General theory for extended-range percolation on simple and multiplex networks

Lorenzo Cirigliano [1,2,*] Claudio Castellano [3,2,†] and Ginestra Bianconi [4,5,‡]
[1]*Dipartimento di Fisica Università "Sapienza", P. le A. Moro, 2, I-00185 Rome, Italy*
[2]*Centro Ricerche Enrico Fermi, Piazza del Viminale, 1, I-00184 Rome, Italy*
[3]*Istituto dei Sistemi Complessi (ISC-CNR), Via dei Taurini 19, I-00185 Rome, Italy*
[4]*School of Mathematical Sciences, Queen Mary University of London, London E1 4NS, United Kingdom*
[5]*The Alan Turing Institute, The British Library, 6 Euston Road, London, NW1 2DB, United Kingdom*

(Received 3 July 2024; accepted 20 August 2024; published 3 September 2024)

Extended-range percolation is a robust percolation process that has relevance for quantum communication problems. In extended-range percolation nodes can be trusted or untrusted. Untrusted facilitator nodes are untrusted nodes that can still allow communication between trusted nodes if they lie on a path of distance at most R between two trusted nodes. In extended-range percolation the extended-range giant component (ERGC) includes trusted nodes connected by paths of trusted and untrusted facilitator nodes. Here, based on a message-passing algorithm, we develop a general theory of extended-range percolation, valid for arbitrary values of R as long as the networks are locally treelike. This general framework allows us to investigate the properties of extended-range percolation on interdependent multiplex networks. While the extended-range nature makes multiplex networks more robust, interdependency makes them more fragile. From the interplay between these two effects a rich phase diagram emerges including discontinuous phase transitions and reentrant phases. The theoretical predictions are in excellent agreement with extensive Monte Carlo simulations. The proposed exactly solvable model constitutes a fundamental reference for the study of models defined through properties of extended-range paths.

DOI: 10.1103/PhysRevE.110.034302

I. INTRODUCTION

Percolation [1–5] is arguably the most fundamental critical phenomenon defined on networks, as it reflects the connectivity properties and the robustness of the network on which it is defined. The existence of a giant cluster is a prerequisite for any collective critical phenomenon [1] defined on networks; thus percolation properties are key to study processes on networks, such as epidemic-spreading phenomena as well as Ising models.

Requiring connectivity might, however, be a too strong request, and in many scenarios it is becoming relevant to study percolation problems in which this requirement is alleviated. This is particularly interesting in quantum communication [6–9] where noisy data transmission can cause signal degradation [10]. Thus, quantum networks require the use of quantum repeaters to extend the range of communication between trusted nodes [11,12]. In order to study connectivity of such quantum networks it is therefore important to investigate percolation problems in which the communication between trusted nodes might be allowed also if trusted nodes are not directly connected to each other. Moreover, for secure quantum communication, hybrid classical-quantum networks [13] between trusted nodes are often needed, thus requiring the investigation of multilayer [14] percolation properties of these networks.

Here we focus on extended-range percolation (ERP), a robust percolation process where nodes may belong to the same component even if they are not directly connected, and we propose a general theory of this model on simple and multilayer networks. This model has been recently proposed and investigated on random networks in Ref. [15]. Also the lattice version of this model has attracted significant attention recently [16–22].

There is an increasing interest in percolation problems that do not require the traditional notion of connectivity. In addition to ERP, several other percolation models have been recently proposed in which percolation is defined through properties of the shortest paths of the network or through generalized notions of connected components. These include concurrence and α percolation [4,23], motivated by quantum communication, shortest path percolation [24], motivated by transportation networks, no-exclaves percolation [25], motivated by the need to enhance network robustness, and color-avoiding percolation [26,27], to reproduce nonuniform vulnerability of nodes to attack or failure. Moreover models assuming a nonlocal definition of connectivity are raising interest in the last few years, also beyond the theory of

*Contact author: lorenzo.cirigliano@uniroma1.it
†Contact author: claudio.castellano@roma1.infn.it
‡Contact author: ginestra.bianconi@gmail.com

percolation with many applications including notably epidemic spreading [28,29]. Thus, a general theory of ERP on simple and multilayer networks might inspire further research in this direction.

In ERP nodes can be trusted with probability p and untrusted with probability $1-p$. Untrusted nodes can be involved in the communication between trusted nodes if they lie on a path between trusted nodes of length at most R. We call these nodes *facilitator* nodes. The extended-range giant component (ERGC) is formed by all the trusted nodes connected by paths of trusted and facilitator nodes and by all the untrusted nodes at distance less than R from these trusted nodes. Recently the exact solution of extended-range percolation on uncorrelated random graphs with given degree distribution was found for R up to 6 [15]. However, this solution relies on involved combinatorial definitions which impede a straightforward extension of the approach to treat larger values of R as well as to address generalized percolation problems on multilayer or higher-order networks.

Here we provide a general theory of ERP for any arbitrary R that is based on a message passing (MP) approach where the messages have a simple and transparent combinatorial interpretation allowing a deeper theoretical understanding of the model as well as an easier generalization to multilayer networks. The message-passing approach [14,30,31] defines a fundamental distributed computation that applies to a large variety of critical phenomena and dynamical processes on networks including percolation, network control, and optimization problems [32–37]. For standard percolation the MP predicts the size of the giant component on arbitrary network topology as long as it is locally treelike; extensions beyond this approximation are a topic of active research [38,39]. Here we fully develop a message-passing theory of ERP that allows us to predict the size of the ERGC for any value of R and for any arbitrary network that is locally treelike. In this work we also use this theory to investigate ERP in random graphs with given degree distribution. We stress that, although the formalism and approach developed here is markedly distinct from the one formulated in Ref. [15], the equations that we obtain for arbitrary R are equivalent to the ones obtained by the previous work for R up to 6.

The general theory for ERP formulated in this work for single networks is then used to investigate the percolation properties of multiplex networks under the extended-range framework. Multiplex networks [14,40,41] are formed by N nodes connected via M distinct networks (layers). Multiplex networks describe a large class of complex interacting systems where nodes are related by interactions of different types. Notable examples include interacting infrastructure and communication networks or biological networks inside the cell. The robustness of multiplex networks has raised significant interest [14,35,42–45], as interdependencies between the layers can lead to an increased fragility of the system, thus providing a framework to model cascades of failure events propagating across the layers of the multiplex network. In particular in Ref. [42] a multiplex interdependent percolation (MIP) problem has been defined. The order parameter of this model is given by the size of the mutually connected giant component (MCGC) formed by nodes (directly) connected to each other by at least one path on each layer. The MCGC emerges exhibiting a discontinuous hybrid phase transition, and its critical properties reflect the increased fragility of the system.

In this work we investigate the trade-off between the effect of interdependencies present in multiplex networks that increase the fragility of the multiplex networks, and the extended-range mechanism that facilitates communication between otherwise disconnected nodes. To this end, we formulate the Multiplex Extended-Range Percolation (MERP) whose order parameter is the size of the Multiplex Extended-Range Giant Component (MERGC). We introduce a notion of interdependency for trusted nodes. However, since untrusted nodes play a significant role in extended-range percolation, the definition of the model is not complete if we do not specify whether untrusted nodes are interdependent. This leads to two variants of the MERP (version $V=1$ and version $V=2$). In version $V=1$ of MERP an untrusted node belongs to the MERGC if it belongs to the ERGC *in each layer*. Thus, this version imposes interdependencies for untrusted nodes. In version $V=2$ instead, it is sufficient that an untrusted node is part of the ERGC in *at least one* layer to belong to the MERGC, i.e., we do not impose interdependencies for untrusted nodes.

We provide an exact solution of both versions of MERP on uncorrelated random multiplex networks with arbitrary degree distributions. Our analysis of the critical phenomena of MERP is based upon analytical predictions of the phase diagram, supported by extensive Monte Carlo simulations. We reveal the important interplay between the effect of interdependencies and of the extended-range mechanism. In particular, the study of version $V=2$ of MERP shows a highly nontrivial phenomenology with a reentrant discontinuous hybrid phase transition, observed in multiplex networks where the MCGC does not exist.

This paper is structured as follows: In Sec. II we define extended-range percolation on simple networks, and we present a general message-passing theory to predict the size of the ERGC on arbitrary treelike networks. In Sec. III we formulate a general theory of extended-range percolation on random networks, valid for any arbitrary choice of the range R, and we compare our theory with Monte Carlo simulations. In Sec. IV we formulate the two versions of MERP (version $V=1$ and version $V=2$). We provide a general analytic theory to calculate the MERGC, and we discuss the critical properties of MERP, including the presence of a characteristic reentrant phase transition in the version $V=2$ of this model. Our theoretical predictions are in excellent agreement with Monte Carlo simulations. Finally in Sec. V we provide the concluding remarks. The paper is enriched with Appendixes, providing details of the derivation of the message-passing theory for ERP, explicit equations for ERP and MERP for finite values of R, and discussion of the equivalence of the equations of ERP for $R \leqslant 4$ with the equations derived in Ref. [15].

II. EXTENDED-RANGE PERCOLATION AND MESSAGE-PASSING APPROACH

Consider a network $\mathcal{G}=(V,E)$ of $N=|V|$ nodes where nodes are either untrusted or trusted. Communication between

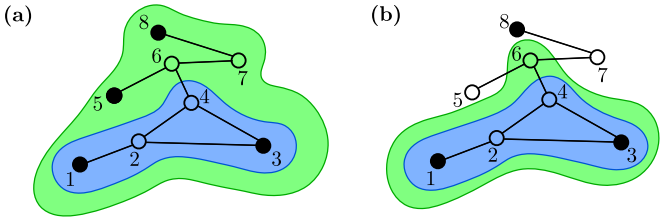

FIG. 1. Schematic representation of extended-range percolation on networks. Trusted and untrusted nodes are represented by filled and empty circles, respectively. The extended-range giant component (ERGC) of range $R = 2$ (smaller, blue component) and $R = 3$ (larger, green component) is highlighted. The two networks in (a) and (b) have the same $R = 2$ ERGC, but different $R = 3$ ERGC. For $R = 2$, node 4 belongs to the ERGC even if it is not a facilitator. For $R = 3$, node 6 is a facilitator in (a) but not in (b); nevertheless, in both cases it is a part of the ERGC. Node 7 instead is in the ERGC in (a) since it is a facilitator but not in (b).

two trusted nodes takes place only if there is at least one walk connecting them including trusted and untrusted nodes and having at most $R-1$ consecutive untrusted nodes. Note that we require the existence of a *walk* and not a *path*. For instance, nodes 3 and 8 in Fig. 1(a) can communicate for $R = 3$ even if the (shortest) path $\{3 \to 4 \to 6 \to 7 \to 8\}$ connecting them contains three consecutive untrusted nodes, due to the existence of the walk $\{3, 4, 6, 5, 6, 7, 8\}$ having at most two consecutive untrusted nodes because of the presence of the trusted node 5.

Strictly speaking, communication is among trusted nodes, but it is clear that untrusted nodes play a crucial role in this process, in particular, untrusted nodes lying on paths between two trusted nodes of length at most R. We call such untrusted nodes *facilitators*, because they are allowing for the communication of distant trusted nodes. For instance, node 2 is a facilitator for $R = 2$ and $R = 3$ in Fig. 1; nodes 4,6,7 are facilitators for $R = 3$ in Fig. 1(a) but not in 1(b). Given this way to communicate, we define the extended-range giant connected component (ERGC) as the giant component formed by trusted nodes connected by paths including exclusively trusted or untrusted facilitator nodes and by all the untrusted nodes at distance less than R from these trusted nodes. This is equivalent to say that any pair of trusted nodes in the ERGC is connected by at least a walk formed by trusted and untrusted nodes including at most $R-1$ consecutive untrusted nodes (facilitators). Moreover the untrusted nodes in the ERGC include all the facilitator nodes and all the untrusted nodes that are not facilitators but are at a distance less than R from the trusted nodes in the ERGC. For a schematic representation of the ERGCs see Fig. 1.

The algorithm to evaluate the ERGC is a generalization of the Depth-First Search algorithm. We assign to each node i of the network a pair of variables (q_i, r_i). Initially no node is assigned to a cluster, i.e., every node has $q_i = 0$. Moreover all trusted nodes have $r_i = 0$, and all untrusted nodes have $r_i = R$. At the end of the algorithm $q_i = q \in \{1, 2, \ldots, Q\}$ indicates to which of the Q clusters node i belongs and r_i indicates the distance (if smaller than R) from the closer trusted node. The algorithm for detecting the ERGC is the recursive Extended-Range Depth First Search ERDFS algorithm. Starting from an arbitrary trusted (unvisited) seed node for cluster q (initially taken to be $q = 1$), we set $q_i = q$ and $r_i = 0$ and we call the ERDFS algorithm.

The recursive ERDFS algorithm is defined as follows. Starting from a node n with $q_n = q$ and $r_n = r$, ERDFS implements (1) and (2) defined as follows:

(1) If $r < R$ the algorithm visits all the neighbor trusted nodes m unvisited previously. For each of these nodes the algorithm sets $r_m = 0$ and $q_m = q$, and the ERDFS is recursively iterated.

(2) If $r < R-1$ the algorithm visits all the neighbor untrusted nodes m with $r_m > r+1$. For each of these nodes the algorithm sets $r_m = r+1$ and $q_m = q$, and the ERDFS is recursively iterated.

When there are no more nodes to visit, the ERDFS stops and all the trusted and untrusted nodes with $q_i = q$ form the ERP cluster q. If there are unvisited trusted nodes, we choose a new trusted seed node for cluster $q+1$ and iterate the procedure until all the trusted nodes are assigned to a cluster and we have Q clusters (where Q is determined by the algorithm). The ERGC is the giant cluster $q = q^\star$ formed by the trusted nodes with $r_i = 0$ and the untrusted nodes with $r_i < R$ all having $q_i = q^\star$.

Here we develop a message-passing (MP) theory to predict the size of the ERGC on any locally treelike network. The general MP equations describing the problem with a given configuration of trusted and untrusted nodes are explained in detail in Appendix A. Here we assume that nodes are trusted with probability p and untrusted with probability $1-p$, and the equations we obtain follow from the more general ones; see Appendix A. We can express the size of the ERGC using two sets of cavity messages $\hat{\sigma}^r_{i\to j}$ and $\hat{\omega}^r_{i\to j}$, for $1 \leqslant r \leqslant R$. The generic message $\hat{\sigma}^r_{i\to j}$ sent from node i to node j indicates the probability that node i is in the ERGC and it is at distance $r-1$ from the closest trusted node when the link (i, j) is removed. The generic message $\hat{\omega}^r_{i\to j}$ sent from node i to node j indicates the probability that node i is not in the ERGC and it is at distance $r-1$ from the closest trusted node when the link (i, j) is removed.

Our message-passing equations (see Appendix A for a detailed derivation) dictate that the messages $\hat{\sigma}^r_{i\to j}$ obey

$$\hat{\sigma}^1_{i\to j} = p\left[1 - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R}\hat{\sigma}^q_{\ell\to i}\right)\right]$$

$$\hat{\sigma}^{r+1}_{i\to j} = (1-p)\left\{\left[\prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant r-1}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant \bar{r}}\hat{\omega}^q_{\ell\to i}\right) - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant \bar{r}}\hat{\omega}^q_{\ell\to i}\right)\right]\right.$$

$$+\theta(R-2r)\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r}\hat{\sigma}^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right)+\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-r}\hat{\sigma}^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right)\right.$$
$$\left.\left.-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r-1}\hat{\sigma}^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right)-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-r}\hat{\sigma}^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right)\right]\right\}. \quad (1)$$

Note that here and in the following we use $\bar{r}$ to indicate $\bar{r}=\min(r-1,R-r)$, we use $\theta(x)$ to indicate the Heaviside function with $\theta(x)=1$ if $x>0$ and $\theta(x)=0$ otherwise, and we use $\partial i\setminus j$ to denote the neighborhood of node i (∂i) without node j.

The messages $\hat{\omega}^r_{i\to j}$ instead obey

$$\hat{\omega}^1_{i\to j}=p\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R}\hat{\sigma}^q_{\ell\to i}\right)\right],$$
$$\hat{\omega}^{r+1}_{i\to j}=(1-p)\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-1}\hat{\sigma}^r_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right)\right.$$
$$\left.-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-1}\hat{\sigma}^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right)\right]. \quad (2)$$

The order parameter P^∞ expressing the fraction of trusted nodes in the ERGC is given by

$$P^\infty=\frac{p}{N}\sum_{i=1}^{N}\left[1-\prod_{\ell\in\partial i}\left(1-\sum_{1\leqslant r\leqslant R}\hat{\sigma}^r_{\ell\to i}\right)\right]. \quad (3)$$

An untrusted node is in the ERGC if it is at distance less than R from a trusted node in the ERGC. Thus, we can define a second-order parameter U^∞ for ERP given by the fraction of untrusted nodes in the ERGC, expressed in terms of the messages as

$$U^\infty=\frac{(1-p)}{N}\sum_{i=1}^{N}\left[1-\prod_{\ell\in\partial i}\left(1-\sum_{1\leqslant r\leqslant R-1}\hat{\sigma}^r_{\ell\to i}\right)\right]. \quad (4)$$

The overall fraction of nodes in the ERGC is the sum between P^∞ and U^∞. Setting $R=1$, we recover the MP equations for standard percolation [14].

Note that the equations for the $\hat{\sigma}^r_{i\to j}$ in (1) involve R variables $\hat{\sigma}^r_{i\to j}$, with $1\leqslant r\leqslant R$, and only $\lceil R/2\rceil-1$ variables $\hat{\omega}^r_{i\to j}$, with $1\leqslant r\leqslant\lceil R/2\rceil-1$. Since Eqs. (3) and (4) for the order parameters contain only the variables $\hat{\sigma}^r_{i\to j}$, the total number of independent equations needed is $R+\lceil R/2\rceil-1$, rather than $2R$. The MP equations (1), (2) and (3) (4) can be used to compute the size of the ERGC on any simple network and for arbitrary interaction range R. They are exact in the limit of large N for locally treelike networks. This theory can also be used as the starting point to derive the equations determining the critical properties of ERP on random graphs with given degree distribution as explained in the following section.

III. THEORY FOR EXTENDED-RANGE PERCOLATION ON RANDOM GRAPHS

A. General theoretical framework

In this section we set up the general theoretical framework to study the critical properties of extended-range percolation on uncorrelated random graphs with arbitrary degree distribution $P(k)$. For $R\leqslant 6$, these equations are equivalent to the equations derived in [15]. We stress, however, that the formalism in [15] is rather cumbersome, and it is not easily generalizable to arbitrary large values of R. Here, using the powerful MP theory developed above, we derive exact equations valid for arbitrary R. The order parameters P^∞ and U^∞ determine the probability that a random node belongs to the ERGC, and it is trusted or untrusted, respectively. We can express these order parameters in terms of the probabilities S_r that following a randomly chosen link we reach a node that is in the ERGC and is at distance $r-1$ from the closest trusted node, and of the probabilities W_r that following a randomly chosen link we reach a node that is not in the ERGC and is at distance $r-1$ from the closest trusted node.

The probabilities S_r and W_r satisfy a set of self-consistent equations that can be derived from the MP equations discussed in the previous section. Indeed, S_r and W_r can be identified as the average of the messages $\hat{\sigma}^r_{i\to j}$ and $\hat{\omega}^r_{i\to j}$, respectively, over the ensemble of random graphs with degree distribution $P(k)$ (see Appendix A for a more detailed discussion).

The equations for S_r and W_r read

$$S_1=p\left[1-G_1\left(1-\sum_{1\leqslant q\leqslant R}S_q\right)\right],$$
$$S_{r+1}=(1-p)\left\{\left[G_1\left(1-\sum_{1\leqslant q\leqslant r-1}S_q-\sum_{1\leqslant q\leqslant\bar{r}}W_q\right)-G_1\left(1-\sum_{1\leqslant q\leqslant r}S_q-\sum_{1\leqslant q\leqslant\bar{r}}W_q\right)\right]\right.$$

$$+\theta(R-2r)\left[G_1\left(1-\sum_{1\leqslant q\leqslant r}S_q-\sum_{1\leqslant q\leqslant r-1}W_q\right)+G_1\left(1-\sum_{1\leqslant q\leqslant R-r}S_q-\sum_{1\leqslant q\leqslant r}W_q\right)\right.$$
$$\left.-G_1\left(1-\sum_{1\leqslant q\leqslant R-r}S_q-\sum_{1\leqslant q\leqslant r-1}W_q\right)-G_1\left(1-\sum_{1\leqslant q\leqslant r}S_q-\sum_{1\leqslant q\leqslant r}W_q\right)\right]\Bigg\}$$
$$W_1=pG_1\left(1-\sum_{1\leqslant q\leqslant R}S_q\right),\quad W_{r+1}=(1-p)\left[G_1\left(1-\sum_{1\leqslant q\leqslant R-1}S_q-\sum_{1\leqslant q\leqslant r-1}W_q\right)-G_1\left(1-\sum_{1\leqslant q\leqslant R-1}S_q-\sum_{1\leqslant q\leqslant r}W_q\right)\right], \tag{5}$$

where $G_0(x)$ and $G_1(x)$ are the generating functions defined as

$$G_0(x)=\sum_k P(k)x^k,\quad G_1(x)=\sum_k \frac{kP(k)}{\langle k\rangle}x^{k-1}. \tag{6}$$

The probability P^∞ that a node is trusted and is in the ERGC is given by

$$P^\infty=p\left[1-G_0\left(1-\sum_{1\leqslant r\leqslant R}S_r\right)\right], \tag{7}$$

while the probability U^∞ that a node is untrusted and is in the ERGC is given by

$$U^\infty=(1-p)\left[1-G_0\left(1-\sum_{1\leqslant r\leqslant R-1}S_r\right)\right]. \tag{8}$$

As noted in the previous section, the total number of independent equations needed is $R+\lceil R/2\rceil-1$, rather than $2R$, since the equations for the S_r in (5) involve R variables S_r and only $\lceil R/2\rceil-1$ variables W_r.

In a more compact way, we can use the vector $\boldsymbol{Y}=(\boldsymbol{S}^\top,\boldsymbol{W}^\top)^\top$ encoding all the relevant S_r [$\boldsymbol{S}=(S_1,S_2,\ldots)^\top$] and W_r variables [$\boldsymbol{W}=(W_1,W_2,\ldots)^\top$], and we can write Eqs. (5) as

$$\boldsymbol{Y}=\boldsymbol{F}_{\boldsymbol{Y}}(\boldsymbol{Y},p) \tag{9}$$

or, alternatively, as

$$\boldsymbol{S}=\boldsymbol{F}_{\boldsymbol{S}}(\boldsymbol{S},\boldsymbol{W},p), \tag{10}$$

$$\boldsymbol{W}=\boldsymbol{F}_{\boldsymbol{W}}(\boldsymbol{S},\boldsymbol{W},p). \tag{11}$$

In Appendix B we write explicitly Eqs. (5) and (7) for $R\leqslant 4$. These equations are shown to be equivalent to the ones derived in [15] in Appendix C.

B. Phase transition and critical threshold

The ERP order parameters P^∞ and U^∞ as functions of p are plotted in Fig. 2 for a Poisson network of average degree $c=2$. The analytic solution is in perfect agreement with results of numerical simulations. Extended-range percolation displays a continuous phase transition at $p=p_c$, in analogy with standard percolation (case $R=1$). As intuitively expected, the percolation threshold decreases as R increases: the presence of a range $R>1$ enhances the robustness of the network. Moreover, while the order parameter P^∞ is monotonically increasing in p, the order parameter U^∞ displays a maximum as a function of p. The physical intuition is as follows. For $p<p_c$ both P^∞ and U^∞ are identically zero as there are no nodes in the ERGC. For $p=1$, the ERGC coincides with the giant component of the network for any R, so $P^\infty(R)=P^\infty$ while $U^\infty(R)=0$. Thus, U^∞ cannot be monotonically increasing and actually displays a single maximum.

As anticipated before, extended-range percolation is characterized by a continuous phase transition at the percolation threshold p_c, where P^∞ becomes nonzero. For $p\leqslant p_c$, there is a unique solution for Eqs. (9), $S_r=S_r^0=0$ for all values of

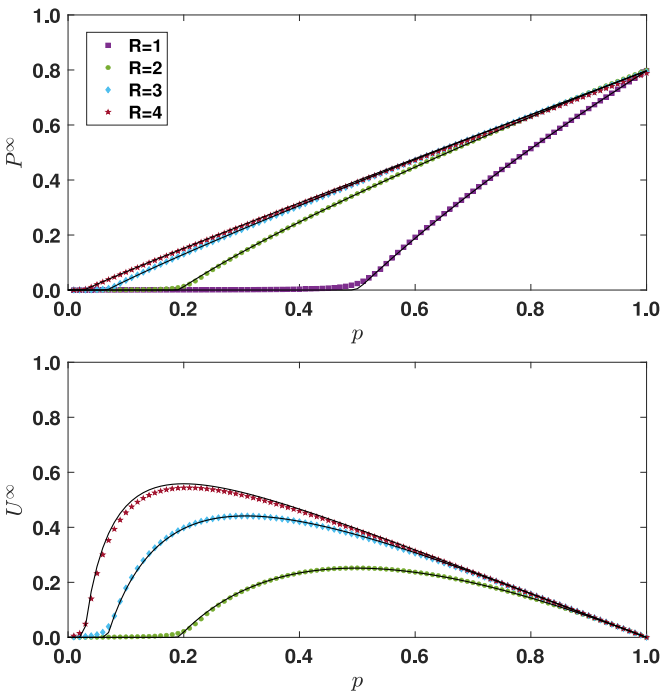

FIG. 2. The ERP order parameters, P^∞ and U^∞, as functions of the fraction of trusted nodes p for $R\in 1,2,3,4$. ERP exhibits a continuous phase transition at the percolation threshold $p=p_c$, which decreases as R increases. Note that for $R=1$, P^∞ reduces to standard percolation and that U^∞ is only nontrivial (i.e., nonzero) for $R>1$. The symbols indicate results of Monte Carlo simulations over 1000 realizations of Poisson networks of $N=2\times 10^4$ nodes and average degree $c=2$.

r and $W_r = W_r^0$ with

$$W_1^\star = p,$$
$$W_{r+1}^\star = (1-p)\left[G_1\left(1 - \sum_{1\leqslant q\leqslant r-1} W_q^\star\right) - G_1\left(1 - \sum_{1\leqslant q\leqslant r} W_q^\star\right)\right], \tag{12}$$

corresponding to $P^\infty = U^\infty = 0$. For $p > p_c$ another solution with positive S_r appears, continuously in $p - p_c$. Let us denote $\boldsymbol{Y}^0 = (\boldsymbol{S}^{0\top}, \boldsymbol{W}^{0\top})^\top$. The percolation threshold p_c can be obtained linearizing Eq. (10) around $\boldsymbol{S} = \boldsymbol{S}^0$ and imposing that

$$\Lambda_0(p_c) = 1, \tag{13}$$

where Λ_0 is the largest eigenvalue of the Jacobian matrix of $\boldsymbol{F}_{\boldsymbol{Y}}$ performed with respect to the variables in $\boldsymbol{Y}$ and calculated in $\boldsymbol{Y}^0$. As shown in [15], ERP on uncorrelated random graphs belong to the same universality class of standard percolation for homogeneous degree distribution and for power-law degree distributions $P(K) \sim k^{-\gamma}$ with $\gamma > 3$, while R-dependent critical exponents are found for strongly heterogeneous networks with $2 < \gamma < 3$.

IV. MULTIPLEX EXTENDED-RANGE PERCOLATION

A. Theoretical framework

Consider a multiplex network [14] $\vec{\mathcal{G}} = (\mathcal{G}^{[1]}, \mathcal{G}^{[2]}, \ldots, \mathcal{G}^{[\alpha]}, \ldots, \mathcal{G}^{[M]})$ formed by M network layers $\mathcal{G}^{[\alpha]} = (V, E^{[\alpha]})$ of $N = |V|$ nodes, with $\alpha \in \{1, \ldots, M\}$. Each network $\mathcal{G}^{[\alpha]}$ is drawn independently at random from the ensemble of uncorrelated random networks with degree distribution $P^{[\alpha]}(k)$, whose generating functions are

$$G_0^{[\alpha]}(x) = \sum_k P^{[\alpha]}(k) x^k, \quad G_1^{[\alpha]}(x) = \sum_k \frac{kP^{[\alpha]}(k)}{\langle k\rangle} x^{k-1}. \tag{14}$$

We assume that the multiplex network has thus a negligible link overlap [46]. Each node of the multiplex network is either a trusted node on every layer or an untrusted node on every layer.

Inspired by the multiplex interdependent percolation (MIP) model [14,42,43], we formulate two versions of the Multiplex Extended-Range Percolation (MERP) model: version $V = 1$ and version $V = 2$ (see Fig. 3 for a schematic representation of the models). Both versions exploit the presence of untrusted facilitator nodes and the extended-range percolation mechanism together with the interdependencies for nodes of different layers.

The Multiplex Extended-Range Giant Component (MERGC) is defined as follows. In both versions of the model, a trusted node is in the MERGC if it belongs to the ERGC *in each layer* of the multiplex network. Version 1 and version 2 impose, however, different conditions on untrusted nodes. In Version 1, we require that each untrusted node in the MERGC must be in the ERGC *in each layer* of the multiplex, as it is required for trusted nodes. In Version 2 instead, untrusted nodes in the MERGC must be part of the ERGC in *at least* one layer. This difference in the condition

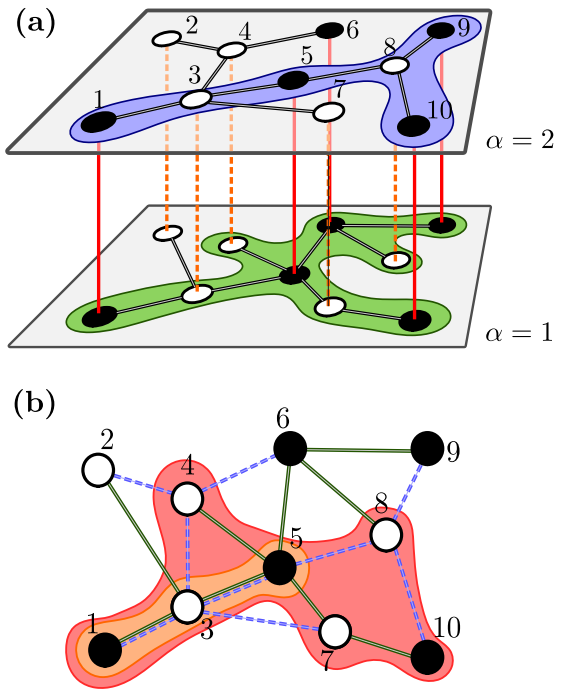

FIG. 3. Schematic representation of multiplex extended-range percolation for $R = 2$ and $M = 2$ layers. Trusted and untrusted nodes are indicated by filled and empty circles, respectively. (a) The ERGC of each single layer is highlighted, in green for layer $\alpha = 1$ and in blue for layer $\alpha = 2$. Red solid interlayer links represent the interdependencies for trusted nodes in both versions of MERP, yellow dashed interlayer links represent the condition on untrusted nodes, considered only in version 1. Note that some nodes are facilitators in only one layer, e.g., node 7, while others are facilitators in both layers, e.g., node 3. (b) The two, different, MERGC for version 1, highlighted in yellow, and version 2 highlighted in red. Since the trusted node 6 is not in the ERGC in layer 2, it cannot be part of the MERGC, causing also node 9 to disconnect. The untrusted node 7 is in the ERGC of layer 1, but not in layer 2. As a consequence, it is in the MERGC for version 2 but not for version 1, and it also affects the presence in the MERGC of node 10. The size of the MERGC for the two versions of the model can thus be significantly different.

imposed on untrusted nodes strongly affects the robustness of the multiplex, as explained in detail below. Let us make some qualitative preliminary remarks on the behavior of MERP. As the ERGC on a single network reduces, for any finite R, to the standard giant component in the network for $p = 1$ (untrusted nodes are absent), in both versions of MERP the MERGC reduces for $p = 1$ to the mutually connected giant component of MIP. For $R = 1$ untrusted nodes have no role, thus both versions of MERP have the same MERGC, which coincides with the mutually connected giant component (MCGC) of MIP.

The exact solution of MERP on uncorrelated random graphs with arbitrary degree distribution can be obtained as follows. First, we introduce the variables $S_r^{[\alpha]}$ and $W_r^{[\alpha]}$, defined as the probabilities S_r and W_r in layer α. Then we can define recursive equations for these variables starting from Eqs. (5), (7), and (8) and implementing the different conditions required by the two versions of MERP. The requirement for trusted nodes to be part of the ERGC in

all layers can be easily implemented with the multiplicative factor

$$\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\beta]}\right)\right]$$

in the equations for $S_1^{[\alpha]}$ and $W_1^{[\alpha]}$, thus obtaining the equations

$$\begin{aligned}S_1^{[\alpha]}&=p\left[1-G_1^{[\alpha]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\alpha]}\right)\right]\left\{\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\beta]}\right)\right]\right\},\\ W_1^{[\alpha]}&=p\left[G_1^{[\alpha]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\alpha]}\right)\right]\left\{\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\beta]}\right)\right]\right\}.\end{aligned}\tag{15}$$

The requirement for untrusted nodes to be in the ERGC in all layers can be instead implemented by means of the multiplicative factor

$$\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R-1}S_r^{[\beta]}\right)\right]$$

in the equations for $S_r^{[\alpha]}$ and $W_r^{[\alpha]}$ with $2\leqslant r\leqslant R$. However, as explained above, this condition is required only in version $V=1$ of the model, while no restriction on untrusted nodes is applied for $V=2$. The two different conditions for untrusted nodes can then be implemented all at once using Kronecker's $\delta_{V,1}$ and $\delta_{V,2}$. We get the equations

$$\begin{aligned}S_{r+1}^{[\alpha]}&=(1-p)\left\{\left[G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant r-1}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant\bar{r}}W_q^{[\alpha]}\right)-G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant r}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant\bar{r}}W_q^{[\alpha]}\right)\right]\right.\\ &\quad+\theta(R-2r)\left[G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant r}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r-1}W_q^{[\alpha]}\right)+G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant R-r}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r}W_q^{[\alpha]}\right)\right.\\ &\quad\left.\left.-G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant R-r}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r-1}W_q^{[\alpha]}\right)-G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant r}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r}W_q^{[\alpha]}\right)\right]\right\}\\ &\quad\times\left\{\delta_{V,2}+\delta_{V,1}\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R-1}S_r^{[\beta]}\right)\right]\right\},\\ W_{r+1}^{[\alpha]}&=(1-p)\left[G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant R-1}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r-1}W_q^{[\alpha]}\right)-G_1^{[\alpha]}\left(1-\sum_{1\leqslant q\leqslant R-1}S_q^{[\alpha]}-\sum_{1\leqslant q\leqslant r}W_q^{[\alpha]}\right)\right]\\ &\quad\times\left\{\delta_{V,2}+\delta_{V,1}\prod_{\beta\neq\alpha}\left[1-G_0^{[\beta]}\left(1-\sum_{1\leqslant r\leqslant R-1}S_r^{[\beta]}\right)\right]\right\}.\end{aligned}\tag{16}$$

Using a notation similar to the one adopted for ERP, we can write these equations in a more compact way. Introducing the vector $\boldsymbol{Y}=(\boldsymbol{S}^\top,\boldsymbol{W}^\top)^\top$ and encoding all the relevant $S_r^{[\alpha]}$ [$\boldsymbol{S}=(S_1^{[1]},S_2^{[1]},\ldots S^{[\alpha]}\ldots)^\top$] and $W_r^{[\alpha]}$ variables [$\boldsymbol{W}=(W_1^{[1]},W_2^{[2]},\ldots,W_r^{[\alpha]}\ldots)^\top$], we can write Eqs. (16), as

$$\boldsymbol{Y}=\boldsymbol{F}(\boldsymbol{Y},p).\tag{17}$$

For the order parameter P^∞, corresponding to the probability that a random node is in the MERGC and it is trusted, we can write the equation

$$P^\infty=p\prod_{\alpha=1}^{M}\left[1-G_0^{[\alpha]}\left(1-\sum_{1\leqslant r\leqslant R}S_r^{[\alpha]}\right)\right],\tag{18}$$

valid for both versions of MERP. For the probability U^∞ that a node is untrusted and belongs to the MERGC we must distinguish between $V=1$ and $V=2$. In version 1, we require that untrusted nodes in the MERGC must be in the ERGC in all layers, hence we have

$$U^\infty=(1-p)\prod_{\alpha=1}^{M}\left[1-G_0^{[\alpha]}\left(1-\sum_{1\leqslant r\leqslant R-1}S_r^{[\alpha]}\right)\right].\tag{19}$$

In version 2 we require that an untrusted node in the MERGC is in the ERGC in at least one layer, hence we get

$$U^\infty=(1-p)\left[1-\prod_{\alpha=1}^{M}G_0^{[\alpha]}\left(1-\sum_{1\leqslant r\leqslant R-1}S_r^{[\alpha]}\right)\right].\tag{20}$$

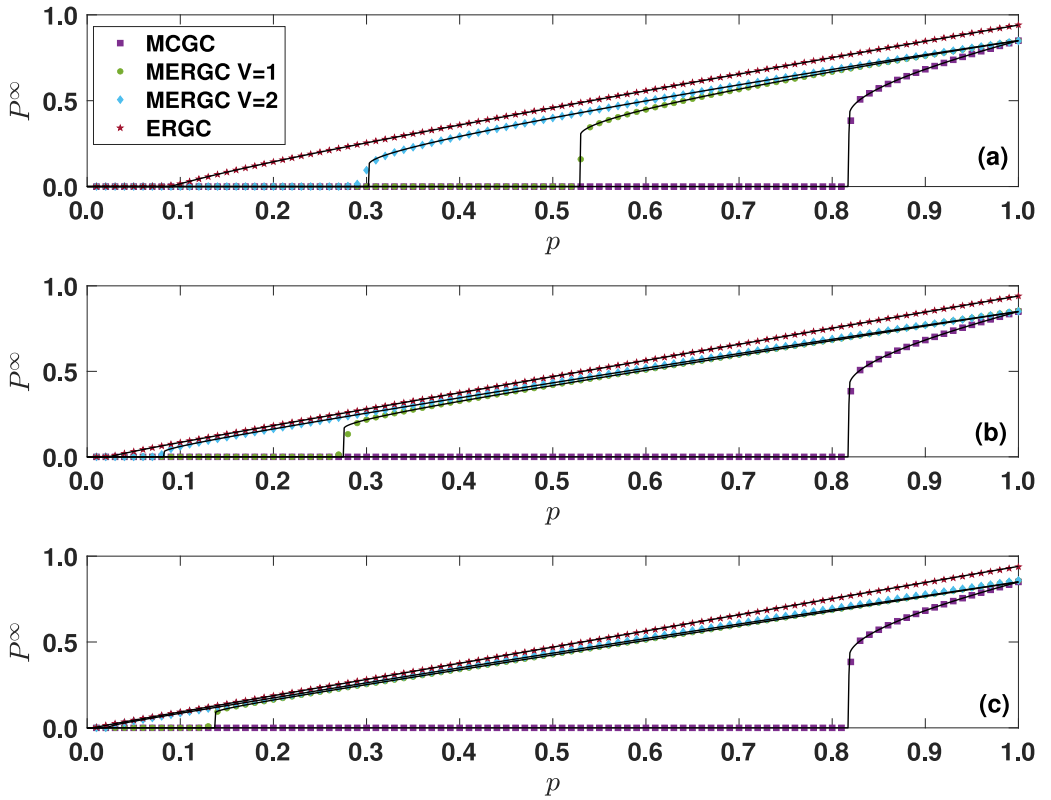

FIG. 4. Comparison between the order parameter P^∞ as a function of p for the MIP, the two versions of MERP (MERP $V = 1$ and MERP $V = 2$), and the single-layer ERP, for (a) $R = 2$, (b) $R = 3$, and (c) $R = 4$. The results of the Monte Carlo simulations (symbols) are in excellent agreement with our theoretical predictions (solid lines). The considered multiplex networks have $M = 2$ uncorrelated layers and $N = 10^5$ nodes. Each layer (or single network for ERP) is formed by a Poisson network with average degree $c = 3$. Data are averaged over 20 runs.

As it will be discussed in detail for a particular case in the next section, MERP may display one or more discontinuous hybrid transitions. The critical value $p = p^\star$ for these transitions can be in general found imposing that Eqs. (17) admits a nontrivial solution $\boldsymbol{Y} = \boldsymbol{Y}^\star = (\boldsymbol{S}^\star, \boldsymbol{W}^\star)$ with $\boldsymbol{S}^\star \neq \boldsymbol{0}$, and that the maximum eigenvalue $\Lambda_\star$ of the Jacobian of the function $\boldsymbol{F}$ with respect to $\boldsymbol{Y}$ evaluated at $\boldsymbol{Y} = \boldsymbol{Y}^\star$ is one, i.e., $p^\star$ is the solution of the equations

$$\boldsymbol{Y}^\star = \boldsymbol{F}\big(\boldsymbol{Y}^\star, p^\star\big), \quad \Lambda_\star(p^\star) = 1. \tag{21}$$

Note the difference with the criticality condition of ERP, and in general of systems exhibiting continuous phase transitions. While for a continuous transition the criticality condition is determined by the largest eigenvalue of the Jacobian evaluated at the trivial fixed point $\boldsymbol{Y}^0$, for discontinuous transitions the critical threshold is determined when the largest eigenvalue of the Jacobian evaluated in $\boldsymbol{Y}^\star$, the nontrivial solution of Eqs. (17), equals 1.

B. Phenomenology of the MERP for $R \in \{2, 3, 4\}$ on Poisson multiplex networks

In this section, we study the critical properties of MERP for $R \in \{2, 3, 4\}$ on multiplex networks composed of M layers independently drawn from the random Poisson networks ensemble[1] with average degree c (where c is the same for each layer). Specifically, here we focus on the relevant phenomenology predicted by our theoretical approach, and we test it by Monte Carlo simulations of the process on multiplex networks with $M = 2$ layers. We defer a deeper theoretical derivation of the phase diagram to the next subsection.

As a general remark, we expect that a nonzero MERGC for version $V = 2$ will be easier to achieve than for version $V = 1$, because version $V = 2$ does not require interdependence of the untrusted facilitator nodes. Thus, the MERGC of version $V = 2$ is always expected to be larger or at most equal to the MERGC of version $V = 2$ for the same choice of the parameters. As we have already remarked the MERGC for $R > 1$ are also expected to be larger than or equal to the MCGC, which is equivalent to the MERGC for $R = 1$. In particular both versions of the MERGC coincide with the MCGC for $p = 1$, independently of the value of p. At the same time, if the layers are independently drawn random networks with the same degree distribution, the MERGC of both versions of the model will always be smaller than the ERGC of a single layer. For an illustration of the relation between the MERGC, the ERGC, and the MCGC see Fig. 4.

[1]Poisson networks are Erdős-Rényi random graphs with link probability $p = c/(N-1)$ in the limit $N \gg 1$, which define random graphs with Poisson degree distribution $P(k) = e^{-c}c^k/k!$.

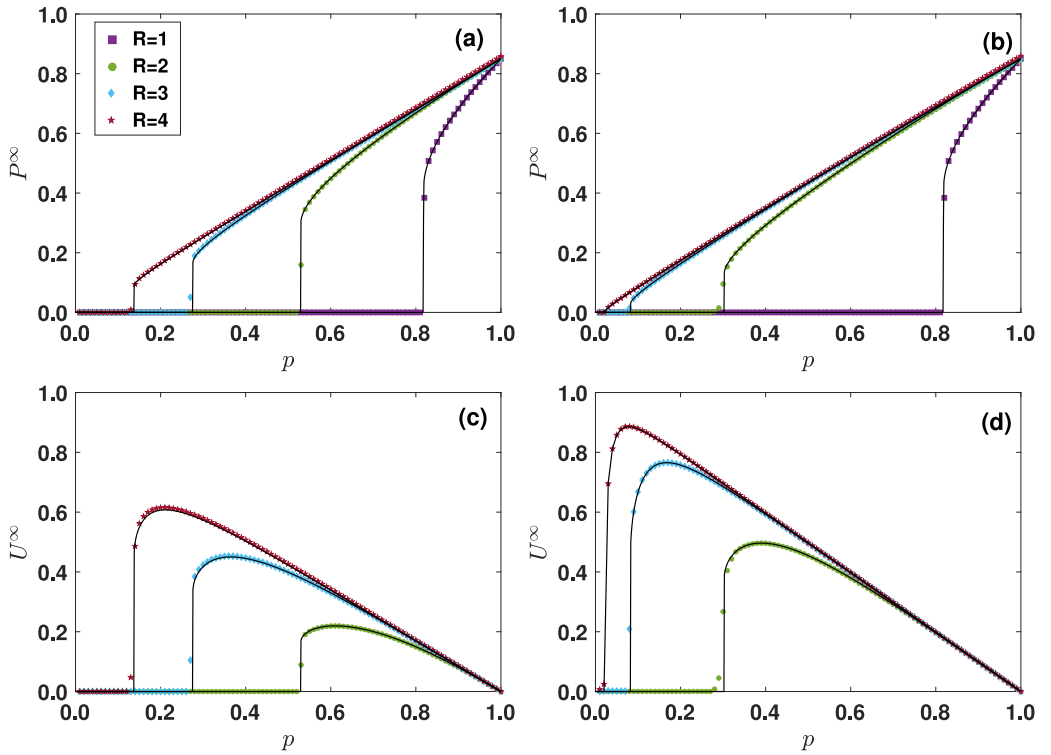

FIG. 5. The order parameters P^∞ and U^∞ of MERP for version $V = 1$ [panels (a) and (c)] and version $V = 2$ [panels (b) and (d)] are plotted as a function of p for different values of $R \in \{1, 2, 3, 4\}$ (note that for $R = 1$ the result reduces to the standard mutually connected giant component-MCGC). The discontinuous (hybrid) transition observed in Monte Carlo simulations (symbols) is in excellent agreement with our theoretical predictions (solid lines). The considered multiplex networks have $M = 2$ uncorrelated layers and $N = 10^5$ nodes. Each layer is formed by a Poisson network with average degree $c = 3$. Data are averaged over 20 runs.

Let us indicate with $\bar{c}$ the minimum average degree required to observe a MCGC (or equivalently a MERGC with $R = 1$). Its value for $M = 2$ is $\bar{c} = 2.45541\ldots$. For version $V = 1$ of MERP $\bar{c}$ also indicates the minimum average degree required to observe a MERGC independently of the value of $R \geqslant 1$. In version $V = 1$ and, as long as $c > \bar{c}$, also in version $V = 2$ we observe a single hybrid discontinuous phase transition at the emergence of the MERGC (see Fig. 5).

For version $V = 2$ of MERP we observe a highly nontrivial behavior for average degree c in an interval of values $c^\star < c < \bar{c}$ where $c^\star$ decreases if R increases (see Fig. 6). For small p there is no giant component. Increasing p, at some point $p^\star_-$ the usual discontinuous transition for percolation on multiplex networks takes place, after which the size of the MERGC increases. However, the behavior is nonmonotonic: P^∞ reaches a maximum and for a value $p^\star_+ < 1$ the MERGC discontinuously disappears. As we discuss in the next section, both transitions at $p^\star_-$ and $p^\star_+$ are hybrid. Thus, our results demontrate the existence of a reentrant discontinuous transition for version $V = 2$ of MERP.

The physical interpretation of this phenomenology is as follows. In the limit of p close to 1, almost all nodes are trusted, untrusted nodes do not really play a role, and version $V = 2$ is practically equivalent to version $V = 1$, which does not admit a MERGC for $c < \bar{c}$. Hence $P^\infty = 0$ for $p \to 1$ for both versions and for any R. When p is reduced from 1 the fraction of untrusted nodes increases; their presence facilitates the formation of the MERGC for $V = 2$, since they can play the role of untrusted facilitator nodes, each in its layer, with no interdependencies. This leads to the discontinuous formation, at $p^\star_+$, of the MERGC. Clearly, when p is reduced further this positive effect starts to be offset by the decrease of trusted nodes, leading to the breakdown of the MERGC for $p^\star_-$. Hence there is a finite interval $[p^\star_-, p^\star_+]$ in which the presence of many but not too many noninterdependent untrusted nodes allows the existence of a MERGC.

C. Phase diagram of MERP for $R = 2$ on Poisson multiplex networks

After recalling the main results [14,42,47] valid for the MIP (i.e., the MERP with $R = 1$), in this subsection we derive the phase diagram of MERP for $R = 2$ on Poisson multiplex networks with M layers having the same average degree c. A similar argument holds for MERP with $R > 2$ on the same multiplex networks.

The fact that layers have identical statistical properties significantly simplifies the equations for MERP. Indeed, we can safely assume that $S^\alpha_r = S_r$ and $W^\alpha_r = W_r$ do not depend on α. Moreover, since the layers of the multiplex network have a Poisson degree distribution, $G_0(x) = G_1(x)$, hence $P^\infty = S_1$.

1. Case $R = 1$ (MCGC)

Let us briefly recall the main results [14,42,47] valid for $R = 1$, where the MERGC reduces to the mutually connected giant component MCGC of the multiplex network. For $R = 1$

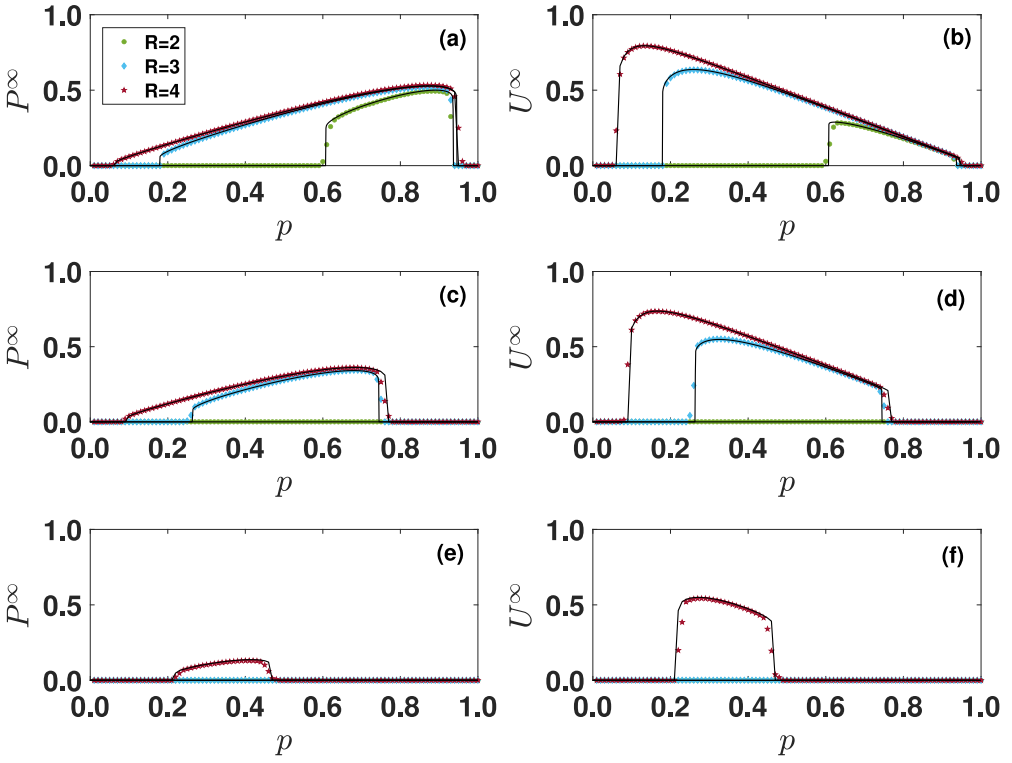

FIG. 6. The order parameters P^∞, U^∞ for MERP, version $V = 2$ and $R \in \{2, 3, 4\}$ are shown to display a reentrant phase transition for multiplex networks that do not display a MCGC. The considered multiplex networks have $M = 2$ uncorrelated layers and $N = 10^5$ nodes. Each layer is formed by a Poisson network with average degree $c = 2.4$ [panels (a) and (b)], $c = 2.2$ [panels (c) and (d)], and $c = 1.9$ [panels (e) and (f)]. As the average degree c decreases, the MERGC disappears for MERP of increasing values of R. Data are averaged over 20 runs. The results of the Monte Carlo simulations (symbols) are in excellent agreement with our theoretical predictions (solid lines).

we have that $S_1 = P^\infty$ obeys

$$S_1 = F_1^{(0)}(S_1) \equiv p(1 - e^{-cS_1})^M. \tag{22}$$

Thus, for each value of p, c and M the fraction S_1 of nodes in the MCGC can be found by considering the zeros of the function

$$\tilde{H}^{(0)}(S_1) \equiv S_1 - F_1^{(0)}(S_1) = S_1 - p(1 - e^{-cS_1})^M. \tag{23}$$

Note that for each choice of the parameters only the largest stable solution is physical. Interestingly, in this case we can further reduce the parameters by introducing the auxiliary variables $x = S_1/p$, $z = cp$, and studying the zeros of the function

$$H^{(0)}(x, z) = x - (1 - e^{zx})^M. \tag{24}$$

For any fixed value of M we can thus study the zeros of $H^{(0)}(x)$ as a function of the product $z = cp$. In this way it is found that for every $M > 1$ the MCGC emerges at a discontinuous (hybrid) transition where $x = x^\star$ and $z = z^\star$ are determined by the equations

$$H^{(0)}(x^\star, z^\star) = 0, \qquad \left.\frac{\partial H^{(0)}}{\partial x}\right|_{x^\star, z^\star} = 0. \tag{25}$$

The value of $z^\star = \bar{c}$ determining the minimal average degree $\bar{c}$ for observing the MCGC, increases as a function of M. For $M = 2$ we obtain in this way $\bar{c} = 2.45541\ldots$.

2. *Case* $R = 2$

We now move to the interesting MERP case with $R = 2$. In the simplified setting of multiplex Poisson networks, the equations for version V read

$$\begin{aligned} S_1 &= F_1^{(V)}(S_1, S_2) = p\big(1 - e^{-c(S_1+S_2)}\big)^M, \\ S_2 &= F_2^{(V)}(S_1) = (1-p)\big(1 - e^{-cS_1}\big)^{M\delta_{V,1}+\delta_{V,2}}, \end{aligned} \tag{26}$$

where again we use the Kronecker delta to implement the two versions $V = 1$ and $V = 2$ all at once. As a first remark, note that for $p = 1$ these equations coincide with the equations for MCGC for values of V; see Fig. 4. Indeed for $p = 1$ all nodes are trusted, hence there is no difference between the MERGC and the MCGC, as already noted above. For $p < 1$, instead the MERGC strongly depends on the version considered and is different from the MCGC.

Since for both versions $F_2^{(V)}$ is a function of S_1 only, in order to investigate the critical properties of the two models we can simply study the solutions of the equation

$$S_1 = F_1^{(V)}\big(S_1, F_2^{(V)}(S_1)\big), \tag{27}$$

or equivalently the zeros of the function

$$H^{(V)}(S_1; c, p) = S_1 - F_1^{(V)}\big(S_1, F_2^{(V)}(S_1)\big), \tag{28}$$

for $V = 1$ and $V = 2$. Note, however, that this function depends independently from c and p, thus we do not have in general the same simplification that we discussed for MCGC.

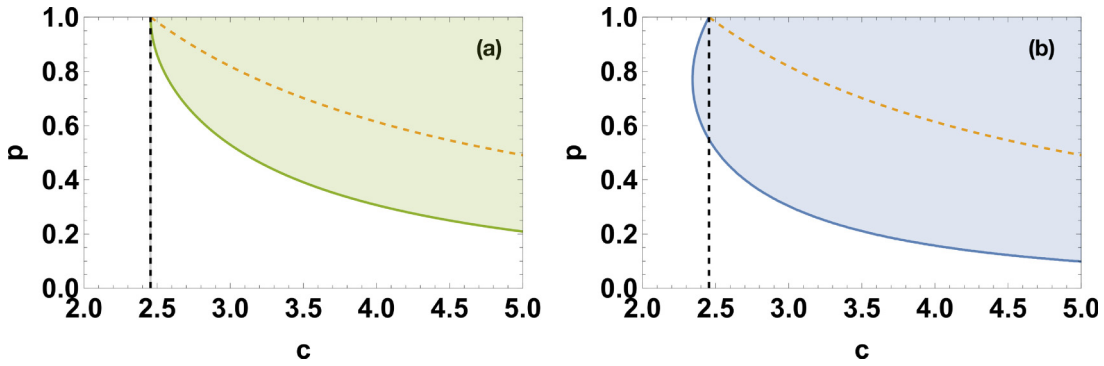

FIG. 7. Phase diagram of $R = 2$ MERP on Poisson multiplex networks with $M = 2$ layers and average degree c. Panels (a) and (b) display the phase diagram for version $V = 1$ and $V = 2$ of MERP, respectively. The filled regions are the region corresponding to a nonzero MERGC. In both panels, the orange dashed line correspond to the critical line for $R = 1$ MERP, i.e., the critical line for the emergence of the MCGC; the vertical dashed line $c = \bar{c} = 2.455$ indicates the critical average degree for the emergence of the MCGC. We observe that for version $V = 2$ there are values $c^\star < c < \bar{c}$ in which the reentrant phase transition is predicted, providing solid understanding of the Monte Carlo results.

Studying Eq. (28) one finds that for any $M > 1$ and for any c the percolation threshold $p = p^\star$ at which the MERGC emerges at a discontinuous (hybrid) transition where the order parameter $P^\infty(p_\star) = S_1^\star$ can be determined by solving the equations

$$H^{(V)}(S_1^\star; p_\star, c) = 0, \quad \left.\frac{\partial H^{(V)}}{\partial S_1}\right|_{S_1^\star, p_\star} = 0. \tag{29}$$

To show that these transitions are hybrid we can study the solution of $H^{(V)}(S_1; p, c) = 0$ for $\delta p = p - p_\star \ll 1$ and $\delta S_1 = S_1 - S_1^\star \ll 1$. Thus, expanding $H^{(V)}(S_1; p, c)$ and using Eq. (29), we obtain

$$0 = H^{(V)}(S_1; p, c) \simeq \left.\frac{\partial H^{(V)}}{\partial p}\right|_{S_1^\star, p_\star} \delta p + \frac{1}{2} \left.\frac{\partial^2 H^{(V)}}{\partial S_1^2}\right|_{S_1^\star, p^\star} (\delta S_1)^2. \tag{30}$$

It follows that if

$$\left.\frac{\partial^2 H^{(V)}}{\partial S_1^2}\right|_{S_1^\star, p^\star} > 0, \quad \left.\frac{\partial H^{(V)}}{\partial p}\right|_{S_1^\star, p_\star} < 0, \tag{31}$$

the transition is hybrid with a square root singularity, i.e.,

$$\delta S_1 \propto (\delta p)^\beta \tag{32}$$

with $\beta = 1/2$.

For version 1 of MERP, Eqs. (29) have a single nontrivial solution as long as $c > c^\star$ where $c^\star = \bar{c}$, i.e., we have a nonvanishing MERGC only for average degrees such that also the MCGC is nonzero. For version 2 of MERP instead, in a certain range of c values, we observe two discontinuous hybrid transitions, both satisfying Eq. (29), one determining the onset of the MERGC and one determining its dismantling; see Fig. 6. This occurs for average degrees $c \in [c^\star, \bar{c}]$ where $c^\star$ can be found imposing the equations

$$H^{(2)}(S_1^\star; p^\star, c^\star) = 0, \quad \left.\frac{\partial H^{(2)}}{\partial S_1}\right|_{S_1^\star, p^\star, c^\star} = 0,$$
$$\left.\frac{\partial H^{(2)}}{\partial p}\right|_{S_1^\star, p^\star, c^\star} = 0. \tag{33}$$

This phenomenology can be observed in Fig. 7, where we plot the phase diagrams of version $V = 1$ and version $V = 2$ of MERP for $M = 2$, clearly demonstrating the reentrant phase transition for $V = 2$. We can derive the behavior of $p - p^\star$ versus $c - c^\star$ expanding the equations $H^{(2)}(S_1; p, c) = 0$ around $p = p^\star$ and $c = c^\star$ with $S_1 = S_1^\star(p, c)$. In this way, using Eq. (33) we obtain

$$0 = \frac{1}{2} \left.\frac{\partial^2 H^{(2)}}{\partial p^2}\right|_{S_1^\star, p^\star, c^\star} (\delta p)^2 + \left.\frac{\partial H^{(2)}}{\partial c}\right|_{S_1^\star, p^\star, c^\star} \delta c, \tag{34}$$

where $\delta p = p - p^\star$ and $\delta c = c - c^\star$. Thus, if the signs of $\partial^2 H^{(2)}/\partial p^2|_{S_1^\star, p^\star, c^\star}$ and $\partial H^{(2)}/\partial c|_{S_1^\star, p^\star, c^\star}$ are opposite, we obtain the scaling

$$|p - p^\star| \propto (c - c^\star)^{1/2}. \tag{35}$$

Finally, in Fig. 8 we show the different behavior of $c^\star$ as a function of the number of layers M for the version $V = 1$ as

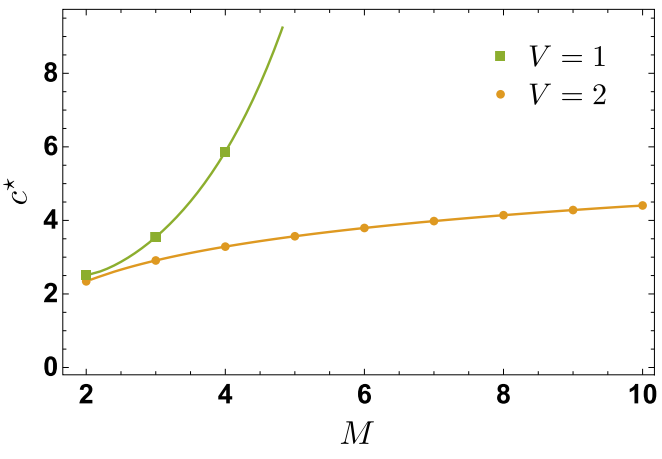

FIG. 8. The critical average degree $c^\star$ of a Poisson multiplex network which allows the emergence of a $R = 2$ MERGC is plotted versus the number of layers M for the version $V = 1$ (green, square symbols) and for version $V = 2$ (orange, circle symbols) of MERP. We observe that $c^\star$ corresponding to version $V = 1$ coincides with the critical average degree $\bar{c}$ for observing the MCGC on the same multiplex network.

well as for the version $V = 2$. We observe that as the number of layer increases, the range of values of the average degree where the reentrant phase is observed increases significantly.

V. CONCLUSIONS

In conclusion, this work establishes a general theoretical framework for extended-range percolation in simple and multiplex networks, providing a relevant new class of exactly solvable percolation problems. Extended-range percolation on simple networks defines a percolation process in which communication between trusted nodes is ensured even if they are not directly connected. Specifically communication between two trusted nodes is allowed if they are connected by paths involving exclusively trusted and untrusted facilitator nodes. These facilitator nodes, although untrusted, can still ensure communication between trusted nodes if they lie on at least a path of distance at most R between two trusted nodes. This percolation process reduces for $R = 1$ to standard percolation and to standard interdependent percolation on single and multiplex networks, respectively. Our theory builds on a message-passing approach providing the exact solution for the size of the extended-range giant component (ERGC) for arbitrary finite R, as long as the network is locally treelike. Our message-passing approach allows us to formulate a general theory for ERP on simple uncorrelated random networks. This general theory coincides with previous results obtained with a different approach for $R \leqslant 6$ [15]. The resulting ERP transition is continuous, and characterized by a percolation threshold that decreases as R increases, demonstrating the improved robustness of the network when this notion of connectivity is adopted. Furthermore, this general framework allows us to introduce and study the multiplex extended-range percolation (MERP). This novel process enforces interdependencies between trusted nodes and can be defined in two variants ($V = 1$ and $V = 2$) depending on how interdependencies for untrusted nodes are considered. We provide the exact solution for the size of the Multiplex Extended-Range Giant Component (MERGC) for arbitrary R. We show that the MERGC emerges with a discontinuous hybrid transition at a percolation threshold $p = p^\star$, which decreases as R increase. Thus, the phase diagram of MERP reflects a trade-off between the increased fragility as a consequence of the multiplex network interdependencies, and the increased robustness implied by the extended-range mechanism. In particular we observe that version $V = 2$, in which interdependencies are present only for trusted nodes, displays a rich phase diagram with the presence of a reentrant phase for some multiplex network topologies.

This work opens new perspectives to study the role of extended-range percolation in a variety of settings. At a fundamental level, it would be interesting to explore the effect of design principles associating the state of trusted nodes to specific nodes of the network, for example, preferably to nodes of low or high degree. Additionally it would be very interesting to build on these results to formulate more specific models which could be applied in a realistic setting of quantum communications or of multilayer models of epidemic spreading. More generally it would also be relevant to explore applications of this framework to hypergraphs and higher-order networks, where several generalized percolation problems have been recently proposed [48–51].

ACKNOWLEDGMENT

The authors thank Gábor Timár for useful discussions in the early stages of this project.

APPENDIX A: MESSAGE PASSING THEORY FOR EXTENDED-RANGE PERCOLATION

The aim of this Appendix is to present a general message-passing (MP) theory for extended-range percolation on single networks. The MP formalism allows to express the equations for extended-range percolation for arbitrary R on single and multiplex networks, as shown in the main body of the paper.

In order to formulate a message-passing algorithm for extended-range percolation determining the giant component of the model, we follow the general approach [14] for percolation problems. This consist by first deriving the message-passing equations when we know for each node i if it is trusted ($x_i = 1$) or untrusted ($x_i = 0$), i.e., we know the exact configuration of trusted and untrusted nodes. Subsequently one can consider the scenario in which the exact configuration of trusted nodes is not known, and the only available information is that probability p that a random node is trusted.

Let us now assume that we know the exact configuration of the trusted nodes, i.e., we have access to the variables $\{x_i\}$. We consider two sets of messages $\sigma^r_{i\to j}$ and $\omega^r_{i\to j}$, with $r \in \{1, 2, \ldots, R\}$, associated to the directed links $i \to j$.

We consider two set of messages $\sigma^r_{i\to j} \in \{0, 1\}$ and $\omega^r_{i\to j} \in \{0, 1\}$, with $r \in \{1, 2, \ldots, R\}$, associated to the directed links $i \to j$. Each message is a binary variable that can be 0 or 1, according to the following rules. The messages $\sigma^{r+1}_{i\to j}$ are 1, i.e., $\sigma^{r+1}_{i\to j} = 1$ when the node i is connected to at least a trusted node in the ERGC by a path of length $r < R$ when the link (i, j) is removed. In all other scenarios we have $\sigma^{r+1}_{i\to j} = 0$.

The messages $\omega^{r+1}_{i\to j} = 1$ if not connected to any trusted node in the ERGC but connected to at least a trusted node not in the ERGC by a path of length $r < R$ when the link (i, j) is removed. In all other scenarios we have $\omega^{r+1}_{i\to j} = 0$.

Note that by construction at most one of the messages from i to j is different from zero; but it may also happen that all messages from i to j are zero.

The equations for $\sigma^1_{i\to j}$ and $\omega^1_{i,j}$ are similar to the messages in standard percolation [14,30,37]:

$$\sigma^1_{i\to j} = x_i \left[1 - \prod_{\ell\in\partial i\setminus j} \left(1 - \sum_{1\leqslant r\leqslant R} \sigma^r_{\ell\to i} \right) \right],$$
$$\omega^1_{i\to j} = x_i \left[\prod_{\ell\in\partial i\setminus j} \left(1 - \sum_{1\leqslant r\leqslant R} \sigma^r_{\ell\to i} \right) \right], \tag{A1}$$

where here and in the following ∂i denotes the neighborhood of node i.

All other messages $\sigma^r_{i\to j}$ and $\omega^r_{i\to j}$ with $r > 1$ are zero for links departing from trusted nodes.

Concerning messages departing from untrusted nodes, to write recursive equations for $\sigma^{r+1}_{i\to j}$ with $r > 0$, it is important to realize that two mutually exclusive scenarios may occur. We call these two scenarios the *standard scenario* and the *bridge node scenario*. In the *standard scenario* node i is connected to the ERGC through a node at distance r from the closest trusted node and node i is at distance larger than $r+1$ from any other trusted trusted node. In the *bridge node scenario* node i is connected to the ERGC through nodes that are a distance $r_1 > r$ from trusted nodes in the ERGC. In this case the value of r is determined by the presence of *bridge nodes*. A bridge node is a trusted node that is not connected to the ERGC if node i is removed, but it is connected to the ERGC if the node i is not removed. Thus, assuming that the bridge node is at distance r for node i we must impose $r + r_1 \leqslant R$ as node i need to act as a untrusted facilitator node (for a schematic representation of the message-passing algorithm and the role of bridge node see Fig. 9). These considerations can thus be used to determine the conditions under which the message $\sigma^{r+1}_{i\to j} = 1$ is sent from node i to node j. Specifically we have that $\sigma^{r+1}_{i\to j} = 1$ if node i is untrusted and if either scenario (1) or scenario (2) occurs (note that the two scenarios are mutually exclusive).

(1) *Scenario bridge nodes:*

(i) Node i receives at least one message $\sigma^{r_1}_{\ell\to i} = 1$ with $r_1 > r$, and no messages $\sigma^{r_2}_{\ell\to i} = 1$ with $r_2 < r_1$.

(ii) Node i receives at least one message $\omega^{r}_{\ell\to i} = 1$ and no messages $\omega^{r_3}_{\ell\to i} = 1$ with $r_3 < r$;

(iii) Additionally we require $r + r_1 \leqslant R$ or $r_1 \leqslant R - r$. (This is to ensure that the bridge node is a *facilitator*, i.e., connected to the ERGC, or equivalently that node i is in a active path between trusted nodes.) Requiring the existence of at least a given r_1 with $r < r_1 \leqslant R - r$ we need to impose $R - r > r$ or equivalently $R - 2r > 0$ for allowing scenario (1) to hold.

(2) *Standard scenario:*

(a) Node i receives at least one message $\sigma^{r}_{\ell\to i} = 1$ with $r < R$ and it does not receive any message $\sigma^{r_1}_{\ell\to i} = 1$ with $r_1 < r$

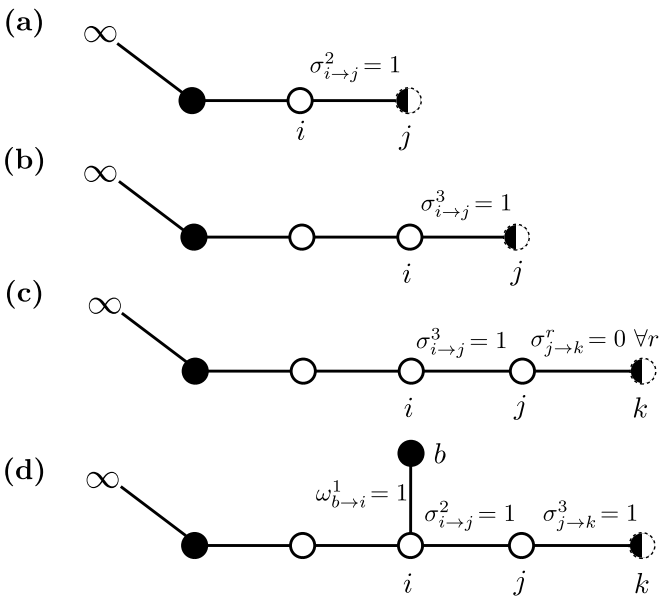

FIG. 9. Schematic representation of the message-passing algorithm for extended-range percolation with $R = 3$, and a visualization of the role of bridge nodes. Trusted nodes are represented by filled circles, untrusted nodes by empty circles, and the dashed nodes can either be trusted or untrusted. Panels (a)–(c) describe the message-passing algorithm in the *standard scenario*. Node j in panel (a) is always part of the ERGC, while in (b) node j belongs to the ERGC only if it is trusted. Node k in panel (c) is not connected to the ERGC as it does not receive any positive message $\sigma^r_{j\to k} = 0$ for $r \in \{1, 2, 3\}$. Panel (d) describes the *bridge node scenario*. The presence of node b, sending the message $\omega^1_{b\to i} = 1$, allows node k—if trusted—to be part of the ERGC.

(b) Node i does not receive any message $\omega^{r_2}_{\ell\to i} = 1$ that has $r_2 \leqslant \bar{r} = \min(r-1, R-r)$. Indeed, we need to exclude the messages $\omega^{r_2}_{\ell\to i} = 1$ with $r_2 < r$ and $r_2 \leqslant R - r$ that could act as bridge nodes and change the r of the message as in the bridge node scenario.

This leads to the following equations:

$$\begin{aligned}\sigma^{r+1}_{i\to j} = (1-x_i)\Bigg\{&\Bigg[\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q\leqslant r-1}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant \bar{r}}\omega^q_{\ell\to i}\Bigg)-\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q\leqslant r}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant \bar{r}}\omega^q_{\ell\to i}\Bigg)\Bigg]\\ &+\theta(R-2r)\Bigg[\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q\leqslant r}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\omega^q_{\ell\to i}\Bigg)+\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q\leqslant R-r}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\omega^q_{\ell\to i}\Bigg)\\ &-\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q<r}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\omega^q_{\ell\to i}\Bigg)-\prod_{\ell\in\partial i\setminus j}\Bigg(1-\sum_{1\leqslant q\leqslant R-r}\sigma^q_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\omega^q_{\ell\to i}\Bigg)\Bigg]\Bigg\}.\end{aligned} \tag{A2}$$

Note that here and in the following we use $\theta(x)$ to indicate the Heaviside function with $\theta(x) = 1$ if $x > 0$ and $\theta(x) = 0$ otherwise. The first row describes scenario (2), the rest of the equations describes scenario (1), and the expression is a direct consequence of the inclusion-exclusion principle.

In particular the expression describing scenario (1) can be deduced by considering the expression valid as long as $\theta(R-2r)=1$:

$$\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r-1}\omega^{q}_{\ell\to i}\right)-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r}\omega^{q}_{\ell\to i}\right)\right]\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r}\sigma^{q}_{\ell\to i}\right)-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-r}\sigma^{q}_{\ell\to i}\right)\right].$$

Here we assume that $\theta(R-2r)=1$ implementing in part condition (iii), while the two multiplicative terms indicate the condition (ii) and the conditions (i) and (iii), respectively. Since any product of $\omega^{r}_{\ell\to i}\sigma^{r_1}_{\ell\to i}=0$ for all r and r_1 (due to the fact that the messages are nonzero in mutually exclusive situations) we recover that the above expression is equivalent to the inclusion-exclusion principle expression:

$$\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant r}\sigma^{q}_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\omega^{q}_{\ell\to i}\right)+\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-r}\sigma^{q}_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\omega^{q}_{\ell\to i}\right)$$

$$-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q<r}\sigma^{q}_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\omega^{q}_{\ell\to i}\right)-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant q\leqslant R-r}\sigma^{q}_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\omega^{q}_{\ell\to i}\right).$$

This is exactly the expression that multiplies the factor $\theta(R-2r)$ in the message-passing equation for $\sigma^{r+1}_{i\to j}$ and that implements the bridge node scenario.

Having derived the equation for the message $\sigma^{r+1}_{i\to j}$ we now derive the equation for the message $\omega^{r+1}_{i\to j}$. The untrusted facilitator node i sends a message $\omega^{r+1}_{i\to j}=1$ with $r>0$ if

(i) It does not receive any positive message $\sigma^{r_1}_{\ell\to i}$ with $1\leqslant r_1<R$

(ii) It receives at least one positive message $\omega^{r}_{\ell\to i}=1$ and no messages $\omega^{r_1}_{\ell\to i}=1$ with $r_1<r$.

This leads then to the message-passing equations:

$$\omega^{r+1}_{i\to j}=(1-x_i)\left[\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant r\leqslant R-1}\sigma^{r}_{\ell\to i}-\sum_{1\leqslant q\leqslant r-1}\hat{\omega}^{q}_{\ell\to i}\right)-\prod_{\ell\in\partial i\setminus j}\left(1-\sum_{1\leqslant r\leqslant R-1}\sigma^{r}_{\ell\to i}-\sum_{1\leqslant q\leqslant r}\hat{\omega}^{q}_{\ell\to i}\right)\right]. \tag{A3}$$

The fraction P^{∞} of nodes that are trusted and are in the ERGC is then given by

$$P^{\infty}=\frac{1}{N}\sum_{i=1}^{N}x_i\left[1-\prod_{\ell\in\partial i}\left(1-\sum_{1\leqslant r\leqslant R}\sigma^{r}_{\ell\to i}\right)\right]. \tag{A4}$$

while the fraction U^{∞} of nodes that are untrusted and are in the ERGC is given by

$$U^{\infty}=\frac{1}{N}\sum_{i=1}^{N}(1-x_i)\left[1-\prod_{\ell\in\partial i}\left(1-\sum_{1\leqslant r\leqslant R-1}\sigma^{r}_{\ell\to i}\right)\right]. \tag{A5}$$

The message-passing equations (A2) and (A3) fully determine the order parameter P^{∞} given by Eq. (A4) when we know the configuration of trusted and untrusted nodes, i.e., the configuration $\{x_i\}$. However, in a number of cases the exact configuration $\{x_i\}$ determining which nodes are trusted and which are untrusted is not known. In this scenario we can assume that the state of a node x_i is drawn independently at random with a probability p that the node is trusted, thus we assume that the probability $\tilde{P}(\{x_i\})$ of a configuration is given by

$$\tilde{P}(\{x_i\})=\prod_{i=1}^{N}p^{x_i}(1-p)^{1-x_i}. \tag{A6}$$

In this case we need to modify the message-passing equations by averaging over the probability $\tilde{P}(\{x_i\})$. This alternative message-passing algorithm is formulated in terms of a new set of messages: the messages $\hat{\sigma}^{r}_{i\to j}\in[0,1]$ indicating the probability that a node i is connected to the ERGC by nodes different from j and at distance r from active trusted nodes and the messages $\hat{\omega}^{r}_{i\to j}\in[0,1]$ indicating the probability that a node i is not connected to the ERGC by nodes different from j and is at distance r from other trusted nodes. We have that $\hat{\sigma}^{r}_{i\to j}$ is the average of $\sigma^{r}_{i\to j}$ and $\hat{\omega}^{r}_{i\to j}$ is the average of $\omega^{r}_{i\to j}$ over the distribution $\tilde{P}(\{\mathbf{x}\})$ of trusted and untrusted nodes.

The messages $\hat{\sigma}^r_{i\to j}$ for $1 \leqslant r \leqslant R$ obey

$$\hat{\sigma}^1_{i\to j} = p\left[1 - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant r\leqslant R}\hat{\sigma}^r_{\ell\to i}\right)\right]$$

$$\hat{\sigma}^{r+1}_{i\to j} = (1-p)\Bigg\{\left[\prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant r-1}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant \bar{r}}\hat{\omega}^q_{\ell\to i}\right) - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant \bar{r}}\hat{\omega}^q_{\ell\to i}\right)\right]$$
$$+\theta(R-2r)\Bigg[\prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right) + \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R-r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right)$$
$$- \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q<r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right) - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R-r}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right)\Bigg]\Bigg\}. \tag{A7}$$

The messages $\hat{\omega}^r_{i\to j}$ with $1 \leqslant r \leqslant \lceil R/2\rceil - 1$ obey

$$\hat{\omega}^1_{i\to j} = p\left[\prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R}\hat{\sigma}^r_{\ell\to i}\right)\right],$$

$$\hat{\omega}^{r+1}_{i\to j} = (1-p)\left[\prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R-1}\hat{\sigma}^q_{\ell\to i} - \sum_{1\leqslant q\leqslant r-1}\hat{\omega}^q_{\ell\to i}\right) - \prod_{\ell\in\partial i\setminus j}\left(1 - \sum_{1\leqslant q\leqslant R-1}\hat{\sigma}^r_{\ell\to i} - \sum_{1\leqslant q\leqslant r}\hat{\omega}^q_{\ell\to i}\right)\right]. \tag{A8}$$

Note that in total the messages are $R + \lceil R/2\rceil - 1$. The order parameter P^∞ expressing the fraction of nodes that are trusted and are in the ERGC is given by

$$P^\infty = \frac{p}{N}\sum_{i=1}^{N}\left[1 - \prod_{\ell\in\partial i}\left(1 - \sum_{1\leqslant r\leqslant R}\hat{\sigma}^r_{\ell\to i}\right)\right], \tag{A9}$$

while the fraction of nodes U^∞ that are untrusted and are in the ERGC is given by

$$U^\infty = \frac{(1-p)}{N}\sum_{i=1}^{N}\left[1 - \prod_{\ell\in\partial i}\left(1 - \sum_{1\leqslant r\leqslant R-1}\hat{\sigma}^r_{\ell\to i}\right)\right]. \tag{A10}$$

These equations are the starting point to formulate the equation determining the size of the ERGC on random networks with given degree distribution. To this end we consider networks $\mathcal{G} = (V, E)$ drawn from the distribution

$$\mathcal{P}(\mathcal{G}) = \prod_{i=1}^{N}\prod_{j=i}^{N} p_{ij}^{a_{ij}}(1-p_{ij})^{1-a_{ij}}, \tag{A11}$$

where **a** indicates the adjacency matrix of the network and p_{ij} indicates the probability of link between nodes i and j. The probability p_{ij} is expressed in terms of the degrees k_i and k_j associated, respectively, to the two nodes i and j, as

$$p_{ij} = \frac{k_i k_j}{\langle k\rangle N}. \tag{A12}$$

Here $P(k)$ indicates the degree distribution, i.e., fraction of nodes of degree k. In order to derive the general equations determining the size of the ERGC, we average the message-passing equations over the distribution $\mathcal{P}(\mathcal{G})$. In this case we indicate with S_r the average of $\hat{\sigma}^r_{i\to j}$ and W_r is the average of $\hat{\omega}^r_{i\to j}$ over the probability $\mathcal{P}(\mathcal{G})$. In this way we derive Eq. (5). Moreover we indicate with P^∞ (and with U^∞) the probability that node is trusted (untrusted) and belongs to the ERGC obtaining Eqs. (7) and (8).

APPENDIX B: EQUATIONS FOR ERP FOR FINITE R

In this Appendix we provide the explicit equations (5) for extended-range percolation with $R \in \{1, 2, 3, 4\}$ on a simple network.

1. The $R = 2$ equations

For $R = 2$ the self-consistent equations involve two average messages, S_1 and S_2, and read

$$S_1 = p[1 - G_1(1 - S_1 - S_2)],$$
$$S_2 = (1-p)[1 - G_1(1 - S_1)]. \tag{B1}$$

The order parameter P^∞ is given by

$$P^\infty = p[1 - G_0(1 - S_1 - S_2)], \tag{B2}$$

while U^∞ is given by

$$U^\infty = (1-p)[1 - G_0(1 - S_1)]. \tag{B3}$$

2. The $R = 3$ equations

For $R = 3$ the self-consistent equations involve four average messages, S_1, S_2, S_3, and W_1 reflecting that for $R > 2$ the effect to bridge nodes needs to be taken into account. These

equations read

$$\begin{aligned} S_1 &= p[1 - G_1(1 - S_1 - S_2 - S_3)], \\ S_2 &= (1-p)[1 + G_1(1 - S_1 - S_2 - W_1) \\ &\quad - G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2)], \\ S_3 &= (1-p)[G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - W_1)], \\ W_1 &= pG_1(1 - S_1 - S_2 - S_3). \end{aligned} \tag{B4}$$

The order parameter P^∞ is given by

$$P^\infty = p[1 - G_0(1 - S_1 - S_2 - S_3)], \tag{B5}$$

while U^∞ if given by

$$U^\infty = (1-p)[1 - G_0(1 - S_1 - S_2)]. \tag{B6}$$

3. The $R = 4$ equations

For $R = 4$ the self-consistent equations involve five average messages, S_1, S_2, S_3, S_4, and W_1 and read

$$\begin{aligned} S_1 &= p[1 - G_1(1 - S_1 - S_2 - S_3 - S_4)], \\ S_2 &= (1-p)[1 + G_1(1 - S_1 - S_2 - S_3 - W_1) \\ &\quad - G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - S_3)], \\ S_3 &= (1-p)[G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - W_1)], \\ S_4 &= (1-p)[G_1(1 - S_1 - S_2 - W_1) \\ &\quad - G_1(1 - S_1 - S_2 - S_3 - W_1)], \\ W_1 &= pG_1(1 - S_1 - S_2 - S_3 - S_4). \end{aligned} \tag{B7}$$

The order parameter P^∞ is given by

$$P^\infty = p[1 - G_0(1 - S_1 - S_2 - S_3 - S_4)], \tag{B8}$$

while U^∞ is given by

$$U^\infty = (1-p)[1 - G_0(1 - S_1 - S_2 - S_3)]. \tag{B9}$$

APPENDIX C: EQUIVALENCE OF EQS. (5) WITH THE EQUATIONS DERIVED IN REF. [15] FOR $R \leqslant 4$

In this Appendix we demonstrate the equivalence of Eqs. (5) for extended-range percolation with $R \leqslant 4$ discussed in Appendix B with the equations previously derived in Ref. [15] using a different formalism. Note that in Ref. [15] the equations were derived explicitly up to $R = 6$. All these equations are equivalent to the equations derived in this work. However, the expressions are rather combinatorially involved, and we prefer for the sake of simplicity to prove the equivalence between only with $R \leqslant 4$.

According to the approach of [15], the equations for ERP on random networks with $R = 4$ are

$$\begin{aligned} u_1 &= G_1(pu_1 + (1-p)u_2), \\ u_2 &= G_1(pu_1 + (1-p)u_2), \\ u_3 &= G_1((1-p)u_4) - G_1((1-p)u_3) + u_2, \\ u_4 &= G_1(1-p) - G_1((1-p)u_3) + u_2, \\ P^\infty &= p[1 - G_0(pu_1 + (1-p)u_2)], \end{aligned} \tag{C1}$$

where $u_1, \ldots, u_4$ are probabilities of not reaching the ERGC following a randomly chosen link conditioned to different configurations; e.g., for u_1 the chosen link ends in a trusted node, for u_2 the chosen link emanates from a trusted node and ends in an untrusted node, while u_3 and u_4 take care of more complex combinatoric configurations including bridge nodes. For the interested reader, we defer to [15] for the details of such a formalism. For the purpose of this Appendix, it is sufficient to know that the $\{u_r\}$ are probabilities and that they have a different physical interpretation from the $\{S_r, W_r\}$. The equations for $R = 3$ are recovered by simply setting $u_4 = 1$. Analogously, setting $u_3 = 1$ we recover the equations for $R = 2$, and setting $u_2 = 1$ finally gives the equation for standard site percolation ($R = 1$). Note that the order parameter U^∞ had not been introduced in [15].

1. The $R = 2$ equations

Let us now prove the equivalence between the Eqs. (B1) and (B2) and Eqs. (C1) with $u_3 = u_4 = 0$. To define a mapping between the two sets of variables S_r and u_r, we proceed as follows. First, comparing the two different equations for P^∞ written in the two sets of variables, we get the condition

$$1 - S_1 - S_2 = pu_1 + (1-p)u_2.$$

Then, from the equation for u_1 and a comparison with the equation for S_1, we get

$$S_1 = p(1 - u_1).$$

The solution of these equations is

$$S_1 = p(1-u_1), \quad S_2 = (1-p)(1-u_2), \tag{C2}$$

and shows the equivalence of the two formalisms.

2. The $R = 3$ equations

Let us now prove the equivalence between the Eqs. (B4) and (B5) and Eqs. (C1) with $u_4 = 0$. Reasoning as we did for $R = 2$ in the previous subsection, from the two equations for P^∞ we get the condition

$$1 - S_1 - S_2 - S_3 = pu_1 + (1-p)u_2. \tag{C3}$$

Using then the equations for u_1 and S_1, we get again $S_1 = p(1-u_1)$. The equation for W_1 gives instead $W_1 = pu_1$. From (C3) we get

$$1 - p - S_2 - S_3 = (1-p)u_2.$$

Using then the two equations for S_2 and S_3, after some simplifications this equation can be rewritten as

$$u_2 = G_1(1 - S_1 - S_2).$$

Comparing this equation with the equation for u_2 in (C1) we finally get

$$G_1(pu_1 + 1 - p - S_2) = G_1(pu_1 + (1-p)u_3),$$

from which $S_2 = (1-p)(1-u_3)$. The equivalence between the two formalisms for $R = 3$ is then proved via the mapping

$$\begin{aligned} S_1 &= p(1-u_1), \quad S_2 = (1-p)(1-u_3), \\ S_3 &= (1-p)(u_3 - u_2), \quad W_1 = pu_1. \end{aligned} \tag{C4}$$

3. The $R = 4$ equations

Let us now prove the equivalence between Eqs. (B7)–(B5) and Eqs. (C1). In perfect analogy to what we did in the two previous subsections, we can determine a mapping between the $\{S_r, W_r\}$ and the $\{u_r\}$ variables to show the equivalence of the two sets of equations. The first step is to compare the equations for P^∞, to get the condition

$$1 - S_1 - S_2 - S_3 - S_4 = pu_1 + (1-p)u_2, \tag{C5}$$

which, together with the equations for S_1 and W_1, determines again $S_1 = p(1-u_1) = p - W_1$. Equation (C5) then gives

$$1 - p - S_2 - S_3 - S_4 = (1-p)u_2,$$

which can be rewritten after some simplifications, using the equations for S_2, S_3, S_4, as

$$u_2 = G_1(pu_1 + 1 - p - S_2 - S_3).$$

By comparison with the equation for u_2 we get

$$1 - p - S_2 - S_3 = (1-p)u_3,$$

which can be in turn rewritten after some simplifications, using again the equations for S_2, S_3 and the expressions derived above, as

$$u_3 = [G_1(1 - p - S_2) - G_1((1-p)u_3) + u_2].$$

By comparison with the equation for u_3 we finally get $S_2 = (1-p)(1-u_4)$. Hence we proved the equivalence of the two formalisms for $R = 4$ via the mapping

$$\begin{aligned} &S_1 = p(1-u_1), \quad S_2 = (1-p)(1-u_4), \\ &S_3 = (1-p)(u_3-u_2), \quad S_4 = (1-p)(u_4-u_3), \\ &W_1 = pu_1. \end{aligned} \tag{C6}$$

APPENDIX D: EQUATIONS FOR MERP FOR FINITE $R \leqslant 4$

In this Appendix we write explicitly the equations for multiplex extended-range percolation (16), (18), (19), and (20) for $R \leqslant 4$ on multiplex uncorrelated random graphs. We assume that the degrees of the same node across different layers are uncorrelated. Under such hypothesis, we have that $S_r^\alpha = S_r, \quad W_r^\alpha = W_r$, thus the equations greatly simplify.

1. The $R = 1$ equations

The equations in this case involve only the message S_1, and they reduce for both versions—since untrusted nodes are not considered at all—to the standard MCGC equations for MIP, [14]. In this case, the order parameter U^∞ is identically zero.

2. The $R = 2$ equations

For $R = 2$ the self-consistent equations involve two average messages, S_1 and S_2, and read

$$\begin{aligned} S_1 &= p[1 - G_1(1 - S_1 - S_2)][1 - G_0(1 - S_1 - S_2)]^{M-1}, \\ S_2 &= (1-p)[1 - G_1(1 - S_1)] \\ &\quad \times \{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1)]^{M-1}\}. \end{aligned} \tag{D1}$$

The order parameter P^∞ is given by

$$P^\infty = p[1 - G_0(1 - S_1 - S_2)]^M, \tag{D2}$$

while U^∞ is given by

$$\begin{aligned} U^\infty &= (1-p)[1 - G_0(1 - S_1)] \\ &\quad \times \{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1)]^{M-1}\}. \end{aligned} \tag{D3}$$

3. The $R = 3$ equations

For $R = 3$ the self-consistent equations involve four average messages, S_1, S_2, S_3, and W_1 reflecting that for $R > 2$ the effect to bridge nodes needs to be taken into account. These equations read

$$\begin{aligned} S_1 &= p[1 - G_1(1 - S_1 - S_2 - S_3)][1 - G_0(1 - S_1 - S_2 - S_3)]^{M-1}, \\ S_2 &= (1-p)[1 + G_1(1 - S_1 - S_2 - W_1) - G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2)]\{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1 - S_2)]^{M-1}\}, \\ S_3 &= (1-p)[G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - W_1)]\{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1 - S_2)]^{M-1}\}, \\ W_1 &= pG_1(1 - S_1 - S_2 - S_3)[1 - G_0(1 - S_1 - S_2 - S_3)]^{M-1}. \end{aligned} \tag{D4}$$

The order parameter P^∞ is given by

$$P^\infty = p[1 - G_0(1 - S_1 - S_2 - S_3)]^M, \tag{D5}$$

while U^∞ is given by

$$U^\infty = (1-p)[1 - G_0(1 - S_1 - S_2)]\{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1 - S_2)]^{M-1}\}. \tag{D6}$$

4. The $R = 4$ equations

For $R = 4$ the self-consistent equations involve five average messages, S_1, S_2, S_3, S_4, and W_1 and read

$$\begin{aligned} S_1 &= p[1 - G_1(1 - S_1 - S_2 - S_3 - S_4)][1 - G_0(1 - S_1 - S_2 - S_3 - S_4)]^{M-1}, \\ S_2 &= (1-p)[1 + G_1(1 - S_1 - S_2 - S_3 - W_1) - G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - S_3)] \\ &\quad \times \{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1 - S_2 + S3)]^{M-1}\}, \\ S_3 &= (1-p)[G_1(1 - S_1 - W_1) - G_1(1 - S_1 - S_2 - W_1)]\{\delta_{V,2} + \delta_{V,1}[1 - G_0(1 - S_1 - S_2 + S3)]^{M-1}\}, \end{aligned}$$

$$S_4 = (1-p)[G_1(1-S_1-S_2-W_1) - G_1(1-S_1-S_2-S_3-W_1)]\{\delta_{V,2} + \delta_{V,1}[1-G_0(1-S_1-S_2+S3)]^{M-1}\},$$
$$W_1 = pG_1(1-S_1-S_2-S_3-S_4)[1-G_0(1-S_1-S_2-S_3-S_4)]^{M-1}. \quad \text{(D7)}$$

The order parameter P^∞ is given by

$$P^\infty = p[1-G_0(1-S_1-S_2-S_3-S_4)][1-G_0(1-S_1-S_2-S_3-S_4)]^{M-1}, \quad \text{(D8)}$$

while U^∞ is given by

$$U^\infty = (1-p)[1-G_0(1-S_1-S_2-S_3)]\{\delta_{V,2} + \delta_{V,1}[1-G_0(1-S_1-S_2+S_3)]^{M-1}\}. \quad \text{(D9)}$$

[1] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Critical phenomena in complex networks, Rev. Mod. Phys. **80**, 1275 (2008).

[2] M. Li, R.-R. Liu, L. Lü, M.-B. Hu, S. Xu, and Y.-C. Zhang, Percolation on complex networks: Theory and application, Phys. Rep. **907**, 1 (2021).

[3] D. Lee, B. Kahng, Y. Cho, K.-I. Goh, and D.-S. Lee, Recent advances of percolation theory in complex networks, J. Korean Phys. Soc. **73**, 152 (2018).

[4] X. Meng, X. Hu, Y. Tian, G. Dong, R. Lambiotte, J. Gao, and S. Havlin, Percolation theories for quantum networks, Entropy **25**, 1564 (2023).

[5] O. Artime, M. Grassia, M. De Domenico, J. P. Gleeson, H. A. Makse, G. Mangioni, M. Perc, and F. Radicchi, Robustness and resilience of complex networks, Nat. Rev. Phys. **6**, 114 (2024).

[6] J. Nokkala, J. Piilo, and G. Bianconi, Complex quantum networks: A topical review, J. Phys. A: Math. Theor. **57**, 233001 (2024).

[7] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[8] S. Perseguers, M. Lewenstein, A. Acín, and J. I. Cirac, Quantum random networks, Nat. Phys. **6**, 539 (2010).

[9] S. Perseguers, J. I. Cirac, A. Acín, M. Lewenstein, and J. Wehr, Entanglement distribution in pure-state quantum networks, Phys. Rev. A **77**, 022308 (2008).

[10] B. C. Coutinho, W. J. Munro, K. Nemoto, and Y. Omar, Robustness of noisy quantum networks, Commun. Phys. **5**, 105 (2022).

[11] S. Pirandola, End-to-end capacities of a quantum communication network, Commun. Phys. **2**, 51 (2019).

[12] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, Long-range big quantum-data transmission, Phys. Rev. Lett. **120**, 030503 (2018).

[13] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu *et al.*, Implementation of a 46-node quantum metropolitan area network, npj Quantum Inf. **7**, 134 (2021).

[14] G. Bianconi, *Multilayer Networks: Structure and Function* (Oxford University Press, Oxford, 2018).

[15] L. Cirigliano, C. Castellano, and G. Timár, Extended-range percolation in complex networks, Phys. Rev. E **108**, 044304 (2023).

[16] K. Malarz, Simple cubic random-site percolation thresholds for neighborhoods containing fourth-nearest neighbors, Phys. Rev. E **91**, 043301 (2015).

[17] K. Malarz, Site percolation thresholds on triangular lattice with complex neighborhoods, Chaos **30**, 123123 (2020).

[18] K. Malarz, Percolation thresholds on a triangular lattice for neighborhoods containing sites up to the fifth coordination zone, Phys. Rev. E **103**, 052107 (2021).

[19] Z. Xun and R. M. Ziff, Bond percolation on simple cubic lattices with extended neighborhoods, Phys. Rev. E **102**, 012102 (2020).

[20] Z. Xun, D. Hao, and R. M. Ziff, Site percolation on square and simple cubic lattices with extended neighborhoods and the their continuum limit, Phys. Rev. E **103**, 022126 (2021).

[21] P. Zhao, J. Yan, Z. Xun, D. Hao, and R. M. Ziff, Site and bond percolation on four-dimensional simple hypercubic lattices with extended neighborhoods, J. Stat. Mech. (2022) 033202.

[22] Z. Xun, D. Hao, and R. M. Ziff, Site and bond percolation thresholds on regular lattices with compact extended-range neighborhoods in two and three dimensions, Phys. Rev. E **105**, 024105 (2022).

[23] X. Meng, J. Gao, and S. Havlin, Concurrence percolation in quantum networks, Phys. Rev. Lett. **126**, 170501 (2021).

[24] M. Kim and F. Radicchi, Shortest-path percolation on random networks, Phys. Rev. Lett. **133**, 047402 (2024).

[25] B. Min, E.-K. Park, S.-H. Gwak, and K.-I. Goh, No-exclaves percolation on random networks, Chaos Solitons Fractals **184**, 115004 (2024).

[26] S. M. Krause, M. M. Danziger, and V. Zlatić, Hidden connectivity in networks with vulnerable classes of nodes, Phys. Rev. X **6**, 041022 (2016).

[27] S. M. Krause, M. M. Danziger, and V. Zlatić, Color-avoiding percolation, Phys. Rev. E **96**, 022313 (2017).

[28] C. Castellano and R. Pastor-Satorras, Cumulative merging percolation and the epidemic transition of the susceptible-infected-susceptible model in networks, Phys. Rev. X **10**, 011070 (2020).

[29] L. Cirigliano, G. Cimini, R. Pastor-Satorras, and C. Castellano, Cumulative merging percolation: A long-range percolation process in networks, Phys. Rev. E **105**, 054310 (2022).

[30] M. Newman, Message passing methods on complex networks, Proc. R. Soc. A **479**, 20220774 (2023).

[31] M. Mézard and A. Montanari, *Information, Physics, and Computation* (Oxford University Press, Oxford, 2009).

[32] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, Controllability of complex networks, Nature (London) **473**, 167 (2011).

[33] B. Karrer, M. E. J. Newman, and L. Zdeborová, Percolation on sparse networks, Phys. Rev. Lett. **113**, 208702 (2014).

[34] G. Menichetti, L. Dall'Asta, and G. Bianconi, Network controllability is determined by the density of low in-degree and out-degree nodes, Phys. Rev. Lett. **113**, 078701 (2014).
[35] F. Radicchi and G. Bianconi, Redundant interdependencies boost the robustness of multiplex networks, Phys. Rev. X **7**, 011013 (2017).
[36] L. Zdeborová and F. Krząkała, Phase transitions in the coloring of random graphs, Phys. Rev. E **76**, 031131 (2007).
[37] A. K. Hartmann and M. Weigt, *Phase Transitions in Combinatorial Optimization Problems: Basics, Algorithms and Statistical Mechanics* (John Wiley & Sons, New York, 2006).
[38] G. T. Cantwell, A. Kirkley, and F. Radicchi, Heterogeneous message passing for heterogeneous networks, Phys. Rev. E **108**, 034310 (2023).
[39] A. Kirkley, G. T. Cantwell, and M. E. J. Newman, Belief propagation for networks with loops, Sci. Adv. **7**, eabf1211 (2021).
[40] S. Boccaletti, G. Bianconi, R. Criado, C. del Genio, J. Gómez-Gardeñes, M. Romance, I. Sendiña-Nadal, Z. Wang, and M. Zanin, The structure and dynamics of multilayer networks, Phys. Rep. **544**, 1 (2014).
[41] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, Multilayer networks, J. Complex Netw. **2**, 203 (2014).
[42] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature (London) **464**, 1025 (2010).
[43] G. J. Baxter, S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Avalanche collapse of interdependent networks, Phys. Rev. Lett. **109**, 248701 (2012).
[44] D. Cellai, S. N. Dorogovtsev, and G. Bianconi, Message passing theory for percolation models on multiplex networks with link overlap, Phys. Rev. E **94**, 032301 (2016).
[45] B. Min, S. Lee, K.-M. Lee, and K.-I. Goh, Link overlap, viability, and mutual percolation in multiplex networks, Chaos Solitons Fractals **72**, 49 (2015).
[46] G. Bianconi, Statistical mechanics of multiplex networks: Entropy and overlap, Phys. Rev. E **87**, 062806 (2013).
[47] S.-W. Son, G. Bizhani, C. Christensen, P. Grassberger, and M. Paczuski, Percolation theory on interdependent networks based on epidemic spreading, Europhys. Lett. **97**, 16006 (2012).
[48] G. Bianconi and S. N. Dorogovtsev, Theory of percolation on hypergraphs, Phys. Rev. E **109**, 014306 (2024).
[49] J.-H. Kim and K.-I. Goh, Higher-order components dictate higher-order contagion dynamics in hypergraphs, Phys. Rev. Lett. **132**, 087401 (2024).
[50] H. Sun and G. Bianconi, Higher-order percolation processes on multiplex hypergraphs, Phys. Rev. E **104**, 034306 (2021).
[51] H. Sun, F. Radicchi, J. Kurths, and G. Bianconi, The dynamic nature of percolation on networks with triadic interactions, Nat. Commun. **14**, 1308 (2023).