Critical field-exponents for secure message-passing in modular networks

To cite this article: Louis M Shekhtman et al 2018 New J. Phys. 20 053001

View the article online for updates and enhancements.

Related content
- Roughening transition and universality of single step growth models in (2+1)-dimensions
  H Dashti-Naserabadi, A A Saberi and S Rouhani
- Cluster-weighted percolation-a novel approach to the Potts model
  T A Larsson
- Critical behaviour of a forest fire model with immune trees
  E V Albano
Critical field-exponents for secure message-passing in modular networks

Louis M Shekhtman 1,2,3, Michael M Danziger 4, Ivan Bonamassa 1, Sergey V. Buldyrev 5, Guido Caldarelli 1,4,5,6, Vinko Zlatić 7 and Shlomo Havlin 8

1 Center for Complex Network Research and Department of Physics, Northeastern University, Boston, MA02115, United States of America
2 Department of Physics, Yeshiva University, New York, United States of America
3 IMT AltStudi Lucca, Piazza San Francesco 19, I-55100 Lucca, Italy
4 CNR-ISC Dipartimento di Fisica, University of Rome Sapienza, Piazzale Aldo Moro 2, I-00185 Rome, Italy
5 Linkalab, Complex Systems Computational Laboratory, I-09129 Cagliari, Italy
6 European Centre for Living Technology (ECLT) Ca’ Foscari San Marco I-2940-30124 Venezia, Italy
7 Theoretical Physics Division, Institute ‘Ruder Boskovic’, Zagreb, Croatia
8 Author to whom any correspondence should be addressed.

E-mail: lsheks@gmail.com

Keywords: complex networks, secure message-passing, network resilience, percolation

Supplementary material for this article is available online

Abstract

We study secure message-passing in the presence of multiple adversaries in modular networks. We assume a dominant fraction of nodes in each module have the same vulnerability, i.e., the same entity spying on them. We find both analytically and via simulations that the links between the modules (interlinks) have effects analogous to a magnetic field in a spin-system in that for any amount of interlinks the system no longer undergoes a phase transition. We then define the exponents δ, which relates the order parameter (the size of the giant secure component) at the critical point to the field strength (average number of interlinks per node), and γ, which describes the susceptibility near criticality. These are found to be δ = 2 and γ = 1 (with the scaling of the order parameter near the critical point given by β = 1). When two or more vulnerabilities are equally present in a module we find δ = 1 and γ = 0 (with β ≥ 2). Apart from defining a previously unidentified universality class, these exponents show that increasing connections between modules is more beneficial for security than increasing connections within modules. We also measure the correlation critical exponent ν, and the upper critical dimension d c, finding that νd c = 3 as for ordinary percolation, suggesting that for secure message-passing d c = 6. These results provide an interesting analogy between secure message-passing in modular networks and the physics of magnetic spin-systems.

As our world becomes more interconnected, the need to pass messages securely has gained increasing importance [1]. The recently developed applications of statistical physics of networks to anonymous browsing networks [2] and secure message-passing [3] promises an interesting new direction of security based on network topology. One application is internet routers, which form a physical communication network with nodes belonging to specific countries that can eavesdrop on information passing through their routers [4]. If two nodes wish to communicate securely and are not directly connected, they could split their messages into separate parts and send each part along a different path such that no single adversary is present on every path. In this way, no adversary would be able to decode the full message. Most likely, many nodes will not be able to communicate in such a manner. For example, a node with only one link must inherently have all its information pass through that link. Whether information can be transferred through such a communication network securely and effectively is strongly dependent on the frequency and structural network properties of vulnerabilities e.g. nodes belonging to a malicious country in the aforementioned example. In this paper we define the giant secure component (GSC) as the fraction of nodes which are capable of communicating securely with one another using the above described method of multiple paths. We note that any node in the GSC can securely communicate
with any other node in the GSC. To find the GSC we generalize the framework of ‘color-avoiding percolation’ (CAP) \[3, 5\] to study a more realistic case of secure message-passing in a communication network with a given community structure and different classes of adversaries (vulnerabilities).

In CAP each node in the network is assigned a specific color. A path between two nodes is considered to avoid a particular color (i.e., is secure from that color) if no nodes of that color exist along the path (not counting its endpoints). We find the set of nodes that can avoid a particular color by removing all nodes of that color, determining the largest component of the remaining nodes, and then adding back those nodes of the removed color that have a direct link to the largest component (see the example in the supplementary material available online at stacks.iop.org/NJP/20/053001/mmedia). If between two given nodes there is for each color at least one path avoiding that color, the two nodes are considered securely connected. Equivalently, only nodes that can communicate such that no single color exists on every path between them are considered secure.

Here we consider CAP on networks with given community structure, a realistic case for many networks \[6–14\]. Continuing the above example of internet routers, in each country most of the routers presumably belong to that country with a smaller number of routers belonging to other countries \[3, 15, 16\]. To study the community structure we use the stochastic block model \[17, 18\], where each community is recognized as a ‘block’ in an adjacency matrix, and assign a certain color to dominate each module. This imposes correlations on the distribution of colors in the network, naturally modeled as a modular network.

For simplicity, we demonstrate our model and results on a network with two communities having an internal average degree \(k_I\) and an external average degree \(k_E\). We begin by assuming (for simplicity but without loss of generalization) that there are two colors with a single dominant color \(C_d = 1\) occupying a fraction \(q\) nodes of each module and the remaining fraction \(1 - q\) being of the other color (see figure 1(a))\(^{10}\). This same framework can be used to describe networks where the links are correlated by color (see SM). To identify the GSC, we find the standard giant component under the removal of nodes of a single color, and then add back nodes of the removed color which have a direct link to the largest component (reflecting the assumption that the endpoints of every path are secure) \[3\]. This is done for each color and then the intersection of all these components is the GSC.

\(^9\) In the supplementary material we consider the case of more than two communities.

\(^{10}\) In the supplementary material we discuss the more general case of different values of \(q\) in each module, which shows similar qualitative results.
To solve our model analytically, we adopt the generating function framework defining \( g_0(z) = \sum_k p_k z^k \) as the generating function of the variable \( k \) with \( p_k \) being the probability of a node having \( k \) links [19, 20]. For our model we have generating functions for the internal and external connections defined by \( g_{0i}(z) \) and \( g_{0e}(z) \) respectively. For the case of 2 colors, we must find: \( u_{1,0} \), the likelihood that a link fails to avoid the color dominant in its module; \( n_{0,1} \), the likelihood that the link fails to avoid the color dominant in the other module; and \( n_{1,1} \), the likelihood that the link does not avoid either of the two colors. We then assume that the sender and receiver nodes are secure, by taking \( g_{0i}(u_{i,j}) g_{0e}(n_{j,1}) \), which adds back nodes with a direct link to the giant component in both the internal and external modules. Naively one might think that to find the size of the GSC, \( S_c \), one could merely take \( 1 - g_{0i}(u_{i,0}) g_{0e}(u_{0,1}) = g_{0i}(u_{i,0}) g_{0e}(u_{0,1}) \) i.e., take the conjugate of the probability that a randomly chosen node fails to avoid both colors. However, this neglects the fact that some nodes fail to avoid either color. To deal with this overcounting we must add back \( g_{0i+1e}(u_{i,1}) \) in accordance with the inclusion–exclusion principle [21]. The \( k_I + k_E \) subscript in this case means that we are now counting over the total number of links of the given node, such that \( g_{0i+1e}(u_{i,1}) = \sum_{k_i = 1}^{k_I} p_{k_I} u_{i,1} \), where \( p_k \) is now the likelihood of the node having a total of \( k = k_I + k_E \) links, independent of whether they are external or internal. For an Erdős–Rényi degree distribution this would be \( g_{0i+1e}(u_{i,1}) = e^{-(k_I+k_E)(1-u_{i,1})} \). Using this, we obtain

\[
S_c = 1 - g_{0i}(u_{i,0}) g_{0i}(u_{0,1}) - g_{0i}(u_{i,0}) g_{0e}(u_{0,1}) + g_{0i+1e}(u_{i,1}).
\]  

To solve equation (1) we need to calculate the probabilities \( u_{i,j} \) which, for Erdős–Rényi topologies of internal and external connections, are obtained by solving self-consistently the system

\[
\begin{align*}
u_{1,0} &= q + (1 - q)e^{-k_I(1-u_{i,0}) - k_E(1-u_{i,0})} \\
u_{0,1} &= (1 - q) + qe^{-k_I(1-u_{0,1}) - k_E(1-u_{0,1})} \\
u_{1,1} &= qe^{-k_I(1-u_{i,1}) - k_E(1-u_{i,1})} + (1 - q)e^{-k_I(1-u_{i,1}) - k_E(1-u_{i,1})}.
\end{align*}
\]  

For more details on the derivation and solving of equations (1) and (2) see supplementary material. Results comparing the above theory to simulations are shown in figure 2.

We find from figure 2 that only in the case where \( k_E = 0 \) does the system undergo a phase transition at the critical point \( q_c = 1 - 1/k_I \) [5], while for any \( k_E > 0 \) there is always some fraction of nodes in the secure component. This is because even if one of the two modules disintegrates when the dominant color is removed from it, there always exists a finite fraction of its nodes which can communicate securely through external links to the other module. Thus \( k_E > 0 \) removes the transition by making the disconnected phase unreachable [22], just as an external magnetic field of magnitude \( H \) does with respect to the disordered phase in the Ising model [23]. In what follows we further support, both analytically and by extensive simulations, this intriguing analogy between spin models and secure message-passing on modular networks.

To this aim, we investigate the scaling relations of our model with \( S_c, q_c \), and \( k_E \) as the CAP analogues of total magnetization, temperature, and the external field respectively. Let us first stress that for the case \( C_d = 1 \), that is a single dominant color in each module, the scaling exponent \( \beta \) defined by \( S_c(q_c) \sim (q - q_c)^\beta \) was found to be
\[ S_c \sim k_F^{1/\delta}. \] (3)

For \( C_d = 1 \), we find from simulations that \( \delta = 2 \) (figure 3(a)), setting the critical properties of this model within the mean-field percolation universality class. On a practical side, these exponents suggest that, in the case of one dominant color, increasing external connectivity between the modules is more beneficial near the critical point than \( 1 = \beta > 1/\delta = \frac{1}{2} \).

Based on the above results, we introduce hereafter the CAP-analogue of the magnetic susceptibility, which we define by means of the scaling relation

\[ \left( \frac{\partial S_c}{\partial k_E} \right)_{k_E=0} \sim |q - q_c|^\gamma. \] (4)

Using equations (1) and (2), we find (figure 3(b)) \( \gamma = 1 \) for \( C_d = 1 \) which, together with the other exponents obtained (\( \delta = 2 \) and \( \beta = 1 \)), is indeed consistent with Widom’s identity \( \delta - 1 = \gamma/\beta \) [24, 25].

The numerical results above can also be found analytically by expanding for \( k_1 \) near its critical value, \( k_1 = \frac{1}{1 - q} \). By defining \( x_{1,0} \equiv 1 - u_{1,0} \) and \( x_{0,1} = 1 - u_{0,1} \) and expanding equation (2) to leading orders in \( x_{1,0} \) and \( k_F \), we obtain

\[ x_{1,0} = q_c - q + \sqrt{(q_c - q)^2 + \frac{2k_F x_{0,1}}{k_I^2}}. \] (5)

It follows that \( \delta = 2 \), as \( x_{1,0} \) scales with the square root of \( k_F \), and \( \gamma = 1 \) as can be found by taking the derivative of equation (5) with respect to \( k_E \).

Having discussed the case of a single dominant color, we now study the case of multiple colors \( (C_d > 1) \) sharing dominance in a single community as depicted in figure 1(b). Each of these dominant colors will occupy a fraction \( q/C_d \) of the module. Following logic similar to that used for \( C_d = 1 \), the GSC in this case can be found by

\[ S_c = \sum_{i=0}^{C_d} \sum_{j=0}^{C_d} (-1)^{i+j} \binom{C_d}{i} \binom{C_d}{j} e^{-k_I(1-u_{ij})-k_F(1-u_{ij})} \] (6)

where the probabilities \( u_{ij} \) satisfy the system of self-consistent equations

\[ u_{ij} = \frac{i}{C_d} e^{-k_I(1-u_{i-1,j})-k_F(1-u_{i-1,j})} + \frac{1}{C_d} e^{-k_I(1-u_{ij}-1)-k_F(1-u_{ij}-1)} \] (7)

with \( i \leq C_d, j \leq C_d \) and \( u_{0,0} = u_{-1,1} = u_{1,0} = 1 \). For \( k_E = 0 \) we recover the equations obtained by Krause et al in [3, 5].

In contrast with the results for \( C_d = 1 \), we find that for every \( C_d \geq 2 \) the critical scaling exponents are given by \( \gamma = 0 \) and \( \delta = 1 \) (figure 3) which, to the best of our knowledge, define a novel universality class. These results,
together with the exponent \( \beta = C_d \) obtained in [5], suggest that for more than one dominant color the system undergoes higher-order phase transitions. In general, for \( C_d = i \) we will have an \( (i + 1) \)-order transition, i.e. for \( C_d = 2 \) we have a third order transition, for \( C_d = 3 \) we have a fourth order transition, etc. To verify this claim, we evaluate the higher-order derivatives of \( S_i \) with respect to \( k_b \), the first of which is given by

\[
\frac{\partial^i S_i}{\partial k_b^i} \bigg|_{k_b=0} \sim |q - q_c|^{-G},
\]

where \( G \) satisfies the generalized scaling relation \( G = \beta (C_d \delta - 1) \) [26]. In particular, for \( C_d = 2 \) we expect an exponent \( G = 2 \), which we confirm with numerical results (see SM). For \( C_d \geq 3 \), equation (8) breaks down and we obtain \( G = 1 \). As far as we know, the present study represents the first time that this novel universality class with higher-order transitions is observed in percolation type systems with the higher-order scaling exponents defined and measured.

Finally, though our model does not have any spatial embedding, we can gain insights into the upper critical dimension of the CAP process, by invoking the scaling relations and the results above. In fact, we can indirectly evaluate the product \( v_d \), where \( v \) is the scaling exponent related to the singular part of the correlation length at criticality and \( d \) is the upper critical dimension [27] of the process. We do this by analyzing how the size of the GSC, \( \text{NS}(q_k) \), scales at criticality with the number of nodes \( N \) in the absence of external connections (i.e., \( k_b = 0 \)). Specifically, we know that the correlation length, \( \xi \), has power-law scaling \( \xi \sim |q - q_c|^{-\nu} \) near criticality, and that in particular it scales with the size of the system, i.e., \( \xi \sim N^{1/d} \) at the critical threshold [24, 25]. Combining these properties with the critical scaling of the GSC, yields \( \text{NS}(q_k) \sim N^{1-\beta v_d} \) for the GSC’s size. Recalling that \( \beta = C_b \) by measuring \( \text{NS}(q_k) \) for varying \( N \), we can find \( v_d \) from simulations. In figure 4 we carry out this simulation for different \( C_d \) and obtain in every case that \( \nu v_d = 3 \), most likely with \( \nu = \frac{1}{2} \) and \( d = 6 \) as for classical percolation on Erdős–Rényi networks.

This result can be equivalently understood as follows. The scaling of \( \text{NS}(q_k) \) is

\[
\text{NS}(q_k) = \frac{N}{N^{2/3}} \times \text{NS}_1(q_k) \times \text{NS}_2(q_k) \times \text{NS}_3(q_k),
\]

where \( \text{NS}_1(q_k), \text{NS}_2(q_k), \text{NS}_3(q_k) \) represent the scaling of the size of the component avoiding color 1, ..., \( C_d \) respectively. Each \( \text{NS}_i(q_k) \) scales like an Erdős–Rényi network [3] with \( \text{NS}(q_k) \) which scales as \( N^{1-\beta v_d} \). If we rearrange and substitute this into our expression above we obtain

\[
\text{NS}(q_k) \sim N^{1-\beta v_d} N^{2/3} \times N^{1/3} \times N^{1/3} \times \ldots \times N^{1/3} = N^{1-\beta v_d/3}.
\]

This can then be set equal to \( N^{1-\beta v_d/3} \), justifying this way the numerical result \( \nu v_d = 3 \).

This constant value of \( \nu v_d \), combined with the increasing value of \( \beta \) as the number of colors increases, leads to the apparently surprising behavior of figure 4 where the size of the largest cluster, \( \text{NS}(q_k) \), decreases with the system size \( N \) when \( C_d \geq 3 \). We explain this scaling by noting that we assume that nodes in the intersection of the largest component avoiding each color respectively are in the GSC (in the next paragraph we will analyze this assumption). The likelihood of being in the largest component avoiding any single color scales with \( N^{-1/3} \), such that when two colors must be avoided the scaling is \( N^{-1/3} \times N^{-1/3} \), and so on for additional colors. Once more
than three colors must be avoided, the decreasing likelihood of being in all of the colors overpowers the linear growth of the system size leading to the observed decrease in the overlap of the largest components for each color. Further, this suggest that at criticality the overlap of the largest components for each color has vanishing or negative fractal dimension for $C_d \geq 3$ [28]. These values of the fractal dimension are indeed surprising in the context of percolation on networks. For instance, in classical percolation on scale-free networks, $\beta$ increases as the degree distribution becomes broader [29, 30], but this increase is counteracted by the simultaneous increase of the upper critical dimension, thus the fractal dimension remains positive.

However, we must note that there is some subtlety in this calculation, especially for $C_d > 3$. Specifically, we return to the above assumption that the overlap of the largest component avoiding each color gives the GSC. In most cases this will indeed be true, however when this overlap is very small, then overlap between smaller components must be considered in both the simulations and the derivation of equation (9). Specifically in the case where the expected overlap of the largest component for each color is less than a single node, we know that the actual GSC must be at least a single node and thus the assumption does not hold. In any case, we can say that for all $C_d > 3$ the actual size of the GSC scales as $O(1)$, as opposed to the negative exponent suggested by equation (9). This also implies that the GSC has a vanishing but non-negative fractal dimension since it always includes at least one node.

Finally, our results suggest the breakdown of the scaling relation $\nu_L = 2\beta + \gamma$ [24, 25] for $C_d > 1$ since $\nu_L = 3$ for all $C_d > 1$ but $2\beta + \gamma = 2C_d$ (for $C_d > 1$) which increases with $C_d$. This scaling relation originated from the distribution of small clusters at criticality, $m(s)$, having finite-size scaling $m(s) \sim N^{-\tau}$ as long as $\tau < 3$ [24, 25]. Its failure here implies that for CAP with $C_d > 1$, the critical exponent $\tau \geq 3$. This can be understood based on previous results on bicomponent-percolation [31], which is less restrictive than CAP [3], where it was shown that there are in general (almost) no small bicomponents in the network, rather only a giant bicomponent can exist. A circumstance is then paved concerning the possibility that also for CAP there are in general almost no small secure components in modular structures.

In summary, our results map the study of secure message-passing between nodes in modular networks to the statistical physics underlying its collective behaviours.

Acknowledgments

We acknowledge the Israel–Italian collaborative project NECST, Israel Science Foundation, ONR, Japan Science Foundation, BSF–NSF, the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister’s Office, and DTRA (Grant no. HDTRA-1-10-1-0014) for financial support. GC acknowledges support from EU projects SoBigData nr. 654024 and CoeGSS nr. 676547. SVB acknowledges the B W Gamson Computational Science Center at Yeshiva College. VZ acknowledges support by the H2020 CSA Twinning Project No. 692194, RBI-T-WINNING, and Croatian centers of excellence QuantixLi and Center of Research Excellence for Data Science and Cooperative Systems. GC and VZ acknowledge support from A M Loguercio and that this publication has been made possible by support from the Italian Ministero degli Affari Esteri e della Cooperazione Internazionale.

ORCID iDs

Louis M Shekhtman  @  https://orcid.org/0000-0001-5273-8363
Michael M Danziger  @  https://orcid.org/0000-0002-2674-0109
Guido Caldarelli  @  https://orcid.org/0000-0001-9377-3616

References

[1] Katz J and Lindell Y 2014 Introduction to Modern Cryptography (Boca Raton, FL: CRC press)
[2] De Domenico M and Arenas A 2017 Modeling structure and resilience of the dark network Phys. Rev. E 95 022313
[3] Krause S M, Danziger M M and Zlatić V 2016 Hidden connectivity in networks with vulnerable classes of nodes Phys. Rev. X 6 041022
[4] Beimel A 2011 Secret-sharing schemes: a survey International Conference on Coding and Cryptology (Berlin: Springer) pp 11–46
[5] Krause S M, Danziger M M and Zlatić V 2017 Color-avoiding percolation Phys. Rev. E 96 022313
[6] Newman M E and Girvan M 2004 Finding and evaluating community structure in networks Phys. Rev. E 69 026113
