# Cascading failures in Cyber-Physical Networks: Research Challenges

Chinwendu Enyioha

***Abstract*—We consider cascading failures (concurrent malfunction or attack propagation) in Cyber-Physical Networks (CPNs). We note a specific properties of CPNs that differentiate them from static networks for which studies on cascades exist, including interdependence of network layers – cyber and physical, inherent in CPNs. Further, we highlight a number of specific research challenges on the problem of optimally controlling outbreaks of cascading failures in CPNs with limited resources.**

***Index Terms*—cyber-physical networks, cascading failure, network interdependence, optimization and optimal control**

## I. Background and Motivation

As Cyber-Physical Networks (CPNs) and systems become pervasive in modern technology infrastructure including power networks, defense and transportation networks, the need for enhanced network resilience, security and robustness to failures and attacks become even more pertinent. Cascading failures in networks are failures that result in concurrent malfunction of parts of a network. The cascade effect is not limited to failures alone, as the negative impact of a malicious attack can easily spread across a CPN especially given the interdependence of the cyber and physical networks. Amongst a number of such cascading failures was the cascading outage of power generation and transmission facilities in the United States in 2003, which resulted in blackouts in parts of New York, Pennslylvania, Ohio and Michigan states. Studies on this major blackout indicated that initial system lapses had a cascading effect that eventually resulted in the the power outages across several states [1, 2]. A more recent incident with cascading system outage happened just a couple of years ago when Hurricane Sandy struck the Northeastern seabord leaving millions of customers without power for days.

The author is with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia PA, USA 19104 cenyioha@seas.upenn.edu

CPNs, by nature, synergize physical and computing/cyber layers. This inherent interaction and interdependence of network layers make them vulnerable to damaging widespread network cascades. For instance, an adversarial attack or a component failure at a controller in the cyber layer can in turn affect the behavior and dynamics at the physical layer, which eventually cascades to other parts of the CPN [3].

Cascades and other spreading processes in networks have been studied in static network; for instance, spread of influence and opinion formation in social networks [4], spread of infection in epidemiology [5]. Dynamics of interdependent networks have also been studied [1]. Our recent research focus has been on developing optimal strategies to control outbreaks of viral infections in networks [6, 7]. We have developed provably optimal intervention strategies for static networks with arbitrary structure, including directed networks. However, the bridge between understanding the effect of interdependent networks on cascades, and developing efficient, provably optimal intervention strategies to control the outbreak of a cascading failure remains an open and promising area of research, more so within the context of CPNs.

## II. Proposed Research & Impact to CPNs

*Our central position* – a sound theoretical framework to study cascades in CPNs is needed to guide the computation of optimal, resource-efficient strategies to control the outbreak of cascading failures and attacks in CPNs. CPNs present special research challenges not suitably addressed by existing literature on cascades in networks [1, 3]. In addition to the inherent network interdependence of CPNs, unlike other contexts in which cascades in networks have been studied, CPNs typically need to be situationally aware and reactive. Further, beyond attaining network-wide objectives via decentralized, local

interactions, CPNs need to be able to incorporate human-in-the-loop and complex interdependencies. Further, CPNs need to be adaptable and designed in such a way that allows for external intervention to enhance normal operation in the event of a malfunction or attack.

In the event there is an outbreak of a cascading failure or attack in a CPN, a critical problem is determining the optimal way to allocate defense or control resources to contain the outbreak. How can resource-efficient intervention strategies can be developed in a manner that prevents a sudden network collapse. For instance, to contain an outbreak of a cascading failure in a CPN, are there strategies that control the cascading failure in a way that allows for graceful degradation in performance of the network? Answers to these problems will ensure effectiveness of interventions to control cascading failures in existing CPNs, and guide the design of next-generation CPNs, since certain network structures are more robust to cascades [8].

Equally vital is the need to develop intervention or control mechanisms that scale in an efficient manner with the size of the CPNs. This calls for investigations into distributed computing paradigms that take into account unique properties of CPNs highlighted earlier. Further, can we develop bio-inspired, passive control strategies where, for instance, certain parts in different network layers temporarily hibernate until the outbreak of a cascading failure is contained [6]? How can we achieve this and simultaneously guarantee an acceptable level of network operation? These are critical questions important in the conversation to guide the design of next-generation CPNs that are robust to cascading failures and cost-effective to defend from attacks.

While much attention in the literature has been given to fault and attack detection in cyber-physical systems, our proposed work seeks to address the next natural question – what are optimal intervention strategies once a cascading attack or failure has been detected. Successful implementation of our proposed work will *guide the design of next-generation CPNs*, since the developed framework for studying cascades will be specific to CPNs. Solutions from our proposed work will, further, find applications in several domains where cyber-physical systems technology is applied today including robotic networks, and power transmission networks amongst others. The need to have high levels of security and robustness to cascading failures and attacks in next-generation CPNs cannot be overemphasized. Our proposed work is a significant step in that direction.

## III. Biographicals

Chiwnendu Enyioha received the B.Sc in Mathematics from Gardner-Webb University (GWU) in 2008, and is currently a final year Ph.D candidate in Electrical and Systems Engineering at the University of Pennsylvania, supervised by Professors George Pappas and Ali Jadbabaie. Affiliated with the GRASP Lab and the PRECISE Center, Chinwendu's current research interests include control of spreading processes in large networks, distributed computation and optimization over networks with applications to epidemiology and cyber physical systems. He is a Fellow of the Ford Foundation; and was named a William Fontaine Scholar at the University of Pennsylvania. He has also received the Mathematical Association of America (MAA) Walt and Susan Patterson Award.

## References


[1] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, 2010.

[2] G Andersson, P Donalek, R Farmer, N Hatziargyriou, I Kamwa, P Kundur, N Martins, J Paserba, P Pourbeik, J Sanchez-Gasca, et al. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *Power Systems, IEEE Transactions on*, 20(4):1922–1928, 2005.

[3] Osman Yagan, Dajun Qian, Junshan Zhang, and Douglas Cochran. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *Parallel and Distributed Systems, IEEE Transactions on*, 23(9):1708–1720, 2012.

[4] David Kempe, Jon Kleinberg, and Éva 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*, pages 137–146. ACM, 2003.

[5] Mark EJ Newman. Spread of epidemic disease on networks. *Physical review E*, 66(1):016128, 2002.

[6] Chinwendu Enyioha, Victor Preciado, and George Pappas. Bio-inspired strategy for control of viral spreading in networks. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 33–40. ACM, 2013.

[7] Victor M Preciado, Michael Zargham, Chinwendu Enyioha, Ali Jadbabaie, and George Pappas. Optimal resource allocation for network protection: A geometric programming approach. *to appear in IEEE Transactions on Control of Network Systems*, 2014.

[8] Lawrence Blume, David Easley, Jon Kleinberg, Robert Kleinberg, and Éva Tardos. Which networks are least susceptible to cascading failures? In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pages 393–402. IEEE, 2011.