

Distributed Dynamic Measures of Criticality for Telecommunication Networks

Yaniv Proselkov, Manuel Herrera, Ajith Kumar Parlikad and Alexandra Brintrup

Abstract Telecommunication networks are designed to route data along fixed pathways, and so have minimal reactivity to emergent loads. To service today's increased data requirements, networks management must be revolutionised so as to proactively respond to anomalies quickly and efficiently. To equip the network with resilience, a distributed design calls for node agency, so that nodes can predict the emergence of critical data loads leading to disruptions. This is to inform prognostics models and proactive maintenance planning. Proactive maintenance needs KPIs, most importantly probability and impact of failure, estimated by criticality, which is the negative impact on connectedness in a network resulting from removing some element. In this paper, we studied criticality in the sense of increased incidence of data congestion caused by a node being unable to process new data packets. We introduce three novel, distributed measures of criticality which can be used to predict the behaviour of dynamic processes occurring on a network. Their performance is compared, and tested on a simulated diffusive data transfer network. The results show potential for the distributed dynamic criticality measures to predict the accumulation of data packet loads within a communications network. These measures are predicted to be useful in proactive maintenance and routing for telecommunications, as well as informing businesses of partner criticality in supply networks.

Yaniv Proselkov,

Institute for Manufacturing, Dept. of Engineering, University of Cambridge, e-mail: yp289@cam.ac.uk

Manuel Herrera,

Institute for Manufacturing, Dept. of Engineering, University of Cambridge, e-mail: amh226@cam.ac.uk

Ajith Kumar Parlikad,

Institute for Manufacturing, Dept. of Engineering, University of Cambridge, e-mail: aknp2@cam.ac.uk

Alexandra Brintrup,

Institute for Manufacturing, Dept. of Engineering, University of Cambridge, e-mail: ab702@cam.ac.uk

1 Introduction

Telecommunications infrastructures are physical networks that support internet services by facilitating data transfers between agents. For example, to watch a film on a streaming service, a user sends a request to the servers that is routed through the infrastructure network. The streaming service sends the film data back to the user. Infrastructures are often represented by graphs, with agents as nodes, and connections as edges. Network topology affects routing speed - shorter distances give in quicker transfers - and its resilience to disruption. Optimal network design has received much attention [2], especially for resilience, particularly in complex communications networks [4]. The impact of a node's failure on the smooth operation of a network, criticality, affects resilience. Criticality estimates the size of the impact of a node's failure on network connectivity, so it can inform prioritisation in network prognostics for proactive maintenance, necessitating finding it to inform operations policy. One way to measure criticality is centrality, which is the importance a node exerts on a network. Many criticality measures are extensions of centrality measures. Classic centrality measures include betweenness, eigenvalue, and degree centrality. The first two are centralised, needing each node to take information from all nodes. Degree centrality requires each node to know the number of their connected nodes, called neighbours. This is a distributed nodal measure, and these are the focus of this paper.

In network systems with objects travelling through them, such as telecommunications infrastructure, overcongestion of objects, such as data packets, can cause node failure. This can be expressed in a three stage process, from generation, to diffusion, and then dissipation [12]. Accurate and quick network control is important in networks that are working near capacity, as is expected for backbone networks of the near future [9]. Irregular stress also increases network criticality, such as the abnormally heavy data traffic in consumer networks due to home-working during the COVID-19 outbreak. Cascade failures also occur in regularly functional systems due to random errors [11]. For similar future problems, there is a clear and present need to develop efficient distributed methods to maximise resilience.

Distributed measures have less data transmission load for communication networks than centralised measures. This is because in centralised methods each node needs information from all nodes, but in distributed methods nodes need local information. Distribution reduces information packet travel time and number of sources, so nodes can make decisions more quickly with more freedom, such as packet routes. This preserves resilience through proactive decision-making.

Assuming criticality is static can lead to problems, since a critical node in an underused region may affect traffic less than a non-critical node in an overused region. Thus it is dynamic, waxing and waning with the number of data packets passing through it. If criticality grows faster than repairs, we must stop congestion to minimise failure spread, dynamically protecting more critical nodes. We hence need dynamic measures of criticality. A centralised, not distributed, dynamic node criticality measure exists. So does a distributed estimate of the effects of congestion cascades [12], but it needs full network information to resolve. There is little re-

search into dynamical measures of distributed nodal criticality. This motivates our work. We take three distributed structural measures of nodal criticality and augment them with dynamic node weights, representing node stress.

In Section 2, we describe the three measures of distributed criticality, and the validation procedure. In Section 3 we analyse which measure more accurately estimates criticality. In Section 4, we discuss our findings, suggest how to apply them, and further research.

2 Methods

We describe three criticality measures for nodes in a network. Each is computed from local network structural information, and we augment them to dynamically compute time dependant node states. We then validate them using an augmented susceptible-infected-susceptible (SIS) model [8] with incremental infection, representing congestion spreading in a multiagent system with fixed storage.

We chose these measures since each has flexibility to incorporate dynamic node states and belongs to a different measure class. To compute criticality, the first, **local centrality**, counts the degrees of local nodes, the second, **Wehmuth centrality**, uses local structural measures and the third, **local bridging centrality**, considers possible paths through a local region. We compare how accurately these three measures estimate criticality, and explain the simulation model.

2.1 Weighted local centrality

Local centrality [3] finds how embedded a node is. It is computationally inexpensive, where for a graph, $G = (V, E)$, with $|V| = n$ nodes, $|E| = m$ edges, and k mean degree, it has $O(nk^2)$ complexity, less than, say, betweenness centrality, which has $O(kn^2)$ complexity. It also distributedly computes centrality which is useful for networks with cognitive agents. First some notation to explain the local centrality. For a node, $u \in V$, denote the set of nodes i edges away from it as $\Gamma_i(u) \subset V$, where when $i = 1$, $\Gamma_i(u)$ is the neighbourhood of u . The set of nodes at most i edges away from u is denoted as

$$H_i(u) = \bigcup_{j=1}^i \Gamma_j(u).$$

To compute the local centrality of u , denoted $C_L : V \rightarrow \mathbb{Z}^+$, first compute its neighbourhood, $\Gamma_1(u)$. Second, compute the neighbourhoods of each node in $\Gamma_1(u)$. Then sum up, for each node, w , in each $\Gamma_1(v)$, $v \in \Gamma_1(u)$, the number of nodes in the set of all nodes at most two edges away from w , such that

$$C_L(u) = \sum_{v \in \Gamma_1(u)} \sum_{w \in \Gamma_1(v)} |H_2(w)|. \quad (1)$$

We may now incorporate incremental weights. In telecoms infrastructure, where nodes represent devices such as routers or switches, if data packets arrive at a rate greater than the node can emit them, they may be queued up, to be emitted later. To model this, suppose that all nodes have a queue length, or weight. Then rather than summing over numbers of nodes, each node is counted the same number of times as their queue lengths, which we list along a row vector, $c \in \mathbb{R}^n$, where position of a value corresponds to a node. Similarly, instead of a set, one can use a binary vector representation to denote the set of nodes at most i edges away from a node, denoted $H_i \in \{0, 1\}^n$. Suppose both are row vectors, and rewrite Equation (1) as

$$C_L(u) = \sum_{v \in \Gamma_1(u)} \sum_{w \in \Gamma_1(v)} c H_i(w)^t.$$

This has the advantage of giving extra weight to local regions with more queued data packets. This serves as a useful estimate of criticality over time. To implement this renormalise the spread of C_L outputs to the range $[0, 1]$, where being closer to one suggests greater criticality. This preserves both ranking and scaling.

2.2 Weighted Wehmuth centrality

The number of neighbours is a straightforward but possibly naive way to estimate criticality. This is degree centrality. The degree of a node u can be denoted as d_u . To display the nodes within a vector \underline{d} , it helps to enumerate them, and for $i \in \{1, \dots, n\}$, denote the degree of the i^{th} node as d_i , such that $\underline{d} = (d_1, \dots, d_n)$. Mapped to the leading diagonal of a matrix $D \in M_n(\mathbb{Z}^+)$, known as the **degree matrix**, we get

$$D = (d_{i,j}) = \begin{cases} d_i \in \underline{d}, & i = j \\ 0, & \text{else.} \end{cases}$$

Node degree counts incident edges. In simple graphs, nodes connect only to other nodes at most once. We denote the number of edges between nodes u_i and u_j as $a_{i,j}$, displayable in a matrix, $A \in M_n(\{0, 1\})$, the **adjacency matrix**, where

$$A = (a_{i,j}) = \begin{cases} 1, & (i, j) \in E \\ 0, & i = j. \end{cases}$$

The degree and adjacency matrices may be used to get the Laplacian matrix, $L \in M_n(\mathbb{Z})$, where $L = D - A$, to find structural network measures, comparable between different networks. This fully captures network topology. Normalising gives

$$L_N = D^{-1/2} L D^{-1/2},$$

whose eigenvalues are all between 0 and 2 such that $0 = \lambda_1 < \dots < \lambda_n \leq 2$. We can perform **spectral analysis** on L_N , studying its eigenvector decomposition, by reducing it into component eigenvectors, each of which has a distinct eigenvalue. Sorting them along the leading diagonal of a square matrix gives

$$\Lambda = (\lambda_i, j) = \begin{cases} \lambda_i, & i = j \\ 0, & \text{else.} \end{cases}$$

The number of connected components in a network is the number of 0 eigenvalues in the spectrum $|\{\lambda_i : \lambda_i = 0\}|$. The smallest nonzero eigenvector, called the **algebraic connectivity** shows how well connected a component is within itself. In connected networks this is the second smallest eigenvector, with eigenvalue λ_2 .

For node u , the **Wehmuth centrality** [13], denoted $C_W(u)$, finds λ_2 of the induced subgraph of nodes at most h edges away from u , denoted λ_2^u . Divide this by $\log_2(d_u)$ to stop non-critical hubs from being ranked too high. If the node is a leaf it is noncritical. We restrict analysis to $h = 2$ to find node embeddedness for its immediate and secondary area. Wehmuth centrality is thus a distributed measure, each node needing local structural information to determine criticality, and is defined as

$$C_W(u) = \begin{cases} \frac{\lambda_2^u}{\log_2(d_u)}, & d_u > 1 \\ \infty, & d_u = 1. \end{cases}$$

Let us incorporate time dependant queue lengths, c , from a dynamic process on the network, such as data packet movement within a telecoms network. Wehmuth centrality uses network structure and node degrees, which are independent of queue lengths. To account for them, redefine the simple graph into a directed multigraph, so that there may be multiple, directed edges between single nodes, such that $d_{i,j} \in \mathbb{Z}^+$ and $d_{i,j} \neq d_{j,i}$. Replace each edge with two opposite directed edges. For each node, u_i , multiply its number of out-edges by c_i . Laplacian properties hold for multigraphs, so apply the original Wehmuth centrality on this new graph, dividing by the log of the out-degree of a node. We define the directed multigraph degree matrix as $D^d = cD$ and the directed multigraph adjacency matrix as

$$A^d = \left(a_{i,j}^d \right) \in M_n(\mathbb{Z}^+), \quad \text{where} \quad a_{i,j}^d = a_{i,j} \cdot c_j.$$

Last, apply the Wehmuth centrality procedure onto D^d and A^d , obtaining the weighted Wehmuth centrality.

2.3 Weighted local bridging centrality

Telecommunications infrastructure routs data packets from source to destination nodes as in supply chains, circuits, or complex waterways. These all fail when paths

between nodes are unusable. This motivates a criticality measure to network track pathway disruptions. To describe such a measure, we first define a network path.

A network path, $P \subset V$, is a sequence of distinct nodes where consecutive members share edges, such that for all $n_i, n_{i+1} \in P$, $(n_i, n_{i+1}) \in E$. The shortest path between two nodes is, when unweighted, a path with the fewest elements that starts with one and ends with the other. If multiple distinct paths share the same length and have the minimum number elements in them, they are all shortest paths. We denote the number of shortest paths from v to w as $\rho_{v,w} : V \rightarrow \mathbb{Z}^+$, and the number of shortest paths from v to w that happen to pass through u as $\rho_{v,w}(u) : V \rightarrow \mathbb{Z}^+$.

Sociocentric betweenness [5], denoted $B_s : V \rightarrow \mathbb{R}$, tracks pathway disruption potential, calculating the fraction of shortest paths between all node pairs that pass through the subject node, defined as

$$B_s(u) = \sum_{\substack{v,w \in V \\ u \neq v \neq w}} \frac{\rho_{v,w}(u)}{\rho_{v,w}}.$$

This measure can be modified into **egocentric betweenness**, which measures the betweenness of a region surrounding a node, and then compares the valuations between nodes in the network. It correlates strongly with sociocentric betweenness [7], and is computable in a distributed manner. For each node, say $u \in V$, it measures the betweenness of the induced subgraph of $\Gamma_i(u)$, such that

$$B_e(u) = \sum_{v,w \in \Gamma_i(u)} \frac{\rho_{v,w}(u)}{\rho_{v,w}}. \quad (2)$$

It compares this value between nodes, where higher values suggest greater criticality. Both are centrality measures and require augmentation to compute criticality. We use the **bridging coefficient** [10], which describes embedding of a node within a connected component using local information. It is defined as the reciprocal of the node's degree, divided by the sum of degrees of its neighbourhood. For a node, u , the formula of the bridging coefficient, $\beta : V \rightarrow (0, 1]$, is

$$\beta(u) = \begin{cases} \frac{\frac{1}{d_u}}{\sum_{i \in \Gamma(u)} d_i}, & d_u > 0 \\ 1, & d_u = 0. \end{cases}$$

By multiplying the sociocentric betweenness centrality and bridging coefficient, we obtain the **sociocentric bridging centrality**, $C_B : V \rightarrow \mathbb{R}$, such that

$$C_B(u) = B_s(u) \cdot \beta(u). \quad (3)$$

This can be changed into the **local bridging centrality** by replacing the sociocentric betweenness in Equation (3) with the egocentric betweenness, and rewriting it into

$$C_B(u) = B_c(u) \cdot \beta(u). \quad (4)$$

To create a dynamic measure, use dynamic queue lengths in nodes so that data packet flow affects network criticality, augmenting the local bridging centrality with node weights associated with criticality. This uses both egocentric betweenness and the bridging coefficient. The bridging coefficient estimates the likelihood that a node is on a bridge between clusters. This is purely structural, so is unchanged, but the egocentric bridging coefficient may be naturally extended. Queues are made of data packets which follow paths, and egocentric betweenness is a path measure, so we may weight each path by the sum of its nodes' queue lengths, which for a given node $u \in V$ we denote as c_u . For the set of shortest paths between nodes v and w , denoted $P_{v,w}$, achieve this by redefining $\rho_{v,w}$ and $\rho_{v,w}(u)$ as

$$\rho_{v,w} = \sum_{\substack{P \in P_{v,w} \\ u \notin P}} \sum_{x \in P} c_x; \quad \rho_{v,w}(u) = \sum_{\substack{P \in P_{v,w} \\ u \in P}} \sum_{x \in P} c_x.$$

By inserting the new $\rho_{v,w}$ and $\rho_{v,w}(u)$ into Equation (2), and this into Equation (4), we obtain the weighted localised bridging centrality.

2.4 Validation Method

The simulation model used to test these measures is based off of the SIS model of disease spread. In it, nodes take one of two states, susceptible, and infected, respectively $\mathbb{S}, \mathbb{I} \subset V$. An infected node $u \in \mathbb{I}$, according to a rate β Poisson process, may randomly synchronise with a randomly chosen neighbouring susceptible node, say, $v \in I_i(u) \cap \mathbb{S}$, and infect it such that $v \in \mathbb{I}$. The infected node $u \in \mathbb{I}$ may also according to an independent Poisson process of rate γ , recover and become susceptible, such that $u \in \mathbb{S}$. This represents the dynamics of a disease that does not confer immunity.

To estimate queued data packet accumulations, give each node a counter denoting queue length, $Q : V \rightarrow \mathbb{Z}^+$, where if a given node's queue reaches the infection threshold, I , it becomes infectious. That is, for a given node, u , if $Q(u) \geq I$ then $u \in \mathbb{I}$, else if $Q(u) < I$ then $u \in \mathbb{S}$. In the augmented SIS, infection and recovery steps become counter additions and reductions. An infected node, u may, at rate β , increase the counter of a neighbouring susceptible node, v according to the SIS infection dynamics. This represents a data packet moving from v to u , but u has a full queue so cannot process it, and returns the packet to v . Nodes may also independently recover at rate γ , where reducing its counter by one according to a Poisson process, representing the resolution of one packet, and no other node's queue grows.

We outline the validation method used to measure the accuracy of the dynamic distributed measures of criticality. We use a Barabasi-Albert preferential attachment network [1], generated by adding nodes to a base and attaching m edges to it if possible, up to the n^{th} node. The augmented SIS is then run on this network.

To find each node's network impact, we run n simulations. This was coded in Python 3.8, using the `networkx`, `pandas`, `numpy`, `random`, `matplotlib`, `math`, `scipy`, and `sklearn` packages. Each simulation $S_i \in S$, where S is the set of all simulations, first sets the queue length of node $u_i \in V$ past its threshold. This is to determine that any failures within the network that occur during simulation S_i come from attacking node u_i . For the runtime of simulation S_i , denoted $T_i \in T$, where T is the set of all runtimes, we have that $T_i = \{0, \dots, T'_i\}$, where T'_i is either a fixed cutoff point or when there are no more queued data packets.

Each measure is node and time dependant, so varying the node and time it is measured at changes the value computed by the measure. This time dependency is because the network model is dynamic. To compare the different measures, we must aggregate across one of the dimensions. We are interested in the performance of the measure for all nodes, as time progressed, so for each dynamic measure per simulation, we sum over all nodes at some timestep and return an aggregated measure.

Suppose the real network criticality can be captured by the sum of the node queues for a short future time horizon. This is because each measure in this paper computes the impact of failure that a node poses to the system at a given time. This is represented in this model by the node infecting neighbouring nodes, increasing their queue length. Since this increases the likelihood of the failure of neighbouring nodes, which would occur after some random time, the impact of a node's failure is delayed, and repairs after another delay, assuming they happen. This results in a peak of total queued data packets which we claim to occur approximately at the half life of an infectious node, assuming independent node lifespans. Using a mean field approximation, the future time window is defined as

$$t_f = \left\lceil \left(\frac{1}{\gamma} \right)^{1/2} \right\rceil.$$

Real criticality is aggregated by summing over all nodes at a timestep and at most t_f steps into the future. No computed measure is defined outside of T_i , so we only analyse the shorter timescale $T_i^{(f)} \in T^{(f)}$, where $T^{(f)}$ is the set of reduced runtimes, such that $T_i^{(f)} = \{0, \dots, T'_i - t_f\}$. With queue length, Q , this gives the set of all dynamic node attributes, $C = \{Q, C_L, C_W, C_B\}$. Let us denote

$$B_{t,i,u}^{(c)} : \{T_i^{(f)}, S, V, C\} \rightarrow \mathbb{R}$$

as the instance of a dynamic node attribute $c \in C$ for node $u \in V$ at time $t \in T_i$ for simulation S_i . We define the aggregated measure as

$$A_{t,i}^{(c)} = \begin{cases} \sum_{u \in V} B_{t,i,u}^{(c)}, & c \in \{C_L, C_W, C_B\} \\ \sum_{u \in V} \sum_{\tau=t}^{t+t_f} B_{\tau,i,u}^{(c)}, & c \in Q. \end{cases}$$

For comparative analysis, we normalise $A_{t,i}^{(c)}$ with respect to t for each attribute and simulation using min-max feature scaling, generating $\hat{A}_{t,i}^{(c)} : \{T_i, S_i, V, C\} \rightarrow [0, 1]$. We then compute the mean squared error (MSE) across time for $\hat{A}_{t,i}^{(C_L)}, \hat{A}_{t,i}^{(C_W)},$ and $\hat{A}_{t,i}^{(C_B)}$, versus the normalised aggregated queue length, $\hat{A}_{t,i}^{(Q)}$, and denote it as

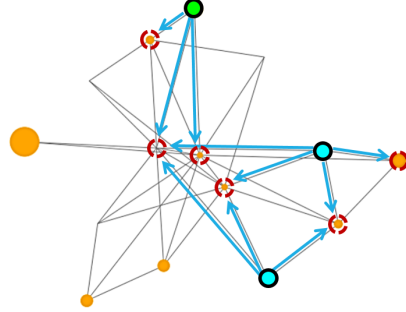
$$M_i^c = \text{MSE} \left(\hat{A}_i^{(c)} \right), \quad c \in \{C_L, C_W, C_B\}.$$

We find the mean for all simulations for each measure, getting the accuracy to which each measure estimates the criticality of each node within the network, giving

$$\bar{M}^c = \frac{\sum_{i=0}^n M_i^c}{n}, \quad c \in \{C_L, C_W, C_B\}.$$

We analyse this procedure for a network model with $n = 15$ nodes, edge attachment number $m = 3$, infection rate $\beta = 0.9$, recovery rate $\gamma = 0.5$, and infection threshold $I = 3$. We simulate a simple network at and beyond capacity. Mean simulation runtime was 4. Network G is visualised in Figure 1. Node size corresponds to Q of each node which has been assigned randomly.

Fig. 1 A Barabasi-Albert network G . Node count $n = 15$, edge attachment number $m = 3$, nodes randomly weighted with queue lengths. The green node u_1 seeds for simulation S_1 , and blue u_2, u_3 seed for S_2, S_3 . Arrows and dashed and rings are possible congestion candidates per timestep. All nodes have a corresponding simulation.



3 Results and Discussion

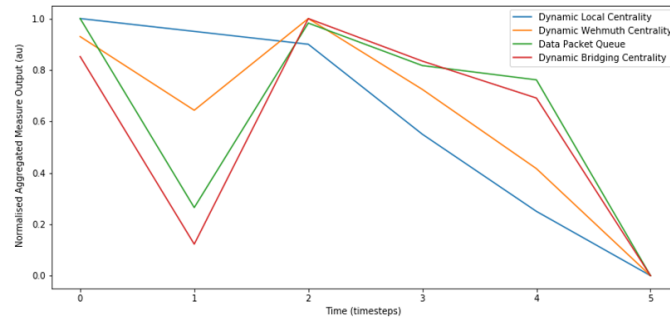
In Table 1 we explore the output of simulation S_1 , initialised from the green node in Figure 1. It shows that weighting measures with queue lengths better tracks the progression of data packets within the network. The aggregated queue length is forward looking, suggesting that the dynamic criticality measures detect risky nodes.

This is seen for dynamic measures in Figure 2, which is normalised for comparative inspection. This is only information for a single simulation instance. It is not obvious which measure more closely estimates future progression. Combining the

Table 1 Aggregated attributes for a simulation S_1 , 5 timesteps, containing $A_{t,1}^{(c)}$ for all measures.

		Time0	Time1	Time2	Time3	Time4	Time5
Queue Length		26	25	24	17	11	6
Static	Local	380	380	380	380	380	380
	Wehmuth	13.509	13.509	13.509	13.509	13.509	13.509
	Bridging	0.068	0.068	0.068	0.068	0.068	0.068
Dynamic	Local	253	200	266	215	158	81
	Wehmuth	29.011	4.166	34.048	28.409	23.517	0
	Bridging	131.882	58.548	130.119	113.635	108.101	32.147

MSEs of each measure from queue length for each simulation instance obtains the average MSE, denoted \bar{M}^c .

**Fig. 2** A plot showing the relationship between normalised aggregated measures and queue length from simulation S_1 , containing $A_{t,1}^{(c)}$ for $c \in C$.

Results show that dynamic local centrality performs best, with $\bar{M}^{C_L} = 0.102$, followed by dynamic bridging centrality, with $\bar{M}^{C_B} = 0.162$, and dynamic Wehmuth centrality is the worst, with $\bar{M}^{C_W} = 0.197$. This may be because the model estimates dynamics via epidemic spread, since momentary rate at which a node obtains data packets is strongly determined by the number of packets held by the given node's neighbours, and dynamic local centrality directly counts this.

All values are bounded in $[0, 1]$, so, in the contexts of this test, each measure computes criticality with between 80% and 90% accuracy, which is quite accurate.

Our criticality measures give a distributed, computationally efficient and fast method of finding an impact indicator to inform maintenance prediction models. This allows for real time control of any network system. Adding raw data such as condition can give probability of failure and other prognostics KPIs. Combining these gives a risk ranking of nodes to help order priority for proactive maintenance. This is a three step framework, first collecting distributed data, generating prognostic KPIs, and informing an optimal maintenance plan, shown in Fig 3. This will

minimise packet drops, latency, congestion, and maximise network operative capacity.

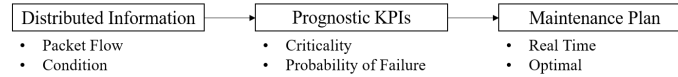


Fig. 3 Three step framework for assessing nodal risk ranking.

This can be integrated into: telecommunications systems for proactive maintenance; autonomous vehicle networks for proactive routing to minimise traffic jams; supply networks, where actors only have primary or secondary connection information; and any system of dynamically communicating agents. With such measures, agents will be able to quickly and reliably establish their short term criticality, allowing for swift, inexpensive action to ensure ongoing network function.

4 Conclusions

In this paper, we have developed and compared the accuracy of three distributed dynamic measures of nodal criticality within a network. Dynamic and distributed approaches had not previously been combined in such a manner. We tested each measure within an augmented SIS and found that for our test they predict criticality with high accuracy. Dynamic local centrality did best, though it yet is unclear why. To our knowledge, no measures which approach the problem of dynamically and distributedly predicting criticality of nodes like this have been previously developed, and it is exciting that they have such high proactive accuracy, suggesting there it is worth researching more dynamically obtained measures for prediction. They are necessary to deal with increasing data traffic demands, especially if more COVID-19-like events occur in the future, where greater network requirements are suddenly imposed on an already at capacity system.

4.1 Future Research

We will need deeper statistical analysis to learn the true accuracy of the measure family, including test repetition, comparing static and classic network measures, and multi-dimensional analysis. We would also like to learn how network structure and model configuration affect the result of the distributed dynamic measures.

In future we will test the dynamic measures in different network models, such as telecommunications data packet routing models, or supply network heuristic movement models. We also plan to test the measures on a spectrum of network topologies, as well as real life network topologies, such as the BT network that was studied

within [6], to gain insights into their dynamics. We will also study the impact of information reach, or how many hops away from itself a given node takes information from, framed as the relationship between accuracy and computational, time, and communication complexity. This will contribute to the general theory of value of information in distributed network analysis, and has applications in any system with limited awareness actors, such as supply chains.

Acknowledgements This research was supported by the EPSRC and BT Prosperity Partnership project: Next Generation Converged Digital Infrastructure, grant number EP/R004935/1, and the UK Engineering and Physical Sciences Research Council (EPSRC) Doctoral Training Partnership Award for the University of Cambridge, grant number EP/R513180/1.

References

1. Albert, R., Barabasi, A.: Statistical mechanics of complex networks. In: *Rev. Mod. Phys.* **74**, 47–97 (2002)
2. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.: Complex networks: Structure and dynamics. *Phys. Rep.* **424** 175–308 (2006)
3. Chen, D., Lü, L., Shang, M., Zhang, Y., Zhou, T.: Identifying influential nodes in complex networks. *Physica A*. **391**, 1777–1787 (2012)
4. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S.: Resilience of the Internet to random breakdowns. *Phys. Rev. Lett.* **85**, 4626–4628 (2000)
5. Freeman, L.C.: A Set of Measures of Centrality Based on Betweenness. *Sociometry* **40**, 35 (1977)
6. Herrera, M., Perez-Hernandez, M., Kumar Jain, A., Kumar Parlikad, A.: Critical link analysis of a national Internet backbone via dynamic perturbation. In: *Advanced Maintenance Engineering, Services and Technologies*. IFAC, Virtual (2020)
7. Marsden, P.V.: Egocentric and sociocentric measures of network centrality. *Soc. Netw.* **24**, 407–422 (2002)
8. Kermack, W.O., McKendrick, A.G., Thomas, W.G.: A contribution to the mathematical theory of epidemics. *Proc. R. Soc. Lond.* **115**, 700–721 (1927)
9. Moura, J., Hutchison, D.: Cyber-Physical Systems Resilience: State of the Art, Research Issues and Future Trends. In: *arXiv preprint*. (2019)
10. Nanda, S., Kotz, D.: Localized Bridging Centrality for Distributed Network Analysis. In: *2008 Proceedings of 17th International Conference on Computer Communications and Networks*, IEEE, St. Thomas, US Virgin Islands (2008)
11. Peterson, I.: *Fatal Defect: Chasing Killer Computer Bugs*. Times Books, (1996)
12. Wang, J., Liu, Y.H., Jiao, Y., Hu, H.Y.: Cascading dynamics in congested complex networks. *Eur. Phys. J. B.* **67**, 95–100 (2009)
13. Wehmuth, K., Ziviani, A.: Distributed location of the critical nodes to network robustness based on spectral analysis. In: *2011 7th Latin American Network Operations and Management Symposium*, IEEE, Quito, Ecuador (2011)