1 CTMC

For each of the scenarios below define a Continuous Time Markov Chain, by

1. identifying the states
2. identifying all activities that cause state transition
3. specify the state transition rate matrix Q
4. identify useful metrics of the system that you can express after having computing the equilibrium state probabilities of the system.

1.1 Intrusion Detection and Incident Response

A computer system is subject to attacks that attempt to compromise it. The system can be in one of four conditions:

Secure : The system is operating normally.

Compromised but undetected : An attacker has successfully compromised the system, but the defender is unaware of it.

Compromised and detected : The intrusion detection system has identified the compromise, but remediation has not yet been initiated.

Under recovery : The compromised system has been isolated and is being restored.

Assume:

- Successful compromises occur at rate λ when the system is secure.
- An undetected compromise is discovered after an exponentially distributed time with rate δ.
- he attacker may lose access spontaneously at rate γ, returning the system to a secure state.
- Once detected, the system enters recovery at rate μ.
- Recovery completes at rate ρ, returning the system to a secure state.

1.2 Distributed Denial-of-Service Attack Against a Web Service

A web service operates using C identical servers, each capable of processing one request at a time. Two classes of requests arrive:

- Legitimate requests arrive according to a Poisson process with rate λ_L.
- Malicious requests arrive according to an independent Poisson process with rate λ_A.

Legitimate request service times are exponentially distributed with rate μ_L, and malicious request processing times are exponentially distributed with rate μ_A.
There is no waiting room. A request arriving when all servers are busy is discarded.
A traffic-filtering mechanism independently identifies and rejects each malicious request with probability p, before it enters service. Legitimate requests are never rejected by the filter.

1.3 Moving-Target Defense and Attacker Reconnaissance

A computer system employs a moving-target defense that periodically changes its network configuration, such as IP addresses, service locations, or communication ports.
An attacker must first discover the current configuration before attempting exploitation.
The system has three states:

State 0 : The attacker does not know the current configuration.

State 1 : The attacker has discovered the configuration but has not compromised the system.

State 2 : The attacker has compromised the system.

Assume:

- Reconnaissance completes at rate λ_r.
- Once reconnaissance succeeds, exploitation succeeds at rate λ_e.
- The defender independently changes the configuration at rate μ_m
- A configuration change invalidates the attacker's reconnaissance information.
- If the system is already compromised, configuration changes do not remove the compromise.
- Compromised systems are detected and restored at rate μ_d. Restoration also changes the configuration.