Indonesian Journal of Computing, Engineering, and Design

Journal homepage: http://ojs.sampoernauniversity.ac.id/index.php/IJOCED

Effective Graph Protection Method to Prevent the Spreading of Attacks in Networks

A. W. Wijayanto[1*], *A. Pindarwati*[2]

[1] Department of Computer Science, Tokyo Institute of Technology, Japan
[2] Badan Pusat Statistik (BPS) Indonesia, Jakarta, Indonesia
Correspondence: E-mail: ariewahyu@net.c.titech.ac.jp

ABSTRACT

Networks are fundamental models for representing and analyzing the structures of real-world systems. For instance, in social networks, nodes are used to represent users and edges represent the connection between users. Networks are also termed as graphs in the discrete mathematics language. One essential problem in networks is how to protect a limited number of nodes to prevent the spreading of malicious attacks or dangerous rumor in the networks, which is known as the graph protection problem. In this paper, an effective graph protection method called PowerShield is proposed which pre-emptively protects critical nodes prior to any incoming attacks. It combines connectivity and centrality criteria of the input graph. Connectivity criterion is measured by the principal eigenvector, i.e., the eigenvector corresponding to the largest eigenvalue of the adjacency matrix of the input graph. Centrality criterion is defined by the degree centrality which considers nodes having more neighborhood relations to be more important. Contrary to the existing state-of-the-art method which takes into account only the connectivity criterion, the proposed method combines both criteria and empirically improves the effectiveness of protection result.

ARTICLE INFO

Article History:
Received 19 Jun 2019
Revised 29 Jul 2019
Accepted 18 Aug 2019
Available online 30 Sep 2019

Keywords:
graph protection,
node immunization,
graph connectivity,
principal eigenvector.

1. INTRODUCTION

With the rising popularity of massive-scale online social networks such as Facebook, Instagram, Twitter, etc., people are more connected and can share information with each other (Wijayanto & Takdir, 2014; Zhuang *et al.*, 2013). These platforms play a vital role in the dissemination of positive information such as new ideas, innovations, and hot topics. However, they may also become channels for the spreading of malicious rumors, misinformation, or even dangerous virus and malware. The rumor spreading can severely threaten public safety and financial stability. For instance, some people may post on social networks a rumor about an upcoming big earthquake. It will cause chaos among society and hence may hinder the normal public order. In this situation, it is necessary to find individuals, if

doi.org/10.35806/ijoced.v1i2.61

their account deactivated or removed from the network, would block further rumor spreading. This problem is known as a graph protection problem with the goal is to select a set of nodes to be protected in order to prevent the spreading of attacks by maximizing the ratio of surviving nodes in a network (Chen *et al.*, 2016; Wijayanto & Murata, 2017). In this problem, the protection budget constrains the number of nodes that are allowed to be protected.

The structure of networks dictates how quickly the infection or information will propagate. We may exploit the network structure to determine specific nodes for protection, such that the spreading of infection is considerably diminished. There are traditional approaches of node importance in graphs such as degree centrality (Newman, 2010), PageRank centrality (Page *et al.*, 1999), closeness centrality (Dangalchev, 2006), etc. However, they are not designed specifically for infection spreading case (Chen *et al.*, 2016; Newman, 2010). Thus, there is no special attention for protection effectiveness, which could lead to poor performance in real-world networks.

The spreading of attacks is commonly modeled using the epidemic model (Zhang & Prakash, 2014b). Most of the existing works in graph protection problem can be classified into two classes: preemptive and post-emptive strategies. The former strategy aims to protect the critical nodes prior to epidemic attacks, behaving as prevention efforts (Wijayanto & Murata, 2018a; Tong *et al.*, 2010). The critical nodes are the set of nodes assumed to contribute in blocking large-scale epidemic spreading if being protected (Chen *et al.*, 2016; Wijayanto & Murata, 2018a, 2019). The later strategy post-allocates the protection while the epidemics have already propagated over the network, simulating as delayed reactions (Song *et al.*, 2015; Zhang & Prakash, 2014b). The pre-emptive protection methods are naturally applicable in the post-emptive strategy but not vice versa (Zhang & Prakash, 2014a, 2015), thus they provide a wider range of applications. Given the benefit as prevention efforts, in this paper, our focus is on developing an effective method for the pre-emptive graph protection strategy.

The current state-of-the-art method in the graph protection problem is NetShield method by (Chen *et al.*, 2016). It presented the utilization of perturbed matrix characteristics to define a submodular protection measurement of a particular set of nodes. It also demonstrated that the largest eigenvalue of the adjacency matrix represents the connectivity of a particular graph. Thus, the set of nodes having a maximum drop in the eigenvalue of the adjacency matrix of the input network, regarding their deletion from the network, have more necessity to be protected in order to break the graph connectivity.

However, the NetShield method focused solely on the graph connectivity and ignored the beneficial property of graph centrality and edge directionality of graphs. In graph centrality, especially the degree centrality, nodes with more connections are considered to be more important. In this paper, a new method called PowerShield was proposed which combines the connectivity and centrality criteria to determine the critical nodes in the preemptive graph protection strategy. Connectivity criterion is measured by the principal eigenvector, i.e., the eigenvector corresponding to the largest eigenvalue of the adjacency matrix (Chen *et al.*, 2016; Prakash *et al.*, 2012; Zhang & Prakash, 2015). Centrality criterion is defined by the degree centrality which considers nodes with more neighborhood connections to be more important. The proposed method will be demonstrated the combined criteria empirically improve the effectiveness of protection result.

Furthermore, in this paper, the graph protection problem on single-layered static networks will be formalized and an extensive experimental evaluation on the multiple real-world network datasets will be performed to demonstrate the effectiveness of the proposed method. It is expected that the proposed method will outperform several other existing methods, such as NetShield, NetShield+, Degree, PageRank, SubGraph, etc.

2. PROBLEM FORMULATION

In this section, the definition of problems and terms used throughout this paper will be formalized. **Table 1** provides the main terms and notations used in the paper.

Definition 1. **Protecting** a node means removing all of its connecting edges. The number of nodes we allow to protect is constrained by the ***protection budget*** ($k \in Z > 0$). At time t, a node in a network can belong to any of the following states: susceptible and infected. ***Attacking*** a node means initially infect the node in a network. **Figure 1** shows the example of protection and attack in a network. Green colored icon indicates the user is protected. Dashed green colored edges indicate the connections are removed or inactivated because of protection. The initial red-colored user on the network indicates the user is attacked. Other red-colored users indicate the infected users.

Definition 2. **Graph Protection Problem**. Let $G = (V, E)$ be a connected single-layered static graph with a set of nodes V and set of edges E. Let ϑ be the surviving ratio of nodes that remain uninfected at the end of epidemics. Given an input graph G, SIS or SIR epidemic model, and a protection budget k, the goal is to find a set of nodes $S \in V$ such that ϑ is maximized, subject to the size of S is equal to constraint protection budget k. The protection is performed by removing all edges connected to the set of nodes S in graph G.

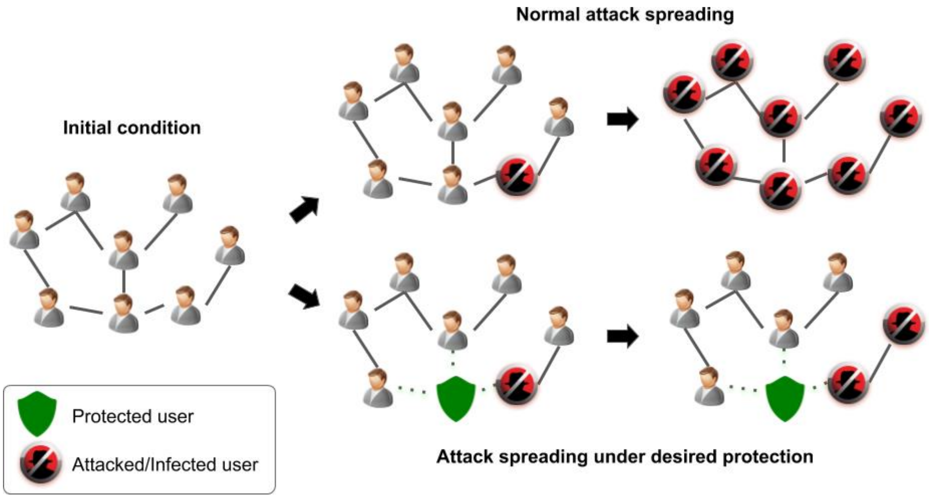

Figure 1. Example of the graph protection in a network

Table 1. Terms and notations

Notations	Definitions and Descriptions
$G = (V, E)$	graph G with the node set V and the edge set E
k	the protection budget (the number of nodes allowed to be protected)
A	adjacency matrix of graph G
$A (i, j)$	the i-th row and j-th column element of A
$A (i,:)$	the i-th row element of adjacency matrix A
$A (:, j)$	the j-th column element of adjacency matrix A
n	number of nodes in graph G
m	number of edges in graph G
λ	largest eigenvalue of adjacency matrix A
η	corresponding eigenvector of λ
$w (i,j)$	weight of edge connecting node i and j
$d (i)$	degree of node i
$PM (i)$	Protection Metric of node i, a metric which represents the necessity of node i to be protected
σ	infection rate
ρ	recovery rate
φ	number of initial infected nodes in graph G
ϑ	ratio of surviving nodes at the end of epidemics in graph G
$S(t)$	the number of susceptible nodes at time t
$I(t)$	the number of infected nodes at time t

Definition 3. **SIS Epidemic Model**. Susceptible – Infected - Susceptible (SIS) is an epidemic model which defines that each node in graph G with n number of nodes would be in one of the following two states: susceptible and infected. Let $S(t)$ be the number of susceptible nodes, and let $I(t)$ be the number of infected nodes at time t. At each timestamp t, susceptible nodes can be infected by their infected neighbors with infection rate σ. Also, each infected node can get recovered to a susceptible state with recovery rate ρ.

Definition 4. **SIR Epidemic Model**. In the Susceptible – Infected - Recovered (SIR) epidemic model, each node in graph G belong to any of the susceptible, infected, or recovered state. Each of recovered node is resistant of any infection.

3. PROPOSED METHOD

In this section, the proposed preemptive graph protection method on networks will be described. The main idea of this method is discussed first, which consists of the following key points: the connectivity criterion and the degree centrality criterion. Then, the proposed method, called PowerShield, which combines both of the criteria will be described.

3.1. The Connectivity Criterion

Chen *et al.* introduced that the largest eigenvalue (λ) of the adjacency matrix of a graph indicates the connectivity of the whole graph (Chen *et al.*, 2016). The higher value of λ, the more connected the graph. **Figure 2** illustrates the value of λ in different network topology. For instance, given the same number of no des n = 5, clique topology (which each of its nodes is connected to all other nodes) has the largest value of λ, that is λ = 4.00, compared to the star and chain topologies with λ = 2.00 and λ = 1.73 respectively. Considering the connectivity, it is more likely that an epidemic will spread out in the graphs on the clique faster than those on the star and chain.

In order to prevent the epidemic spreading in the networks, Wang *et al.* also demonstrated the role of the largest eigenvalue as the epidemic threshold of arbitrary epidemic models on arbitrary networks (Wang *et al.*, 2003). Epidemic threshold is an intrinsic property of a network. When the strength of the infection is smaller than the epidemic threshold, then the epidemic could not spread over the network. Prakash *et al.* provided theoretical analysis and proof that if the infection strength < 1/λ, where λ is the largest eigenvalue of adjacency matrix of the input network, an epidemic would not spread (Prakash *et al.*, 2012). Prakash *et al.* also confirmed the finding of Wang et al. in their evaluation that the epidemic threshold can be predicted using the largest eigenvalue since the threshold relies upon the structure of the graph (Wang *et al.*, 2003).

In graph theory, the largest eigenvalue (λ) of a graph also represents the capacity of the graph in terms of loop capacity and path capacity (Chen *et al.*, 2016; Prakash *et al.*, 2012). Van Dam and Kooij also show that the smaller the value of λ, the more robust a network against infection spreading (van Dam & Kooij, 2007). The largest eigenvalue of the adjacency matrix (λ) of the input graph as the connectivity criterion is considered in this paper. To assign the connectivity of each node, following Chung and Brouwer, each node is associated with a vector element of the principal eigenvector (η) (Brouwer & Haemers, 2012; Chung, 1997). The principal eigenvector (η) is the corresponding eigenvector of λ.

3.2. The Degree Centrality Criterion

(Borgatti, 2005) and (Newman, 2010) discussed the important role of the degree centrality in networks. There are many advantages of prioritizing the high degree nodes among the other nodes (Newman, 2010). The degree centrality can be interpreted in terms of the immediate risk of a node for catching whatever is flowing through the network (for instance: a virus, or some information) from its neighboring nodes. Regards to a directed network (where edges have direction), two distinct measures of degree centrality are known, specifically indegree and outdegree.

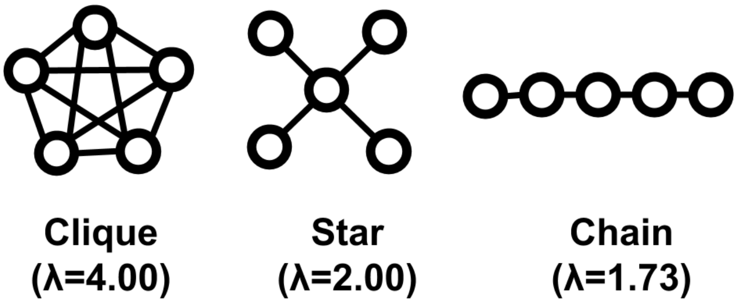

Figure 2. The largest eigenvalue (λ) indicates the graph connectivity (Chen et al., 2016).

In real-world social networks, when edges are associated with some positive aspects such as friendship or collaboration, indegree is commonly presumed as a type of popularity, and outdegree as companionship.

Borgatti (2005) analyzed and demonstrated the correlation of the degree centrality to information flow which is beneficial to be considered in preventing the spreading of information or epidemics in networks. In the proposed method, the beneficial property of this centralization is incorporated to the method and considered it to be an important factor of the infection spreading process. In any arbitrary undirected networks, the use of degree centrality as one of the criteria to determine the critical node will be suggested.

In information or infection spreading, outdegree centrality is highly associated with how to control and prevent cascading infection as emphasized by (Borgatti, 2005) and (Lee, Cotte, & Noseworthy, 2010). Outdegree represents the possibility of certain infected nodes to infect their neighbors. Thus, in the proposed method, the outdegree as a centrality criterion for directed networks will be applied. In weighted networks, the weighted outdegree as the degree centrality criterion will be considered.

3.3. PowerShield Algorithm

To protect the set of critical nodes against the infection spreading, a metric for each node, called the Protection Metric (PM), representing its necessity to be protected is considered. The higher score of the metric, the higher importance of the node to be selected in the protection scheme.

The Protection Metric of node i is calculated by combining the connectivity and the degree centrality criteria. The connectivity criterion of each node which is represented by the principal eigenvector (η) has different order of magnitude with the degree value. According to (Marler & Arora, 2004) and (Gerasimov & Repko, 1978), given that both criteria have different orders of magnitude and are assumed of the same importance, without having to normalize each criterion, a combination of both criteria can be calculated as multicriterial optimization using product formulation as follows:

$$PM\,(i) = |\eta_{\,i}.d(i)| \qquad (1)$$

Algorithm 1. ***PowerShield*** **method**

```
Data: Graph $G = (V, E)$
Input: the adjacency matrix $A$ and the protection budget $k$
Output: a set $S$ of $k$ nodes

Compute the largest eigenvalue $\lambda$ of $A$ using Power method approximation;
Let $\eta$ be the corresponding eigenvector of $\lambda$ where $\eta_i$ = 1,…,n;
Let $d\,(i)$ be the degree value of node $i$ for $i$= 1,…,n;
Initialize $S$ to be empty;
begin
        $PM\,(i) = |\eta_{\,i}.d(i)|$;
        for i = 1 to $k$ do
                Let $j \leftarrow argmax$ i $PM\,(i)$, add $j$ to set $S$;
        end
        return $S$
end
```

Algorithm 1 provides the detail of the proposed PowerShield. It provides a set S of k nodes as the output and requires the adjacency matrix A and the protection budget k as the input. The largest eigenvalue (λ) and its corresponding eigenvector (η) from the adjacency matrix A were computed. PM value of each node in step 6 was assigned and k nodes with the highest PM score in step 7-9 was selected.

4. EXPERIMENTAL SETTINGS

4.1. Datasets

The experiments were simulated on various real-world network datasets. Two types of network structures are provided: undirected and directed networks as summarized in **Table 2**.

- Highschool is a social friendship network between boys in a small highschool in Illinois in 1957-1958.
- Moreno-Sheep is a social network describes the dominance relationships between female bighorn sheep in Montana in 1984.
- US Airports contains the flights network between US airports in 2010.
- Facebook Ego is the social network of user–user friendships in Facebook.
- NeuralNetwork (Watts & Strogatz, 1998) represents the neural network of C. Elegans species.
- Dolphins (Lusseau *et al.*, 2003) is a social network of frequent associations between 62 dolphins in New Zealand.

4.2. Parameter Settings

For effectiveness evaluation, the same parameters were used for all methods. Unless stated otherwise, the infection rate σ = 0.9 and the recovery rate ρ = 0.6 under SIS epidemic model were used, as used by (Zhang & Prakash, 2015) and (Chen et al., 2016); the protection budget k = 20% for smaller datasets (less than 200 nodes), k = 10% for larger datasets, and the number of initial infected nodes in a graph φ = k as suggested by (Chen et al., 2016) were also applied. Random initialization to determine the infected nodes in was used. On each dataset, 100 times of simulations were conducted and the average was taken. For NetShield+ method, the default batch size was 2.

4.3. Evaluation Metric

The protection effectiveness result of all methods using the ratio of surviving nodes (ϑ) was compared.

4.4. Comparison Methods

The proposed method was compared with some existing baseline methods: Degree (Newman, 2010), PageRank (Page et al., 1999), EigenVector (Newman, 2010), SubGraph (Newman, 2010), KCoreness (Newman, 2010), Closeness (Dangalchev, 2006), Greedy (Chen *et al.*, 2016), and the state-of-the-art methods: NetShield and NetShield+ (Chen *et al.*, 2016).

Table 2. Statistics of the dataset

Name	#nodes	#edges	Type
Highschool	70	316	Directed Weighted
Moreno-Sheep	28	250	Directed Weighted
US Airports	1,574	28,236	Directed Weighted
Facebook Ego	2,888	2,981	Undirected Unweighted
Neural Network	297	2,345	Directed Weighted
Dolphins	62	159	Undirected Unweighted

5. RESULTS AND DISCUSSIONS

5.1. Effectiveness Evaluations

The methods were simulated on random attack and provide average after 100 simulations. **Table 3** shows that PowerShield outperforms the other methods regarding the highest average of surviving nodes ratio (ϑ) at the end of propagation after 100 timesteps.

PowerShield also performs well in undirected networks by assuming the bi-directionality of edges. In the directed weighted networks (Neural Network, US Airport, and Highschool), PowerShieldis able to improve the protection effectiveness of the current state-of-the- art method: NetShield and its variant, called NetShield+. PowerShield could improve up to 2% of surviving nodes ratio.

Table 3. Effectiveness Evaluation

Methods	Highschool		Moreno-Sheep		US Airports	
	Average	Std. Dev.	Average	Std. Dev.	Average	Std. Dev.
Degree	0.7040	0.0081	0.7293	0.0244	0.7319	0.0013
PageRank	0.7049	0.0089	0.7321	0.0261	0.7319	0.0012
EigenVector	0.7037	0.0083	0.7332	0.0256	0.7319	0.0014
SubGraph	0.7030	0.0074	0.7318	0.0256	0.7322	0.0014
Kcoreness	0.7049	0.0082	0.7318	0.0251	0.7321	0.0013
Greedy	0.7043	0.0080	0.7325	0.0261	0.7319	0.0013
NetShield	0.7037	0.0083	0.7325	0.0261	0.7768	0.0145
NetShield+	0.7054	0.0083	0.7332	0.0261	0.7315	0.0015
PowerShield	**0.7064**	0.0087	**0.7479**	0.0300	**0.7326**	0.0015

Methods	Facebook Ego		Neural Network		Dolphins	
	Average	Std. Dev.	Average	Std. Dev.	Average	Std. Dev.
Degree	0.8817	0.0843	0.7079	0.0032	0.8592	0.0200
PageRank	0.8978	0.0806	0.7072	0.0031	0.8639	0.0243
EigenVector	0.8944	0.0777	0.7074	0.0037	0.8616	0.0216
SubGraph	0.8903	0.0743	0.7071	0.0038	0.8618	0.0244
Kcoreness	0.8804	0.0791	0.7078	0.0034	0.8634	0.0241
Greedy	0.8966	0.0811	0.7082	0.0032	0.8611	0.0229
NetShield	0.8858	0.0729	0.7072	0.0032	0.8581	0.0205
NetShield+	0.8886	0.0777	0.7074	0.0031	0.8603	0.0254
PowerShield	**0.9059**	0.0779	**0.7086**	0.0034	**0.8685**	0.0239

5.2. Sensitivity to Epidemic Parameters

In this section, the parameter sensitivity of the PowerShield method when applied to several different combination of simulation parameters was analyzed. Simulations to investigate the performance of the PowerShield method under three scenarios were performed:

(1) Comparison of survival ratio ϑ when the infection rate (σ) changes

(2) Comparison of survival ratio ϑ when the recovery rate (ρ) changes

(3) Comparison of survival ratio ϑ when the epidemic propagation rate (σ / ρ) changes

For a fair analysis and comparison, simulations are performed under a fixed protection budget (k).

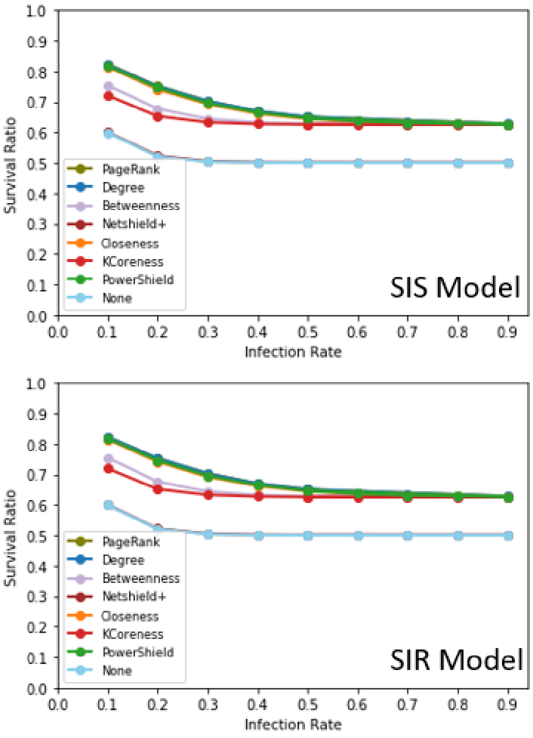

Figure 3. Sensitivity evaluation to the infection rate (σ)

5.2.1. Comparison of survival ratio (ϑ) when the infection rate (σ) changes

Figure 3 shows the comparison of survival ratio (ϑ) of all methods with the changing of the infection rate (σ) from {0.9; 0.8; 0.7; 0.6; 0.5; 0.4; 0.3; 0.2; 0.1} and fixed recovery rate (ρ = 0.5). The results are averaged from 100 simulations with a fixed protection budget $k = 0.25N$, where N is the number of nodes of the input network. The proposed method achieves the highest survival ratio regardless of the value of infection rate and epidemic models.

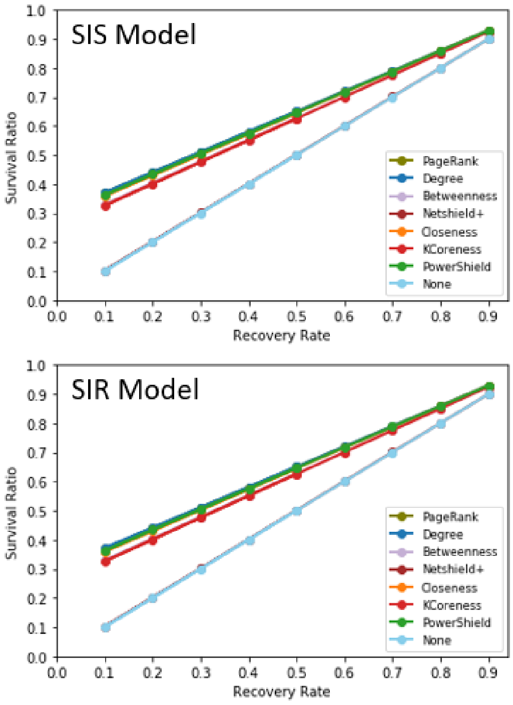

Figure 4. Sensitivity evaluation to the recovery rate (ρ)

5.2.2. Comparison of survival ratio (ϑ) when the recovery rate (ρ) changes

Similarly, in the sensitivity analysis to the recovery rate (ρ), as shown in **Figure 4**, the recovery rate (ρ) from {0.9; 0.8; 0.7; 0.6; 0.5; 0.4; 0.3; 0.2; 0.1} was changed. The infection rate (σ = 0.5) and protection budget $k = 0.25N$, where N is the number of nodes of the input network were fixed. The PowerShield method maintain the highest survival ratio (ϑ) regardless the value of recovery rate and epidemic models.

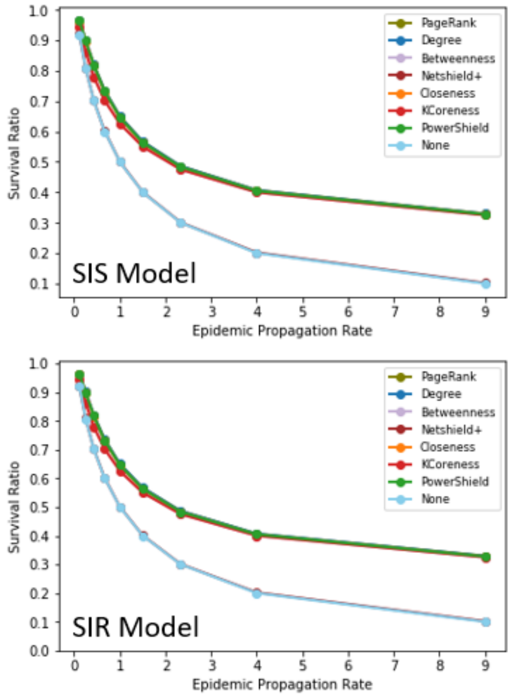

Figure 5. Sensitivity evaluation to the epidemic propagation rate (σ/ρ)

5.2.3. Comparison of survival ratio (ϑ) when the epidemic propagation rate (σ/ρ) changes

The changing of the epidemic propagation rate (σ/ρ) from { 0.9/0.1 ; 0.8/0.2 ; 0.7/0.3 ; 0.6/0.4 ; 0.5/0.5 ; 0.4/0.6 ; 0.3/0.7; 0.2/0.8 ; 0.1/0.9} was simulated. Figure 5 shows the comparison of survival ratio in SIS and SIR epidemic models. The results are averaged from 100 simulations under the fixed protection budget $k = 0.25N$, with N is the number of nodes of the input network. All comparison methods achieve very high survival ratio when the epidemic propagation rate (σ/ρ) is very small, then by the increasing the value of σ/ρ, the resulted survival ratios are also decreasing. The PowerShield method maintain the superiority regardless the values of σ/ρ but with a small margin.

6. CONCLUSION

In this paper, the problem of protecting a limited number of nodes to restrain the spreading of malicious attacks or dangerous rumor in the networks, called as the graph protection problem were addressed. An effective graph protection method on networks, called PowerShield which combines the connectivity and degree centrality criteria was proposed. Evaluation on various real graph datasets shows that the PowerShield outperforms the state-of-the-art algorithm in terms of protection effectiveness.

Future direction on this problem might be focused on the investigation of more complex network settings such as probabilistic network and partially observable network. The theoretical framework using discrete optimization could also worth be studied to provide the estimated upper and lower bound of protection result.

REFERENCES

Borgatti, S. P. (2005). Centrality and network flow. Social Networks, 27(1), 55–71.

Brouwer, A. E., & Haemers, W. H. (2012). Spectra of Graphs. New York, NY: Springer New York.

Chen, C., Tong, H., Prakash, B. A., Tsourakakis, C. E., Eliassi-Rad, T., Faloutsos, C., & Chau, D. H. (2016). Node Immunization on Large Graphs: Theory and Algorithms. IEEE Transactions on Knowledge and Data Engineering, 28(1), 113–126.

Chung, F. R. K. (1997). Spectral Graph Theory. Providence, Rhode Island, USA: American Mathematical Society.

Dangalchev, C. (2006). Residual closeness in networks. Physica A: Statistical Mechanics and

Its Applications, 365(2), 556–564.

Gerasimov, E. N., & Repko, V. N. (1978). Multicriterial optimization. Soviet Applied Mechanics, 14(11), 1179–1184.

Kermack, W. O., & McKendrick, A. G. (1927). A Contribution to the Mathematical Theory of Epidemics. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 115(772), 700–721.

Lee, S. H. (Mark), Cotte, J., & Noseworthy, T. J. (2010). The role of network centrality in the flow of consumer influence. Journal of Consumer Psychology, 20(1), 66–77.

Lusseau, D., Schneider, K., Boisseau, O. J., Haase, P., Slooten, E., & Dawson, S. M. (2003). The bottlenose dolphin community of doubtful sound features a large proportion of long-lasting associations: Can geographic isolation explain this unique trait? Behavioral Ecology and Sociobiology, 54(4), 396–405.

Marler, R. T., & Arora, J. S. (2004). Survey of multi-objective optimization methods for engineering. Structural and Multidisciplinary Optimization, 26(6), 369–395.

Newman, M. (2010). Networks: An Introduction. New York, NY, USA: Oxford University Press, Inc.

Page, L., Brin, S., Motwani, R., & Winograd, T. (1999). The pagerank citation ranking: Bringing order to the web (No. Previous number=SIDL-WP-1999-0120).

Prakash, B. A., Chakrabarti, D., Valler, N. C., Faloutsos, M., & Faloutsos, C. (2012). Threshold conditions for arbitrary cascade models on arbitrary networks. Knowledge and Information Systems, 33(3), 549–575.

Song, C., Hsu, W., & Lee, M. L. (2015). Node Immunization over Infectious Period. In Proceedings of the 24th ACM International Conference on Information and Knowledge Management (pp. 831–840).

Tong, H., Prakash, B. A., Tsourakakis, C., Eliassi-Rad, T., Faloutsos, C., & Chau, D. H. (2010). On the vulnerability of large graphs. Proceedings - IEEE International Conference on Data Mining, ICDM, 1091–1096.

van Dam, E. R., & Kooij, R. E. (2007). The minimal spectral radius of graphs with a given diameter. Linear Algebra and Its Applications, 423(2–3), 408–419.

Wang, Y., Chakrabarti, D., Wang, C., & Faloutsos, C. (2003). Epidemic spreading in real networks: an eigenvalue viewpoint. In 22nd International Symposium on Reliable Distributed Systems, 2003. Proceedings. (pp. 25–34). IEEE Comput. Soc.

Watts, D., & Strogatz, S. (1998). Collective dynamics of ’small-world’ networks. Nature, 393(June), 440–442.

Wijayanto, A. W., & Murata, T. (2017). Flow-Aware vertex protection strategy on large social networks. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2017.

Wijayanto, A. W., & Murata, T. (2018a). Learning Adaptive Graph Protection Strategy on Dynamic Networks via Reinforcement Learning. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 534–539). Santiago, Chile: IEEE.

Wijayanto, A. W., & Murata, T. (2018b). Pre-emptive spectral graph protection strategies on multiplex social networks. Applied Network Science, 3(1), 5.

Wijayanto, A. W., & Murata, T. (2019). Effective and scalable methods for graph protection strategies against epidemics on dynamic networks. Applied Network Science, 4(1), 18.

Wijayanto, A. W., & Takdir. (2014). Fighting cyber crime in email spamming: An evaluation of fuzzy clustering approach to classify spam messages. In 2014 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 19–24). IEEE.

Zhang, Y., & Prakash, B. A. (2014a). DAVA: Distributing Vaccines over Networks under Prior Information. In Proceedings of the 2014 SIAM International Conference on Data Mining (pp. 46–54). Philadelphia, PA: Society for Industrial and Applied Mathematics.

Zhang, Y., & Prakash, B. A. (2014b). Scalable Vaccine Distribution in Large Graphs given Uncertain Data. In Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management - CIKM ’14 (pp. 1719–1728). New York, New York, USA: ACM Press.

Zhang, Y., & Prakash, B. A. (2015). Data-Aware Vaccine Allocation Over Large Networks. Acm Transactions on Knowledge Discovery from Data, 10(2), 20.

Zhuang, H., Sun, Y., Tang, J., Zhang, J., & Sun, X. (2013). Influence maximization in dynamic social networks. Proceedings - IEEE International Conference on Data Mining, ICDM, 1313–1318.