Dynamics and Steady-State Behavior of Self-Healing Cyber-Physical Networks in Light of Cyber-Node Delays

Ali Behfarnia and Ali Eslami
Department of Electrical Engineering and Computer Science
Wichita State University, Wichita, KS, USA
Email: {axbehfarnia, ali.eslami}@wichita.edu

***Abstract*—The interconnected nature of cyber-physical networks gives rise to numerous engineering challenges and opportunities. An important challenge is the propagation of failure from one network to another, that can lead to large-scale cascading failures. On the other hand, *self-healing* ability emerges as a valuable opportunity where the overlay cyber network can cure failures in the underlying physical network. This paper extends an analytical framework established in a previous work to study the interaction of failure propagation and healing in cyber-physical networks. In particular, the case where propagation of failure in the physical network is faster than the healing response of the cyber network is investigated. Such scenarios are of interest in many real-life applications such as smart grid. The analysis results in a closed-form formula that captures the dynamics of failure propagation and healing in the network. In addition, it is shown that as the time goes by, the network reaches a steady state condition that would be either a complete healing or a complete collapse. Extensive numerical results are provided to verify the analysis and investigate the impact of the network parameters on the resiliency of the network. Particularly, it is shown that even small delays in cyber-nodes' response to physical failures may significantly reduce the network resiliency.**

***Index Terms*—Self-Healing Cyber-Physical Systems, Message Passing, Cascading Failure.**

I. Introduction

The interconnected nature of cyber-physical systems creates numerous engineering challenges and opportunities. An important challenge is the contagion of failure from one system to another in a coupled network. Such contagion may lead to large-scale catastrophic failure triggered by a smaller failure, such as the 2003 blackout in the Northeastern United States. Here, the *self-healing* ability emerges as a valuable opportunity where the overlaying cyber network can heal failures in the underlying physical network. For example, after detecting the failure in the power system, smart grid exploits "self-healing" abilities such as control of the production and distribution of electricity to halt the damage instantaneously [1]. This paper employs an analytical framework to study the interaction of failure propagation and healing in cyber-physical systems, and provides extensive numerical results to investigate the role of network parameters in this interaction.

The study of interdependent networks was sparked by Buldyrev et al. [2], where a simple "one-to-one" interdependence model was considered. Several authors [3]–[12] then aimed to extend the findings of [2] to more realistic scenarios. Authors in [3], [6], [10] investigated the robustness of one-to-one interdependent networks after an attack happens in the networks. In particular, Schneider et al. [10] assumed that some nodes can work without inter-link connections, called autonomous nodes. The autonomous nodes then were chosen in such a way that the network reaches its maximum robustness. Authors in [4], [5], [7], [13] studied the behavior of interdependent networks through percolation theory. Parshani et al. [7] analytically proved that the reduction of coupling between networks leads to a change from a first-order percolation phase to a second-order percolation phase. A "regular allocation" algorithm was proposed [9] to allocate the same number of inter-links to each node. The authors proved that in terms of robustness i) such allocation is optimal for a network with an unknown topology, and ii) it is better to employ bi-directional inter-links than unidirectional links. Huang et al. [12] studied the influence of active small clusters appearing after an attack on the whole network performance. In particular, they obtained an upper bound for the fraction of operating active small clusters after a cascading failure.

The majority of above works apply percolation theory while focusing on the size of the remaining giant component after a cascading failure. On the other hand, self-healing, and its modeling and design advantages in cyber-physical systems have been mostly overlooked in the literature. Recently, authors in [14] and [15] suggested a healing process by creating new links after each node's failure. However, they did not consider two issues. First, if a node fails, there is no strategy to recover the failed node. Second, creating new links is not always possible without considering a long amount of time, e.g., power lines in the physical network of the smart grid. To cover these points, we provided a self-healing algorithm in [16] that considers the functionality of all nodes in a cyber-physical system. To this end, we proposed a factor graph representation for cyber-physical systems (CPSs), where factor nodes represent network functionalities of cyber and physical nodes, and the edges capture the interactions between them. We then employed a fixed-point analysis using the concept of message-passing used in low-density parity-check (LDPC) codes to investigate the behavior of a self-healing CPS. During each iteration, some nodes would heal and some would fail due to the propagation of failure. In the analysis in [16], we assumed that each iteration is completely done in one time slot. However, in many real-life systems, if a failure occurs in a physical node, then the corresponding cyber node usually needs a few time slots to respond to the failure and heal the physical node. This delay could be for a number of reasons, such as recovering data from the database, collecting data from other physical nodes, gathering information from neighboring cyber nodes, etc. Therefore, one iteration needs a few time slots to be accomplished.

In this paper, we apply *density evolution* (DE) analysis used in LDPC codes to study the behavior of a CPS in the presence of a processing-time delay. Our analysis shows that selecting network parameters could significantly impact on the resiliency of a cyber-physical network. Also, we find that as the number of iterations increases, the network reaches a steady state condition that would be either a complete healing or a complete collapse. Through extensive simulation results, we obtain the following:

1) As the number of iteration grows, the fraction of failed nodes in the system goes to a step function where "0" implies a completely healed network and "1" states a completely failed network.
2) The probability of failure propagation among physical nodes should be kept small to preserve the healing ability of the system.
3) If the processing-time delay takes more than a few time slots, the probability of complete healing will significantly reduce.
4) The healing ability of the system depends on the fraction of defected messages in the network. Even though the cyber nodes could still heal the failures, the effect of defected messages gradually outweighs the healing abilities of cyber nodes during message passing iterations.

The rest of this paper is organized as follows. Section II describes the system model, notations, and message passing in our model of CPS. Section III explains the density evolution analysis of the proposed message-passing algorithm in the presence of processing-time delay. Section IV is devoted to numerical results, and Section V concludes the paper.

II. Network Model and Problem Formulation

This section presents our network model for both physical and cyber networks. It also describes our models for the initial disturbance, healing, and failure propagation within each network and between the two networks. These models are the same as in [16], which are reviewed here as they are essential to understanding the analysis in this paper. The message passing algorithm is also briefly described in this section, however, for a thorough review we refer the reader to [16].

A. Network Model

For our analysis, we consider random networks with given degree distributions as models of cyber and physical networks. This enables us to model random networks with arbitrary degree distributions such as scale-free networks with a power law degree distribution [17], and Erdős-Rényi random graphs with a Bernoulli degree distribution [18]. We define cyber (physical) degree of a node as the number of nodes in the cyber (physical) network connected to the node. In a similar fashion to LDPC codes, we use polynomials to represent the degree distributions of the networks. We denote by

$$\rho(z) = \sum_{i\geq 1} \rho_i z^i, \quad \text{and} \quad \lambda(z) = \sum_{i\geq 1} \lambda_i z^i \qquad (1)$$

the degree distributions of the cyber and physical networks, respectively, where ρ_i is the fraction of cyber nodes with cyber degree i, and λ_i is the fraction of physical nodes with physical degree i.

To capture the interconnections between the two networks, two more polynomials are needed: one for the physical degree distribution of cyber nodes, and one for the cyber degree distribution of physical nodes. However, in order to simplify the presentation of results, we assume that each cyber node can control a physical nodes, while each physical node is connected to one cyber node. The analysis for the general case of degree distributions could be carried out along the same lines as the analysis in this paper.

B. Initial Disturbance, Contagion, and Healing

Here, we explain our models for the initial disturbance, contagion within each system and between the two, and healing of the physical system by the cyber system. Our methodology, however, could be extended to a wide range of models.

Initial disturbance: We adopt a simple model assuming that each physical node initially fails with a small probability ϵ, where $\epsilon \ll 1$. In this paper, we only consider the initial disturbance for the physical network. The analysis for the case of a cyber attack could be conducted in a similar fashion.

Contagion within physical network: After being defected, a physical node may defect each of its neighbors with probability p. This probabilistic model is commonly used in the literature for a range of applications [19].

Healing of physical nodes: A cyber node heals a physical node if that physical node is its only defected physical neighbor. An example of this could be a control center that has all measurements but one from the power grid, so it must derive the phase or voltage value for the remaining component.

Contagion from physical to cyber system: A cyber node with no functioning physical neighbor will go out of service. A case for this could be an internet server that looses its power supply in a power outage.

Contagion within cyber system: If all cyber neighbors of a cyber node are out of service, then the cyber node itself will go out of service. An example could be an internet server whose neighboring servers have all been disconnected from the network.

C. Message Passing in Cyber-Physical Systems

In our model, the interactions between the nodes are represented by messages. Accordingly, all sorts of contagions and the healing process scenarios explained above could be interpreted in a message-passing framework as follows:

1) Defection (D) message:

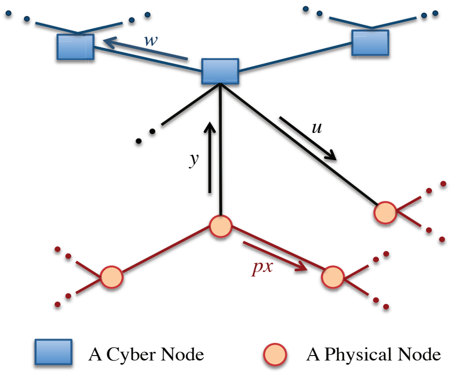


Fig. 1: An example of messages in a cyber-physical system.

- A defected physical node sends a defection message D to its cyber neighbors. It also sends a message D to each of its physical neighbors with probability p.
- A defected cyber node sends a D-message to its cyber and physical neighbors.
- A functioning cyber node that cannot heal a physical node sends a D-message to that node.

2) Healing (H) message: A cyber node which is able to heal a physical node sends a healing message H to that node.

Note that these messages are introduced to only capture the interactions in the CPS, while they may not be actually exchanged between the nodes in the underlying networks. However, we use y, u, and w messages to analyze the interactions in a cyber-physical network. Fig. 1 shows these messages.

III. Density Evolution Analysis for Cyber-Physical Systems

In order to study the impact of an initial disruption, we keep track of D and H messages by employing a technique originally introduced for LDPC codes, called "Density Evolution (DE)." Density of D messages is defined as the fraction of D messages among all the messages exchanged between the nodes in the network. The density evolution finds an iterative equation for this value, referred to as "density evolution equation". The network heals completely if and only if the density of D messages converges to 0 as the number of iterations grows. By employing the concept of DE in LDPC codes, we obtain a DE equation for the CPS defined in the previous section.

A. Analysis of Message Passing with Time Delays in Cyber Nodes

We now analyze the impact of processing-time delays using message passing in a cyber-physical system. To this end, we employ the definition of time slots. We assume that one iteration in the DE analysis needs a few time slots to be accomplished. One iteration contains the time that is needed for messages to be exchanged between cyber and physical nodes and also processed in cyber nodes. We expect that a cyber node reacts against a failure in a few time slots. We obtain a DE equation assuming that a cyber node needs two time slots to respond to a D message. The density evolution analysis can be similarly extended for more than two time slots.

Theorem 1. *For the cyber-physical system defined in section II, a density evolution equation for the l-th iteration with a processing delay of two time slots can be obtained as*

$$x_l(t+3) = f(x_{l-1}(t)),$$
$$f(x_{l-1}(t)) = A \times B + C \times \Big[1 - B\Big], \tag{2}$$

where A, B, and C are given as

$$A = \left\{\lambda\Big[1 - p\Big(\lambda\Big(1 - px_{l-1}(t)\Big) \times \Big(x_{l-1}(t) - 1\Big) + 1\Big)\Big]\right\} \times \left\{\lambda\Big(1 - px_{l-1}(t)\Big) \times \Big(x_{l-1}(t) - 1\Big)\right\} + 1, \tag{3}$$

$$B = 1 - \left\{\lambda\Big(1 - px_{l-1}(t)\Big) \times \Big(x_{l-1}(t) - 1\Big)\right\}^{(a-1)} \times \left\{1 - \rho\Big(x^a_{l-1}(t)\Big)\right\}, \tag{4}$$

$$C = 1 - \lambda\Big(1 - p\,A\Big). \tag{5}$$

The system heals if and only if $x_l(t+3) \to 0$ as $l \to \infty$ (or equivalently, $t \to \infty$).

Proof: The proof is a generalization of the one of Theorem 1 in [16]. Here, we give an outline of the proof for the sake of brevity. Let $x(t), y(t), u(t)$ and $w(t)$ denote the messages in the t-th time slot (see Fig. 1). If the probability of failure at the beginning of the t-th time slot is ϵ, then we have $x(t) = \epsilon$. In the next time slot, according to the model described in Sections II-B and II-C, we have

$$y(t+1) = x(t) + \Big[1 - x(t)\Big]\Big[1 - \lambda\Big(1 - px(t)\Big)\Big],$$
$$u(t+1) = 1 - \Big[1 - y(t)\Big]^{(a-1)}\Big[1 - \rho\Big(w(t)\Big)\Big],$$
$$w(t+1) = \Big(y(t)\Big)^a, \quad x(t+1) = y(t+1), \tag{6}$$

where $y(t) = x(t)$, and $w(t) = \Big(x(t)\Big)^a = \epsilon^{\,a}$. Similarly, in the $(t+2)$-th time slot, we obtain

$$y(t+2) = x(t+1) + \Big[1 - x(t+1)\Big] \times \Big[1 - \lambda\Big(1 - px(t+1)\Big)\Big],$$
$$u(t+2) = 1 - \Big[1 - y(t+1)\Big]^{(a-1)}\Big[1 - \rho\Big(w(t+1)\Big)\Big],$$
$$w(t+2) = \Big(y(t+1)\Big)^a, \quad x(t+2) = y(t+2). \tag{7}$$

After two time slots for processing the data in a cyber node, the probability of failure of a physical node can be calculated as

$$x_l(t+3) = y(t+2)\ u(t+2)\ + \Big[1-\lambda\Big(1-px(t+2)\Big)\Big]\Big[1-u(t+2)\Big]. \quad (8)$$

If we substitute equation (6) into (7) and then the result into (8), equation (2) will be obtained. ■

In section IV, we will study the impact of processing-time delays on a self-healing cyber-physical network.

B. Steady-State Condition for Cyber-Physical Systems

We now study the behavior of the cyber-physical system against a failure using the developed message-passing framework. After a failure occurs in the network, the message-passing algorithm tracks the failures. It is expected that as the number of iterations increases, the system reaches a steady-state condition that would be either a complete healing or a complete failure. We prove this claim in the following theorem and verify it by simulation results in section IV.

Theorem 2. *For the cyber-physical system defined in section II, if the number of message-passing iterations increases ($l \to \infty$), the system will reach a steady state condition, which is either complete healing state ($x_l(t) \to 0$) or complete failure state ($x_l(t) \to 1$).*

Proof: We first show that the theorem holds for a simple network. We then extend the arguments to more general networks. To begin with, consider a network with one cyber node and two physical nodes, as shown in Fig. 2a. Let μ_1 denote the probability of failure for a physical node, then one of the following cases may occur:

$$\begin{cases} \binom{2}{0}\ \mu_1^0\ \big(1-\mu_1\big)^2 & Case\ I : 0\ node\ failure, \\ \binom{2}{1}\ \mu_1\ \big(1-\mu_1\big) & Case\ II : 1\ node\ failure, \\ \binom{2}{2}\ \mu_1^2\ \big(1-\mu_1\big)^0 & Case\ III : 2\ nodes\ failure. \end{cases}$$

For cases I and III, the system is already in a steady-state condition, as follows. In case I, none of the nodes is affected by the failure and the network is healthy. In case III, two nodes are lost due to the failure. According to Section II-B, if more than one physical node is lost, then the corresponding cyber node cannot heal them. Hence, the physical nodes remain failed and in turn cause the cyber node to fail. Therefore, the network goes into complete collapse. In case II, however, the system would be in a transient condition, which means that the network has neither completely healed nor completely failed. This occurs when a cyber node heals the failed node, but the failed node already propagates the failure to one of its neighbors. The probability of this propagation failure is denoted by p. Hence, there is one failed node in the next state. After the l-th iteration, the probability of the network to be in a transient condition is

$$\binom{2}{1}\ \mu_1\ \big(1-\mu_1\big)\ \Big((1-p)^{(\alpha-1)}\ p\Big)^l, \quad (9)$$

where α shows the number of physical neighbors for the failed node ($\alpha = 1$ in Fig. 2a). For simplicity, we have assumed that all nodes have the same number of neighbors. As l grows, the probability above goes to zero. Therefore, the system reaches a steady-state healing condition (case I) or a steady-state collapsed condition (case III).

The assumption of two physical nodes can be extended to n physical nodes, as shown in Fig. 2b. In the same fashion as above, the probability of transient condition in such a network after the l-th iteration would be

$$\binom{n}{1}\ \mu_1\ \big(1-\mu_1\big)^{(n-1)}\ \Big((1-p)^{(\alpha-1)}\ p\Big)^l. \quad (10)$$

As $l \to \infty$, the probability of transient condition goes to zero.

We then increase one cyber node to m cyber nodes by defining clusters. A cluster includes a cyber node and its supporting physical nodes. Fig. 2c, for example, shows two clusters ($m = 2$). Similar to the previous case where $m = 1$, the probability of one cluster with k physical nodes being in a transient condition can be obtained as

$$\binom{k}{1}\ \mu_2\ \big(1-\mu_2\big)^{(k-1)}\ \Big((1-p)^{(\alpha-1)}\ p\Big)^l, \quad (11)$$

where μ_2 is the probability of failure for a physical node in one cluster. Hence, for v out of m clusters with one failed physical node, the probability of a transient condition in the entire network after the l-th iteration would be

$$\binom{k_1}{1}\ \mu_2\ \big(1-\mu_2\big)^{(k_1-1)}\Big((1-p)^{(\alpha-1)}\ p\Big)^l, \times \ldots \times \binom{k_v}{1}\ \mu_2\ \big(1-\mu_2\big)^{(k_v-1)}\ \Big((1-p)^{(\alpha-1)}\ p\Big)^l, \quad (12)$$

where $k_i, i = 1, ..., v$ represents the number of nodes in i-th cluster. As the number of iterations grows, the transient condition gradually vanishes. In other words, if during one of these iterations all nodes become healthy, then the network stays healthy. Also, if two nodes in one cluster fail during the iterations, then the failures gradually permeate among the nodes in the cluster and then to all nodes in the network. Therefore, a cyber-physical system with m cyber nodes and n physical nodes reaches a steady-state condition. ■

IV. Simulation Results

To make more sense of the above analysis, we present numerical results for the message passing over a self-healing cyber-physical network. First, we simulate the network for the different number of iterations to understand the behavior of the network against an initial disturbance. Then, we investigate the performance of the self-healing algorithm in the presence of a processing-time delay. To begin with, Fig. 3 shows the performance of the self-healing method for different number of iterations, l. As can be seen, as $l \to \infty$, the fraction of physical node failures converges to a step function. This

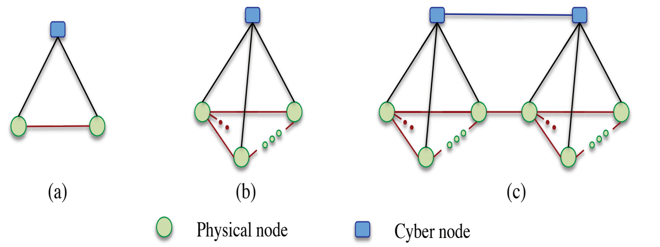


Fig. 2: Expanding the cyber-physical network in the proof of Theorem 2.

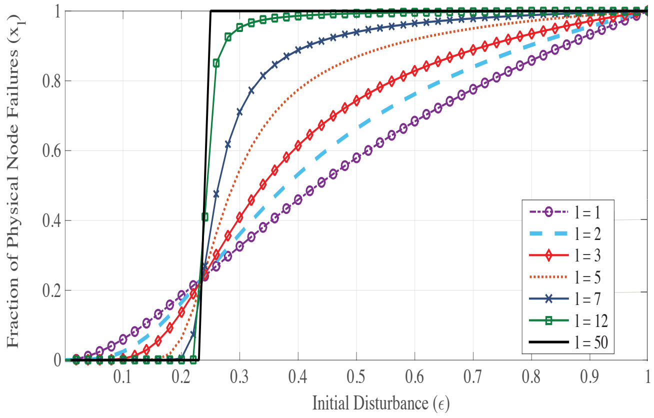
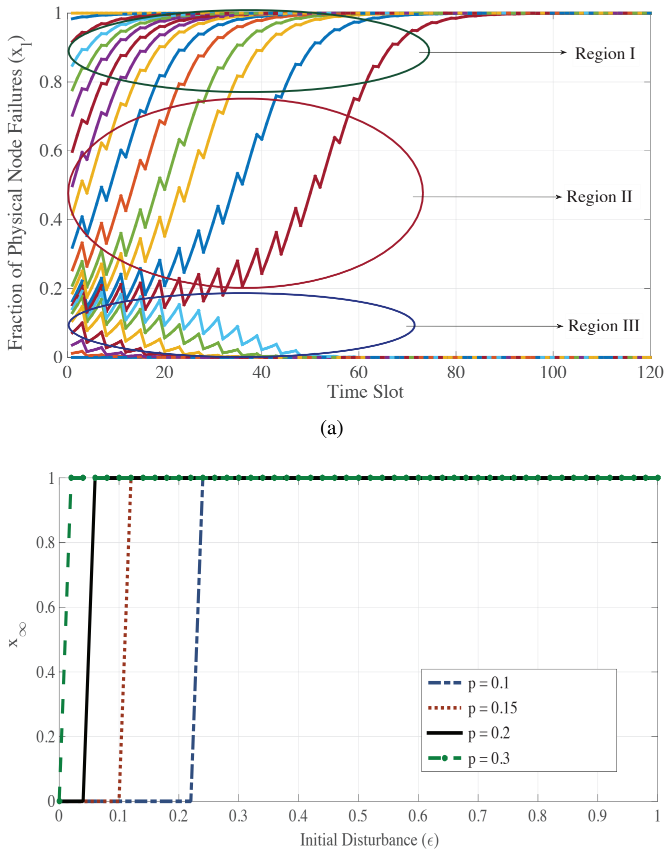


Fig. 3: Probability of failure for physical nodes in different iterations w.r.t the initial disturbance. This simulation is set for network parameters $a = 5$, $p = 0.2, \lambda(z) = z^2$, and $\rho(z) = z^3$.

function implies two steady-state conditions that would be either a complete healing or a complete failure scenario in the network. This confirms Theorem II in section III-B. Note that the transition from complete healing to complete failure occurs at a *threshold* value of the initial disturbance.

Now, we numerically evaluate the findings in section III-A to obtain the influence of processing-time delay on the probability of failure in the CPS. We begin with a processing delay of three time slots. Hence, each iteration can be accomplished in four time slots. Fig. 4a shows the number of time slots needed for the network to reach a steady-state condition. As can be seen, jagged lines occur as a result of the processing time delay. Considering this delay, a cyber node needs k time slots (here, $k = 3$) to respond to the failure. During this time interval, the failure propagates in the physical network and could constantly increase the probability of failure for physical nodes. After the k-th time slot in each iteration, however, the network would experience three cases for the probability of failure, depending on the ability of cyber nodes to heal their associated physical nodes:

- Region I: Cyber nodes healing ability is diminishing due to the large number of failures in the network, hence, probability of physical failures only increases.
- Region II: Cyber nodes are still able to heal their physical nodes, but this is not enough to stop the propagation of failures and change the overall trend. That is, the number of failures at the end of the iteration is still higher than that of the beginning of the iteration.
- Region III: Healing ability of cyber nodes outweighs the propagation of failure, leading to complete healing of the network after a few iterations.

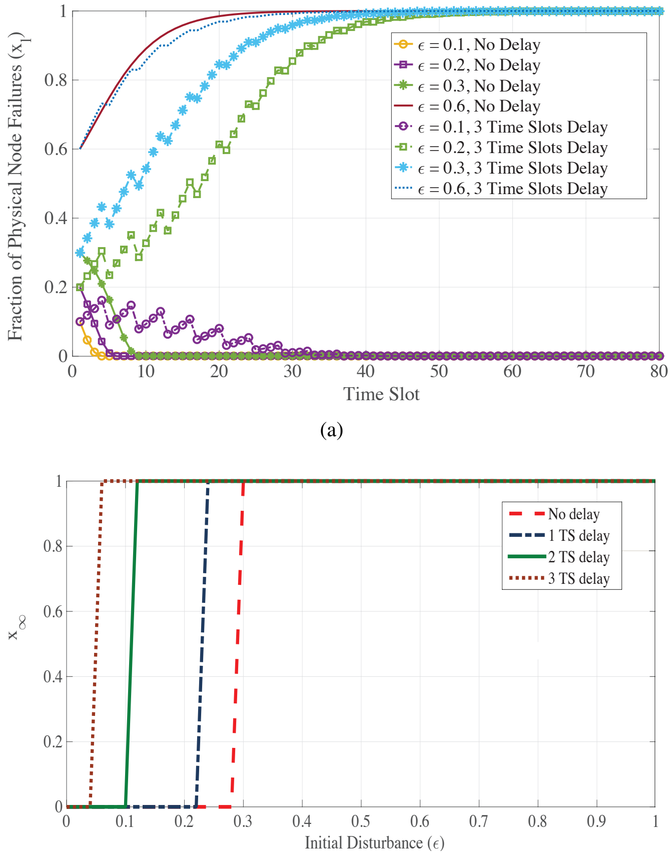


(a)

(b)

Fig. 4: a) Probability of failure for physical nodes in presence of processing-time delay. Processing delay = 3 Time slots, and network parameters are $a = 5$, $p = 0.2, \lambda(z) = z^2$, and $\rho(z) = z^3$. b) Impact of p on the steady-state behavior of the network.

The probability that each physical node gets affected by the failure of its physical neighbors, p, is decisive to the resiliency of a cyber-physical system. One example of this parameter in power systems could be revealed in protective relays. The mission of protective relays is to sense a fault and initiate a trip, disconnection, or order. Therefore, good relays result in lower probability of failures in a network. The performance of relays, in a very abstract sense, can be mapped to p. The influence of p becomes more crucial, when there is a processing time delay for cyber nodes. Fig. 4(b) shows the steady-state behavior of the network for different values of p, when the processing time slots is 3 ($k = 3$). As can be seen, the higher value of p dramatically increases the vulnerability of the network against an initial disturbance. For instance, for $p = 0.3$, network resiliency is almost non-existent against any initial disturbance in the physical network.



(a)

(b)

Fig. 5: Comparison between non-delayed systems and delayed systems for network parameters $a = 5,\ p = 0.15, \lambda(z) = z^2$, and $\rho(z) = z^3$. a) shows the effect of time slot processing delay on systems, b) shows the impact of time slot (TS) delays on maximum tolerated threshold in the network.

Finally, we compare the dynamic and steady-sate behavior of the non-delayed self-healing network against the same network with cyber-node delays. First, consider Fig. 5(a), which shows the direct impact of delay on maximum resiliency of a network. Delayed systems need considerably more time slots to be healed in comparison to non-delayed systems. This can be observed for $\epsilon = 0.1$. In addition, at $\epsilon = 0.3$, the non-delayed system can be cured after nine time slots. However, the delayed system completely collapses. The reason is that the failure propagates throughout the physical network during the three time slot delay interval. Fig. 5(b) displays the steady-state behavior for delayed and non-delayed systems w.r.t the size of the initial disturbance. A comparison of resiliency thresholds effectively demonstrates the essential need for a quick response from cyber nodes.

V. Conclusion

We studied self-healing cyber-physical networks where cyber-nodes' response to failures in the physical network is delayed. We applied a density evolution analysis that captured the interplay of failure propagation and healing in a closed-form formula. We studied the steady-state behavior of such networks after an initial disturbance, proving that the network reaches one of the two conditions, either a complete healing or a complete failure. We provided extensive simulation results to study the impact of the processing-time delays of cyber nodes on the resiliency of the network. The results clearly demonstrated the essential need for a quick response from cyber nodes in order to achieve any resiliency in the network.

References

[1] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, July 2008, pp. 1–5.

[2] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, no. 464, pp. 1025–1028, April 2010.

[3] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, "Interdependent networks with identical degrees of mutually dependent nodes," *Physical Review E*, vol. 83, no. 1, p. 016112, 2011.

[4] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, 2012.

[5] P. Grassberger, "Percolation transitions in the survival of interdependent agents on multiplex networks, catastrophic cascades, and solid-on-solid surface growth," *Phys. Rev. E*, vol. 91, p. 062806, Jun 2015.

[6] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 6, p. 065101, 2011.

[7] R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition," *Physical Review Letters*, vol. 105, no. 4, p. 048701, 2010.

[8] D. Zhou, H. E. Stanley, G. D'Agostino, and A. Scala, "Assortativity decreases the robustness of interdependent networks," *Physical Review E*, vol. 86, no. 6, p. 066103, 2012.

[9] O. Yağan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1708–1720, 2012.

[10] C. M. Schneider, N. Yazdani, N. A. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Scientific reports*, vol. 3, 2013.

[11] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependent relations," *arXiv preprint arXiv:1011.0234*, 2010.

[12] Z. Huang, C. Wang, A. Nayak, and I. Stojmenovic, "Small cluster in cyber physical systems: Network topology, interdependence and cascading failures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2340–2351, 2015.

[13] D. Cellai, E. López, J. Zhou, J. P. Gleeson, and G. Bianconi, "Percolation in multiplex networks with overlap," *Physical Review E*, vol. 88, no. 5, p. 052811, 2013.

[14] M. Stippinger and J. Kertsz, "Enhancing resilience of interdependent networks by healing," *Physica A: Statistical Mechanics and Its Applications*, vol. 416, pp. 481 – 487, 2014.

[15] L. K. Gallos and N. H. Fefferman, "Simple and efficient self-healing strategy for damaged complex networks," *Phys. Rev. E*, vol. 92, p. 052806, Nov 2015.

[16] A. Behfarnia and A. Eslami, "Message passing for analysis and resilient design of self-healing interdependent cyber-physical networks," to appear in *25th International Conference on Computer Communication and Networks (ICCCN 2016)*, Hawaii, USA, August 2016. [Online]. Available: {http://arxiv.org/pdf/1606.00955v1.pdf}

[17] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[18] B. Bollobás, *Random graphs*. Springer, 1998.

[19] I. Dobson, B. Carreras, and D. Newman, "A branching process approximation to cascading load-dependent system failure," in *37th Annual Hawaii International Conference on System Sciences*, Hawaii, USA, January 2004.