39Mathematical Model IIDoc-Start

Mathematical models for Security

Dr. A.Balu
Department of Cyber Security
IIIT Kottayam

balu@iiitkottayam.ac.in

June 6, 2023

Overview

- Mathematical Model I
- Mathematical Model II

Mathematical Models for Security

- **Cryptography:** Mathematical models such as modular arithmetic, number theory, and finite fields are fundamental to encryption algorithms, digital signatures, secure key exchange protocols, and other cryptographic techniques.
- **Access Control Models:** Access control models, such as the Bell-LaPadula model and the Biba model, use mathematical concepts to define and enforce security policies. These models establish rules and mechanisms for managing and controlling access to resources based on user permissions, clearance levels, and security levels.
- **Intrusion Detection Systems (IDS):** Mathematical models are used in IDS to detect and identify abnormal or malicious activities. Techniques such as anomaly detection algorithms, statistical analysis, and machine learning models are employed to analyze network traffic, system logs, and other data sources to identify potential security breaches.

Mathematical Models for Security

- **Game Theory:** Game theory models strategic interactions and decision-making in security scenarios. It is used to analyze conflicts between attackers and defenders, assess optimal defense strategies, and understand the incentives and behaviors of different entities in security-related contexts.
- **Queuing Theory:** Queuing theory is used to analyze the behavior of systems with queues, such as network traffic or service requests. It helps in understanding performance characteristics, resource allocation, and capacity planning in security systems.

Mathematical Models for Security

- **Formal Methods:** Formal methods, such as formal verification and model checking, use mathematical techniques to rigorously analyze and verify the correctness and security properties of software and systems. These methods help identify vulnerabilities, ensure system integrity, and prevent security flaws.
- These are just a few examples of how mathematical models are utilized in security. There are numerous other mathematical models and techniques employed in different security domains, including network security, system security, data privacy, and threat intelligence.

Model I

- A.M Del Rey " Mathematical modeling of the propagation of malware a review", Security and Communication Networks. vol8 no 15 pp 2561-2579, 2015.

Model I

- **The Classical SIR model**
- **SIR** (Susceptible/Infected/Recovered) model is used in the field of Epidemiology, for the analysis of communal diseases, which spread from an infected individual to a population.
- Divide the population into the separate groups of Susceptible **(S)**, Infected **(I)** and those who recovered or become immune to a type of infection or a disease **(R)**.
- A total population of size N is thus divided into three stages or compartments:

$$N = S + I + R \tag{1}$$

The Classical SIR model

- Since the population is going to change with time t, we have to express these stages as a function of time. S(t), I(t), R(t).
- β (infection rate) and α(recovery rate) are the transition rates between $S \rightarrow I$ and $I \rightarrow R$ respectively are both in [0,1]
- SIR model is homogeneous, means everybody makes contact with each other randomly.
- It can be captured with the following differential equations :

$$\frac{dS}{dt} = -\beta IS \qquad (2)$$

$$\frac{dI}{dt} = \beta IS - \alpha I \quad (3)$$

$$\frac{dR}{dt} = \alpha I \qquad (4)$$

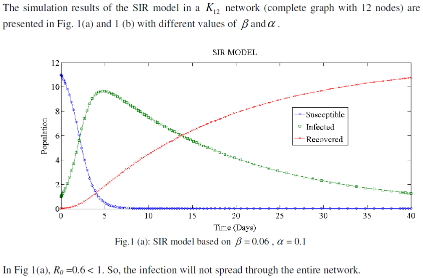
- a basic reproduction rate as

$$\mathrm{R}_0 = \frac{\beta}{\alpha} \qquad (5)$$

The Classical SIR model

- R_0 is a useful parameter to determine if the infection will spread through the population or not.
- If $R_0 > 1$ the infection will be able to spread in a population, to a stage that is called Endemic Equilibrium .
- If $R_0 < 1$, infection will die out in the long run. This is called disease free equilibrium .

The Classical SIR model



The simulation results of the SIR model in a K_{12} network (complete graph with 12 nodes) are presented in Fig. 1(a) and 1 (b) with different values of β and α .

Fig.1 (a): SIR model based on $\beta = 0.06$, $\alpha = 0.1$

In Fig 1(a), R_0 =0.6 < 1. So, the infection will not spread through the entire network.

Figure: Simulation result of the SIR model with a small complete network

The Classical SIR model

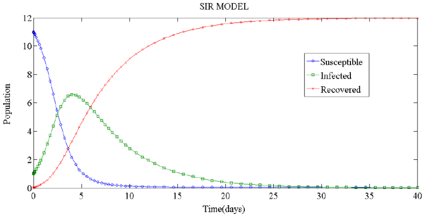


Fig. 1 (b): SIR model based on $\beta = 0.1$, $\alpha = 0.2$

Figure: Simulation result of the SIR model with a small complete network

The Classical SIR model

The Classical SIR model

- In Fig 1 , $R_0 = 0.6 < 1$, So the infection will not spread through the entire network
- In Fig 2, $R_0 = 2 > 1$, in this case, infection will spread to most of the nodes and the network will be in an endemic stage.

SEIRS Model

- A network with a scale free distribution of the node connectivity degrees
- Possible re-infection and the time delay incurred during incubation(between exposition and infection)
- An additional stage(Exposed) in the model represents the phenomenon of incubation, leading to delay between susceptibility to infection and actual infection.

SERIS Model

- N(t) Total population size
- S(t) Susceptible population
- E(t) Exposed Population
- I(t) Infected population
- R(t) Recovered population
- β Birth rate
- ν Death rate due to causes other infection
- ϵ Death rate due to virus
- γ average number of contacts of a node
- ωtime delay
- τ period of temporary immunity
- p probability of temporary immunity

SERIS Model

- N(t)= S(t)+I(t)+E(t)+R(t)

$$\frac{dS(t)}{dt}=\beta N(t)-\mu S(t)-\gamma\frac{S(t)I(t)}{N(t)}+\alpha I(t-\tau)e^{-\mu\tau}$$

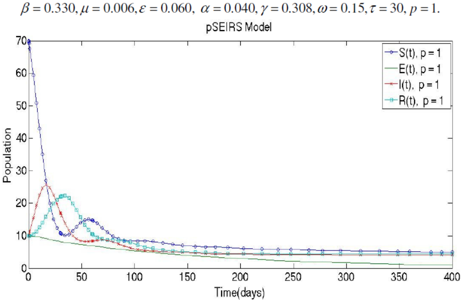
$$E(t)=\int_{t-\omega}^{t}\gamma\frac{S(x)I(x)}{N(x)}e^{-\mu(t-x)}\,dx,$$

$$\frac{dI(t)}{dt}=\gamma\frac{S(t-\omega)I(t-\omega)}{N(t-\omega)}e^{-\mu\omega}-(\mu+\varepsilon+\alpha)I(t),$$

$$R(t)=\int_{t-\tau}^{t}p\alpha I(x)e^{-\mu(t-x)}\,dx.$$

$$R_0=\frac{\gamma e^{-\beta\omega}}{\varepsilon+\beta+\alpha}\ .$$

SEIRS model


$\beta = 0.330, \mu = 0.006, \varepsilon = 0.060, \alpha = 0.040, \gamma = 0.308, \omega = 0.15, \tau = 30, p = 1.$
pSEIRS Model
S(t), p = 1
E(t), p = 1
I(t), p = 1
R(t), p = 1
Population
0
10
20
30
40
50
60
70
Time(days)
0
50
100
150
200
250
300
350
400

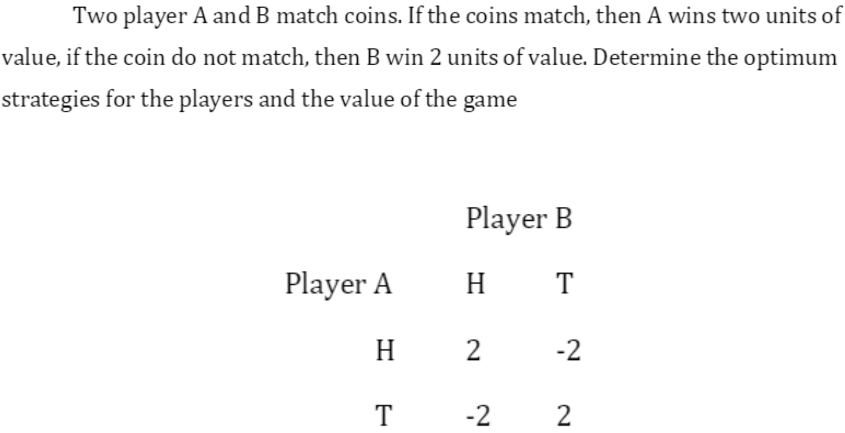
Model II

- A. Attiah, Mainak Chatterjee, Cliff C.Zou, ”A Game Theoretic Approach to Model Cyber Attack and Defense Strategies”

Game Theory Fundamentals

- **Zero- Sum Game** Algebraic sum of gain and loss is zero
- **Two Person Zero Sum Game** A game with only two players in which the gain(loss) of one player is exactly to the loss(gain) of the other
- **Pay-off matrix** In a two person zero-sum game, the resulting gain can be expressed in the form of a matrix is called pay-off matrix
- **Strategy** Strategy of a player is the pre-determined rule by which a player decides his course of action from his own list of courses of action during the game.
- **Pure Strategy** It is a decision in advance of all plays will to choose a particular course of action
- **Mixed Strategy** It is a decision in advance of all plays to choose a course of action for each play with respect to some probability distribution

Game Theory Fundamentals



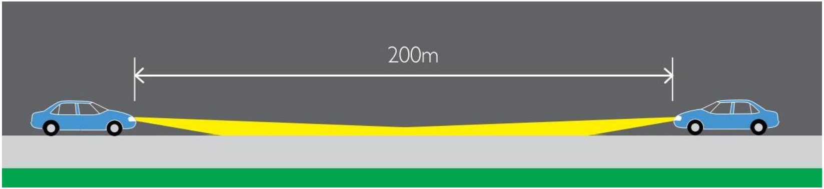
Two player A and B match coins. If the coins match, then A wins two units of value, if the coin do not match, then B win 2 units of value. Determine the optimum strategies for the players and the value of the game

	Player B	
Player A	H	T
H	2	-2
T	-2	2

Chicken Game

- The Chicken Game, also known as the Hawk-Dove game, is a classic game-theoretic scenario that illustrates the dynamics of a conflict where both parties face a choice between risky aggression and peaceful cooperation.
- The game derives its name from a metaphorical situation where two drivers are heading towards each other and must decide whether to swerve or continue driving straight, risking a potential collision.
- In the Chicken Game, there are two players who simultaneously choose between two strategies: "Swerve" or "Straight."
- The payoffs associated with different outcomes determine the players' preferences. The four possible outcomes and their associated payoffs are as follows:

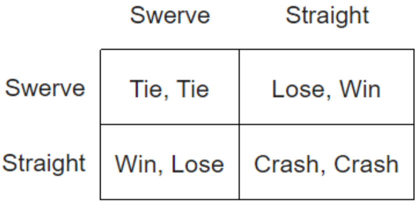
Chicken Game



Chicken Game

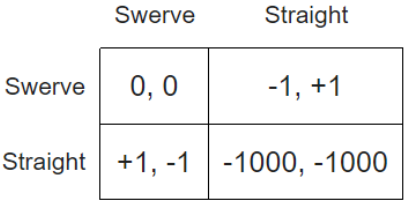
- Both players choose "Swerve": Both players avoid conflict, resulting in a low-risk outcome with a moderate payoff for each player.
- Both players choose "Straight": Both players engage in aggression or continue on their current course, leading to a high-risk outcome with a negative payoff for both players.
- One player chooses "Swerve" while the other chooses "Straight": The player who swerved is seen as weaker or less aggressive, resulting in a negative payoff for that player, while the player who went straight achieves a positive payoff for their perceived dominance.

Chicken Game



	Swerve	Straight
Swerve	Tie, Tie	Lose, Win
Straight	Win, Lose	Crash, Crash

Fig. 1: A payoff matrix of Chicken



	Swerve	Straight
Swerve	0, 0	-1, +1
Straight	+1, -1	-1000, -1000

Fig. 2: Chicken with numerical payoffs

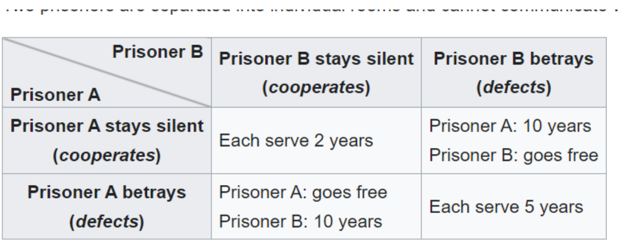
Prisoner’s Dilemma

- The prisoner’s dilemma is a thought experiment in game theory that shows why two completely rational individuals might not cooperate, even if it appears that it is in their best interests to do so.
- The classic prisoner’s dilemma is as follows:
- Two suspects are arrested for a crime.
- The police do not have enough evidence to convict either suspect.
- The police interrogate each suspect separately and offer each suspect a deal:
- If you confess and your partner does not, you will go free and your partner will get 10 years in prison.

Prisoner's Dilemma

- If you do not confess and your partner does, you will get 10 years in prison and your partner will go free.
- If you both confess, you will both get 5 years in prison.
- The best outcome for both suspects would be to cooperate and remain silent.
- If they both cooperate, they will each get 2 year in prison.
- However, the best outcome for each individual suspect is to defect and confess.
- If one suspect defects and the other cooperates, the defector will go free and the cooperator will get 10 years in prison.

Prisoner's Dilemma



Two prisoners are separated into individual rooms and cannot communicate .

Prisoner B Prisoner A	Prisoner B stays silent (*cooperates*)	Prisoner B betrays (*defects*)
Prisoner A stays silent (*cooperates*)	Each serve 2 years	Prisoner A: 10 years Prisoner B: goes free
Prisoner A betrays (*defects*)	Prisoner A: goes free Prisoner B: 10 years	Each serve 5 years

Game Model

- Let G = {N, S, U}, where N= {A,D} represents the two players : Player A is a malicious-node/ attacker and the other player D is a defender.
- S $= \{a_0, a_1, d_0, d_1\}$
  is the strategy space, which is the set of actions that are available for each player, and their utilities are given by U.
- a_0 = No attack a_1 = Attack
- d_0= No defend
- d_1= Defend
- We assume that the value of the protected assets by the defender D is worth of $\omega_n > 0$, ω_1 is the value of the assets compromised by Attack 2.

Game Model

- c_{a1} is the cost of attack 1
- c_{d1} is the cost to deploy Defend 1
- p_{a0} be the probability of playing strategy a_0
- $p_{a1} =$ 1-p_{a0} be the probability of playing strategy a_1
- p_{d0} be the probability of playing strategy d_0
- p_{d1} be the probability of playing strategy d_1

Game Model

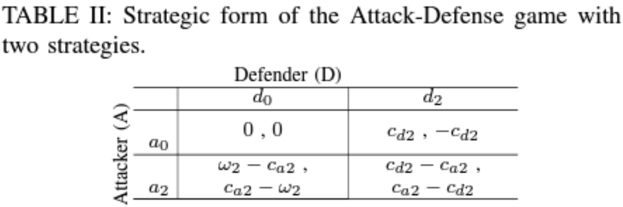
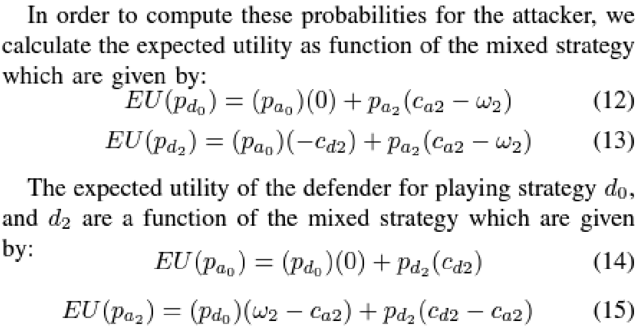


TABLE II: Strategic form of the Attack-Defense game with two strategies.

		Defender (D)	
		d_0	d_2
Attacker (A)	a_0	0 , 0	c_{d2} , $-c_{d2}$
	a_2	$\omega_2 - c_{a2}$, $c_{a2} - \omega_2$	$c_{d2} - c_{a2}$, $c_{a2} - c_{d2}$

Game Model



In order to compute these probabilities for the attacker, we calculate the expected utility as function of the mixed strategy which are given by:

$$EU(p_{d_0}) = (p_{a_0})(0) + p_{a_2}(c_{a2} - \omega_2) \tag{12}$$

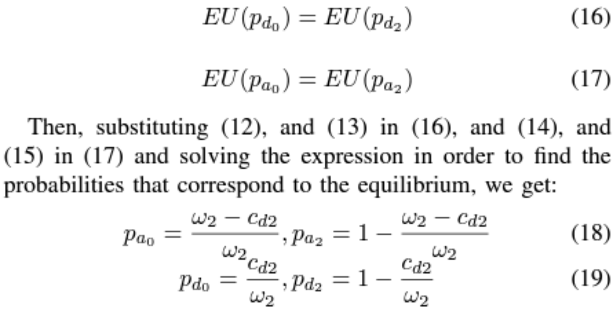
$$EU(p_{d_2}) = (p_{a_0})(-c_{d2}) + p_{a_2}(c_{a2} - \omega_2) \tag{13}$$

The expected utility of the defender for playing strategy d_0, and d_2 are a function of the mixed strategy which are given by:

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_2}(c_{d2}) \tag{14}$$

$$EU(p_{a_2}) = (p_{d_0})(\omega_2 - c_{a2}) + p_{d_2}(c_{d2} - c_{a2}) \tag{15}$$

Game Model



$$EU(p_{d_0}) = EU(p_{d_2}) \tag{16}$$

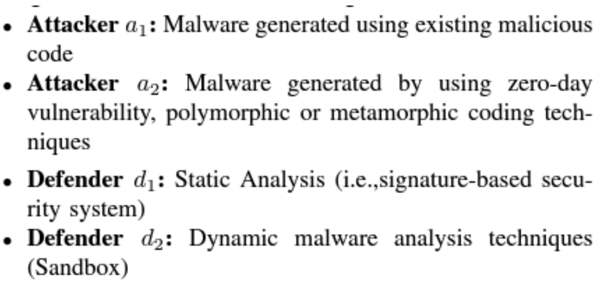
$$EU(p_{a_0}) = EU(p_{a_2}) \tag{17}$$

Then, substituting (12), and (13) in (16), and (14), and (15) in (17) and solving the expression in order to find the probabilities that correspond to the equilibrium, we get:

$$p_{a_0} = \frac{\omega_2 - c_{d2}}{\omega_2}, p_{a_2} = 1 - \frac{\omega_2 - c_{d2}}{\omega_2} \tag{18}$$

$$p_{d_0} = \frac{c_{d2}}{\omega_2}, p_{d_2} = 1 - \frac{c_{d2}}{\omega_2} \tag{19}$$

Defense System Against Malware Attack



- **Attacker a_1:** Malware generated using existing malicious code
- **Attacker a_2:** Malware generated by using zero-day vulnerability, polymorphic or metamorphic coding techniques
- **Defender d_1:** Static Analysis (i.e.,signature-based security system)
- **Defender d_2:** Dynamic malware analysis techniques (Sandbox)

Defense system against Malware Attack

- In the Simulated experiment, we assume that the security value is greater than the attacking and defending cost
- Attacking cost is less than Defending cost
- Attacking cost is greater than the Defending cost
- Average residual energy is calculated in these scenarios and compared with constant level approach.