IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/44AI/2024/4443424/
Vol. 2024 (22), Article ID 4443424

Summary of Stochastic Models 2024*

Jerzy Dorobisz

Affiliation e.g. Institute of Information Technology and Cyber-security,
Faculty of Cybernetics, WAT, 2 Gen. Sylwestra Kaliskiego St., 00-908 Warsaw

Correspondence should be addressed to: Jerzy Dorobisz, jerzy.dorobisz@wat.edu.pl

* Presented at the 44th IBIMA International Conference, 27-28 November 2024 Granada, Spain

Abstract

A probabilistic model is a mathematical tool for describing and analyse random phenomena. These models are widely used in cyber security, Why is it important for cyber security because it gives the possibility of forecasting, it also helps to predict future events, such as the time between attacks and the size of possible losses. The effectiveness of the various security measures is also a risk analysis: the various threats and their probabilities of occurrence, possible consequences, can be assessed. Optimisation : They help in deciding on the appropriate allocation of security resources, and they also allow the detection of various types of anomalies, of which there are more and more at this time. They also detect deviations from the normal behaviour of the system, which may indicate that various types of attacks are taking place. Probabilistic models are powerful tools in cyber security. These models give a better understanding of the complexity of threats and make informed decisions to protect ICT systems, as well as providing opportunities to implement forms of security . The introduction of randomness into mathematical models and computer algorithms is a very powerful and useful idea. It makes it possible to model uncertainty in the parameters of various models in science, engineering and economics. Reflects structural uncertainty. Reduces the complexity of existing models many deterministic problems can be solved more efficiently using probabilistic techniques. Stochastic models play a key role in modern cyber security, enabling prediction, analysis and risk management in dynamic and complex IT environments. The use of these models yields the development of more sophisticated and effective strategies to protect against everyday cyber threats.

Keywords: Stochastic Processes, Stochastic Volatility, Hidden Markov Models (HMMs), Monte Carlo Simulation, Stochastic Models;

Table of Stochastic Models in Cyber Security to 2024

Stochastic model	Description	Application
1. Markov Chains	State-based models, where the transition probability depends only on the current state.	Modelling of attacker behaviour, risk analysis, prediction of system failure.
2. Hidden Markov Models	Unfinished or perturbed observations in Markov chains.	Anomaly detection, network traffic analysis, identification of malicious activities.
3. Poisson Processes	Stochastic models describing random events.	Anomaly detection, network traffic analysis, identification of malicious activities.
4. Bayesian Networks	Probabilistic graphical models.	Anomaly detection, network traffic analysis, identification of malicious activities.

Cite this Article as: Jerzy Dorobisz, Vol. 2024 (22) "Summary of Stochastic Models 2024" Communications of International Proceedings, Vol. 2024 (22), Article ID 4443424, https://doi.org/10.5171/2024.4443424

5. Queuing Theory (Queuing Theory)	Workflow models in resource-constrained systems.	Network traffic management, resource optimisation, incident response modelling.
6. Monte Carlo Simulations (Monte Carlo Simulations)	Numerical methods with randomisation.	Analysis of attack scenarios, risk forecasting, incident response planning.
7. Game Theory	Mathematical models analysing strategic interactions between different actors.	Modelling of attacker-defender interactions, defence strategy, analysis of attacking behaviour.
8. Random Forests (Random Forests)	Algorithms machine learning with multiple decision trees.	Threat detection, network traffic classification, security breach prediction.
9. Hidden Semi-Markov Models (Hidden Semi-Markov Models)	An extension of the hidden Markov model, taking into account the duration of states.	Analysis of APT (Advanced Persistent Threats) attacks, modelling of long-term incidents.
10. Gaussian Mixture Models	Probabilistic models describing data as combinations of multiple Gaussian distributions.	Anomaly detection, classification of malicious activities, threat analysis.
11. Markov Decision Processes (Markov Decision Processes)	Probabilistic models describing data as combinations of multiple Gaussian distributions.	Security strategy optimisation, incident management, resource planning.
12. Time Series Analysis (Time Series Analysis)	Trended data modelling techniques.	Attack forecasting, security trend analysis, time anomaly detection.
13. Stochastic Differential Equations	Mathematical models describing the development of systems taking into account randomness.	Modelling the dynamics of security systems, predicting behaviour in IT systems.
14. Hidden Markov Decision Processes	A combination of hidden Markov models and decision-making processes in which states are hidden and decisions affect transitions.	Optimising decisions under uncertainty, APT defence strategy.

Stochastic process

Probabilistic models are more realistic than deterministic models. Observations at different points in time instead of at a fixed point in time introduced the new concept of indeterminism. Dynamic studies encompass the physical sciences, natural sciences, social sciences, engineering and management as phenomena that change over time. Stochastic processes are families of random variables that are functions of time. Stochastic process specification:

A stochastic process is a set of random variables indexed by some parameter, most commonly interpreted as time. In other words, it is a family of random variables whose values vary randomly over time.

Why is specification important?

Precise specification allows more accurate modelling of real-world phenomena, simulations and statistical inference to help predict future events and assess risk. Elements of stochastic process specification:

1. **Probabilistic space:**

   - ✓ Set of elementary events Ω
   - ✓ σ - event body F
   - ✓ Measure of probability P

2. **Collection of indexes T:**

   - ✓ This is usually a set of real numbers (continuous time) or natural numbers (discrete time).

3. **State space S:**

   - ✓ The set of values that a random variable can take at a given point in time.

4. **Family of random variables$(Xt)\ t \in T$:**
   - Each random variable Xt, takes values from the state space S and is defined on a probabilistic space (Ω, F, P) [7]

1. Markov Chains

- One special type of discrete time is a Markov chain. **Definition:** a discrete stochastic process is a **Markov chain** if for $t=0,1,2\ldots$ and all states $Px_t+I=i_t+I\left|X_t=i_t,X_t(I_t=i_t+l=l,i_t+l,\right|X_t=i_1=i_1,X_0)=i_t$

Essentially, this says that the probability distribution of a state at time $t+1$ depends on the state at time $t(i_t)$ and does not depend on the states the chain has passed through on its way to it at time t. In the study of Markov chains, we further assume that for all states i and j and for each t, $P(X_{t+1}=j|X_t=i)$ is independent of t.

Under this assumption, we can write $P(X_{t+1}=j|X_t=i)=p_{ij}$ where pij is the probability that the system is in state j at time $t+1$, assuming that it is in state i at time t.

The transition of the system from the state i in one period to the state j in the next period is called the transition from the state i to j.

The values p_{ij} are often referred to as transition probabilities for Markov chains. This equation means that the probability laws linking the state of the next period to the current state do not change over time.

This is often called the stationarity assumption, and a Markov chain that fulfils this is called stationary.

We also need to define q_i as the probability that the chain will be in the i state when 0. In other words, $P(X_0=i)=q_i$.

The vector $q=\left[q_1,q_2,q_{3,}\ldots q_s\right]$ is called the initial probability distribution of the Markov chain.

In most applications, the acquisition probability is expressed as an acquisition probability matrix $s\times s$. The takeover probability matrix P can be written as:

$$P=\begin{bmatrix} p_{11} & p_{12} & \ldots & p_{1s} \\ p_{21} & p_{22} & \ldots & p_{2s} \\ \vdots & & \vdots & \\ p_{s1} & p_{s2} & \cdots & p_{ss} \end{bmatrix}$$

for everyone I

$$\sum_{j=1}^{j=s} p_{ij} = 1$$

We also know that all entries of the matrix P must not be negative. Therefore, all entries in the capture probability matrix must be non-negative, and the entries in each row must add up to .1 [3]

Hidden Markov Models

Used when the state cannot be observed directly, suitable for noisy data .

Requirements: A finite number of states, each with an initial probability distribution. Probability of transition between states An observed phenomenon that can be generated randomly from the probabilities associated with the conditions.

States are designated as $S_1,\ S_2, \cdots S_n$

For a specific sample:

Let T be the number of observations

T is also the number of states through which it has passed

$O = O_1 O_2 \cdots O_T$ is a sequence of observations

$Q = q_1 q_2 \cdots q_T$ notation for the state path

Formal definition of HMM

HMM, λ is a 5-fold consisting of

N - number of states

M - number of possible observations

$\{\pi_1, \pi_2, \cdots \pi_N\}$ -Probability of initial state

$P(q_0 = S_i) = p_i$

$$\left.\begin{matrix} a_{11} & a_{22} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & & \vdots \\ a_{N1} & a_{N2} & & a_{NN} \end{matrix}\right\} \text{ Probability of change of state } P(q_{t+1} = S_i \mid q_t = S_i) = a_{ij}$$

$$\left.\begin{matrix} b_1(1) & b_2(2) & \cdots & b_1(M) \\ b_2(1) & b_2(2) & \cdots & b_2(M) \\ \vdots & \vdots & & \vdots \\ b_N(1) & b_N(2) & \cdots & b_N(M) \end{matrix}\right\} \text{Probability of observation } P\left(O_t = k \mid q_t = S_i\right) = b_i(k)$$

Assumptions: Branded

- ✓ States depend on previous states
- ✓ Assumption of stationarity
- ✓ Transition probabilities are independent of time ("memoryless")
- ✓ Output independence
- ✓ Observations are independent of previous observations

Three main questions about HMM:
Assessment:

a) What is the probability that the observations were generated by the model under consideration?

Decoding:

b) Given the model and the sequence of observations, what is the most likely state of the observations?

Learning:

c) Given a model and a sequence of observations, how should we modify the model parameters to maximise p {observation|model)?

Three main questions about HMM:

1. Evaluation

Given HMM M and the sequence x, FIND Sample $\left[x|M\right]$

2. Deciphering

Considering HMM M and the sequence x,

FIND a sequence of π states that maximises the $P\left[x, \pi|M\right]$

3. Learning

Considering HMM M, with unspecified transition/emission probabilities, and the sequence x,

FIND the parameters $\Theta = \left(b_i(.), a_{ij}\right)$ that maximise $P\left[x|\Theta\right]$

$P\left[x|M\right]$: The probability that sequence x was generated by model. Model is: architecture (states .) + parameters $\Theta = a_{ij}, e_j(.)$

So $P\left[x|\Theta\right]$ and $P\left[x\right]$ are the same when implying architecture and the whole model respectively.

Similarly $P\left[x, \pi \mid M\right]$ and $P\left[x, \pi\right]$ are the same

In the SCIENCE task we always write $P\left[x, \Theta\right]$, to emphasise which maximises $P\left[x, \Theta\right]$. [3]

Poisson processes

Let $N(t)$ be the number of events that occurred in the interval $\left[0, t\right]$.

The Poisson process with intensity $\lambda > 0$ is a stochastic process satisfying the following conditions:

1. $N(0) = 0$
2. For any t and S, where $t < S$, the difference $N(s) - N(t)$ is independent of) for $N(u)$ $dla\ u \leq t$ (independence of increments).
3. The number of events$(N + h) - N(t)$ over a short time interval h has a Poisson distribution with parameter λh :

$$P(N(t+h)-N(t)=k)=\frac{(\lambda h)^k}{k!}e^{-\lambda h},\quad k=0,1,2,\cdots$$

In particular, the number of events in the interval $[0,t]$ has a Poisson distribution with parameter : λt

$$P(N(t)=k)=\frac{(\lambda h)^k}{k!}e^{-\lambda h},\quad k=0,1,2,\cdots$$

Mean and variance

For a Poisson process with intensity λ the number of events $N(t)$ in the interval $[0,t]$ has:

- **Medium**: $E[N(t)]=\lambda t$
- **Variation:** $Var[N(t)]=\lambda t$

This means that the number of events increases linearly over time and the standard deviation increases with the square root of time. [4]

Bayesian Networks:

Bayes networks, also known as probabilistic networks, are graphical structures used to model complex probabilistic relationships between random variables. They represent causal relationships and facilitate analysis under uncertainty. They are used in areas such as artificial intelligence, data analysis, medicine and economics. Their structure consists of nodes representing random variables, directed edges and conditional probability tables (CPTs).

A Bayesian network B is defined as a pair $B=(G,P)$, where $G=(V,G)$, $A(G)$ is an acyclic directed graph with a set of vertices or nodes $V(G)=\{X_1,X_2,\cdots,X_n\}$

and the set of arcs $A(G)\subseteq V(G)\times V(G)$ where P is the joint probability distribution defined on the variables corresponding to the vertices .$V(G)$

A fundamental property of a Bayesian network is that the joint probability distribution$P\{X_1,X_2,\cdots,X_n\}$ is equivalent to the product of the (conditional) probabilities that are specified for the network;

Formally:

$$P=(X_1,X_2,\cdots,X_n)=\pi_{i=1}P(X_i|Parents(X_i))$$

Where (X_i) is the set of parents of the vertex corresponding to the variable X_i

Thus, $P(X_i|(X_i))$ are (conditional) probability distributions that are defined

for the variable X_i for$i=1,\cdots,n$ when creating a Bayesian network. [7]

Queue theory

Queuing theory is the science that deals with the analysis of queuing systems, where customers come in, wait to be served and are served by a server. It has applications in various fields such as engineering, computer science, management and logistics. In network security, it allows to model processes such as handling requests, detecting and neutralising attacks and controlling traffic flow. The mathematical M/M/1 model can be used to analyse network security, taking into account the arrival of requests and their handling time. This model allows the network to be properly monitored and securing the network against various threats. The server busy indicator (system load) is:

$\rho=\frac{\lambda}{\mu}$where ρ is the average server load.

Analytical formulae in the M/M/1 model:

Average number of requests per system :(L)

$$L = \frac{\lambda}{\mu - \lambda} = \frac{\rho}{1 - \rho}$$

Average number of requests per queue : $\left(L_q \right)$ **[2]**

$$L = \frac{\lambda^2}{\mu(\mu - \lambda)^2} = \frac{\rho^2}{1 - \rho}$$

Average waiting time for service : $\left(W_q \right)$

$$W_q = \frac{\rho^2}{\mu(1 - \rho)}$$

The probability that the system is empty:

$$P_0 = 1 - \rho$$

Probability that the system is full (in a capacity-constrained model): For capacity-constrained systems, e.g. the M/M/1/K model, the probability that the system is full is particularly important as it indicates how often the system rejects requests.[1]Monte Carlo simulations

Simulation is the imitation of a real process or system over time. To carry out modelling and simulation, a model approximating an event must first be created. The model is then simulated, allowing for multiple observations. Simulations are followed by analysis to help draw conclusions and make decisions. Simulation is defined as a method using a sequence of random numbers and a statistical simulation technique. Monte Carlo simulations are useful for analysing systems with high complexity and uncertainty, such as cyber security. They involve running a large number of trials to assess risk and predict outcomes.

Monte Carlo methods:

When calculating properties of statistical models, it is often necessary to calculate, in the multidimensional state space D, integrals of the form:

$$I = E_{x \sim \pi}[f(x)] := \int_D f(x)\, \pi(x)\, dx$$

Why do we need Monte Carlo methods? Suppose $D = [0, 1]^d$ and that we want to apply numerical quadrature.

Select a grid of grid points in the state space, with grid size h

Calculate$f\left(x_i \right) \pi\left(x_i \right)$ for each grid pointx_i .

Apply the quadrature scheme to approximate the integral.

Monte Carlo methods

However, let us assume that we can generate samples: $x_1, x_2, \cdots$ with a π distribution.

Then, using the law of large numbers (LLN), we have

$I_N := \frac{1}{N} \sum_{i=1}^{N} f\left(x_n \right) \xrightarrow{N \to \infty} \mathbb{E}[f(x)]$ almost certainly, so we can approximate I by

I_N! The coefficient of convergence is: $O\left(N^{-\frac{1}{2}} \right)$. This means that [8]

Game Theory

Game theory in cyber security is an analytical approach that describes the interactions between attackers and defenders as games with specific strategies, costs and rewards. By doing so, the decisions of both parties can be better understood and predicted, leading to more effective defensive strategies and risk management. Examples of game theory applications in cyber security include attack and defence modelling, DDoS threat analysis, vulnerability management and protection against phishing and social engineering. Different types of games can be used in cyber security, such as one-off, recursive, zero-sum and asymmetric games. Asymmetric games, where players have different resources and capabilities, are particularly useful in modelling real-world threats, as the defender has a limited budget and the attacker has different attack techniques. Through game theory, companies can better understand the risks of of cyber attacks and develop more effective defence strategies. [11]

Random Forests

Random Forests is a machine learning algorithm that uses a set of randomly generated decision trees. Random forests can effectively detect anomalies and classify patterns even with complex and multidimensional data. Random Forests are used in intrusion detection systems due to their high performance and resistance to overfitting. Random Forest has applications in cyber security. Random Forest is used to classify network traffic as normal and malicious. The algorithm can search for deviations from normal in traffic patterns. Random Forest is used to classify files according to their characteristics. System behaviour, signatures and file structure are related. The model is more robust to changing techniques due to the random selection of features. Random Forest can be used to analyse system logs to look for unusual user or device behaviour that may indicate intrusion attempts. Network traffic can be divided into legitimate and illegitimate packets using network traffic classification. It can be used to identify applications and services based on traffic patterns. Phishing protection: Random Forest can be used to identify suspicious emails based on their characteristics. [5]

Hidden Half Markov Models(Hidden Markov Models)

Hidden Markov models (HMMs) are used in cyber security analysis to model sequential events when full system information is not available. They consist of hidden and observable states, allowing analysis of network traffic patterns and user behaviour. They can be used to analyse malware behaviour, detect botnets and C2 servers, and analyse data flows. Examples of threats that can be detected using HMM include brute-force attacks, unusual network activity and changes in user behaviour. HMM's modelling of malware behaviour sequences and botnet communication patterns supports automatic detection and response to differences in data flow during an attack.

HMM, consists of a discrete-time and discrete-state Markov chain with hidden states $\{1, \cdots, K\}$ and an observation model $p(xt|zt)$

$$p\left(Z_{1:T}, X_{1:T}\right) = p\left(Z_{1:T}\right) p\left(X_{1:T} | Z_{1:T}\right) = \left[p\left(z_1\right) \prod_{t=2}^{T} p\left(z_t | z_{t-1}\right)\right]\left[\prod_{t=1}^{T} p\left(x_t | z_t\right)\right]$$

Observations in the HMM model can be discrete or continuous.

If they are discrete, a common case is an observation model in the form of an observation matrix:

$$p\left(x_t = l | z_t = k, \Theta\right) = B(k, l)$$

If observations are continuous, a common model for observations is the conditional Gaussian distribution:

$$p\left(x_t = l | z_t = k, \Theta\right) = \mathcal{N}\left(x_t | \mu_k, \sum_k\right)$$

HMM models can be used as black-box density models in sequences . They have the advantage over Markov models in that they can represent long-term relationships between observations.[7]

Gaussian mixture models

Gaussian Mixture Models (GMMs) are often used in cyber security for anomaly detection, network traffic clustering and user behaviour analysis. GMM models data as a combination of multiple Gaussian distributions,

enabling flexible and efficient pattern recognition. The EM algorithm is used to estimate GMM parameters through optimisation. Anomaly detection is based on the identification of abnormal data using the GMM.

GMMs are flexible in analysing complex data, feature a probabilistic approach and allow unsupervised learning from unlabelled data. They are an ideal tool for analysing network traffic and user behaviour in cyber security. GMM: a weighted sum of multiple Gaussians, where the weights are determined by the distribution:

$$p(x) = \pi_0 N\left(x|\mu_0, \sum_0\right) + \pi_1 N\left(x|\mu_1, \sum_1\right) + \cdots + \pi_k N\left(x|\mu_k, \sum_k\right)$$

Where: $\sum_{i=0}^{k} \pi_i = 1$

$$p(x) = \sum_{i=0}^{k} \pi_i N\left(x|\mu_k, \sum_k\right)$$

GMM representation involving a latent variable:

$$p(x) = \sum_{i=0}^{k} \pi_i N\left(x|\mu_k, \sum_k\right) = \sum_z p(z)\, p(x|z)$$

$$p(z) = \prod_{k=1}^{K} \pi_k^{z_k} \qquad p(x|z) = \prod_{k=1}^{K} N\left(x|\mu_k, \sum_k\right)^{z_k}$$

Markov Decision Processes

Markov Decision Processes (MDPs, or Markov Decision Processes) provide a mathematical model to help make optimal decisions in situations of uncertainty. In such cases, the outcome of each decision depends on the current state of the system and random factors. In the context of cyber-security, MDPs are used to create protection, risk management and response strategies, enabling the analysis of different scenarios and the selection of the most effective actions.

Applications of MDP in cyber security

The Markov Decision Process (MDP), characterised by a stepwise S, A, T, R

S a set of states,

A set of actions

$T: S \times A$ transition function

$R: S \times A$ reward function

The Markov Decision Method (MDP) allows defence strategies to be optimised to minimise the risk of attacks and costs. With MDP, the system can react dynamically to incidents, analyse risks and select effective actions, such as blocking suspicious network traffic or forwarding cases to the security team. Modelling of advanced persistent threats (APTs) allows the creation of effective defence strategies. Risk analysis, resource allocation and the use of appropriate algorithms are key to successfully optimising defence strategies.

4. Time series analysis

Time series analysis uses statistical methods to understand and predict quantitative variables. It helps organisations make data-driven decisions, increase productivity and effectively adapt to changing conditions.

Why analyse time series data?

a) Graphical and numerical summary: Displays point data over time.
b) Interpretation of series characteristics: analyses patterns such as seasonality, trends and links to other data series.

c) Forecasting: Predicts the future values of a series, e.g. at times $t+1, t+2, \cdots t+n$

d) Hypothesis testing and simulation: comparing different scenarios to assess outcomes.[12]

5. Stochastic Differential Equations

A stochastic differential equation is a differential equation whose coefficients are random numbers or random functions of the independent variable(s). As in normal differential equations, the coefficients should be given independently of the solution to be found.

Differential equation of the form:

$$dX = \mu(t, X(d))\, dt + \sigma(t, X(t))\, dB(t)$$

for given functions a and b and Brownian motion $B(t)$. A function (or path) X is a solution of the above differential equation if it satisfies the following conditions

The general form of the stochastic differential equation is as follows [13]

$$X(T) = \int_0^T \mu(t, X(t))\, dt + \int_0^T \sigma(t, X(t))\, dB(t)$$

Hidden Markov Decision Processes

Markov models describe the evolution of randomly varying systems based on the based on the basic Markov assumption, which states that the future states of a system, given the current state, are independent of past events. Depending on whether the state is fully observable or not and whether the system is controlled or not, Markov models are

Autonomous systems: Markov chains (if the state is fully observed) and HMM (if the state is partially observed).

Controlled systems: Markov decision processes (if the state is fully observable) and partially observable MDPs or POMDPs (if the system state is partially observable).

HMMs correspond to partially observable Markov processes of the form$(X, Y) = \left\{\left(x_n, y_n\right)\right\}_{n \in Z_+}$ for which only one of the two components is (fully) observable. The main purpose of these models is to formalise the statistical inference configuration for the hidden (unobservable) component of a given Markov process based on the full observation of the remaining component.
The hidden (unobservable) component X is called a signal (or state or plant), and statistical analysis inference, which is based on the observed realisation Y , which corresponds to the observable component of the Markov process(X, Y) .[14]

Literature

- Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. New York: Springer.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- Ghamizi, M., Dhouib, A., & Ben Ayed, D. (2021). *Markov Chains and Hidden Markov Models in Network Intrusion Detection*. *Journal of Cybersecurity Research*, 5(3), 120-136.
- Poisson, S. D. (1837). *Recherches sur la probabilité des jugements*. Bachelier.
- Montgomery, D. C., Jennings, C. L., & Kulahci, M. (2015). *Introduction to Time Series Analysis and Forecasting*. Wiley.
- Russell, S. J., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson.
- Papoulis, A., & Pillai, S. U. (2002). *Probability, Random Variables, and Stochastic Processes*. McGraw-Hill.
- Ghosh, D., & Reilly, D. (2019). *Monte Carlo Simulation and Finance*. Cambridge University Press.
- Sammut, C., & Webb, G. I. (2017). *Encyclopedia of Machine Learning and Data Mining*. Springer.
- Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing*. Pearson.
- Luce, R. D., & Raiffa, H. (1989). *Games and Decisions: Introduction and Critical Survey*. Dover Publications.

- Koller, D., & Friedman, N. (2009). *Probabilistic Graphical Models: Principles and Techniques*. MIT Press.
- Norris, J. R. (1997). *Markov Chains*. Cambridge University Press.
- ECE 586 - Markov Decision Processes and Reinforcement Learning Hidden Markov Models, Partially Observable Markov Decision Processes and Linear Quadratic Regulation Dimitrios Katselis Acknowledgment: R. Srikant's Notes and Discussions