JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 8 : 1487~1493 Aug. 2016

Viral 통신에서의 SEIR모델을 위한 최적제어 기법

Amr Radwan*

Optimal Control Scheme for SEIR Model in Viral Communications

Amr Radwan*

Department of Information and Communications Engineering at Inje University, Gimhae 50834, Korea

요 약

최근 SNS (Social Networking Services)를 통한 사용자들 간 정보 확산이 폭발적으로 증가하고 있다. SEIR (Susceptible-Exposed-Infectious-Recovered model)모델은 전염병 예측에 널리 사용되는 수학적 모델로, 이러한 정보 확산은 SEIR를 이용하여 모델링 할 수 있다. 본 논문에서는 SEIR모델을 이용하여 최적 제어 이론의 관점에서 SNS의 정보 확산 모델을 도출하였다. 본 논문에서는 PMP (Pontryagin's Minimum Principle)에 기반한 forward-backward algorithm을 제안하였다. 이 알고리즘은 전방과 후방으로 가면서 state와 adjoint equation들을 통합하면서 동작한다. 수치해석을 통해 정보 내용의 impact value와 birth rate이 작으면 작을수록 더 많은 노드들이 해로운 정보를 필터링하는 것을 보였다.

ABSTRACT

The susceptible, exposed, infectious, and recovered model (SEIR) is used extensively in the field of epidemiology. On the other hand, dissemination information among users through internet grows exponentially. This information spreading can be modeled as an epidemic. In this paper, we derive the mathematical model of SEIR in viral communication from the view of optimal control theory. Overall the methods based on classical calculus, In order to solve the optimal control problem, proved to be more efficient and accurate. According to Pontryagin's minimum principle (PMP) the Hamiltonian function must be optimized by the control variables at all points along the solution trajectory. We present our method based on the PMP and forward backward algorithm. In this algorithm, one should integrate forward in time for the state equations then integrate backward in time for the adjoint equations resulting from the optimality conditions. The problem is mathematically analyzed and numerically solved as well.

키워드 : 최적제어문제, SEIR Model, Viral Communication, Pontryagin의 최대 원리, 전후방 알고리즘

Key word : Optimal Control Problem, SEIR Model, Viral Communication, Pontryagin's Minimum Principle, Forward-Backward Algorithm

Received 09 June 2016, **Revised** 20 June 2016, **Accepted** 28 June 2016

* **Corresponding Author** Amr Radwan(E-mail:amr_or@yahoo.com, Tel:+82-55-320-3745)
Department of Information and Communications Engineering at Inje University, Gimhae 50834, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.8.1487 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. INTRODUCTION

The term of viral communication refer to communication phenomenon which the number of information sharing grow exponentially like how viruses spreading in population. Viral communication is a new paradigm in communication which is empowered by the development of digital technologies especially in internet communication [1,2]. As many Social Networking Services (SNS) has emerged and become mass media tool, people can easily receive any information and at the same time spread the information into public. This ease of SNS can be used for various purpose, e.g. marketing, campaign, social message, publication. Viral communication in SNS and in other platform has closed relation with content, so the information contents which are spread in public hold a critical role to create social influence and public opinion. In one hand, it will give a benefit for ease of information sharing if the information contain valuable information and for positive purposes. In another hand, If the information violating the law, contain fake or false information, or contain malicious contents, it will give the negative impact to public. Fortunately, in the latter case, internet system and SNS's users itself have some kind of "anti bodies" to resist against malicious content or fake information. Internet has security system to detect malware or any kind of malicious content and prevent it from being accessed. For the fake information case which could public opinion crisis if it is spread, the SNS's users can identify by themselves whether the information correct or not and they will decide whether it should be shared or not. If the users notice that the information is fake, then he will decide not to share the information content. So, by researching in information propagation mechanism in internet especially in SNS, for example like above scenario, can help us to analyze the information flow in the network and make a better understanding how the information spreading can create an impact in public. The contribution of the paper can be summarized as follows.

- We model and formulate the SEIR model of information dissemination as a control problem.
- We propose a very efficient method based on Pontryagin's minimum principle.
- We evaluate the proposed algorithm with numerical analysis.

The remainder of this paper is organized as follows. We describe our SEIR model and the problem formulation in section II. Section III presents our proposed algorithm. Section IV gives the evaluation of the proposed algorithm and section V eventually concludes the paper.

Ⅱ. Data Dissemination Model

2.1. Analysis of information data spreading

Each social network site has their own subscribers. We define a social network users as active users when they do some activities, e.g. read article, share picture, streaming video, in the social network site. For active users, they can share any information content in a social network. When the content contain fake or false information, or has malicious data inside, it will create a problem not only for the accessing users, but also for public if the content is related to some information that is not suitable if leaked to public. To overcome this, the network has some system to filter the content which are shared by active users then the system will allowed the content to be shared. This system is an action control in the internet networks and in our model is referred as a control function of the data dissemination. Any users which their content is free from malicious date will pass from filtering control system and their content is allowed to be share.

2.2. SEIR Model

We introduce variable control u as the successful level of all active users are being filtered. If $u = 1$, it means that all nodes which contain malicious content in it are

successfully being filtered and all of malicious content are being blocked. In the case $u<1$ the malicious content which leaked from filtering control system will spread in the network and become users who exposed with malicious data. Any users who access the content by clicking the malicious link, will become infected users. In this state, users have some option what they will do next. Users can share the content under same or different social network site. Second possibility is, users only access the content and then directly leave the content without share it. In the last condition, the malicious content will not spread by these users network, and the impact are only felt by them. These users become recovered who does not have malicious content in their network after cleaning the malicious data. We define four states for users as a nodes in the network based on propagation model denoted by S, E, I, and R [3,4]. State S represents active nodes which ready to share information. State E represents the unfiltered nodes and contain malicious data but still not accessed yet. State I represents any nodes which browse and access the malicious information. The nodes in state I become the infected nodes. State R represents condition that nodes are filtered and exempted from unwanted information. Nodes in this state become immune nodes. Adding control function to the propagation model we have the information dissemination model as shown in Figure 1. The process of $S->R$ represents active nodes in the social network site are being filtered with control function constant and become immune node. $S->E$ represent there are some nodes which not filtered and do activity in the network with probability c.

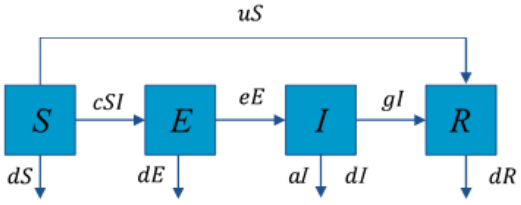

Fig. 1 Proposed SEIR model

It becomes exposed node which prone to access the malicious files. The process of $E->I$ represents any nodes who browse a web content or access the link which contain malicious data and become infected nodes with probability e. In this step, users have option to share the malicious content to other social network site by probability a. The process of $I->R$ represent the infected nodes which did not continue to share the malicious content and become recovered nodes. Denote $T=S+E+I+R$ as total number of active users in a social network. The value of active users T is dynamic, so we model this condition by introducing birth rate and death rate constant, b and d. Birth rate represents users who change their state from active to idle and death rate represents users who change their state from idle to active at time $\tau+1$ in a social media network. We use $S(\tau), E(\tau), I(\tau)$, and $R(\tau)$ to denote the number of nodes in the susceptible, exposed, infected and recovered state at time respectively. By this analysis, at time $\tau+\triangle\tau$, we get following equation:

$$S(\tau+\triangle\tau)-S(\tau)=bN(\tau)\triangle\tau-dS(\tau)\triangle\tau-cS(\tau)I(\tau)\triangle\tau - u(\tau)S(\tau)\triangle\tau$$

and we get the differential equation as follows:

$$\dot{S}(\tau)=bT(t)-dS(\tau)-cS(\tau)I(\tau)-u(\tau)S(\tau)$$

Similarly, other differential equation can be obtained as:

$$\begin{aligned}
&\dot{S}(\tau)=bT(\tau)-dS(\tau)-cS(\tau)I(\tau)-u(\tau)S(\tau),\ S(\tau_0)=S_0\\
&\dot{E}(\tau)=cS(\tau)I(\tau)-(e+d)E(\tau),\ E(\tau_0)=E_0\ \geq 0\\
&\dot{I}(\tau)=eE(\tau)-(g+a+d)I(\tau),\ I(\tau_0)=I_0\ \geq 0\\
&\dot{R}(\tau)=gI(\tau)-dR(\tau)+u(\tau)S(\tau),\ R(\tau_0)=R_0\ \geq 0\\
&\dot{T}(\tau)=(b-d)N(\tau)-aI(\tau),\ T(\tau_0)=T_0
\end{aligned}$$

For simplicity, we express the above ODEs by using a new function as follow:

$$\dot{x}(\tau)=f(x(\tau),u(\tau)) \qquad (1)$$

where, $x=(S, E, I, R, T):[\tau_0,\tau_f]\rightarrow R^5$. Let $u(\tau)$, the control that represents the percentage of active nodes

which ready to share information being filtered for the unwanted contents. As in reality taking such a control in data dissemination is difficult, blocking contents sometimes not effective for whole nodes and some nodes may still share the unwanted information. So we bound the control of blocked contents with

$$0 \le u(\tau) \le 0.9 \tag{2}$$

The objective functional is defined as

$$\min_u \int_{\tau_0}^{\tau_f} (kI(\tau) + u(\tau)^2)\, d\tau \tag{3}$$

where k is constant, can be interpreted the rates of loss if the information leaked to public. We want to minimize the loss and the effort for blocking the contents.

Table. 1 FB-SEIR Algorithm

1: Choose initial control trajectory
u^0, $k=0$, ϵ, $MAXITER$
2: Do:
3: Original initialization $x_\tau^0 = (S_\tau^0, E_\tau^0, I_\tau^0, R_\tau^0)$
4: Original sweep $\tau: \tau_0 \rightarrow \tau_f$
5: if $k>0$:
6: $\delta u^k = \arg min\, H_\tau(x_\tau^k, u_\tau^k, \overline{x}_{\tau+1}^k)$
7: $u^{k+1}(\tau) = u^k + \delta u^k$
8: integrate forward:
9: $x_{\tau+1}^k - x_\tau^k = \nabla_{\overline{x}^k} H_\tau(x_\tau^k, u_\tau^k, \overline{x}_{\tau+1}^k)$
10 Backward sweep $\tau: \tau_f \rightarrow \tau_0$
12: integrate backward:
13: $\overline{x}_{\tau+1}^k - \overline{x}_\tau^k = -\nabla_{x_\tau^k} H_\tau(x_\tau^k, u_\tau^k, \overline{x}_{\tau+1}^k)$
15: $k = k+1$
16: $while:\ \| \nabla_{u_\tau} H_\tau \| \le \epsilon$ and $k < MAXITER$.

Ⅲ. Proposed Algorithm of SEIR Model

We derive the first order necessary conditions for optimality via the Pontryagin minimum principle of SEIR model (1-3). These necessary conditions form differential algebraic equations (DAEs).

Theorem.1 [5-8] (Pontryagin minimum principle): Assume u^* is optimal for the problem (1-3), and $x^* = (S^*, E^*, I^*, R^*, T^*)$ are the corresponding trajectory. Then there exists a function $\overline{x^*} = (\overline{S^*}, \overline{E^*}, \overline{I^*}, \overline{R^*}, \overline{T^*}) : [\tau_0, \tau_f] \rightarrow R^5$ such that

(ODE-adjoint):

$$\dot{\overline{x^*}}(\tau) = -H_x(x^*(\tau), u^*(\tau), \overline{x^*}),\ \overline{x}(\tau_f) = 0 \tag{4}$$

and

$$u^* = \arg min H_u(x(\tau), u(\tau), \overline{x}(\tau)) = 0 \tag{5}$$

In addation, the mapping $\tau \rightarrow H(x^*(\tau), u^*(\tau), \overline{x^*})$ is constant, and,

$$H = (kI(\tau) + u(\tau)^2) + \overline{x}(\tau)(f(x(\tau), u(\tau)) + \lambda_1(u - 0.9) + \lambda_2(-u)$$

is the Hamiltonian function, and the H_x, H_u are the derivative of the H with respect to the state and the control, respectively. This leads to the forward backward algorithm for SEIR model (FB-SEIR) as depicted in Table 1 [6]. The FB-SEIR algorithm is shown in Table 1. The first line shows the initialization for the control u^0, the tolerance ϵ, and the maximum number of iterations $MAXITER$. Line 3 shows the initialization for the state functions x_τ^0. It is obvious that at each iteration k of FB-SEIR Algorithm consists of two sweeps, the original sweep (see the line 4 of Table 1) and backward sweep (see the line 10), through the time interval $[\tau_0, \tau_f]$ which one should integrate forward and backward, respectively, in time to obtain the state and the adjoint functions (see lines: 9, 13). In case $k>0$, adjust the piecewise-constant control function by: $u^{k+1}(\tau) = u^k + \delta u^k$ where, δu^k is the step size form, see lines 6, and 7. In line 16, we notice also that the algorithm terminates if the norm of the gradient of the Hamiltonian w. r. t. the control u, during the run time of the program is smaller than the tolerance ϵ or the maximum number of iterations has been reached.

Ⅳ. Numerical Analysis

4.1. Performance Evaluation

Reference to the parameters settings in paper of Neilan and Lenhart [9], simulation uses parameters as depicted in table.2. Figure 2 shows the convergence of optimal control $u(\tau)$. The control function is decreasing in exponential, means that the blocking content as control function strategy has big impact for preventing the spread of malicious information. It will converge nearly to zero when the malicious information is annihilated form social network and stop from proliferating.

4.2. The Influence of bad impact value on information contents

Taking two values of bad impact value of leaked unwanted information $k=0.1,0.9$, we get the trend of $S(\tau), E(\tau), I(\tau)$, and $R(\tau)$ shown in Figures 3 and 4. As seen in Figures 3 and 4, there are two different trend in the beginning of time interval and in the following time. The short period in the beginning is the treatment phase for the spread of unwanted information in social network. The following period is convalescence phase of the social network as the unwanted content is begin to stop from being spread and start to annihilated.

Table. 2 Simulation parameters and constants as in [9]

Parameter	Value
b	.3,.8
d	.5
c	.0001
τ_0	0
g, e	.1, .5
a	.2
k	.1
S_0	1000
E_0	100
I_0	50
R_0	15
τ_f	20

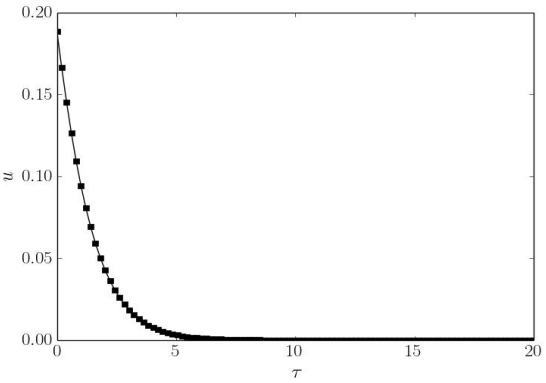

Fig. 2 Control function at $k=0.1,\ b=0.3$

When k is small, the value S is reduced slowly at the beginning of time interval and the value of R is increase slowly at the beginning of time interval. This condition indicates only few number of nodes being filtered and as the result only few number of nodes become immune nodes. As the increase of value of k, the curve of S shows the decreasing trend more sharply at the beginning of time interval and then begin to increase in the following unit times. As the opposite of S, the curve of shows the increasing trend at the beginning of time interval and begin to decrease and goes to 0. Both minimum and maximum value of S and R are also increase as the value of k is increase. This phenomena indicates the higher value of k is, the more number of nodes are filtered to prevent the spread of harmful information. The effort of content filtering to the more

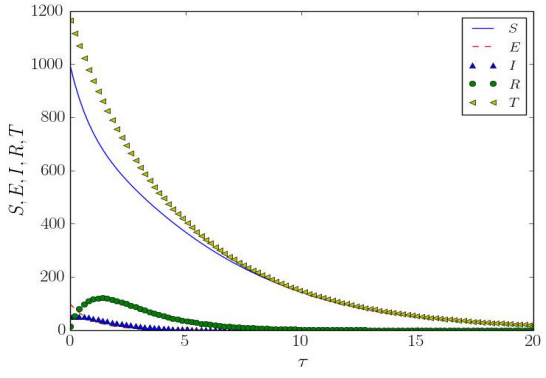

Fig. 3 State functions at $k=0.1,\ b=0.3$

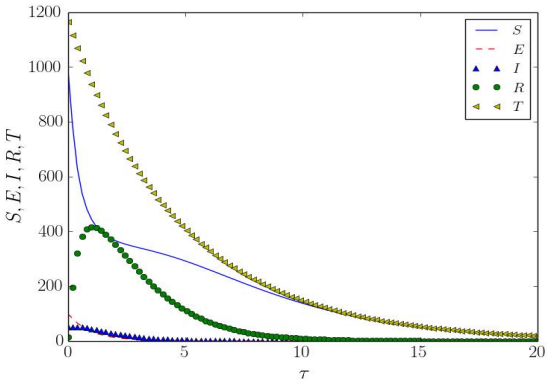

Fig. 4 State functions at $k=0.9,\ b=0.3$

nodes for the more harmful information is for maintaining the effect of the spread of unwanted information, as modeled in objective function in (1), in the same level for certain number of inspected nodes I. As we can see in Figures (3,4), the number of infected nodes I, which is the users who access the unwanted information, is almost exactly same. So, to minimize, we need to increase the control function $u(t)$, which represents the number of nodes are being filtered, for the different value of k. When the bad impact of leaked information is low ($k=0.1, 0.9, b=0.3$) as is shown in Figures 3 and 4 the network feel less threat, so the effort to create security systems in social network sites and to do information filtering is minimal. Thus, the number of nodes which are filtered from susceptible nodes S, to become immune nodes R, is only few nodes.

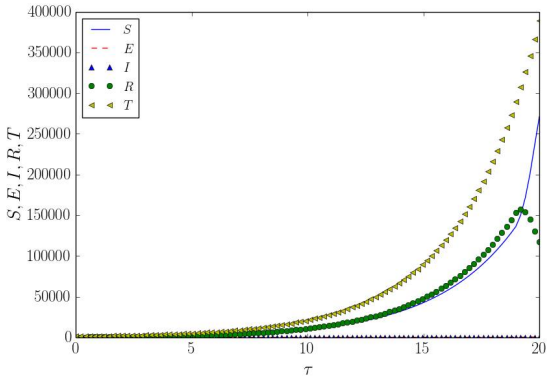

Fig. 5 State functions at $k=0.1,\ b=0.8$

The curve of E and I almost has same trend among all values of k. This condition shows that our algorithm is trying to maintain certain values for nodes in state E and I for different values of parameter in objective function. We only need focus in managing values in control function $u(t)$ for the tradeoff information. It indicates for higher level of information harmfulness, to keep the number of user accessing the unwanted information in the same level, we need to upgrade the filtering system to block more number of the unwanted information from nodes and prevent it from spread more widely. Simulation result shows that the degree of information maliciousness is affected the network effort for do filtering by improving the network security system. It is for preventing proliferation of inspected nodes and keep it in certain values. The higher of degree of information maliciousness, the more number of nodes should be blocked from accessing the information.

4.3. The influence of birth rate in SN users

In this subsection of simulation, we change the value for birth rate parameter b. This parameter denoted as users who just active and also new subscribers of the social media. Taking the value of $b=0.8$, the birth constant parameter affect the total number of active user T in social networks as depicted in Figure 5. For these conditions, $b<d$, $b=d$, and $b>d$, the total number of active nodes T declined to zero, constant, and increasing by time, respectively.

Ⅴ. CONCLUSION

We modeled and formulated the SEIR model of information dissemination as a control problem in this paper. We presented a very efficient approach, based on Pontryagin Minimum Principle for the numerical solution of a SEIR model, which provides solutions with much higher accuracy than any alternative numerical methods in solving the control problems such as the direct approach. We introduced some numerical tests

based on the forward backward algorithm to analyze the influence of birth rate and the bad impact factor in the SEIR model as well. We showed that the higher value of bad impact prevents the spread of harmful information.

Ⅵ. FUTURE WORKS

Future work aims to compute the parametric sensitivity derivatives of the switching points using automatic differentiation which allows to determine the sensitivity analysis derivatives of the optimal state trajectories S, E, I, R and T.

REFERENCES

[1] R. Xu, H. Li, and C. Xing, "Research on Information Dissemination Model for Social Networking Services," *IJCAS*, vol. 2, no. 1, pp. 1-6, Feb. 2013.

[2] C. B. Belker, "The Paradigm of Viral Communication," *Journal of Information Service and Use*, vol. 22, no. 1, pp. 3-8, First Issue 2002.

[3] S. Lenhart, and T. Workman, *Optimal Control Applied to Biological Models*, Chapman and Hall/CRC Mathematical and Computational Biology Series, 2007.

[4] D. Moualeu, M.. Weiser, R. Ehrig, and P. Deuflhard, "Optimal Control for a Tuberculosis model with Undetected Cases in Cameroon," *Commun Nonlinear Sci Numer Simulat*, vol. 20, no. 3, pp. 986-1003, Mar. 2015.

[5] J. T. Beets, *Practical Methods for Optimal Control using Nonlinear Programming*, 2nd ed. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2010.

[6] A. Radwan, "Dynamic Optimization of Active Queue Managment Routers to Improve Queue Stability," *Journal of the Korea Multimedia Society*, vol. 18, no. 11, pp. 1375 - 1382, Nov. 2015.

[7] O. Von Stryk and R. Bulirsch, "Direct and Indirect Methods for Trajectory Optimization," *Annals of Operations Research*, vol. 37, no. 1, pp. 357-373, Dec. 1992.

[8] C. Darby, W. Hager, and A. Rao, "Direct Trajectory Optimization Using a Variable Low-Order Adaptive Pseudospectral Method," *Journal of Spacecraft and Rockets*, vol. 48, no. 3, pp. 433-445, May 2011.

[9] R. M. Neilan and S. Lenhart, "An Introduction to Optimal Control with an Application in Disease Modeling," *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, vol. 75, pp. 67-81, 2010.

Amr Radwan

received his B.S. and M.S. degrees in Mathematics from Sohag University, Sohag, Egypt, in 1999 and 2005. He received the Ph.D. degree in Mathematics from Humboldt University zu Berlin, Germany in 2012. From Aug. 2012-Sep.2014, he worked as a lecturer at Mathematics Department, Faculty of Science, Sohag University, Egypt. Dr. Radwan was awarded an NRF Postdoctoral Research Fellowship (2014, Oct.-2015, Feb.), and joined Prof. Won-Joo Hwang's research group in the Department of Information and Communications Engineering at Inje University. Since Mar. 2015, he has been an assistant professor at Department of Information and Communications Engineering, Inje University, Republic of Korea. His research interests are in the area of nonlinear optimization, optimal control problem, and wireless networks.