Conflict Control of Spreading Processes on Networks

Oleksii Ignatenko [1][0000-0001-8692-2062]

[1] Institute of Software Systems NAS Ukraine
o.ignatenko@gmail.com

Abstract. The focus of this work is to provide introduction to the current state of art of the field of spreading processes on networks in connection with optimal control theory and game theory. This is challenging problem which remains open, so we present problem formulation, make suggestion of possible ideas of solution and show simulations to substantiate these ideas.

Keywords: Networks, game theory, optimal control, epidemic model.

1 Introduction and the Main Idea

This work presents development of the problem of conflict control of epidemic processes on networks. This area has been topic of research interest among different fields, including biology, computer science, economics, and the social sciences. Epi demic dynamic in population, computer virus spreading over communication network, and rumors or fake news widening through social networks are examples of very different processes with the same nature.

One of the first epidemic models was developed by D.Bernulli in 1760, motivated by smallpox in England. Later on, other researchers also studied mathematical models of decease spreading. These models were quite simplistic, but provided insights into mechanisms how different deceases can affect population. After initial development this direction of study become classical topic without promising findings. Recently, however, there has been returning to these problems due to "network paradigm". Nowadays, we can see meeting in one point three different fields:

- spreading (for example epidemic) models [1]
- network analysis [2]
- game theory [3]

supported by parallel computational algorithms, sufficient to perform computation for networks dynamic in realistic scale. So far main problem was to build and analyze epidemic models, but today the point of efforts shifting towards effective control of spreading under conflict and uncertainty. Taking into account the most recent attacks on computer networks and security issues it is very natural to expand results to the field of malware mitigation [4]. Consider the heterogeneous SI dynamics:

$$\dot{p}_i = \sum_{j=1}^{M} \beta_{ij}\, p_j(1 - p_j) - u_i$$

where p_i is the probability of infection of *i*th node, β_{ij} - are elements of matrix with infection rates for every i-j node interaction, u_i - our influence on process, or in other words, control.

It is natural to set constraints for control in geometric and integral form

$$u_i \in [0, u_i^{max}], \int_0^T u_i(t)dt \leq u_i^{int}$$

also it is usual to define the objective function to be minimized (for example in form with linear costs):

$$\int_0^T (cp_i(t) + bu_i(t))dt \to min$$

For this problem there is idea to use Pontryagin's maximum principle. As shown in [5] (for simplistic setup) that the optimal solution is in form of bang-bang control. Our main goal to extend this approach for more general setup.

Consider a network, defined by adjacency matrix $A = \{a_{ij}\}$. Dynamic of epidemic process on this network is described by system of equations:

$$\dot{p}_i = \beta(1 - p_i)\sum_{j=1}^{M} a_{ij}p_j$$

with p_0 - vector of initial infection probabilities.

Optimal control idea. Control $u_i(t)$ could be applied to (every) node to delay spreading process. The main goal is to delay infection with minimal cost.

Conflict-control idea. If we reformulate original problem to set imaginary "player", responsible for infecting. Let us define $v_i(t) = \beta(1 - p_i)\sum_{j=1}^{M} a_{ij}\, p_j$, then the process

$$\dot{p} = v - u$$

is a conflict-controlled process [6]. The goal is to find $u_i(\cdot)$ as a function of $v_i(t)$ to protect the network from infection (or at least formulate conditions when it is possible to do). This is challenging problem which should be supported with theoretical and practical tools to analyze.

In this work we provide a simulation tool to compute spreading process (in SI model setup) for arbitrary networks.

2 Simulations

Simulation models were developed using R environment and available for working at [7]. For arbitrary network topology and initial infection distribution we run SI model and calculate spreading process on the network. There are two input files: network structure – .csv file with pairs of nodes. Each pair is a connection between them. Second file is names of infected (at the beginning) nodes. There are two methods imple-

mented – network dynamic without additional infection (classical SI model) and network dynamic 2 – infection, which gives influence on other nodes starting from any non-zero level. The results are presented on Fig. 1.

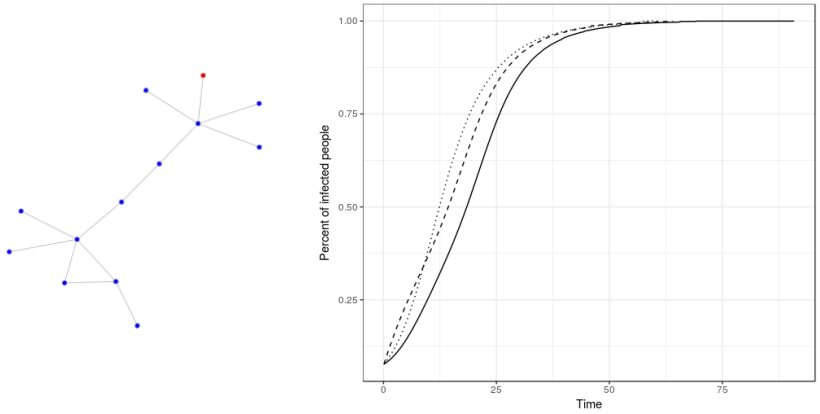

Fig.1. Example network topology and spreading graph.

Solid line shows dynamic for the case when infected node is at the most distant node from the center. Dotted line is for the case when infected node is on the border. Dashed line is for the case when infected node is in the centre. As we can understand from simulations network topology has immediate and strong effect on the spreading process.

Second direction of simulations was to calculate bang-bang control and its effect on SI model dynamic [8]. On the fig.2 there is simple SI model for $\beta = 0.2$ and $p_0 = 0.02$. There are two controls: red (starts at 5 and ends at 10, power 0.07) and green (starts at 13 and ends at 29, power 0.24).

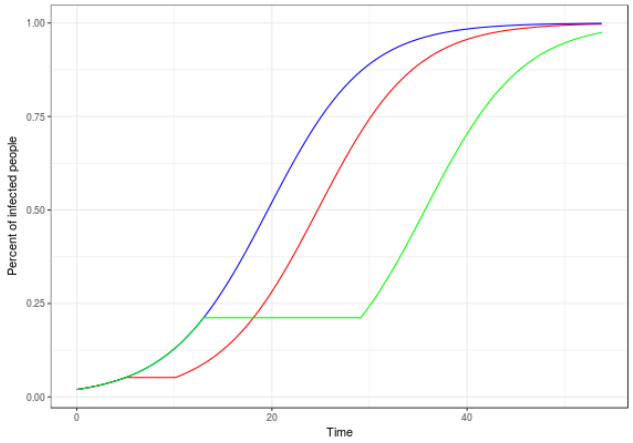

Fig. 2. Different setup of bang-bang control.

On fig. 3 it is shown result of different controls with the time of working 10 – 20 (red) and 15 – 25 (green). As we can conclude – it is much more effective to deal with spreading at the beginning them after some time.

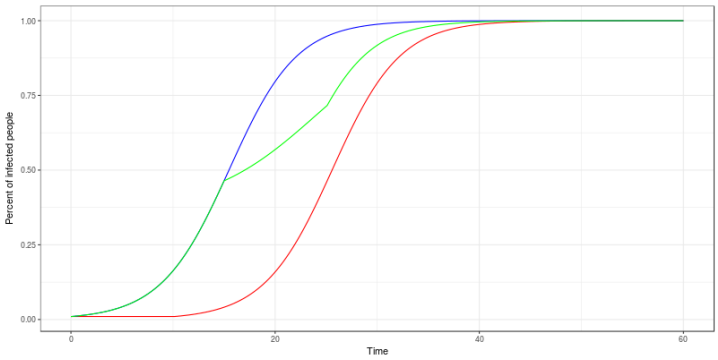

Fig. 3. Step-type control with the same power.

In this work we present tool for network simulations, developed to get better understanding of spreading dynamics. Also we create bang-bang control simulation to illustrate its efficiency.

References

1. Nowzari, C., et al.: Analysis and control of epidemics: A survey of spreading processes on complex networks. IEEE Control Systems 36(1), 26–46 (2016).
2. Newman, M.: Networks: an introduction. Oxford university press, (2010).
3. Ignatenko, A.: Game-Theoretical Model of Users Interaction in Computer Networks. Journal of Automation and Information Sciences 49.8, 68–81 (2017).
4. Eshghi, S., et al.: Optimal patching in clustered epidemics of malware. IEEE Trans. Network 24(1), 283 – 298 (2015).
5. Khanafer, A., Basar, T.: An optimal control problem over infected networks. In Proc. Int. Conf. Control, Dynamic Systems, Robotics, pp.1–6. Ottawa, ON, Canada (2014).
6. Chikrii, A.: Conflict-controlled processes. Vol. 405. Springer Science & Business Media, (2013).
7. Shiny application, https://ignat.shinyapps.io/Networks/, last accessed 2018/04/16
8. Shiny application, https://ignat.shinyapps.io/SI_simple_control/, last accessed 2018/04/16