INSTITUT DE FRANCE
Académie des sciences

Royaume du Maroc

Académie Hassan II

MADEV 17

Rabat, Maroc, 16-19 octobre 2017

Posters de la session *Mathématiques appliquées et santé*

S. Talssi & N. Yousfi - *An Expert System for Identification of HIV drug therapy using adaptive fuzzy clustering.*

M. Bachraoui , K. Hattaf & N. Yousfi - *Dynamics of a fractionnal-order HIV infection model with cure rate*

H.Besbassi, Z. El Ghoubari, K. Hattaf & N. Yousfi - *Dynamics of an HBV infection model with cell-to-cell transmission and CTL immune response.*

F. Kouilily, F-Z. Aboulkhouatem, M. El Khasmi, N. Yousfi & N. Achtaich - *Hearing loss model result from the viral infection and noise.*

F.-Z.. Aboulkhouatem, F. Kouilily, M. El Khasmi, N. Achtaich & N. Yousfi - *Mathematical model for the linear active cochlea in Alport*
Syndrome.

I. Saif, Y. Kasmi, K. Allali & My M. Ennaji - *Modèle de Markov caché pour la prédiction de la méthylation de l'ADN : les gènes suppresseurs de tumeur.*

M. El Hankouri, M. Kharbach & M. Ouardouz - *Modélisation d'allocation des ressources sous contraintes dans le milieu hospitalier :*
approche combinée automate cellulaire et multi-agent.

T. Serraj, A. Azizi & M. Chrif Ismaili - *On the Security and Efficiency of Cryptographic Protocols in Telecare Medicine Information*
Systems.

S. Ben Rhila, M. Rachik & R. Ghazzali - *Optimal Control of an SIR Model with delayed State variable.*

H. Ferjouchia, S. El Bouanani, M. Rachik, F. Iftahy & A. Chadli - *Physiological Model of Type 1 Diabetes : Analysis and Control.*

An Expert System for Identification of HIV drug therapy using adaptive fuzzy clustering

S. TALSSI, N. YOUSFI
samirtalssi@gmail.com nourayousfi@hotmail.com
Laboratory Analyse, Modelization and Simulation,
University Hassan II of Casablanca

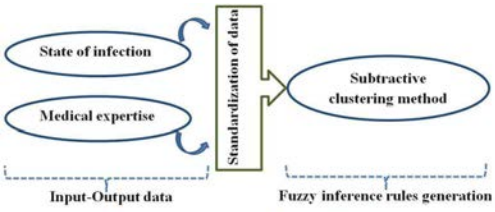
Introduction

Over 70% of the world's 40 million people living with HIV/AIDS are in Africa. Besides the human cost, HIV/AIDS is having profound effects on Africa's economic development and hence its ability to cope with the pandemic. While the impact of HIV/AIDS on people has been well documented, it has been much more difficult to observe the pandemic's effects on the African economy as a whole or to assess how it might affect Africa's future development.

Problematic

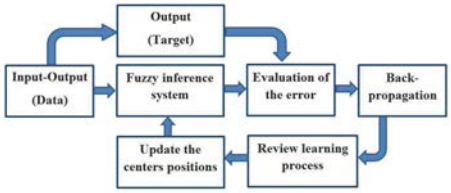
The development of decision-making tools for the optimization of drug treatments is one of the priority actions to fight against HIV and the mitigation of its impacts.

An expert system for identification of HIV drug therapy using adaptive fuzzy clustering was developed in this work. This approach relies on modeling in a fuzzy system, the changes of viral load, CD4+ T-cells counts and the quantities of injected drugs during treatment. A fuzzy clustering strategy was used to determine the fuzzy system parameters, and the backpropagation algorithm was introduced to perform these parameters. The result of this work is An Expert System able to mimic and predict the interaction between HIV and the immune system under drug therapy. The design of the expert system was carried out in two steps:



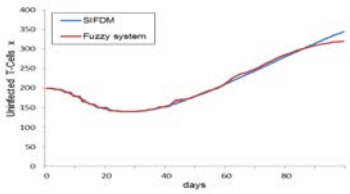
Step1: Construction of the Fuzzy Inference

Each cluster center can be used as the basis of a rule that describes the system behavior. A learning process using the back-propagation algorithm is applied to adjust the centers positions in the second step.

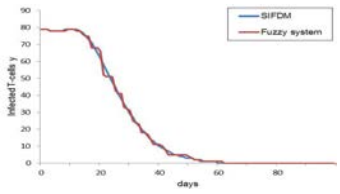


Step 2: learning process

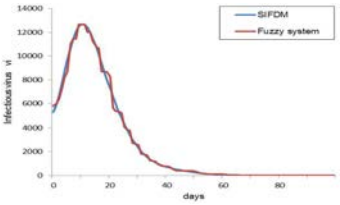
Results and discussions



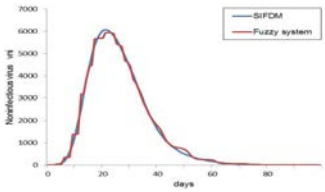
Non- infected cells during therapy



Changes in the number of infected cells during therapy



Changes in the infectious viral load during therapy



Changes in the non-infectious viral load during therapy

The results of the numerical simulations, which are shown in the form of a curve (above), shows that the fuzzy inference system has successfully identified the drug therapy.

Fighting against HIV and the mitigation of its impacts on Africa's future development

The approach presented here, provides us with an independent perspective mechanism of ideas specific to the therapy, and allows rapid understanding of the behavior of HIV during treatment. This speed will help us to make good decisions with the aim of reducing the cost of treatment and avoiding critical phases of the disease.

Dynamics of a fractionnal-order HIV infection model with cure rate

M. BACHRAOUI, K. HATTAF, N. YOUSFI
bachraouiimoussa@gmail.com
Laboratory Analyse, Modelization and Simulation,
University Hassan II of Casablanca

Introduction

Fractional derivatives provide an excellent instrument for the description of memory and hereditary properties of various materials and process. This is the main advantage of fractional derivatives, which such effect are in fact neglected in classical integer-order models. The human immunodeficiency virus (HIV) is a lentivirus that causes acquired immunodeficiency syndrome (AIDS) by infecting vital cells in the human immune system, specifically CD4+T cells. Many mathematical models have been done and it has been restricted to integer-order models. A classical model was proposed by Nowak and Bangham study to HIV infection . The infection rate is assumed to bilinear with respect to virus and uninfected targets cells. However, there are some evidence which show that a bilinear infection might not be an effective assumption. In this study we propose a new model for description of virus dynamics with general functional responses and cure rate.

Problematic

we introduce a fractional-order model of HIV infection of the CD4+ T-cells The system is described by the following set of fractional ODEs of order α,

$$\begin{cases} D^{\alpha}T(t) = \boldsymbol{\lambda} - f(T(t),V(t))V(t) - \mu_T T(t) + \rho E(t) \\ D^{\alpha}E(t) = f(T(t),V(t))V(t) - (\rho + \mu_E + \gamma)E(t) \\ D^{\alpha}I(t) = \gamma E(t) - \mu_I I(t) \\ D^{\alpha}V(t) = kI(t) - \mu_V V(t) \end{cases} \quad (1)$$

Where $f(T,V) = \frac{\beta T(t)}{1+\alpha_1 T+\alpha_2 V+\alpha_3 TV}$ is the incidence function proposed by Hattaf $\boldsymbol{T(t), E(t), I(t)}$ *and* $\boldsymbol{V(t)}$ represent the densities of uninfected CD4+T cells, unproductive cells, productive infected cells, and free virus particles respectively. The constant $\boldsymbol{\lambda}$ is the recruitment rate of the uninfected cells. The constants μ_T μ_E, μ_I and μ_V represent the death rates of uninfected cells, unproductive cells, productive cells and virus, respectively, The constant $\rho$is the rate at which the unproductive infected cells may revert to the uninfected cells. The term $f(T,V)$ describes the incidence of HIV infection of health CD4+T cells where β is the infection rate, The constant γ is the rate at which infected cells in the eclipse stage become productive infected cells and the constant k is the rate of production of virions by infected cells.

We define the basic reproduction number of the model (1) by

$$R_0 = \frac{\beta\gamma k\lambda}{\mu_V\mu_I(\lambda+\alpha_1\lambda)(\rho+\mu_E+\gamma)}$$

Biologically, R_0 denotes the average number of secondary infections produced by one productive infected cell during the period of infection when all cells are uninfected. We prove that both infected cells and virus are cleared and the infection will die out if R_0<1 while the HIV infection may become endemic if R_0>1.

Results and discussions

Theorem1:

All solutions of model (1) starting from a non-negative initial conditions remain non-negative and bounded for all t>0. Moreover, we have

$$i)\ S(t) \le S(0) + \frac{\lambda}{\delta}.$$
$$ii)\ I(t) \le I(0) + \frac{\gamma\|E\|_\infty}{\mu_I}.$$
$$iii)\ V(t) \le V(0) + [I(0) + \frac{\left(I(0)+\frac{\gamma\|E\|_\infty}{\mu_I}\right)1}{\mu_V}.$$

where $S(t) = T(t) + E(t)$ *and* $\delta = \min(\mu_T, \mu_E + \gamma)$.

Theorem2:

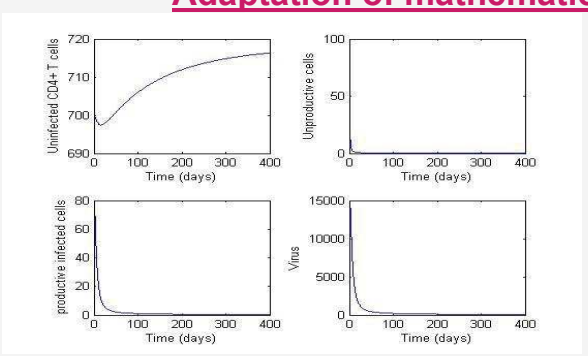
1.If $R_0 \le 1$, the disease-free equilibrium of the form $E_0 = \left(\frac{\lambda}{\mu_T}, 0,0,0\right)$ of the system (1) is locally asymptotically stable.

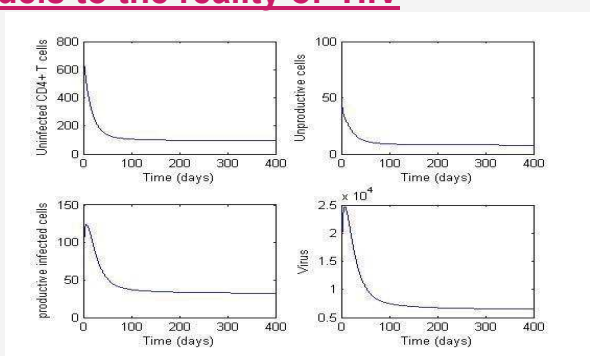
2.If $R_0 > 1$, the chronic infection equilibrium of the form $E^* = (T^1, E^1, I^1, V^1)$ *with* $E^1, I^1, V^1 \ge 0$ *and* $T^1 \in \left[0, \frac{\lambda}{\mu_T}\right]$ is locally asymptotically stable.

Numerical Simulations

In this section, we give some numerical simulation to illustrate our theoretical results. We simulate system (1) with initials conditions T(0)=700 cells mm⁻³; E(0)=20 cells mm⁻³; I(0)=0 cells mm⁻³, V(0)=102 virions mm⁻³. First, we choose the following parameter values: $\lambda = 10, \mu_T = 0.0139, \beta = 2.4 \times 10^{-4}, \alpha_1 = 0.1, \alpha_3 = 0.00001, \alpha_2 = 0.01, \gamma = 1.1, \mu_I = 0.27, \mu_E = 0.0347, k = 600, \mu_V = 3$. By calculation, we have R_0=0.1685. Hence, system (1) has a disease-free equilibrium E_0=(719.4245,0,0,0). Secondly , we choose $\beta = 0.0012$ and we keep the other parameter values. By calculation, we have $R_0 = 8.4247$ and $E^* = (92.0039, 7.6859, 31.3128, 6262.56)$.

Adaptation of mathematical models to the reality of HIV





Dynamics of an HBV infection model with cell-to-cell transmission and CTL immune response

H. BESBASSI, Z. ELGHOUBARI, K. HATTAF and N. YOUSFI

hajar.besbassi@gmail.com

Laboratory Analysis, Modelization and Simulation,
University Hassan II of Casablanca

Introduction

Hepatitis B is a potentially life-threatening liver infection caused by the hepatitis B virus (HBV). It is a major global health problem that can cause chronic infection and puts people at high risk of death from cirrhosis and liver cancer.
In 2015, hepatitis B resulted in 887000 deaths, mostly from complications (including cirrhosis and hepatocellular carcinoma) according to World Health Organization (WHO).

Problematic

ICytotoxic T Lymphocytes (CTL) cells play an important role in antiviral defense by killing
the infected cells. in addiction, HBV can spread by two fundamental modes, one by virus-to-cell infection through the extracellular space and the
other by cell-to-cell transfer involving direct cell-to-cell contact
For these reasons, we propose the following model:

$$\begin{cases} \dot{x} &= \lambda - dx - f(x,y,v)v - g(x,y)y + \rho y, \\ \dot{y} &= f(x,y,v)v + g(x,y)y - (a+\rho)y - pyz, \\ \dot{v} &= ky - \mu v, \\ \dot{z} &= s + \dfrac{cyz}{\omega + y} - bz, \end{cases}$$

where x(t), y(t), v(t) and z(t) represent the concentrations of uninfected cells, infected cells, free virus and CTL cells at time t, respectively.
Susceptible host cells are produced at rate λ, die at rate dx and become infected either by free virus at rate f(x, y, v)v or by direct contact with an infected cell at rate g(x, y)y.
Hence, the term f(x, y, v)v + g(x, y)y denotes the total infection rate of uninfected cells.Infected cells cured at rate ρy, die at rate ay and are killed by the CTL immune response at rate pyz. Free virus is produced by an infected cell at rate ky and decays at rate μv.

Objective

The main objective of this work is to investigate the dynamical behavior of system (1). To do this end, we start with the existence, the positivity and boundedness of solutions, which implies that our model is well-posed . After that we determine the basic reproduction number R0 and steady states of the model. Finally, the local and global stabilities of the disease-free equilibrium and the chronic infection equilibrium are established.

Results

Theorem 1. *All solutions starting from nonnegative initial conditions exist for all $t > 0$ and remain bounded and nonnegative.*

Theorem 2.

(1) *If $R_0 \leq 1$, then the system (3) has a unique disease-free equilibrium of the form $E_f(\lambda/d, 0, 0, b/\mu)$.*

(2) *If $R_0 > 1$, then the system (3) has a unique chronic infection equilibrium of the form $E^*(x^*, y^*, v^*, z^*)$ with $x^* > 0$, $y^* > 0$, $v^* > 0$, and $z^* > 0$.*

Theorem 3. *The disease-free equilibrium E_f is globally asymptotically stable when $R_0 \leq 1$.*

Theorem 4. *The chronic infection equilibrium E^* is globally asymptotically stable if $R_0 > 1$.*

The strategies to control the HBV infection

From our main results summarized above, we conclude that the dynamical behavior of our model is completely determined by the basic reproduction number R0.This allows determining the strategies to control the HBV infection by reducing the value of R0 to below or equal one.we see that R0 can be decreased by increasing the export of precursor CTL cells from the thymus and cytolytic .This observation shows that the CTL immune response plays a critical role in eradication of virus from the liver.

Hearing loss model result from the viral infection and noise

F. KOUILILY, F. ABOULKHOUATEM, M. EL KHASMI, N. YOUSFI and N. ACHTAICH
kouililyfatiha@gmail.com
Laboratory Analyse, Modelization and Simulation
Laboratory of Physiopathology and Molecular Genetics
University Hassan II of Casablanca

Introduction

Hearing losses can be classified according to the location of the portion of the hearing system affected, to whether the loss is unilateral or bilateral, and to its intensity or degree. The location of the portion affected of hearing loss has to do with transmission (or conduction), perception (sensorineural), or a mixture of these (mixed). Sensorineural losses arising from some affection of the outer and middle ear are called transmission or conductive losses. Sensorineural losses result from lesions on the hair cells of the cochlear organ of Corti (inner ear) and/or of the cochlear nerve. When there are concomitant conductive and sensorineural affections, the hearing loss is classified as mixed.

Hearing loss can occur due to a genetic, congenital, acquired cause, viral infection (mumps, herpex...) and risk factors such as Cochlear aging and noise exposure. In this study, we propose a new mathematical model formulated in terms of ordinary differential equations (ODEs) that takes into account the infectious disease and risk factor of hearing loss. In addition, we present some numerical simulations in order to validate our theoretical results.

Problematic

The population is divided into three epidemiology classes: H is the number of susceptible individuals (normal hearing), L is the number of infected individuals (loss of hearing) , R is the number of removed individuals (recovered hearing) and N is the total population size.

We assume that an individual can be infected by infectious individuals and by noise. Our Hearing loss model is given by the following nonlinear system of differential equations:

$$\frac{dH}{dt} = \mu N - \mu H - [\beta L + \varepsilon]H$$

$$\frac{dL}{dt} = [\beta L + \varepsilon]H - (\mu + \gamma)L$$

$$\frac{dR}{dt} = \gamma L - \mu R$$

Where β is the transmission rate due to infectious disease mumps, μ is the natural death and birth rates, γ is the rate that the infectious individuals becomes recovered individuals and ε is the hazard hearing of loss due to noise .

The compartment R contains who are recovered the individuals. With the initial conditions H(0) >0, L(0) >0, R(0) >0.

By equalizing to zero the rights members of the system, we find one endemic point that exist for above model

$$H^* = \frac{2\mu N(\gamma+\mu)}{\beta\mu N + (\varepsilon+\mu)(\gamma+\mu) + \sqrt{\Delta}}$$

$$L^* = \frac{\mu\beta N - (\mu+\gamma)(\mu+\varepsilon) + \sqrt{\Delta}}{2\beta(\gamma+\mu)}$$

$$R^* = \gamma \frac{\mu\beta N - (\mu+\gamma)(\mu+\varepsilon) + \sqrt{\Delta}}{2\mu\beta(\gamma+\mu)}$$

Where $\Delta = (\beta\mu N - (\mu+\gamma)(\mu+\varepsilon))^2 + 4\varepsilon\mu N\beta(\mu+\gamma)$

The Jacobian matrix of the system is given by :

$$\begin{pmatrix} -\mu - (\beta L + \varepsilon) & -\beta H & 0 \\ \beta L + \varepsilon & \beta H - (\gamma + \mu) & 0 \\ 0 & \gamma & -\mu \end{pmatrix}$$

The characteristic equation of the endemic equilibrium point is given by

$$(-\mu-\lambda)(\lambda^2 + C1\lambda + C2) = 0$$

Note that coefficients

$C1 = \varepsilon+\gamma+\beta L^*-\beta H^*+2\mu$ and $C2 = \varepsilon\gamma+\beta\gamma L^*+\mu^2+\varepsilon\mu+\gamma\mu+\beta L^*\mu - \beta H^*\mu$

are both positive if $R_0 = \frac{\mu\beta N}{(\mu+\gamma)(\mu+\varepsilon)} > 1$, then all roots have negative real part. Consequently the endemic point is locally asymptotically stable whenever $R_0 > 1$.

Results and discussions

We use the parameter values presented in Table 1 to illustrate the different result obtained for each of the two cases $\varepsilon > 0$ and $\varepsilon = 0$.

Parameter	Definition	Value
N	Population size	1000(assumed)
μ	the birth and death rate	$1.8200\ 10^{-2}$
β	the transmission rate due to infectious disease	$3.3890\ 10^{-4}$
γ	recovered rate	1/17
ε	the hazard hearing loss due to noise	0.0025

Table 1: Values and definitions of the parameters

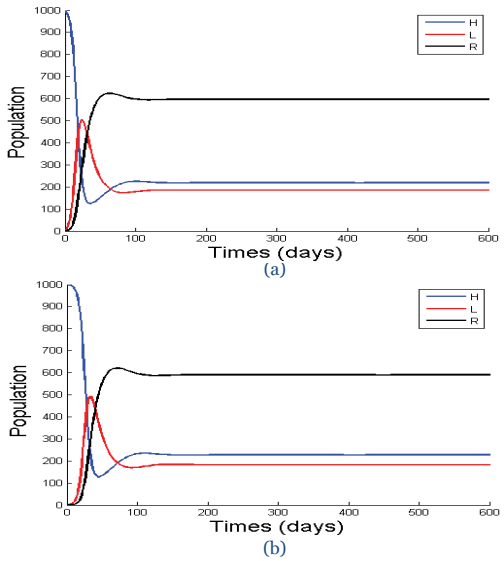


Figure 1: The population hearing loss: (a) with the infectious disease and noise $\varepsilon > 0$ (b) with only the infectious disease $\varepsilon = 0$

The population of normal hearing, loss of hearing and recovered individuals converge asymptotically to endemic equilibrium state as time increases .

Computational mathematics to simulate hearing loss

In this work, we propose a mathematical model describing and modeling the hearing loss, we analysis the hearing loss resulting from the infectious disease mumps and the risk factor noise, we shows in the case when $\varepsilon = 0$ that the disease free equilibrium is locally asymptotically stable if the basic reproductive number $R_0 = \frac{\mu\beta N}{(\gamma+\mu)} < 1$ and the endemic point is locally asymptotically stable when $R_0 = \frac{\mu\beta N}{(\gamma+\mu)} > 1$.

On the other hand, considering the hearing loss result from the infection viral (mumps) and noise $\varepsilon > 0$, we found that the system has a unique endemic point which is locally asymptotically stable.

In addition, the simulation of this model provide that the number of individuals with hearing loss increase when we introduce the risk factor noise.

Mathematical model for the linear active cochlea in Alport Syndrome

F-Z. ABOULKHOUATEM, F. KOUILILY, M. EL KHASMI, N. ACHTAICH and N. YOUSFI
fatiaboulkhouatem@gmail.com
Laboratory Analyse, Modelization and Simulation, University Hassan II of Casablanca.
Laboratory of Physiopathology and Molecular Genetics, University Hassan II of Casablanca.

Introduction

The cochlea plays a crucial role in mammal hearing. The basic function of the cochlea is to map sounds of different frequencies onto corresponding characteristic positions on the basilar membrane. A proposed theory of the active cochlea that the feed-forward/feed-backward are two mechanisms for the outer hair cell force amplification of the traveling wave. Genetic mutations of type IV collagen lead to a malfunction of Basilar Membrane (BM), resulting in the hearing loss associated with Alport Syndrome (AS), which is a disease that affects the cochlea due to the abnormal structure of the BM. Therefore, a mathematical model of the BM was developed to investigate and show numerically the effect of the stiffness on its structure with the objective to study the ear dysfunction in the active cochlea.

Problematic

The cochlea is modeled as a rectangular divided into two symmetric compartments by an elastic partition, which will be referred to as the BM. Stapes motion sets the cochlear fluid into motion and causes a vibratory deformation of the BM.

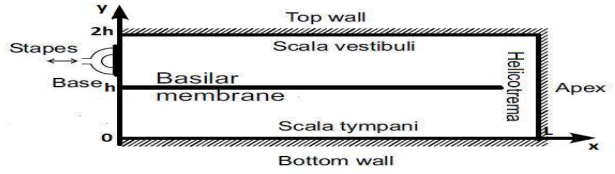


Fig. 1. Two-dimensional cochlear model

The vertical motion of the BM can be described as follows

$$m(x)\frac{\partial^2\eta}{\partial t^2}(x)+C(x)\frac{\partial\eta}{\partial t}(x)+k(x)\eta(x)=P_d(x)+F_{ohc}(x) \quad \text{at } y=h$$
$$F_{ohc}(x)=\alpha k(x)(\gamma\eta(x-d)-\eta(x+d))$$

Our purpose in this work is to perturb the stiffness k(x). So, if we put k(x)->k(x)+ε, the differential equation describing the resulting motion of the system is as follows:

$$m(x)\frac{\partial^2\eta}{\partial t^2}(x)+C(x)\frac{\partial\eta}{\partial t}(x)+(k(x)+\varepsilon)\eta(x)=P_d(x)+F_{ohc}(x) \quad \text{at } y=h$$
$$F_{ohc}(x)=\alpha(k(x)+\varepsilon)\gamma\eta(x-d)-\eta(x+d))$$

The amplitude A(x) of the BM can be defined in response to a pure tone as a function of x, we make the assumption that the system is linear and in a periodic steady state.

$$\eta(x,t)=A(x)e^{j\omega t},\ P_d=\widetilde{P_d}e^{j\omega t}$$

If we use the Taylor formula of the function $\eta(x-d)$ and $\eta(x+d)$ the equation that model the force of OHC can be written as following:

$$F_{ohc}(x)=\alpha(k(x)+\varepsilon)\{(\gamma-1)\eta(x)-d(\gamma+1)\frac{\partial\eta}{\partial x}(x)+\theta(d)\}$$

While the value of d=71.10-3mm is very small (d->0) so $d(\boldsymbol{\theta})$->0 and also $\frac{\partial\eta}{\partial x}$ small. the expression $d(\gamma+1)\frac{\partial\eta}{\partial x}(x)$ can be neglected. If we consider that w= 2πf, the amplitude A(x) can be expressed by:

$$A(x)=\frac{\widetilde{P_d}}{\sqrt{(2\pi fC(x))^2+[(k(x)+\varepsilon)(\alpha(\gamma-1)-1)+(2\pi fm(x))^2]^2}}$$

Results and discussions

In our work, we modeled the abnormal case (AS) of the BM for which the harmonic oscillator depends on stiffness k(x), mass m(x) and damping C(x). We used the parameters of Neely.

Parameter	Symbol	Value	Unit
Mass	m(x)	0.15	g/cm²
Damping	C(x)	200	dyn.s/cm³
Stiffness	k(x)	$10^9\ e^{-2x}$	dyn/cm³
OHC motility factor	α	0.2	
Forward/backward	γ	0.3	

We use the method of resonance analysis , and we increase the value of ε, then; we can observe how an increase of ε might lead to the decrease of amplitude A(x) (AS). For example, if we take $\varepsilon=10^4$

Distance(cm)	Amplitude^N(cm)	Amplitude^A(cm)	Frequency(Hz)
0.1209	$6.47269619*10^{-8}$	$6.47269267*10^{-8}$	12 294
0.6095	$1.05513526*10^{-7}$	$1.05513327*10^{-7}$	7 560
1.7470	$3.29375915*10^{-7}$	$3.29370902*10^{-7}$	2 433

The results confirm the difference between the values of the amplitude in normal and abnormal cases of the BM displacement. For the position x = 1.7470 cm, we can show the figures follows:

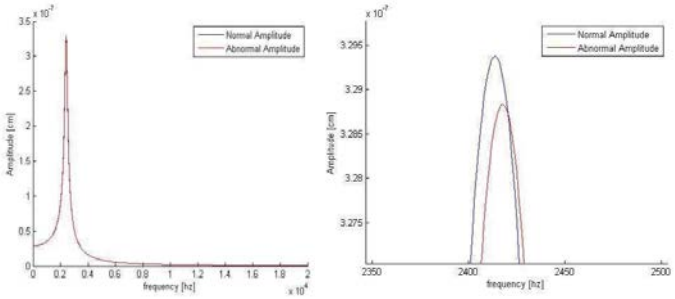


Fig. 1. BM displacement for the normal case and the abnormal cases, $\epsilon= 10^5$

We remark that when we increase the perturbation ε the value of the maximum amplitude decrease, also the frequency increase. So this changes lead to loss of hearing, which demonstrates the effect of the stiffness on the maximum amplitude displacement of the BM.

Mathematical approach for the observation of the Alport Syndrome

Our study observed mathematically the AS and showed that the amplitude decreases when we increase the stiffness of the BM, also the comparison between normal and abnormal cases showed that there is a decrease in the maximum amplitude displacement of the BM, also an increase in the value of the frequency when the epsilon very large. Although the model of this paper could be improved in many ways, the most important direction for future research, in our opinion, is to model the active mechanism in a more physiological way, taking into account the details of the tilt distance d of the OHC.

Thème : Mathématiques Appliquées et Santé

Modèle de Markov Caché pour la Prédiction de la Méthylation de l'ADN: les Gènes Suppresseurs de Tumeur

Imane Saif[1], Yassine Kasmi[1], Karam Allali[2] & My Mustapha Ennaji[1]

1. Equipe de Virologie, Oncologie et Biotechnologie Médicale, Laboratoire de Virologie, Microbiologie, Qualité & Biotechnologies/ETB, Faculté des Sciences et Techniques Mohammedia-Université Hassan II de Casablanca.

2. Laboratoire de Mathématiques & Applications, Faculté des Sciences et Techniques Mohammedia-Université Hassan II de Casablanca, PO Box 146 Mohammedia 20650, Morocco.

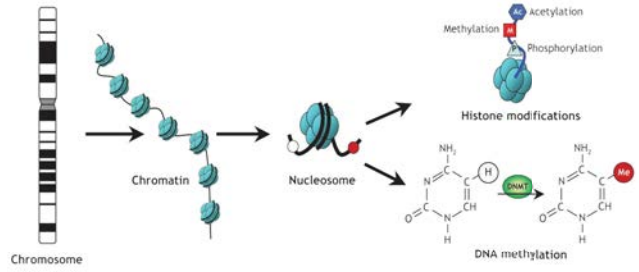
Adresses e-mail des auteurs

Imane Saif : imanesaif@yahoo.fr ; *Yassine Kasmi* : kasmi.yassin@gmail.com ; *Karam Allali* : allali@fstm.ac.ma ; *My Mustapha Ennaji* : m.ennaji@yahoo.fr

Introduction :

L'hyperméthylation des îlots CpG situés dans les régions promotrices des gènes suppresseurs de tumeurs est maintenant fermement établie comme un mécanisme important pour l'inactivation des gènes. L'hyperméthylation de l'île CpG a été décrite dans presque tous les types de tumeurs. Cependant, les mécanismes de méthylation aberrante et pourquoi certains gènes sont sélectionnés plutôt que d'autres sont encore non maitrisables. L'hyperméthylation n'est pas isolée des autres facteurs d'épigénétique, Or, elle est liée aux autres parties du puzzle telles que les protéines de liaison méthylique, l'ADN méthyltransférase et l'histone désacétylase, malgré que les rôles et les interactions entre ces facteurs restent incomplets et limites au niveau compréhensive pour les gènes suppresseurs de tumeurs.

Dans ce travail, nous visons à prédire et identifier les régions hyper-méthylées, au niveau des gènes BRCA1, - connus pour leur rôles clés dans le cycle des cellules-.



Méthodologie :

Data set

Prédiction of CpG

Frommer algorithme

Dans une région d'au moins 200bp, avec une proportion de G + C, plus de 50%, et un rapport CpGo/e supérieur à 0,6 formule 1). Les fenêtres coulissantes consistent à calculer la concentration moyenne de l'île avec un pas de 100 bases. Et N longue de la séquence,

$$CpG_{o/e} = \frac{Number\ of\ CpG}{(Number\ of\ C)\times(Number\ of\ G)} \times N\ ,$$

Modéle Caché Markov (HMM)

Algorithme de Viterbi

$$p_t(i,x) = e_t(i) \times max\,(p_k(j,x-1), p_{kl}),$$

où $e_t(i)$ est la probabilité d'observer l'élément i (brins pour C ou G) dans statel; $p_k(j,x-1)$ est la probabilité du chemin le plus probable se terminant à la position x-1, j;p_{kl} est la probabilité de la transition de l'état l à l'état k.

Algorithme Baum-Welch

$$P(X,O|\mu) = \prod_{T=1}^{N} a\,[x_{t-1},x_t]b[o_t,x_t]$$

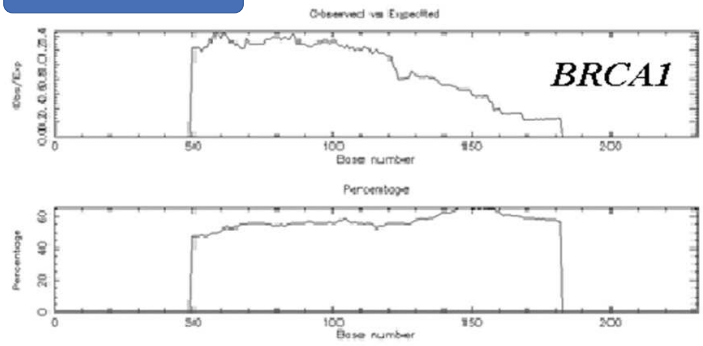
X est la séquence d'états cachés, O est la séquence d'observation. La probabilité de démarrage dans un état est pliée dans A, soit x0 toujours l'état de départ

la formule de Poisson

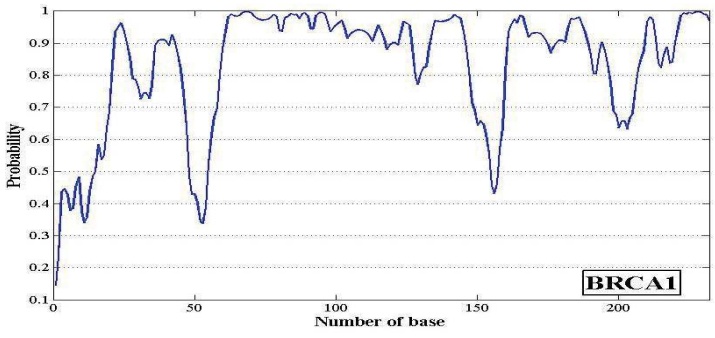
$$\frac{a_i \times L \times p(s)^2}{4}$$

Où a_i est l'Observe / attendu pour le CGI, L est la longueur de la séquence (i = 1 et la ligne de base i = 0) et le p (s) est le contenu du GC pour le segment calculé dans la première étape.

Résultats :



Analyse de séquence de région promotrice par l'algorithme de Frommer a démontré que BRCA1, méthylé entre les [50-182]



Probabilité maximale a posteriori de l'algorithme de Viterbi. Analyse des séquences de gène BRCA1 a considéré la présence au moins de 2 CGI. L'algorithme de Viterbi fournit un moyen efficace de trouver la séquence d'états la plus probable dans le sens de la probabilité maximale a posteriori d'un processus de Markov supposé être un temps discret d'état fini.

Conclusion :

Les trois sélections étudiées révèlent des régions de CGI différentes selon la base de données. En effet, les résultats de HMM est plus probable que celle donnée par l'algorithme de Frommer. La méthylation de l'ADN est un phénomène qui est identifié dans des régions précises et localisé qui nécessite des méthodes de calcul plus adéquates. En plus de l'inactivation des gènes par hyperméthylation des promoteurs de certains gènes, il existe des phénomènes mutationnels intrinsèquement liés à la présence de groupes méthyle sur l'ADN. Pour expliquer cette collaboration inter générique, l'étude des protéines et leur interaction protéine-protéine sont recommandées et constituent un levier important de l'épigénétique.

Modélisation d'allocation des ressources sous contraintes dans le milieu hospitalier : Approche combinée Automate Cellulaire et Multi-agent

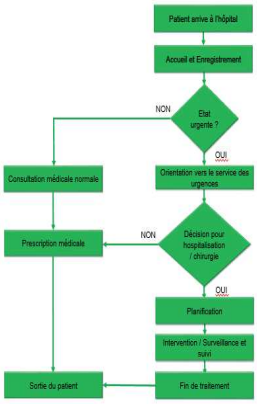
M. El Hankouri, M. Kharbach, M. Ouardouz

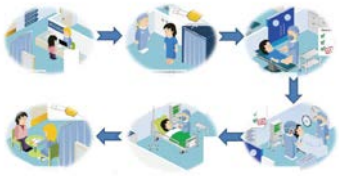
Modélisation Mathématique et Contrôle, Faculté des Sciences et Techniques, B.P. 416, Tanger, Maroc

mohammed.elhankouri@gmail.com, skharbach@yahoo.fr, ouardouz@gmail.com

Contexte et objectif

- Vers une affectation dynamique des ressources.
- Faciliter la prise de décision aux Managers.
- Développer une architecture combinée SMA et ACs.

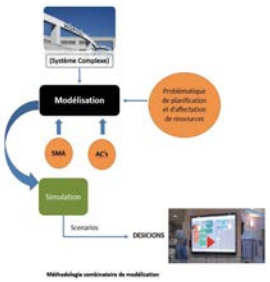


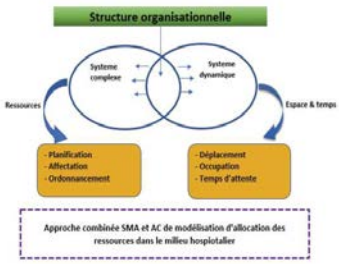


Le circuit de prise en charge des patients

L'objectif :
Améliorer la prise en charge des patients en terme de temps d'attente

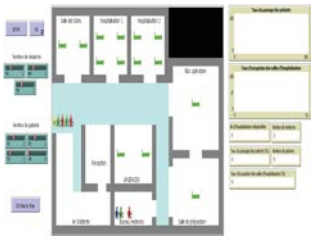
Approche proposée

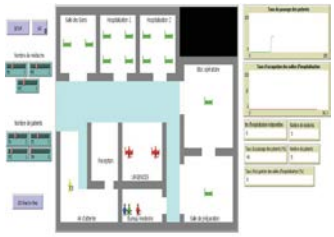




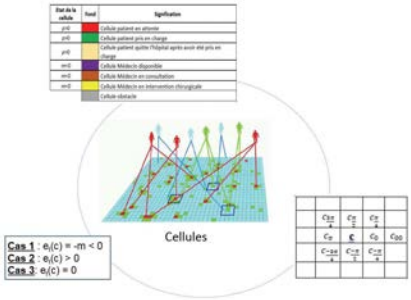
Modélisation & Simulations par système multi-agents

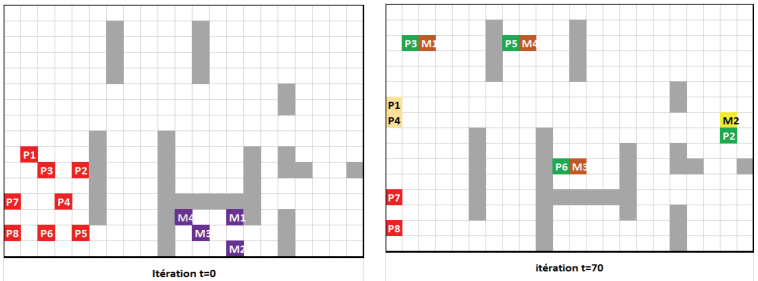
Ces figures représentent, comment la prise en charge des patients est assurée, selon leur degré de priorité, en modélisant l'affectation et l'ordonnancement du corps médical, à travers différentes itérations.





Modélisation & Simulations par automates cellulaires





Itération t=0 Itération t=70

Cette simulation nous a permis de trouver une solution d'allocation optimale et l'adoption de règles de déplacements et a garanti une meilleure exécution de planification hospitalière

Conclusion

La modélisation proposée permet aux managers de :

- Planifier les ressources dans un système complexe tel qu'un hôpital.
- Simuler en temps réel les déplacements des patients et du corps médical dans un cadre spatio-temporel.

Remerciements

Ce travail est réalisé dans le cadre du projet : PPR2/2016/79, OGI-Env, Soutenu par le MENFPESRS et le CNRST et le Réseau International Théorie des Systèmes (TDS) soutenu par l'Académie Hassan II des Sciences et Techniques

On the Security and Efficiency of Cryptographic Protocols in Telecare Medicine Information Systems

Taoufik Serraj, Abdelmalek Azizi & Moulay Chrif Ismaili
ACSA Laboratory, Mohammed First University, Faculty of Sciences, Oujda 60000, Morocco
Emails: taoufik.serraj@gmail.com; abdelmalekazizi@yahoo.fr; mcismaili@yahoo.fr

Royaume du Maroc
Académie Hassan II des Sciences et Techniques
Mathématiques appliquées et santé

Abstract

In this paper, we discuss the security and the efficiency of some cryptographic protocols proposed to secure the information exchanges between a patient and a server in telecare medicine information systems (TMIS). Particularly, we propose two approaches to improve authenticated key exchange protocols, the first is to design other simple schemes without requiring public key infrastructures (PKIs), and the second is to construct new cryptographic schemes based on NTRU instead of RSA or ECC. Also, these solutions may be more suitable to secure connected medical devices.

Introduction

Nowadays, information and communication technologies are increasingly deployed in our everyday live. Indeed, the Internet and mobile telecommunications are the basis of new forms of communication, commerce, administration and entertainment. Currently, new online services are provided, such as e-Government, e-Commerce, e-Banking, e-Health, and e-Learning. In the health area, chronic diseases (e.g., cardiovascular and respiratory diseases) are the principal causes of mortality in the world [11]. Patients, especially in aging countries, require continuous health monitoring, health information processing to improve the future disease diagnosis. To overcome these problems Telecare Medicine Information Systems (TMIS) services are deployed. In the aim of protecting medical data exchanged in TMIS, several cryptographic protocols were proposed.

In [5], Giri et al. proposed an authentication protocol for TMIS based on RSA. Also, Xu et al. [12], Zhang et al. [13] proposed authenticated and key agreement schemes using elliptic curves cryptography. All these schemes require public key infrastructures and they will be vulnerable to quantum attacks in the future.

The rest of the paper is organized as follows: section 2 provide some mathematical notions related to RSA, ECC and NTRU. The proposed schemes are presented in section 3. Finally, a conclusion is provided.

Mathematical Preliminaries

Modular Arithmetic and RSA

Let p and q be two large primes, $n = p.q$, e an integer such that $\gcd(e, \varphi(n)) = 1$ and $d \equiv e^{-1} \mod \varphi(n)$ where φ is Euler's function. The security of RSA-based protocols relies on the hardness of some factorization problems [10]. More precisely, it is based on the RSA problem which can be defined as finding the value of $x \in \mathbb{Z}/n\mathbb{Z}$ such that $x^e \equiv y \pmod n$ for a given $y \in \mathbb{Z}/n\mathbb{Z}$.

For a secure and efficient use of the RSA, the following parameters should satisfy: $p \approx q \approx 1024$ bits, $e \geq 65537$, and $d \geq \sqrt{n}$ [3].

Arithmetic in Elliptic Curves over Finite Fields and Cryptography

For a prime $p > 3$, let $\mathbb{K}$ be a finite field of characteristic p. An elliptic curve over $\mathbb{K}$ is given by the reduced Weierstrass equation

$$y^2 = x^3 + ax + b \tag{1}$$

where $a, b \in \mathbb{K}$ and $4a^3 + 27b^2 \neq 0$. If $\overline{\mathbb{K}}$ is an extension field of $\mathbb{K}$, we denote by $E(\overline{\mathbb{K}})$ the set of points $(x, y) \in \overline{\mathbb{K}}^2$ satisfying (1), together with the point at infinity $\mathcal{O}$. $\left(E(\overline{\mathbb{K}}), +\right)$ is an additive abelian group. The most important operation in elliptic curve cryptography (ECC) is the scalar multiplication defined by:

$$[k]P = P + P + \cdots + P \,(k \text{ times}).$$

Let E be an elliptic curve over a finite field $\mathbb{F}_p$, and $P, Q \in E$, such that Q is in the subgroup of E generated by P. The elliptic curve discrete logarithm problem (ECDLP) is the problem of determining an integer $k \geq 1$ such that $[k]P = Q$. The security of ECC-based protocols relies on the presumed intractability of the ECDLP.

For a secure and efficient use of the ECC, we should use an elliptic curve E defined over a finite prime field $\mathbb{F}_p$ of a prime order q, such that $p \equiv 3 \pmod 4$ of size ≈ 256 bits [2].

Euclidean Lattices and NTRU

Let N, p, q and d in $\mathbb{N}^*$, where N and p are primes, $q > (6d + 1)$ and $\gcd(N, q) = \gcd(p, q) = 1$. $R = \mathbb{Z}[X]/(X^N - 1)$ (resp. $R_q = \mathbb{Z}_q[X]/(X^N - 1)$) the ring of convolution polynomials (resp. the ring of convolution polynomials $\mod q$). We denote $T(d_1, d_2)$ the set of polynomials $f(X) \in R$ of coefficients in $\{-1, 0, 1\}$, such that $f(X)$ has d_1 coefficients equal to 1 and d_2 coefficients equal to -1. The parameters of the Encryption and Decryption functions using NTRU are N, p, q and d. These functions use two polynomials $f(X) \in T(d+1, d)$ and $g(X) \in T(d, d)$, the calculations are performed in R, R_p and R_q. For secure and efficient applications of the NTRU, we can use $N = 443$, $q = 2048$, $p = 3$ and $d = 115$ [7].

New Constructions of Cryptographic protocols in TMIS

An ECC Password-Based Protocol without PKIs

In this section we present the elliptic curve version of J-PAKE protocol [6], this version uses short keys (compared to protocols based on modular exponentiations) and do not require PKIs, it will be more suitable to secure contactless communications between medical devices.

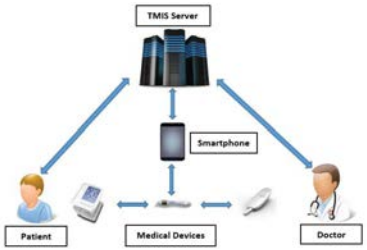


Figure 1: Telecare Medicine Information Systems

Let E be an elliptic curve over $\mathbb{F}_p$ of order q and $P \in E$. Let A and B be the communicating parties in TMIS which share a small secret password pw.

In the first round:

- A (resp. B) chooses randomly (x_1, x_2) (resp. (x_3, x_4)) from $[1, q-1]^2$.
- A (resp. B) sends $([x_1]P, [x_2]P)$ (resp.$([x_3]P, [x_4]P)$) and knowledge proofs for x_1 and x_2 (resp. x_3 and x_4) to B (resp. A).
- A and B verify the received knowledge proofs and check $[x_2]P$, $[x_4]P \neq \mathcal{O}$.

In the second round:

- A (resp. B) sends $\mathcal{A} = [(x_1 + x_3 + x_4).x_2.pw]P$ (resp. $\mathcal{B} = [(x_1 + x_2 + x_3).x_4.pw]P$) and a knowledge proof for $x_2.pw$ (resp. $x_4.pw$) to B (resp. A).
- A (resp. B) computes $K = [x_2](\mathcal{B} - [x_2.x_4.pw]P) = [(x_1 + x_3).x_2.x_4.pw]P$ (resp. $K = [x_4](\mathcal{A} - [x_2.x_4.pw]P) = [(x_1 + x_3).x_2.x_4.pw]P$).
- A session key k can be derived from K using hash functions.

A NTRU-Based Protocol for Authenticated Keys Exchange

NTRU were proposed by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman [8] as a post-quantum alternative to many of the dominant public-key cryptosystems (e.g., RSA and ECC) [4]. In addition, NTRU achieves the same security level comparing to RSA or ECC using significantly smaller system parameters [1, 9], which gives NTRU an advantage in terms of efficiency for both software and hardware implementations.

For example, we can improve the Giri et al. [5] protocol in TMIS by using the NTRU encryption and decryption functions instead RSA in the registration and the authentication phases.

In fact, using the PARI/GP system in the environment (CPU: 2.16 GHZ; RAM: 2 GB) with the recommended parameters mentioned above, we obtain the following results:

Cryptographic Operations	RSA	ECC	NTRU
Time	488 ms	15 ms	5 ms

Table 1: Computational cost comparisons

In the NIST report [3], AES is considered as a post-quantum symmetric encryption scheme. Therefore, we propose the combination of NTRU based schemes with AES-256 to preserve the forward quantum-resistance.

Conclusions and Forthcoming Research

- We presented two approaches to improve security and efficiency of authenticated key exchange protocols.
- NTRU is more efficient and ensures security in the presence of quantum attacks.
- Researches should be devoted to post-quantum cryptographic protocols.

References

[1] ANSI X9.98: LatticeBased Polynomial Public Key Establishment Algorithm for the Financial Services Industry. Tech. rep., American National Standards Institute (2010)

[2] Barker, E.B.: Digital Signature Standard (DSS) . Tech. Rep. FIPS PUB 186-4, National Institute of Standards and Technology (Jul 2013)

[3] Barker, E.B., Roginsky, A.L.: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths . Tech. Rep. NIST SP 800-131A R1, National Institute of Standards and Technology (Nov 2015)

[4] Chen, L., Jordan, S.P., Liu, Y.K., Moody, D., Peralta, R.C., Perlner, R.A., Smith-Tone, D.C.: Report on Post-Quantum Cryptography. Tech. Rep. NISTIR 8105, National Institute of Standards and Technology (Apr 2016)

[5] Giri, D., Maitra, T., Amin, R., Srivastava, P.: An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems. Journal of medical systems 39(1), 1 (2015)

[6] Hao, F., Ryan, P.: J-PAKE: Authenticated Key Exchange without PKI. Transactions on computational science XI pp. 192–206 (2010)

[7] Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W., Zhang, Z.: Choosing Parameters for NTRUEncrypt. In: Cryptographers Track at the RSA Conference. pp. 3–18. Springer (2017)

[8] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. In: International Algorithmic Number Theory Symposium. LNCS. vol. 1423, pp. 267–288. Springer (1998)

[9] IEEE P1363.1: Standard Specification for PublicKey Cryptographic Techniques Based on Hard Problems over Lattices. Tech. rep., Institute of Electrical and Electronics Engineers (Oct 2008)

[10] Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21(2), 120–126 (1978)

[11] WHO: World Health Statistics. Tech. rep., World Health Organization (2016)

[12] Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., He, L.: A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. Journal of medical systems 38(1), 1–7 (2013)

[13] Zhang, L., Zhu, S.: Robust ECC-Based Authenticated Key Agreement Scheme with Privacy Protection for Telecare Medicine Information Systems. Journal of medical systems 39(5), 1–11 (2015)

Optimal Control of an SIR Model with delayed State variable

S. BEN RHILA, M. RACHIK, and R. GHAZZALI
benrhilasoukaina@gmail.com
Laboratory Analyse, Modelization and Simulation,
University Hassan II of Casablanca

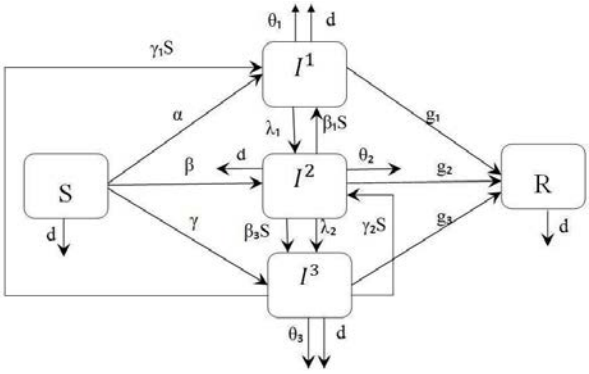
Introduction

For a long time, infectious diseases have caused several epidemics, leaving behind them not only millions of dead and infected individuals but also severe socioeconomic consequences. Nowadays, mathematical modeling of infectious diseases is one of the most important research areas. Indeed, mathematical epidemiology has contributed to a better understanding of the dynamical behavior of infectious diseases, its impacts, and possible future predictions about its spreading. Mathematical models are used in comparing, planning, implementing, evaluating, and optimizing various detection, prevention, therapy, and control programs.

Problematic

Mathematical Model

We investigate the optimal control strategy of an epidemic SIR model with delays in state. The model was developed to consider several treatment strategies with vaccination and determine their effects on the spread of the infection.



Model with Treatment and Vaccination

The first control objective is to restrict the spread of the epidemic, by introducing a vaccination control variable in our discrete delayed SIR model, as a second task, we try to treat the infected classes to reduce the spread of the epidemic .

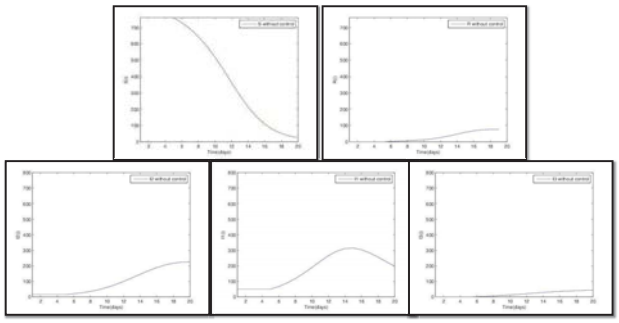
$$
\begin{aligned}
S_{i+1} &= S_i - \alpha I_i^1 S_i - \beta I_i^2 S_i - \gamma I_i^3 S_i - \varepsilon_1 v_i S_i - dS_i \\
I_{i+1}^1 &= I_i^1 + \alpha I_i^1 S_i + \beta_1 I_i^2 S_i + \gamma_1 I_i^3 S_i - \lambda_1 I_{i-p}^1 \\
&\quad - (\theta_1 + g_1 + d) I_i^1 - \varepsilon_2 u_i^1 I_i^1 \\
I_{i+1}^2 &= I_i^2 + \lambda_1 I_{i-p}^1 + \beta_2 I_i^2 S_i + \gamma_2 I_i^3 S_i - \lambda_2 I_{i-q}^2 \\
&\quad - (\theta_2 + g_2 + d) I_i^2 - \varepsilon_3 u_i^2 I_i^2 \\
I_{i+1}^3 &= I_i^3 + \beta_3 I_i^2 + \gamma_3 I_i^3 S_i + \lambda_2 I_{i-q}^2 - (\theta_3 + g_3 + d) I_i^3 \\
&\quad - (\theta_3 + g_3 + d) I_i^3 - \varepsilon_4 u_i^3 I_i^3 \\
R_{i+1} &= R_i + g_1 I_i^1 + g_2 I_i^2 + g_3 I_i^3 + \varepsilon_1 v_i S_i + \varepsilon_2 u_i^1 I_i^1 \\
&\quad + \varepsilon_3 u_i^2 I_i^2 + \varepsilon_4 u_i^2 I_i^2 - dR_i
\end{aligned}
$$

Results and discussions

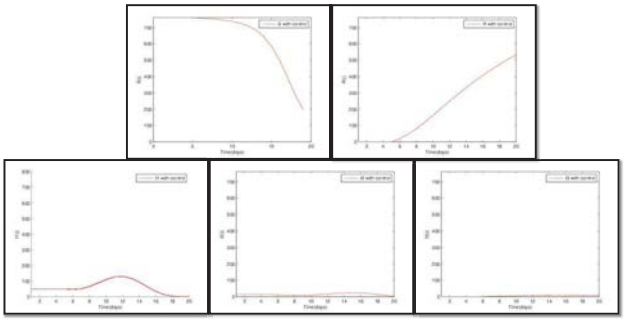
Numerical results

We now present numerical simulations associated with the above mentioned optimal control problem. To solve this system we wrote a code in MATLAB and simulated our results using different data. We solve the optimality systems using an iterative method.

Without controls



With controls



Une analyse mathématique pour comprendre des pathologies

In this work we discussed an efficient numerical method based on optimal control to study the several treatment strategies with vaccination in our discrete delayed SIR model, on the spread of the infection. The numerical simulation of both the systems i.e with control and without control, shows that the several strategies helps to reduce the number of infected and susceptible individuals and increase the number of the removed individuals greatly. The results obtained shows also that the effectiveness of vaccination campaign.

Physiological Model of Type 1 Diabetes : Analysis and Control.

H. FERJOUCHIA[1] , S. ELBOUANANI[2], M. RACHIK[1], F. IFTAHY[3] and A. CHADLI[3]

ferjouchiahanane@gmail.com

1. Laboratory of Analysis, Modeling and Simulation (LAMS), University Hassan II of Casablanca.
2. High School of Electricity and Mechanics (ENSEM) Morocco.
3. Ibn Rochd CHU, Casablanca. Morocco.

Introduction

The beta cells in the pancreas of people with type 1 diabetes are not able to produce insulin. Insulin is a hormone that lowers the blood glucose concentration by catalyzing storage of glucose. In this work, the construction of a mathematical model describing the whole blood glucose-insulin system was tried. The model was derived both based upon the two minimal models of Bergman's minimal model, which is primarily used to interpret an IVGTT. The PID controller is described to show how a controller could be used together with the modified model.

Problematic

Type 1 diabetes is a chronic illness where the cells in the pancreas that make insulin are destroyed, and the body is not longer able to produce insulin. Patients with type 1 diabetes require lifelong insulin therapy. Most require two or more injections of insulin daily, with doses adjusted based on self-monitoring of glucose levels. This therapy replaces the continuous insulin secretion, which should be provided by the pancreas. The body naturally tightly regulates blood glucose levels in a tight range (70 - 110((mg)/(dl))).

Minimal model involves two physiological compartments : a glucose compartment and a plasma insulin compartment, which is assumed acting through a remote form to influence net glucose uptake. The glucose-insulin systems is given as follows.

$$\begin{cases} G'(t) = -p_1 G(t) - X(t)(G(t) - G_b) + m(t) \\ X'(t) = -p_2 X(t) + p_3 (I(t) - I_b) \\ I'(t) = -n(I(t) - I_b) + u(t) \end{cases}$$

With the parameters given in the following table:

Parameter	Unit	Description
G(t)	[mg/dL]	Blood glucose concentration
I(t)	[1/min]	Blood insulin concentration
X(t)	[mU/L]	The effect of active insulin
G_b	[mg/dL]	Basal blood glucose concentration
I_b	[mU/L]	Basal blood insuline concentration
P_1	[1/min]	Glucose clearance rate independent of insuline
P_2	[1/min]	Rate of clearance of active insuline
P_3	[L/min^{2}mU]	Increasein uptake ability caused by insulin
n	[1/min]	Decay rate of blood insuline
m(t)	[mg/dL/min]	Meal disturbance function
U(t)	[mu/min]	Exogenous insulin

And the PID controller defined by this expression:

$$u(t) = K_c \left[e(t) + \frac{1}{T_i} \int^t e(\tau) d\tau + T_d \frac{de(t)}{dt} \right]$$

- **The proportional P:**

The proportional part of the controller is : $P = K_c e(t)$ where K_c is a constant known as proportional gain.

- **The integral I:**

The integral of the controller is: $K_c \frac{1}{T_i} \int^t e(t)\, d\tau$ where T_i is th reset time.

- **The derivative D:**

The derivative part of the controller is : $K_c T_d \frac{de(t)}{d}$ where T_d is the derivative time.

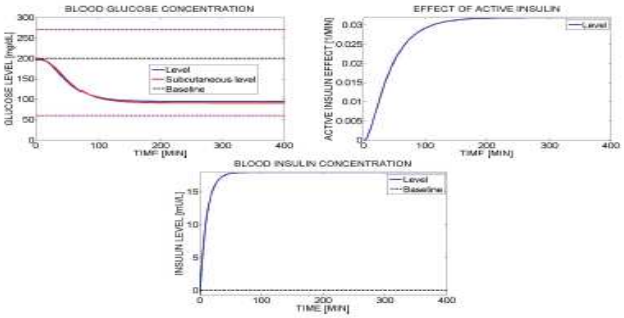
Results and Discussions

In this section a tuning and a testing of the PID controller is described. in order to use the U(t) function and see how the model reacts to an insulin shot, and or a change in the basal delivery. The parameters used are:

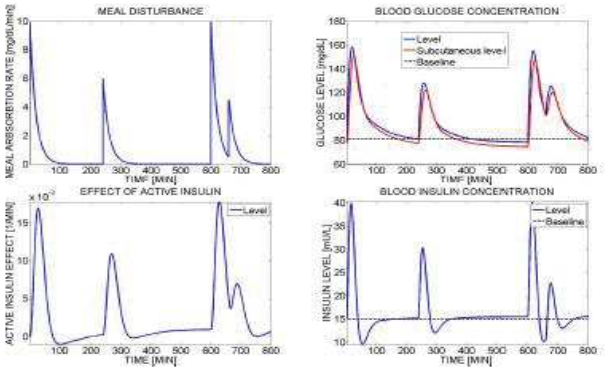
$$G_b = 81 \frac{mg}{dL}, \quad I_b = 15 \frac{mU}{L}, \quad n = 0.3 \frac{1}{\min}$$

$$p_1 = 0.028735 \frac{1}{\min}, \quad p_2 = 0.028344 \frac{1}{\min}, \quad p_3 = 5.035.10^{-5} \frac{1}{\min^2 mU}$$

$$K_C = 0.2, \quad T_i = 500, \quad T_d = 120, \quad N = 10$$



Basal delivery changed to U(t) = 20. Black dotted lines are baselines G_b and I_b



Testing the tuned PID controller. Meal test, with breakfast, lunch, dinner and snack. The first graph show the meal rates. initial values for the meal rates are chosen to be between 5-10 mg/dL

Conclusion and Perspectives

In this work, a mathematical physiological system of (DT1) open-loop model has been validated by the diabetologists /endocrinologists of Ibn Rochd CHU Casablanca, this model contained the possibility to simulate the reaction to a insulin injection or a change in basal insulin delivery. The other, a PID Controller was also implemented to show how the model could be used to test controllers.

In morocco, we don't currently have available application adapted to the Moroccan context. So, in future work and in collaboration with the endocrinology department of CHU Casablanca, we will try to implement our model with parameters adapted to Moroccan habits (family meal, to fast in ramadan...) using android or smartphone.