Reliable Communication Models in Interdependent Critical Infrastructure Networks

Sisi Duan, Sangkeun Lee, Supriya Chinthavali, Mallikarjun Shankar
Oak Ridge National Laboratory
Email: {duans, lees4, chinthavalis, shankarm}@ornl.gov

***Abstract*—Modern critical infrastructure networks are becoming increasingly interdependent where the failures in one network may cascade to other dependent networks, causing severe widespread national-scale failures. A number of previous efforts have been made to analyze the resiliency and robustness of interdependent networks based on different models. However, communication network, which plays an important role in today's infrastructures to detect and handle failures, has attracted little attention in the interdependency studies, and no previous models have captured enough practical features in the critical infrastructure networks. In this paper, we study the interdependencies between communication network and other kinds of critical infrastructure networks with an aim to identify vulnerable components and design resilient communication networks. We propose several interdependency models that systematically capture various features and dynamics of failures spreading in critical infrastructure networks. We also discuss several research challenges in building reliable communication solutions to handle failures in these models.**

I. Introduction

Modern critical infrastructure (CI) networks are becoming increasingly dependent on communication network with the development of technologies such as IoT and smart grid. Due to the rising of the technologies, the networks are more interdependent [12] than before where the failures of one network may cause the failures of other dependent networks. The 2003 North American blackout [1], [11], the 2003 Italian blackout [19], and 2012 Hurricane Sandy [2] are all such canonical examples. During the 2003 U.S. Northeastern power outage, 3,175 communication networks suffered from abnormal connectivity outage [11]. Indeed, reliable communication systems play an increasingly important role in today's critical infrastructure networks. For instance, in the 2012 Hurricane Sandy report [2], it was recommended that backup communication systems with batteries be prepared for both residential and business continuity.

In this paper, we study the interdependency between communication network and other CI networks. We propose several interdependency models, each of which captures some important features in heterogeneous CI networks. For simplicity, we use an example between a communication network and a power grid network, although the models can be extended to other heterogeneous CI networks. We study the effect of the *zigzag cascading failures*, where the two networks are mutually dependent. The failures of one network may cause failures both within the same network and the other dependent network. Such failures may cascade several times between the two networks. Indeed, depending on scenarios in different heterogeneous CI networks, the way failures cascade among the networks can vary. The interdependency models we propose consider different features in modeling the failures and the way in which cascading failures occur.

A number of previous efforts have been made on the analysis of the interdependent networks. Different models have been proposed to understand the relationship between CI networks. For instance, the *simple model* was presented in previous works [14], [25], which captures the essential features of CI networks about the relationship between the networks. However, most of these approaches ignore several factors such as the power supply and demand in the power grid network. To the best of our knowledge, existing interdependency models do not capture enough practical features in the CI networks that can serve the purpose of building a reliable communication network.

To address the limitations, we propose several practical interdependency models. For instance, the *weighted model* considers factors such as the power supply and demand. In addition, we consider the fact that a node failure will not only cascade to other networks but will also cause effects in the same network, e.g., the traffic control problem in road network where the congestion due to traffic at a node will cause failures of neighboring nodes. To capture this feature, we propose *spread model* and *weighted spread model*. In addition, the *cluster model* considers the failures such as network partition and the *probabilistic model* includes the facts where the failures are not deterministic, which works especially for modeling multiple heterogeneous network. Each model includes several features of some CI networks, which makes it challenging in building reliable broadcast solutions considering various types of failures such as software bugs and cyber attacks.

Based on the proposed interdependency models, we can identify vulnerable components in various CI networks and

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan). Support and requirements input from DOD Network Command are also gratefully acknowledged.

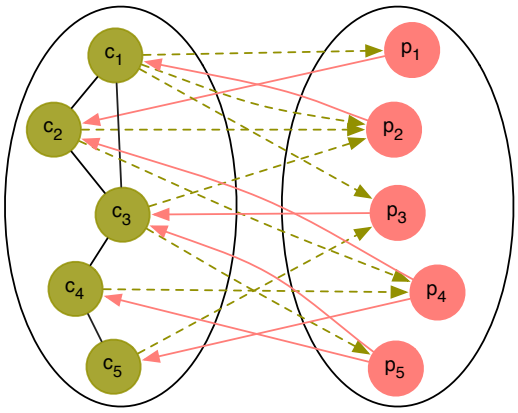


Fig. 1. A c-network with 5 c-nodes and a p-network with 5 p-nodes.

build reliable communication models in the communication network. Specifically, due to the communication capabilities of the nodes such as routers and sensors, nodes will be able to analyze the network and predict the failures in a fully distributed manner, based on which we can handle the failures before they are present.

II. Related Work

Modeling interdependencies between critical infrastructure networks is challenging due to the heterogeneity of CI networks such as the types of coupling and types of failures [26], [28]. A lot of previous work focus on the analysis and simulation of CI networks [5], [15]–[17], [24], [25], [31], which are broadly categorized into: empirical approaches, agent based, system dynamics based, economic theory based, and network based approaches [24]. We use graphs to represent the relationship between CI networks, which belongs to the network-based approaches [10], [17], [27]. It is a natural approach to the problem of reliable broadcast.

The mathematical frameworks for understanding the robustness of interdependent networks have been widely studied [6], [18], [22]. Those models focus on different types of connections between different models of networks, e.g., one-to-one correspondence [5], connections between nodes with the same degree [6], and interdependency between lattice networks [22]. We consider the interdependency models that capture features in real network and focus on the relationship between communication network and other CI networks.

Several previous efforts study the interdependency between communication network and power grid. Most of them focus on the simulation to find the vulnerabilities of existing network [25] or the design of a robust topology [16]. Our previous work [14] studies a resilient communication solution to predict cascading failures and handle it through the use of soft communication links so that messages can still be reliable delivered in the presence of crash failures in the communication network. In this paper, we propose several interdependency models between communication network and other CI networks. While our previous work uses a simple model as we show in this paper, this paper aims to capture more features in modeling heterogeneous CI networks.

Reliable broadcast is an essential tool in guaranteeing messages are reliably delivered at correct nodes in the presence of failures. It has been widely studied to tolerate both crash failures [20], [30] and Byzantine (arbitrary) failures [8] in both loosely connected graphs [13], [23], [30] and highly connected graphs [9], [20]. It has a wide application in distributed systems [7], storage systems [30], and communication network [29]. In this paper, we study the interdependency models to build reliable communication solutions.

III. Preliminaries

We study the interdependency between communication network *c-network* and other heterogeneous critical infrastructure networks. Specifically, we use the interdependency between two networks to represent the models, as shown in Fig. 1. Without loss of generality, we use power grid network *p-network* as an example in the rest of the papers to represent the models. The communication network consists of a set of m *c-nodes* $c_1, c_2, \cdots, c_m$ (e.g., routers, sensors, etc.). The power grid consists of a set of n *p-nodes* $p_1, p_2, \cdots, p_n$ (e.g. substations). The sizes of the two networks may or may not be the same.

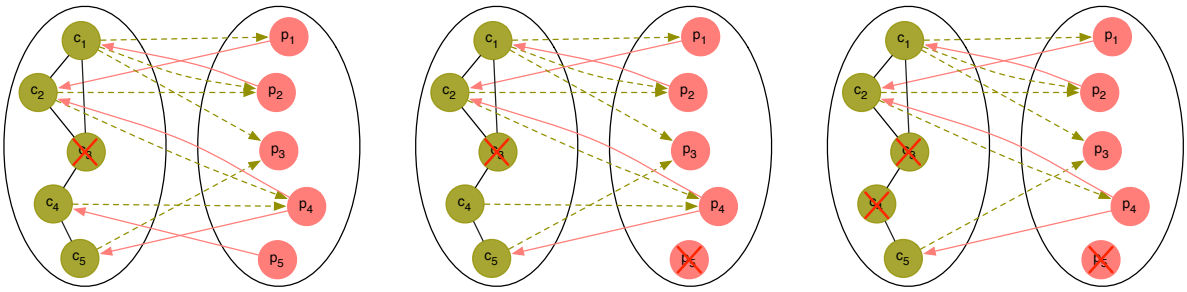
The interdependency between the networks can be represented in a directed graph $G = (V, E)$. We use edges and links interchangeably. $V = V_c \cup V_p$ is the set of the nodes where V_c is the set of c-nodes and V_p is the set of p-nodes. $E = E_c \cup E_p \cup E_{cp} \cup E_{pc}$ is the set of edges, where E_c represents the edges between c-nodes, E_p represents the edges between p-nodes, E_{cp} is the set of edges from c-nodes to p-nodes, and E_{pc} is the set of edges from p-nodes to c-nodes. The E_{cp} and E_{pc} edges, also referred to as *interdependency edges*, are directional. The E_c and E_p edges are bi-directional. Without loss of generality, we call two c-nodes *neighbors* or *direct neighbors* if there is an edge between them, i.e, they can communicate with each other. If a c-node c_i has an edge to a p-node p_i, we call p_i a *p-neighbor* of c_i. Similarly, if a p-node p_i has an edge to a c-node c_i, we call the c-node a *c-neighbor* of p_i. For any node, e.g., c-node c_i, we use $P(\overrightarrow{c_i})$ to represent the p-neighbors of c_i and $P(\overleftarrow{c_i})$ to denote the p-nodes that have an edge to c_i, i.e., c_i is a c-neighbor of $P(\overleftarrow{c_i})$. Similarly, for any p-node p_i, $C(\overrightarrow{p_i})$ represents the c-neighbors of p_i and $C(\overleftarrow{p_i})$ represent the c-nodes that have an interdependency edge to p_i, i.e., p_i is a p-neighbor of them.

IV. Interdependency Models

In this section, we introduce several models that model the interdependency between c-network and other critical infrastructure networks, as summarized in TABLE **??**. Based on different features of the models, we are able to build reliable communication solutions in different CI networks.

A. Simple Model

Models used in several previous works [14], [16], [25] can be generalized into a simple model, where a p-node *operates*



(a) Node c_3 fails and it cannot support p_2 and p_5.

(b) Node p_2 still has incoming interdependency edges from c_1 and c_2. Node p_5 fails.

(c) Node c_4 fails since p_5 does not have an edge to it.

Fig. 2. The simple model.

if it receives control signals from at least one c-node and a c-node *operates* if it receives power from at least one p-node, i.e., each node operates if there is at least one incoming interdependency edge. As illustrated in Fig. 2 based on the graph in Fig. 1, node c_3 fails, all its edges are removed, and it cannot support p_2 and p_5. Node p_2 still operates since it still has incoming edges from c_1 and c_2. However, node p_5 fails. Since there are not incoming interdependency edges, c_4 fails.

The simple model does not include much information about the heterogeneity of different networks, e.g., each substation (p-node) is connected to a generator that is sufficient for receiving power, the power supply or demand is not considered, the operating c-nodes are connected to the control center that is robust to failures, etc. In addition, it does not consider the relationship between nodes in the same network, i.e., network partition is not considered. Instead, this model captures the essential properties of the networks and is useful for analysis on the understanding of interlinking between different networks.

As we study in previous work [14], since the simple model only captures the topology of the networks, it provides a natural approach for the nodes to analyze and predict cascading failures in a fully distributed manner. Therefore, we can handle failures before they are present.

B. Weighted Simple Model

We use weighted graph to include the features such as the power supply or demand. In this specific case, it is meaningful to only make the E_{pc} edges weighted and other edges remain the same with the simple model. As shown in Fig. 3, the number on the links represent the weights as power supply, e.g., in Watts. For example, the failure of p_4 will make node c_2 lose 15W. Assuming that each c-node requires at least 10W to operate, c_2 will fail.

The weighted simple model can also be useful to also include the backup battery at c-nodes, e.g., uninterrupted power supply (UPS) for the routers. For instance, if node c_2 has an ups of 2W for 24 hours, it can operate continuously before the failures are handled. Based on this weighted model, the reliable communication solutions can handle both the failures caused by the interlinking of networks and the control issues in CI networks such as the power grid.

C. Spread Model

It can be observed that the simple model and weighted simple model do not consider the links among p-nodes, which can be only meaningful in networks where each node represents a single entity and the nodes are not interconnected, e.g., power substations, gas stations, etc. However, in other cases where nodes are connected in a natural way, such as flow lines and transportation networks, we must consider the links between the nodes, i.e., traffic tolerance. For instance, in road network *r-network*, a faulty node (*r-node*) may also spread to other neighboring r-nodes. In the c-network, it is also possible where a faulty causes the failures of neighboring nodes due to attacks, e.g., DoS attack.

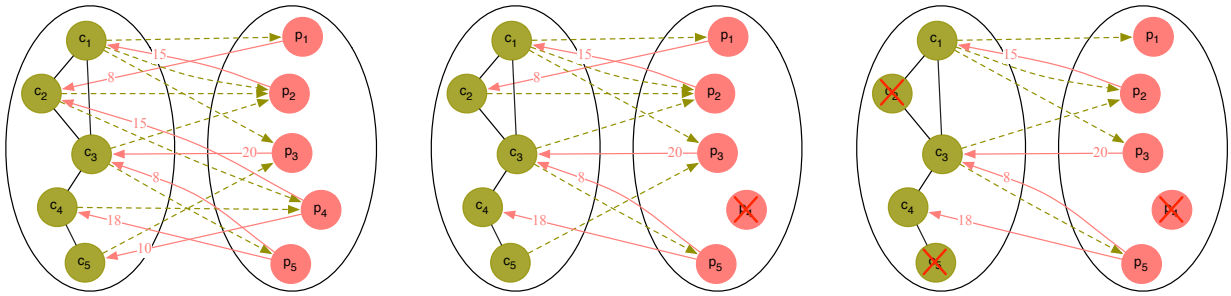
The spread model captures the feature where a faulty node will first spread and cause the failures of the same network. For instance, as shown in Fig. 4, similar with previous cases, the failure of c_3 causes the failures of p_5. The failure of p_5 spreads to p_4, which can not support c_2 and c_5. Node c_5 fails due to p_4 and node c_4 fails due to p_5.

The spread model can be extended in several ways. For instance, a faulty node can spread to all the direct neighbors in the same network, nodes within certain number of hops, etc. It provides a model for the reliable communication between c-network and the CI networks that are connected in a natural way, e.g., reliable traffic control between c-network and r-network.

D. Weighted Spread Model

The weighted spread model uses the weighted model to capture the spreading of failures. For instance, as shown in Fig. 5, the failures of p_5 spreads to p_4, which not only cause the failure of node c_4 and c_5, but also cause the failure of c_2 assuming c_2 requires 10W to operate but it can only receive 8W from node p_1.

In addition, the weighted spread model has other useful extensions. For instance, a faulty node spreads to the nodes within x hops where the nodes at the i^{th} hop decrease j in their supply. For instance, the failure of node p_5 spreads to

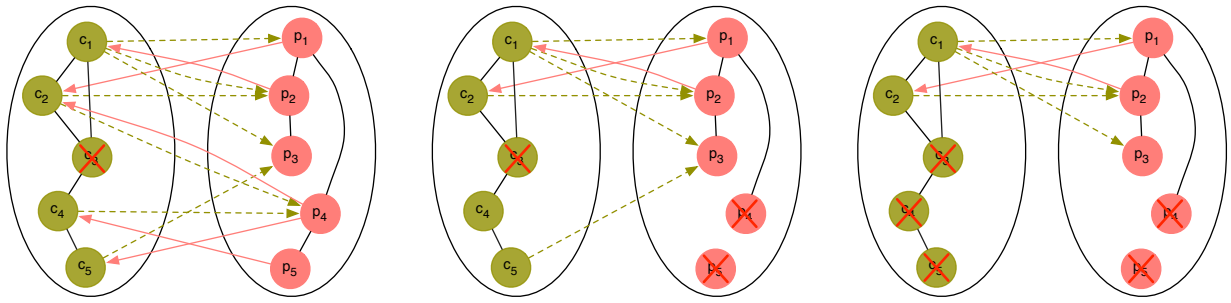


(a) The interdependency edges from p-nodes to c-nodes are weighted.

(b) Node p_4 fails.

(c) Node c_2 only receives 8 from p_1 and it requires 10 to operate, it fails.

Fig. 3. Weighted simple model where the weights represent the supply from p-nodes and each c-node requires at least 10 to operate.

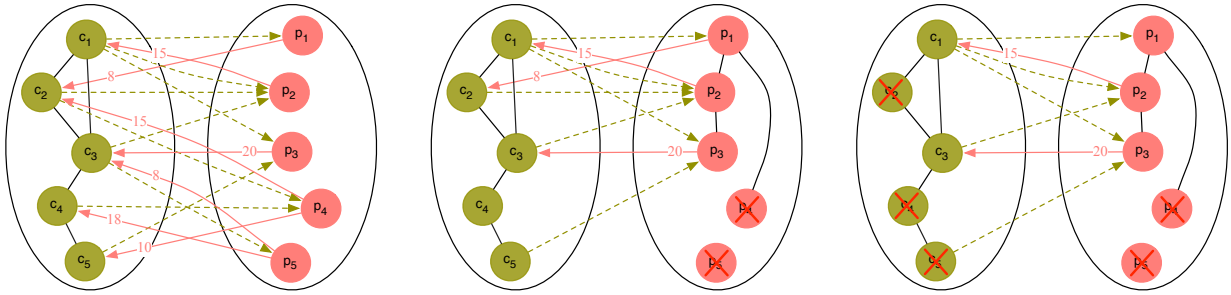


(a) Node c_3 fails.

(b) Node p_5 fails due to c_3. Its failure spreads to its neighbor p_4.

(c) Node c_4 fails due to p_5 and node c_5 fails due to p_4.

Fig. 4. The spread model



(a) Weighted graphs between c-network and p-network.

(b) Node p_5 fails and spreads to p_4.

(c) Node c_2 fails since there are no incoming edges. Node c_4 and c_5 then fail afterwards.

Fig. 5. The weighted spread model.

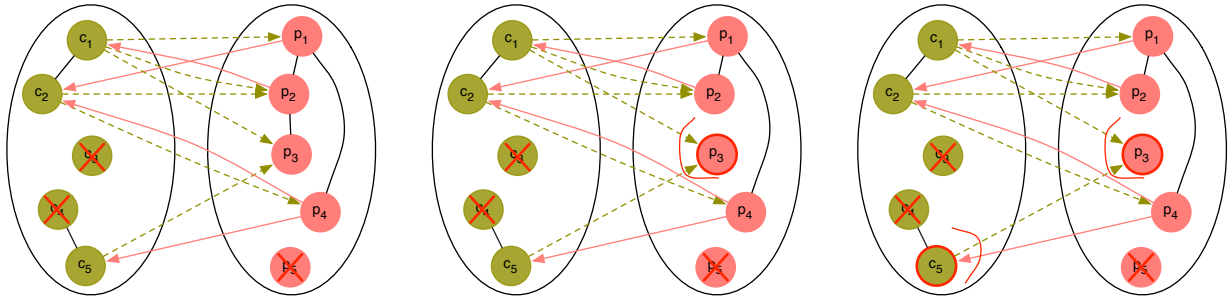
its direct neighbor p_4 and p_4 directly fails. The failure further spreads to p_1 and its supply amount is reduced to 5 from 8.

The weighted spread model can be used to build reliable communication between CI networks that are connected in a natural way and desire traffic tolerance, e.g., road network and flow line network.

E. Cluster Model

The cluster model considers a model based on any of previous models but considers an additional property: only nodes that are mutually dependent are potentially functional. For instance, as illustrated in Fig. 6, nodes c_3, c_4, and p_5 fail and other nodes all have at least one incoming interdependent edges. The c-nodes are partitioned and form two clusters: c_1 and c_2, and c_5. Node p_1, p_2, and p_4 are in the same cluster with c_1 and c_2 since each node has at least one outgoing interdependency edges and at least one incoming interdependency edges from the other network. Node p_3 only receives signals from node in the cluster, i.e., c_1. However, it does not provide power to the nodes int the cluster. Similarly, node c_5 does not form a cluster with any p-nodes. Therefore, only c_1, c_2, p_1, p_2, and p_4 are potentially functional.

The cluster model is similar with the model in previous work [5], which considers bidirectional interdependent edges



(a) Nodes c_3, c_4, and p_5 fail. Other nodes have incoming interdependency edges.

(b) Node p_3 is excluded from the cluster (c_1, c_2, p_1, p_2, p_4) since it does not have an outgoing interdependency edge to the cluster.

(c) Node c_5 is excluded form the cluster and c_5 and p_3 are potentially not functional.

Fig. 6. The cluster model.

and each node only has one dependent node from the other network. The cluster model is more general and considers directional edges between networks and each node can have multiple dependent nodes.

The cluster model captures the feature where partition in a network may cause the failures of dependent networks. In a c-network, if no prior solutions are made to build connections in the presence of failures, the partition of network will make the dependent networks more vulnerable, e.g., since p_3 does not support any c-node in the cluster, it may not be functional even if it can receive signals from c-nodes in the cluster. It can also be useful to identify the usable connected components and provide a solution to build resilient topology.

F. Probabilistic Model

Most models are more practical if they are probabilistic. For instance, the spread model makes more sense in some networks if the failures that spread in the same network are probabilistic, e.g., consider traffic control in flow line network, the failure of an intersection flow point may cause failures to its direct neighbors while it does not spread to other neighbors depending on the capacities of the links. Similarly, in the interdependency between c-network and p-network, if a p-node fails, it is possible that a power plant that transmits power to it fails. In this case, other p-nodes that are connected to the power plant may also fail with certain probability.

Similarly, the failures of interdependency edges are probabilistic in several cases. For instance, consider the interdependency between c-network and r-network. It is straightforward that r-network depends on the c-network that c-nodes provide signals to the r-nodes in r-network for the purposes such as traffic control. However, it is less straightforward that c-nodes depend on the r-nodes. But if we consider the interdependency between the r-network and p-network, the physical failure of a road may cascade to the power grid network and causes the failures of power lines and power plants (e.g. by causing restoration delays). The failures will further cascade to c-network. In this way, this model is more practical if its is probabilistic, i.e., there is certain chance where the failure of a r-node r_i will cascade to $C(\overrightarrow{r_i})$.

The probabilistic model can be useful to build reliable communication by considering multiple heterogeneous CI networks, where it requires c-nodes to maintain knowledge about the other CI networks.

V. Reliable Communication

The interdependency models represent different features between communication network and other critical infrastructure networks. Based on the models, in this section, we discuss the challenges in building reliable and resilient communication techniques based on the interdependency models.

A. Distributed Analysis

Reliable broadcast guarantees messages are reliably distributed to all the correct nodes in the network. However, in today's large scale and dynamic network with frequent failures, reliable broadcast desires fast response and even timely recovery. In the interdependency model, indeed, we can use a powerful centralized agent that analyzes the cascading failures for all the nodes and build a resilient topology to prevent failures. However, it is challenging to use a centralized agent for reliable broadcast to handle failures. First, it is difficult for the centralized agent to maintain the whole topology, especially in highly dynamic networks, which makes the analysis results inaccurate. Second, it generates high computational and communication overhead for the centralized agent. Indeed, if all the nodes that detect failures in the network sends a request to the computing agent for an analysis, the centralized agent may have high overhead in calculating for all the nodes and sending the results to them. Although distributed agents may be a choice, they are still difficult to maintain and can generate high overhead. To summarize, it is desirable for the nodes to analyze the failures in a distributed manner. Due to the communication capability of the c-nodes, e.g., routers, nodes can analyze the cascading failures while maintaining minimum information. For instance, our previous work [14] builds a reliable broadcast solution in the interdependency between communication network and power grid network where nodes analyze the failures in a fully distributed manner using the simple model.

B. Handling Various Types of Failures

The cascading failures described in §IV mainly refer to the cases where faulty nodes are not functional. However, in the interdependency model between communication network and other critical infrastructure networks, there are other types of failures to be considered. For instance, a *timing* failure [3], [4] refers to a c-node that responds correctly but in an untimely fashion. Although these type of failures are benign, which may not cause wrong analysis results when analyzing cascading failures, it will make it challenging where nodes may have incomplete information. In comparison, other types of failures such as Byzantine failures [21] can be harmful, where Byzantine faulty nodes behave arbitrarily due to any reasons such as hardware errors and cyber attacks. For instance, faulty nodes may cooperate together to make correct nodes accept a message that is not generated by the corresponding sender. In the interdependency model, these types of failures may cause inaccurate results in analyzing the cascading failures distributively to build reliable broadcast solutions.

C. Detecting Failures from other Networks

Indeed, through the techniques of communication network, failures in the network can be detected and handled in a certain way. However, it is hard for nodes in communication network to analyze the failures in the dependent networks. For instance, in the spread model where failures in the p-network may spread to the neighbors, it will be challenging for the c-nodes to learn the failures without knowing all the dependent nodes in addition to its p-neighbors. Similarly, since each node does not maintain the whole topology, it can be impossible for the c-nodes to analyze the results in the weighted models. Among all the models, it is the most challenging to build distributed solutions in the cluster model. Indeed, c-nodes will not learn the clusters that are mutually connected without maintaining the whole topology.

VI. Conclusion

In this paper, we study the interdependency between critical infrastructure networks. We propose six (simple, weighted simple, spread,weighted spread, cluster, probabilistic) interdependency models focusing on the interactions between communication network and other critical infrastructure networks. Each model captures some specific features in different networks and can be used for analysis of heterogeneous networks. Based on the models, we are able to build reliable communication using distributed analysis of vulnerable components prior to the failures and handle them when they are present.

References

[1] Final report on the august 14, 2003 blackout in the united states and canada: causes and recommendations. Technical report, U.S. - Canada Power System Outage Task Force, 2004.

[2] Hurrican sandy in new jersey and new york: Building performance observations, recommendations, and technical guidance. Technical report, FEMA, 2013.

[3] A. Avižienis, J.-C. Laprie, and B. Randell. Dependability and its threats: a taxonomy. In *Building the Information Society*, pages 91–120. Springer, 2004.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33, 2004.

[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. 464:1025–1028, 2010.

[6] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich. Interdependent networks with identical degree of mutually dependent nodes. *Physical Review*, 83(1), 2011.

[7] M. Burrows. The chubby lock service for loosely-coupled distributed systems. In *OSDI*, pages 335–350, 2006.

[8] C. Cachin, R. Guerraoui, and L. Rodrigues. *Introduction to reliable and secure distributed programming*. Springer, 2011.

[9] M. Castro and B. Liskov. Practical byzantine fault tolerance. In *OSDI*, pages 173–186, 1999.

[10] E. K. Çetinkaya, M. J. Alenazi, A. M. Peck, J. P. Rohrer, and J. P. Sterbenz. Multilevel resilience analysis of transportation and communication networks. *Telecommunication Systems*, 60(4):515–537, 2015.

[11] J. H. Cowie, A. T. Ogielsk, B. Premore, E. A. Smith, and T. Underwood. Impact of the 2003 blackouts on internet communications. Technical report, Renesys Corporation, 2003.

[12] M. M. Danziger, A. Bashan, Y. Berezin, L. M. Shekhtman, and S. Havlin. An introduction to interdependent networks. In *NDES*, pages 189–202, 2014.

[13] D. Dolev. The byzantine generals strike again. *Journal of Algorithms*, 3(1):14–30, 1982.

[14] S. Duan, S. Chinthavali, S. Lee, and M. Shankar. Reliable broadcast under cascading failures in interdependent networks. Technical report, Oak Ridge National Laboratory, 2016.

[15] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin. Networks formed from interdependent networks. *Nature Physics*, 8:40–48, 2012.

[16] M. F. Habib, M. Tornatore, and B. Mukherjee. Cascading-failure-resilient interconnection for interdependent power grid-optical networks. In *OFC*, 2015.

[17] A. J. Holmgren. Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis*, 26(4):955–969, 2006.

[18] X. Huang, S. Shao, H. Wang, S. V. Buldyrev, H. E. Stanley, and S. Havlin. The robustness of interdependent clustered networks. *EPFA*, 101(1), 2013.

[19] C. W. Johnson. Analysing the causes of the italian and swiss blackout, 28th september 2003. In *SCS*, 2007.

[20] L. Lamport. The part-time parliament. *ACM Transactions on Computer Systems*, 16(2):133–169, 1998.

[21] L. Lamport, R. E. Shostak, and M. C. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[22] W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin. Cascading failures in interdependent lattice networks: the critical role of the length of dependency links. *Physical Review Letters*, 108(22), 2011.

[23] A. Maurer and S. Tixeuil. On byzantine broadcast in loosely connected networks. In *DISC*, pages 253–266, 2012.

[24] M. Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety*, 121:43–60, 2014.

[25] M. Parandehgheibi and E. Modiano. Robustness of interdependent networks: the case of communication networks and the power grid. In *GLOBECOM*, pages 2164–2169, 2013.

[26] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. Critical infrastructure interdependency modeling: a survey of us and international research. *Idaho National Laboratory*, pages 1–20, 2006.

[27] S. Pinnaka, R. Yarlagadda, and E. K. Çetinkaya. Modelling robustness of critical infrastructure networks. In *Design of Reliable Communication Networks (DRCN), 2015 11th International Conference on the*, pages 95–98. IEEE, 2015.

[28] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6):11–25, 2001.

[29] J. Sun and S. Duan. A self-adaptive middleware for efficient routing in distributed sensor networks. In *SMC*, pages 322–327, 2015.

[30] R. van Renesse and F. B. Schneider. Chain replication for supporting high throughput and availability. In *OSDI*, pages 91–104, 2004.

[31] J. Winkler, L. Dueñas-Osorio, R. Stein, and D. Subramanian. Interface network models for complex urban infrastructure systems. *Journal of Infrastructure Systems*, 17(4):138–150, 2011.