Hindawi
Scientific Programming
Volume 2021, Article ID 2390466, 9 pages
https://doi.org/10.1155/2021/2390466

Research Article

ITDPM: An Internet Topology Dynamic Propagation Model Based on Generative Adversarial Learning

Hangyu Hu, Xuemeng Zhai, Gaolei Fei, and Guangmin Hu

School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Correspondence should be addressed to Xuemeng Zhai; zxm@uestc.edu.cn

Received 26 April 2021; Accepted 19 May 2021; Published 29 May 2021

Academic Editor: Yi-Zhang Jiang

Network information propagation analysis is gaining a more important role in network vulnerability analysis domain for preventing potential risks and threats. Identifying the influential source nodes is one of the most important problems to analyze information propagation. Traditional methods mainly focus on extracting nodes that have high degrees or local clustering coefficients. However, these nodes are not necessarily the high influential nodes in many real-world complex networks. Therefore, we propose a novel method for detecting high influential nodes based on Internet Topology Dynamic Propagation Model (ITDPM). The model consists of two processing stages: the generator and the discriminator like the generative adversarial networks (GANs). The generator stage generates the optimal source-driven nodes based on the improved network control theory and node importance characteristics, while the discriminator stage trains the information propagation process and feeds back the outputs to the generator for performing iterative optimization. Based on the generative adversarial learning, the optimal source-driven nodes are then updated in each step via network information dynamic propagation. We apply our method to random-generated complex network data and real network data; the experimental results show that our model has notable performance on identifying the most influential nodes during network operation.

1. Introduction

Nowadays, from various telecommunication systems to power grid systems, it can be seen that everyone's lives are affected and dominated by today's real-world complex networks [1–5]. However, although various emerging network technologies have brought about more and more convenience to humans in many fields, the network is also vulnerable to potential risks and threats. The research of the information propagation such as spreading of rumors, influence diffusion, packet forwarding, and epidemic proportions has a long tradition in network science including social network analysis, Internet topology analysis, and complex biological network analysis. Identifying the influential source nodes that make the information propagates as quickly as possible is one of the most important problems in network science, and many researchers did hard works on finding such influential nodes [6–11].

With the classic infectious disease models including SI, SIS, and SIR model proposed, researchers began to pay attention to the impact of the network structure on the propagation behavior. However, most analyses of the propagation are directed to macroscopic statistical characteristics of network structures, ignoring the actual connection of links. Research on influential nodes' identification has to be based on the clear network structure, and the optimal influence problem is shown to be NP-hard [12]. Artificial intelligence emerging in recent years aims to solve the difficult problems using machine learning such as the generative adversarial network (GAN) [13]. The ideal of the GAN is to optimize the results of the generator through constant confrontation between the generator and the

discriminator. The process of generator optimization could be regarded as a kind of generative adversarial learning [14, 15]. Therefore, with the mature complex network theory and new artificial intelligence methods, the problems of the influential nodes' identification could be solved efficiently.

In this paper, we propose an Internet Topology Dynamic Propagation Model (ITDPM) to find the influential nodes in the Internet topology. The model consists of two parts: the generator and the discriminator like the GANs. The generator aims to identify the influential nodes that make the information propagate as quickly as possible in the Internet topology at the current stage. Two famous theory methods in network science are used and modified to be adaptive to the characteristics of the Internet topology: network controllability and node importance parameters. The discriminator is designed to simulate the information propagation and evaluate the performance based on the influential nodes that the generator generates. The performance of the propagation will be fed back to the generator to help the model update the set of influential nodes. The propagation rate and the coverage are used as the general parameters to evaluate the performance of the generator and determine the stopping conditions of the model. Experiments on routing attack propagation are conducted based on both simulated and real-world network topology to show the performance of ITDPM on the influential nodes' identification. The experimental results show notable performance in identifying the optimal influential nodes to make the information propagate as quickly as possible through our model.

The main contributions of the present research are summarized as follows:

(1) According to the minimum input theorem, we can discover the minimum set of driving nodes in the Internet topology to ensure that the speed and breadth of information propagation from these nodes can reach the fastest speed.

(2) This paper utilizes ITDPM as an effective tool to identify the optimal influential nodes in Internet topology. The model consists of two processing stages: the generator and the discriminator like the GANs.

(3) The experimental results show that, compared to traditional methods, our approach effectively identifies the optimal influential nodes in Internet topology and is also useful for improving network security management by enhancing critical nodes' security policy.

The rest of this paper is organized as follows: Section 2 briefly surveys the related work of network vulnerability analysis and GAN. Section 3 introduces the preliminaries and problem definition of critical node detection in Internet topology. The framework of using the ITDPM for the optimal influential node identification is discussed in Section 4. Section 5 presents the experiments on information propagation and simulated routing attack. Finally, Section 6 gives the conclusions and presents possible future work.

2. Related Work

The study on epidemics offers powerful models for analyzing the information propagation, such as the SI, SIS, and SIR model [16, 17]. However, those models do not care about the specific structure of the networks. Therefore, the problem of influential nodes' identification based on the actual structure of the networks has become a significant issue in recent years. In [6], the problem to find the minimal set of influential nodes was mapped onto optimal percolation in random networks, which were arisen by minimizing the energy of a many-body system, where the form of the interactions is fixed by the nonbacktracking matrix of the network. In [18], the influential nodes were identified through the family of H-indices. The convergence to coreness could be guaranteed even under an asynchronous updating process, allowing a decentralized local method to calculate a node's coreness in large-scale evolving networks. In [19], the optimal percolation theory was used to predict and subsequently target nodes that are essential for global integration of a memory network in rodents. In [20], a node information dimension is proposed by synthesizing the local dimensions at different topological distance scales. In [21], the spreading capacity of the focal node was accurately characterized by assigning different weights for each class of neighbors and summing up the neighbors' contributions.

However, the GAN in the field of artificial intelligence is widely used to solve difficult problems in various disciplines [22]. In [23], the GAN was used to predict socially plausible futures and encourage diverse predictions with a novel variety loss. In [24], a novel method to fuse two types of information using a GAN was proposed, termed as FusionGAN. In [25], a new GAN-based model was presented to calculate for each large transfer probability that it is fraudulent, such that the bank can take appropriate measures to prevent potential fraudsters from taking the money if the probability exceeds a threshold. To the best of our knowledge, few works of the GAN are applied on the Internet topology or the complex structure.

3. Problem Definition

In the real-world Internet topology, network packets are delivered based on the specific routing protocol, such as BGP, TCP, and ICMP. The forwarding path of the packets can be used as propagation path of the information because the packets themselves can be the carriers of network information propagation or some malicious attacks. Therefore, we can model the forward path of the Internet topology to form a complex network with nodes and edges. Figure 1 shows the routing example of the real word by the CAIDA research institute [26]. The definition is shown as follows.

Definition 1. Internet Routing Propagation Network. Given a directed network $G = <V, E>$, where V refers to the set of nodes and E refers to the set of directed edges among nodes, the routers and hosts are abstracted as the nodes in G and the forwarding path for router i to router j is abstracted as the

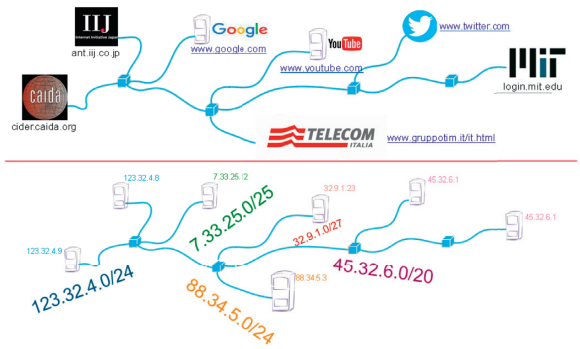

Figure 1: The routing example of the real word by CAIDA research institute.

edge e_{ij} meaning that node i points to the node j. The directed network G denotes the Internet routing propagation network.

Figure 2 shows a graph model example of the Internet routing propagation network built based on the data from CAIDA [27]. The hosts are hidden for the visualization. Though the real-world forwarding paths based on the Internet topology are abstracted as the theoretical network, they cannot be processed directly by the machine or participate in computing operations. In network science, the adjacency matrix addresses the problem as a two-dimension matrix to represent the network. Therefore, we use the adjacency matrix to describe the directed Internet routing propagation network, denoted as follows.

Definition 2. Transfer Adjacency Matrix. Given an adjacency matrix A_{N*N} of directed network G, where N refers to the number of nodes in G, the elements $a_{ij} = 1$ if there is an edge pointing from node i to node j and otherwise $a_{ij} = 0$. The adjacency matrix A_{N*N} is donated as the transfer adjacency matrix only if it is the adjacency matrix of the Internet routing propagation network. The element a_{ij} refers to the packets forwarding path between the routers or the hosts.

The Internet routing propagation network could be abstracted as a complex network and be represented through the transfer adjacency matrix. Our goal is to find the source nodes that make the information propagates as quickly as possible. Therefore, a propagation model has to be built to simulate and analyze the propagation process. Since the router protocol is updated regularly during a specific interval, ideally, we assume that information is propagated through each update. Therefore, our main problems could be summarized as follows.

Problem 1. Propagation Model Construction. Given the Internet routing propagation network G and its transfer adjacency matrix A, the first problem is to build a propagation model to simulate the propagation process of the information. The information is assumed to propagate through each specific interval of the routing update.

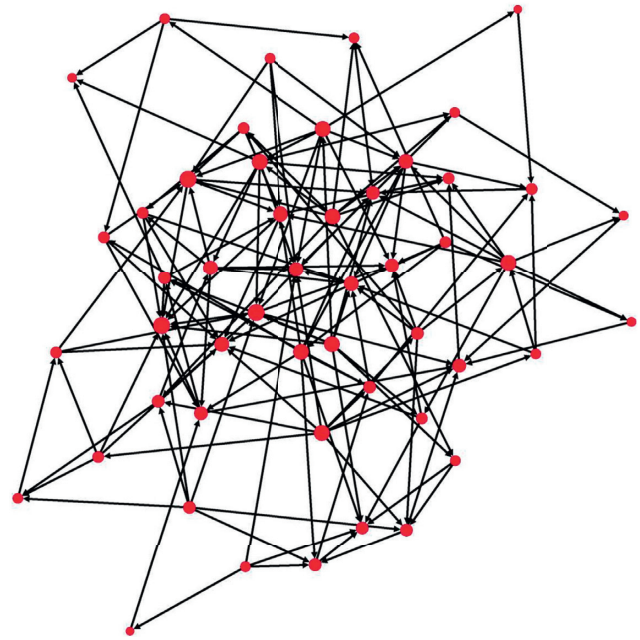

Figure 2: The graph model of the Internet routing propagation network.

Problem 2. Influential Nodes' Identification. Given the propagation model, the problem is to find a set of optimal source nodes that make the information propagate as quickly as possible. Such a set of source nodes is denoted as the set of influential nodes R.

With the two problems, we build the ITDPM as the propagation model M to identify the influential nodes R. The detailed model is discussed in the next section.

4. Internet Topology Dynamic Propagation Model

In this section, a detailed description of our ITDPM is given. The main idea of the ITDPM is based on generative adversarial learning. It consists of two parts, including the generator and the discriminator like the GANs. However, there is no network in the model. Therefore, the generation and discrimination process could be regarded as a kind of generative adversarial learning. The components of ITDPM are shown in Figure 3.

The two main components of ITDPM are the generator and discriminator. The task of the generator is to analyze the Internet routing propagation network and identify the influential nodes that make the information propagate as quickly as possible. The methods of influential nodes' identification combine the network controllability and node importance parameter in the complex network. Both theories have been modified to be adaptive to the characteristics of the Internet topology. The discriminator aims to simulate the information propagation process and compute the spreading parameters to evaluate the performance of the generator. The remaining topology will be fed back to the

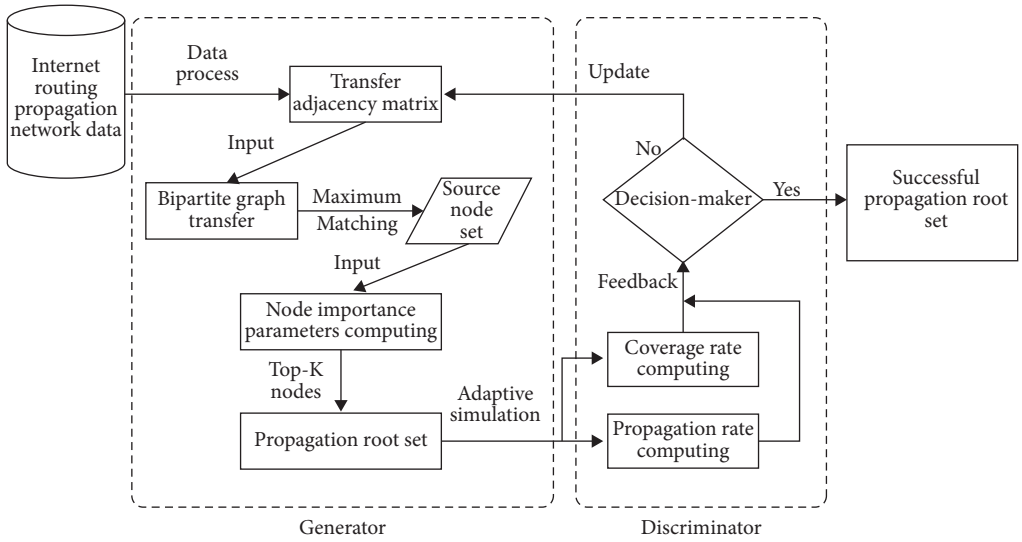

Figure 3: The system components of the ITDPM.

generator to find other better source nodes. There are two situations that cause the feedback: (1) the performance dissatisfies the requirements including slow propagation speed and low coverage; (2) the propagation stops due to the structure of the directed network. These two situations will lead to the stagnation of information dissemination in the Internet.

The ITDPM gets the optimal influential nodes R after several times of generating and discriminating. The outputs of the generator are the influential nodes in each propagation stage. The outputs of the discriminator are the parameters that could evaluate the performance of the information propagation based on the influential nodes from the generator. Two general parameters are used in the ITDPM: the propagation rate curve and the coverage. Other discriminant parameters could be added to the discriminator to evaluate the performance of the generator and determine the stopping conditions of the model, such as the propagation delay and packet loss rate in the routing attack propagation network. The ITDPM will stop and output the final optimal influential nodes.

4.1. The Generator Stage. The generator aims to identify the influential nodes in the Internet routing propagation network. Given a directed Internet routing propagation network G, the primary task is to identify the source routers for the packet forwarding. The second task is to filter the optimal nodes from the source routers that could make the information propagate as quickly as possible. Therefore, two well-known theoretical methods in network science are used and modified to be adaptive to the characteristics of the Internet topology: network controllability and node importance parameters. We first give the details of the two theories in the generator.

4.1.1. Network Controllability. The network controllability is also known as the structural controllability [28]. In the most real-world network system, the topology structure is the only known condition, and the weights of the connection are usually unknown. The structural controllability is to study how to identify the minimum number of driver nodes to control the whole network under the unknown strength of the interaction among nodes. Therefore, the minimum input theorem is proposed to get the driver nodes. It is proved that, in order to fully control a directed network G, the minimum number of input nodes (or equivalently the minimum number of driver nodes) is related to the size of a maximum matching in G. Therefore, we first introduce the concept of the network matching.

4.1.2. Network Matching. M is an independent edge set without common nodes. A node is matched if it is incident to an edge in the matching. For a directed network, an edge subset M is matching if no two edges in M share a common starting node or a common ending node. A node is matched if it is an ending node of an edge in the matching.

In both networks, the matching of maximum size is called maximum matching. In general, there could be many different maximum matchings for a given network. A maximum matching is called perfect if all nodes are matched. Therefore, to analyze the structural controllability of the network, the directed network G needs to be transferred to the bipartite graph set B. The bipartite graph contains two sets of nodes: the set of starting nodes S and the set of end nodes D. The edges only exist between the nodes in different two sets. The unmatched nodes and matched starting nodes in the maximum matching of the bipartite graph are the driver nodes. The process of bipartite graph transfer and matching is shown in Figure 4.

The driver node set contains two categories: the source nodes of the propagation links and the nodes on the branch links. The source nodes of the propagation links are our target nodes. Therefore, the minimum input theorem is changed to only get the root nodes in the maximum matching of the bipartite graph shown in Figure 4. It is easy to find the root nodes because each matching edge consists

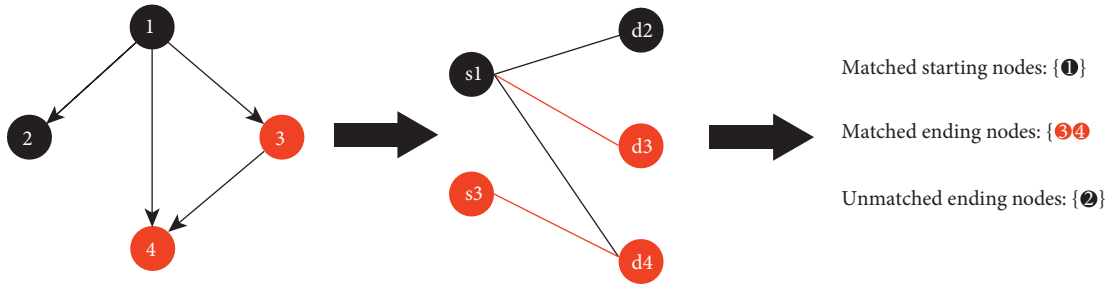

Figure 4: The process of the bipartite graph transfer and matching.

of the starting node and the end node. The root node of the link could be traced back by finding the matching between the starting node and the ending node of the two edges.

The root nodes found through the modified minimum input theorem are the source nodes of the directed links in a directed network. In the Internet routing propagation network, those nodes are the starting nodes of the packet forwarding. In other words, they are the source nodes of information propagation, denoted as set S.

4.1.3. Node Importance Parameter. With the development of network science, several parameters that describe the importance of nodes are proposed in the past decades. In this paper, two node importance parameters that best match the characteristics of the Internet topology are used to measure the influence of the source nodes S. The influence here refers to the impact of the source nodes on the information propagation rate and coverage of the entire Internet topology. These node importance parameters are the betweenness centrality and k-shell. The basic conception of the two parameters is as follows.

Betweenness centrality is a parameter of the influence measurement of a node over the links of information between every pair of nodes under the assumption that information primarily propagates over the shortest paths between them, denoted as follows:

$$BC_i = \sum_{s \neq i \neq t} \frac{n_{st}^i}{g_{st}}, \tag{1}$$

where g_{st} refers to the number of shortest paths from node s to node t and n_{st}^i refers to the number of all shortest paths from node s to node t through node i.

K-shell decomposition is an extension of the importance ranking of nodes based on the node degree. The process of k-shell decomposition is to iteratively remove the nodes of which degree equals k until there is no such node in the network from $k = 1$. The k-shell nodes consist of the removed nodes at k times.

Figure 5 shows the betweenness centrality and k-shell. The betweenness centrality is consistent with the requirements of most routing protocols such as RIP and OSPF for the shortest path propagation. The k-shell matches the hierarchical structure of the Internet topology. The nodes with large k-shell tend to be the core routers in the Internet topology. Therefore, the information carried by the packet forwarding can be propagated faster from nodes with both high betweenness centrality and k-shell.

In order to measure the influence of the nodes in the set of source nodes S, the normalization equation of the two node importance parameters is used to describe such influence I, denoted as follows:

$$I_S = \alpha * BC_i + \beta * k_{i-\text{shell}}, \tag{2}$$

where α and β are the coefficients that balance the weights of the two parameters.

4.1.4. The Process of the Generator Stage. When computing the influence I_s of each source node s in S, the i-step influential nodes R_i could be defined as the top-k influence source nodes in the set of source nodes S. At each step of the propagation, the current optimal influential nodes are generated through the improved methods in network science and transferred to the discriminator to get the simulated performance of the propagation. The influential nodes are updated after the discriminator sends a new network topology.

4.2. The Discriminator Stage. The main task of the discriminator is to simulate the information propagation and evaluate the performance based on the influential nodes that the generator generates. The performance of the propagation will be fed back to the generator to help the model update the set of influential nodes. Our ITDPM assumes that the information is propagated through each update of the router protocol during a specific interval. Therefore, each interval could be regarded as a time unit of propagation. The information is propagated from one node to another over a time unit. With the ideal hypothesis, it is easy to simulate and evaluate the performance of the propagation process. We first introduce the two general parameters for the propagation evaluation.

4.2.1. Evaluation. The two parameters are the propagation rate and the coverage rate. Both parameters only require the basic abstracted nodes and propagation links. They do not require any other specific requirements such as node attributes and edge weights. Therefore, the two parameters are the general measurements for the evaluation.

Propagation rate refers to the number of nodes that are propagated per time unit, denoted as

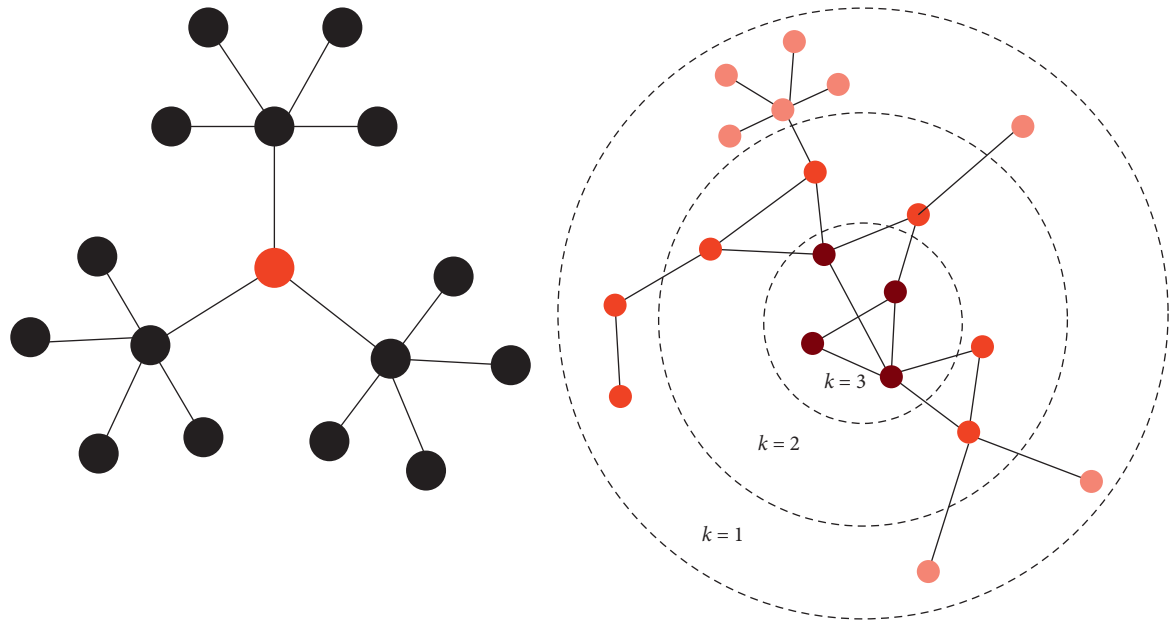

Figure 5: The schematic diagram of betweenness centrality and (k)-shell: (a) the red node is with the highest betweenness centrality; (b) the nodes with darker color refer to the larger (k)-shell.

$$v_r = \frac{dN_p}{dt}, \tag{3}$$

where N_p is the number of nodes that are propagated. The average propagation rate $v_a = N_p/t$.

Coverage rate refers to the ratio of the number of propagated nodes to the total number of nodes in the network, denoted as

$$c_r = \frac{N_p}{N}. \tag{4}$$

The propagation rate describes the speed of the propagation, and the coverage rate stands for the breadth of the propagation. The two parameters comprehensively evaluate the propagation process in a general sense. To some specific situation, some other parameters could be used to evaluate the performance such as the propagation delay and packet loss rate in the routing attack propagation.

4.2.2. The Process of the Discriminator Stage. The discriminator will determine whether it is a successful propagation according to the value of the propagation rate v_r and coverage rate c_r. If both v_r and c_r are larger than the specified thresholds, the decision parameter D will be 1 to show that it is a successful propagation. Otherwise, the decision parameter D will be 0, and the generator will update the propagation roots based on the remaining network structure which consists of those nodes not propagated.

5. Experimental Results

In order to show the performance of our ITDPM on the influential nodes' identification, experiments on the routing attack propagation are conducted based on both simulated and real-world network topologies. It is assumed that the attack could cause the routers unworkable and the attack will be carried on the updated packets of the routing protocol. The simulated network topology is generated by NS-3 simulator with 3,000 nodes and 4,513 directed edges. The forwarding paths are computed through the router table of each router in the simulated network topology. The real-world network topology is generated based on the data from SNAP. It is the AS Internet topology from CAIDA and contains 26,475 nodes and 27,562 edges. Table 1 shows the detailed topological parameters of simulated data and real-world data. Both networks are directed. The simulated network topology is like a local network topology of the small scale and the AS Internet topology is the global networks of a large scale.

Two methods are compared with our ITDPM to identify the influential nodes that make the attack propagate as quickly as possible: the random identification (RI) and the maximum out-degree identification (MDI). The RI selects n nodes randomly as the root nodes to propagate the attack information. The MDI is to select the top-n nodes with the largest out-degree. The number of influential nodes is limited to 0.5% of the total number of nodes in the network topology. Therefore, in the simulated network topology, n is

Table 1: Topological parameters of simulated data and real-world data.

Name	Number of nodes	Number of edges	Avg. deg.	Diameter	K-shell layers
NS-3 data	3,000	4,513	2.75	15	3
CAIDA data	26,475	27,562	2.08	18	5

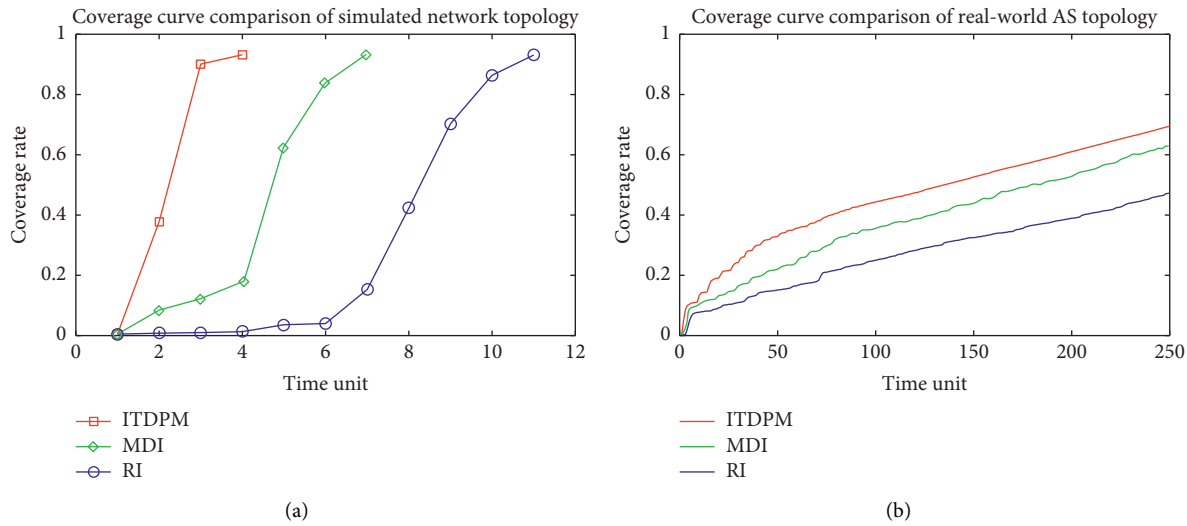

Figure 6: The comparison results of the coverage curve in both simulated network topology and real-world AS topology.

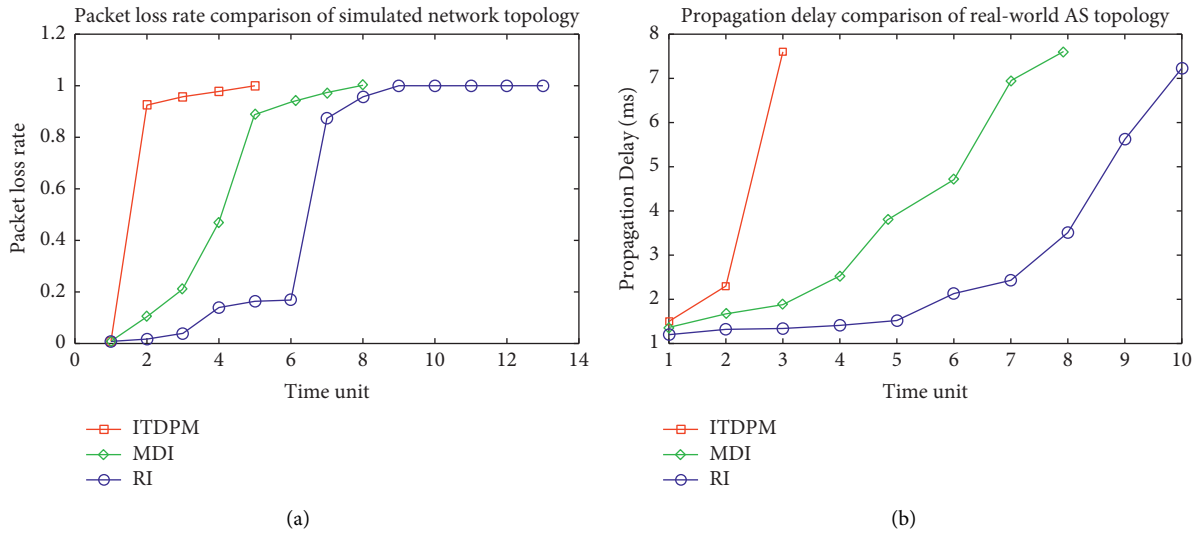

Figure 7: The comparison results of packet loss rate and propagation delay in simulated network topology and real-world topology.

no larger than 15, and in the real-world AS topology, n is smaller than 130. To make the two methods get the most optimal influential nodes, the value of n is selected as the upper bound of the range.

The coverage curve is used to evaluate the performance of the propagation. The coverage curve describes the coverage of propagated nodes at time unit. The derivative of the curve is the propagation rate. The curve can be computed in both simulated network topology and real-world AS topology. Particularly, in the simulated environment, two parameters could be computed to describe the influence of the attack: packet loss rate and propagation delay. The two parameters could describe the degree of damage to the network topology. Therefore, two parameters are computed to evaluate the simulated network topology as the additional measures.

The comparison results of the coverage curves in both simulated network topology and real-world AS topology are shown in Figure 6. Both results show the better performance of our method. In the simulated network topology with 1,000 nodes, the attack could be propagated nearly all nodes in 4 time units with our method and in 7 and 11 time units,

respectively, with the MDI and RI. In the small-scale network, it only needs one iteration for our ITDPM to find the optimal influential nodes, which demonstrates the effectiveness of the algorithms in the generator. In the real-world AS topology with 26,475 nodes, after 100 time units, the coverage rate of all methods is nearly linear. Before 100 time units, the result of ITDPM keeps the fast propagation rate. Each jump of the red curve represents the antagonism between the generator and the discriminator. The propagation rate will jump after the generator updates the set of the influential nodes.

The comparison results of the packet loss rate and the propagation delay in simulated network topology are shown in Figure 7. The two parameters evaluate the performance of the attack. As shown in experiment results, our ITDPM shows the best performance among all three methods. The packet loss rate and propagation delay show a strong correlation with the coverage rate shown in Figure 6. The packet loss of ITDPM reaches a quite high point at the second time unit, which means that the attack based on our ITDPM breaks the topology fast and completely. After 4 time units, all packets are lost under nearly 100% coverage rate of the propagated nodes. With the increase of the packet loss rate and coverage rate, the propagation delay based on our ITDPM grows exponentially to very high at the third time unit. After that, it becomes positive infinity because most of the nodes are unreachable.

6. Conclusion and Prospection

The results of both general parameters and specific parameters show a notable preference on the information propagation analysis and influential nodes' identification of our ITDPM. The rapid coverage rate demonstrates that our method can find the source nodes that make the information propagate as quickly as possible. The process of the antagonism between the generator and the discriminator could update the influential nodes based on the current network topology structure to help the information propagate faster. Our ITDPM works effectively on the attack propagation of the Internet routing topology based on the results of the packet loss rate and the propagation delay. The specific parameters indicate that the Internet topology is effectively broken based on our ITDPM.

In general, our ITDPM is a theoretical model of propagation analysis and influential nodes' identification based on generative adversarial learning. It can be used for any propagation problem based on the practical network structure, such as the spread of influence and rumors in social networks. The basic task for our model is to find the influential nodes that make the information propagate as quickly as possible. Our future work is dedicated to improving both generator and discriminator to get a more effective model in information propagation analysis.

Data Availability

The data sets used to obtain the results in this manuscript are available at http://snap.stanford.edu/.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 62071095) and the Sichuan Science and Technology Program under Grant 2019YFG0456.

References

[1] J. Su, Z. Sheng, A. X. Liu, Y. Han, and Y. Chen, "Capture-aware identification of mobile RFID tags with unreliable channels," *IEEE Transactions on Mobile Computing*, vol. 1, 2020 (in press).

[2] J. Su, A. X. Liu, Z. Sheng, and Y. Chen, "A partitioning approach to RFID identification," *IEEE/ACM Transactions on Networking*, vol. 28, no. 5, pp. 2160–2173, 2020.

[3] J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Idle slots skipped mechanism based tag identification algorithm with enhanced collision detection," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 5, pp. 2294–2309, 2020.

[4] J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Redundant rule detection for software-defined networking," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 6, pp. 2735–2751, 2020.

[5] J. Su, Z. Sheng, A. X. Liu, Z. Fu, and Y. Chen, "A time and energy saving-based frame adjustment strategy (TES-FAS) tag identification algorithm for UHF RFID systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 2974–2986, 2020.

[6] F. Morone and H. A. Makse, "Influence maximization in complex networks through optimal percolation," *Nature*, vol. 524, no. 7563, pp. 65–68, 2015.

[7] W. Chen, M. Jiang, C. Jiang et al., "Critical node detection problem for complex network in undirected weighted networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 538, 2020.

[8] M. Lalou, M. A. Tahraoui, and H. Kheddouci, "The critical node detection problem in networks: a survey," *Computer Science Review*, vol. 28, pp. 92–117, 2018.

[9] D. Santos, A. de Sousa, and P. Monteiro, "Compact models for critical node detection in telecommunication networks," *Electronic Notes in Discrete Mathematics*, vol. 64, pp. 325–334, 2018.

[10] G. Alozie, A. Arulselvan, K. Akartunali et al., "Efficient methods for the distance-based critical node detection problem in complex networks," *SSRN Electronic Journal*, vol. 131, 2021.

[11] M. Ficco, M. Choraś, and R. Kozik, "Simulation platform for cyber-security and vulnerability analysis of critical infrastructures," *Journal of Computational Science*, vol. 22, pp. 179–186, 2017.

[12] D. Kempe, J. Kleinberg, and É Tardos, "Maximizing the spread of influence through a social network," in *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 137–146, Washington, DC, USA, August 2003.

[13] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza et al., Generative adversarial networks, 2014.

[14] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial

networks: an overview," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 53–65, 2018.

[15] J. Ho and S. Ermon, "Generative adversarial imitation learning," in *Proceedings of the 30th International Conference on Neural Information Processing Systems*, pp. 4572–4580, Barcelona, Spain, December 2016.

[16] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[17] M. Boguná and R. Pastor-Satorras, "Epidemic spreading in correlated complex networks," *Physical Review E*, vol. 66, no. 4, Article ID 047104, 2002.

[18] L. Lü, T. Zhou, Q. M. Zhang et al., "The H-index of a network node and its relation to degree and coreness," *Nature Communications*, vol. 7, no. 1, pp. 1–7, 2016.

[19] G. Del Ferraro, A. Moreno, B. Min et al., "Finding influential nodes for integration in brain networks using optimal percolation theory," *Nature Communications*, vol. 9, no. 1, pp. 1–12, 2018.

[20] T. Bian and Y. Deng, "Identifying influential nodes in complex networks: a node information dimension approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 4, Article ID 043109, 2018.

[21] C. Li, L. Wang, S. Sun, and C. Xia, "Identification of influential spreaders based on classified neighbors in real-world complex networks," *Applied Mathematics and Computation*, vol. 320, pp. 512–523, 2018.

[22] X. Wu, K. Xu, and P. Hall, "A survey of image synthesis and editing with generative adversarial networks," *Tsinghua Science and Technology*, vol. 22, no. 6, pp. 660–674, 2017.

[23] A. Gupta, J. Johnson, L. Fei-Fei et al., "Social gan: socially acceptable trajectories with generative adversarial networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2255–2264, Salt Lake, UT, USA, June 2018.

[24] J. Hou, D. Zhang, W. Wu, J. Ma, and H. Zhou, "A generative adversarial network for infrared and visible image fusion based on semantic segmentation," *Entropy*, vol. 23, no. 3, 376 pages, 2021.

[25] Y.-J. Zheng, X.-H. Zhou, W.-G. Sheng, Y. Xue, and S.-Y. Chen, "Generative adversarial network based telecom fraud detection at the receiving bank," *Neural Networks*, vol. 102, pp. 78–86, 2018.

[26] D. Clark and K. Claffy: Knowledge of Internet Structure: Measurement, Epistemology, and Technology https://www.caida.org/projects/kismet/.

[27] K. Claffy: Center for applied internet data analysis, http://www.caida.org/home/.

[28] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Controllability of complex networks," *Nature*, vol. 473, no. 7346, pp. 167–173, 2011.