeneste som tilbys av $N$ noder. Forklar resonnementet bak modellen og definer notasjonen som brukes. For tilfellet $N = 2$ tegn en fullstendig Markovmodell av tjenesten. Angi hvorvidt fungerer (er oppe) eller ikke i de ulike tilstandene og gi tilstandene en tydlig angivelse av den operasjonelle tilstand de representerer.