BAYESIAN NETWORK DETECTION USING ABSORBING MARKOV CHAINS

*Steven T. Smith, Edward K. Kao, Kenneth D. Senne, and Garrett Bernstein**

MIT Lincoln Laboratory; 244 Wood Street; Lexington MA USA 02420
{ stsmith, edward.kao, senne, garrett.bernstein }@ll.mit.edu

ABSTRACT

A Bayesian framework for network detection is developed based on random walks on graphs. Networks are detected using partial observations of their activity, and the Bayesian approach is proved to be optimum in the Neyman-Pearson sense, assuming random walk propagation on a given graph and diffusion model with absorbing states. The equivalence of the random walk and harmonic solutions to the Bayesian formulation is proven. A general diffusion model is introduced that utilizes spatio-temporal relationships between vertices, and is used for a specific space-time formulation that leads to significant performance improvements.

1. INTRODUCTION

A new Bayesian approach to network detection [4, 6, 8, 10–13, 19–21] is developed and analyzed. The novel approach involves propagating cued threats from one or more observations on an underlying graph, an a priori threat diffusion model, and a new threat propagation model based on random walks on the graph, using Markov chains with absorbing states. The random walk framework provides a connection with many other well-known graph analytic methods that may also be posed in this context [1, 2, 10, 14]. The resulting network detection algorithm is proved to be optimum in the Neyman-Pearson sense of maximizing the probability of detection at a fixed false alarm probability.

2. BAYESIAN NETWORK DETECTION

Network detection is the problem of identifying a specific subgraph within a given graph $G = (V, E)$ [3, 4, 6, 8, 10–13, 21]. Assume that within G, a foreground or "threat" network V^Θ exists defined by an (unknown) $\{0, 1\}$-valued discrete random function $\Theta \in \mathscr{V}(G)$, the vertex space of functions $f\colon V \to \{0, 1\}$. A vertex $v \in V$ is in the foreground if $\Theta_v = 1$, otherwise v is in the background, i.e. $V^\Theta = \{\, v : \Theta_v = 1\}$.

A *network detector* ϕ on G is a $\{0, 1\}$-valued function $\phi \in \mathscr{V}(G)$. The correlation between a network detector ϕ and the actual threat network defined by the function Θ determines the detection performance of ϕ, measured using the detector's probability of detection (PD) and probability of false alarm (PFA). The network detection problem for a graph G of order N results in 2^N-ary multiple hypothesis test over the vertex space $\mathscr{V}(G)$, and, when detection optimality is considered, an optimal test involves partitioning the measurement space into 2^N regions yielding a maximum PD. This NP-hard combinatoric problem is clearly computationally and analytically intractable; however, the general 2^N-ary multiple hypothesis test may be greatly simplified by applying the random walk model, which via Eq. (1) reduces the 2^N-ary multiple hypothesis test to N independent binary hypothesis tests.

The Bayesian model developed here depends upon threat observation and propagation over both space and time, and the underlying probabilistic models that govern inference from observation to threat, then propagation of threat throughout the graph. General observation models are provided next, then applied with threat propagation models to specific contexts. An *observation on the graph* is a vector $\mathbf{z}\colon \{\, v_{b_1}, \ldots, v_{b_C}\,\} \subset V \to M \subset \mathbb{R}^C$ from C vertices to a *measurement space* $M \subset \mathbb{R}^C$. Bayes's rule for determining how likely a vertex is to be a foreground member or not depends on the model linking observations to threat. The conditional probability density $f(\mathbf{z}(v) \mid \Theta_v)$ is called the *observation model* of vertex $v \in V$.

This section is devoted to the development of Bayesian methods of using measurements on a graph to determine the probability of threat on a graph, then showing that these methods are optimum in the Neyman-Pearson sense of maximizing the probability of detection at a given false alarm rate. The motivating problem is to detect the foreground graph $G^\Theta = G[V^\Theta]$ in the graph $G = (V, E)$ with an unknown foreground $\Theta \in \mathscr{V}(G)$ and known observation vector $\mathbf{z}(v_1, \ldots, v_k)$.

2.1. Spatial Threat Propagation

We wish to compute the probability of threat $\theta_v = P(\Theta_v \mid \mathbf{z})$ at all vertices in a graph G given an observation $\mathbf{z}(v_{b_1}, \ldots, v_{b_C})$. There is an a priori probability ψ_v at each vertex representing threat diffusion at $v \in V$, the probability that threat propagates through that vertex to a neighbor. The *threat diffusion model* of a graph G is the a priori $\{0, 1\}$-valued event Ψ_v that threat Θ_v propagates through v with probability ψ_v.

Threat propagation on the graph from the observed vertices to all other vertices is defined as an average over all random walks between the observations to the rest of the graph. Assume that $G = (V, E)$ is strongly connected, and let $\theta_{v_{b_1}}, \ldots, \theta_{v_{b_C}}$ be the threat probabilities at observed vertices $v_{b_1}, \ldots, v_{b_C}$. For

*This work is sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

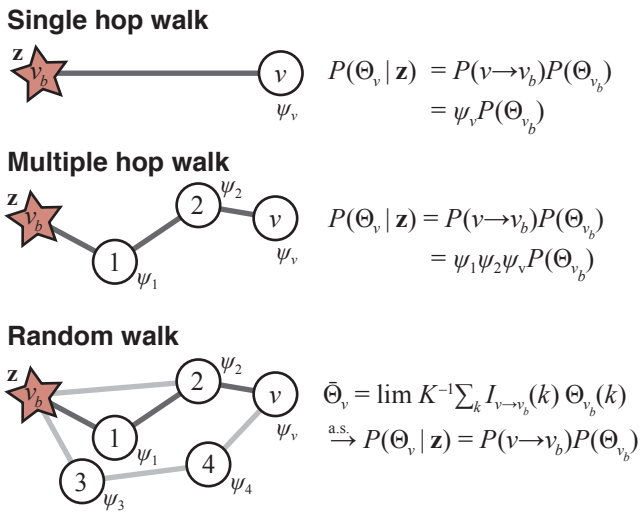

Fig. 1. Illustration of the random walk representation for threat propagation for the case of a single observation. The upper illustration shows the simplest, trivial case with a single hop from the observation to the vertex. The middle illustration shows the next simplest case with multiple hops. The lower illustration shows an example of the general case, comprised of the simpler multiple hop case.

a random $\text{walk}_{v \to v_{b_c}}$ on G from v to observed vertex v_{b_c} with transition matrix $\mathbf{T}$ and sequence $(v_{w_1}{=}v, \ldots, v_{w_L}{=}v_{b_c})$, if events $\Psi_{w_l} \equiv 1$ for all vertices w_l along the walk, then the *threat propagation from v_{b_c} to v along* $\text{walk}_{v \to v_{b_c}}$ is defined to be the probability $\theta_{v_{b_c}}$. *Threat propagation* to vertex v is defined as the expectation of threat propagation to v along all random walks emanating from v and terminating at an observed vertex.

An equivalent definition of threat propagation assigns the random variable

$$\bar{\Theta}_v = \lim_{K \to \infty} \frac{1}{K} \sum_k I_{\text{walk}^{(k)}_{v \to v_{b_{c(k)}}}} \Theta^{(k)}_{v_{b_{c(k)}}} \tag{1}$$

via independent random walks that terminate at $v_{b_{c(k)}}$ with indicator function $I_{\text{walk}^{(k)}_{v \to v_{b_{c(k)}}}} = \prod_{l=1}^{L} \Psi^{(l)}_{v_{w_l}}$, multiplied by independent draws $\Theta^{(k)}_{v_{b_{c(k)}}}$ of the observed threat. Figure 1 illustrates threat propagation. By the law of large numbers, $\bar{\Theta}_v \overset{\text{a.s.}}{\to} \theta_v$ as $K \to \infty$. Each step of the random walk is defined by the transition probabilities t_{vu} from vertex v to u, multiplied by the a priori probability ψ_v that threat propagates through v. The simplest models for both the transition and a priori probabilities are uniform: $t_{ij} = 1/\text{degree}(v_i)$, i.e. $\mathbf{T} = \mathbf{D}^{-1}\mathbf{A}$, and $\psi_v \equiv 1$, where $\mathbf{T}$, $\mathbf{D}$, and $\mathbf{A}$ are, respectively, the transition, degree, and adjacency matrices. This definition of threat propagation has two, equivalent interpretations: stochastic and probabilistic.

2.1.1. Stochastic Realization Approach

The stochastic realization interpretation of the Bayesian threat propagation is given by Eq. (1), i.e. probability of threat θ_v at v equals the threat probability averaged over all random walks emanating from v. This is equivalent to an absorbing Markov chain with absorbing states [16] at which random walks terminate. The absorbing vertices for the threat diffusion model are the C observed vertices, and an augmented state reachable by all unobserved vertices representing a transition from threat to non-threat with probability $1 - \psi_v$. The $(N+1)$-by-$(N+1)$ transition matrix for the Markov chain corresponding to threat propagation equals

$$\mathbf{T} = \begin{array}{c} \\ N{-}C \\ C \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} N{-}C & C & 1 \end{array} \\ \begin{pmatrix} \mathbf{G} & \mathbf{H} & \mathbf{1} - \psi_{N-C} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 1 \end{pmatrix} \end{array} \tag{2}$$

in which $\mathbf{G}$ and $\mathbf{H}$ are defined by the block partition

$$\mathbf{\Psi}\mathbf{D}^{-1}\mathbf{A} = \begin{array}{c} \\ N{-}C \\ C \end{array} \begin{array}{c} \begin{array}{cc} N{-}C & C \end{array} \\ \begin{pmatrix} \mathbf{G} & \mathbf{H} \\ * & * \end{pmatrix} \end{array} \tag{3}$$

with '$*$' denoting unused blocks, $\psi_{N-C} = (\psi_1, \psi_2, \ldots, \psi_{N-C})^{\mathrm{T}}$ is the vector of a priori threat diffusion probabilities from 1 to $N - C$ and $\mathbf{\Psi} = \text{Diag}(\psi_v)$ a diagonal matrix. The observed vertices $v_{b_1}, \ldots, v_{b_C}$ are assigned to indices $N - C + 1, \ldots, N$, and the augmented non-threatening state is assigned to index $N + 1$. Ignoring the a priori probabilities, this is also precisely the stochastic realization model for equilibrium thermodynamics and solutions to Laplace's equation [15, 18].

The probability of threat on the graph is determined by the vector $\boldsymbol{\theta}^{\mathrm{a}} = \begin{pmatrix} \boldsymbol{\theta}_{\mathrm{i}} \\ \boldsymbol{\theta}^{\mathrm{a}}_{\mathrm{b}} \end{pmatrix}$ such that $\mathbf{T}\boldsymbol{\theta}^{\mathrm{a}} = \boldsymbol{\theta}^{\mathrm{a}}$ and $\boldsymbol{\theta}^{\mathrm{a}}_{\mathrm{b}}$ is determined by the probabilities of threat $\theta_{N-C+1}, \ldots, \theta_N$ at observed vertices $v_{b_1}, \ldots, v_{b_C}$ along with zero threat $\theta^{\mathrm{a}}_{N+1} = 0$ at the augmented "non-threat" vertex. The vector that satisfies the proscribed boundary value problem equals,

$$\boldsymbol{\theta}^{\mathrm{a}} = \begin{pmatrix} (\mathbf{I} - \mathbf{G})^{-1}\mathbf{H}\boldsymbol{\theta}_{\mathrm{b}} \\ \boldsymbol{\theta}^{\mathrm{a}}_{\mathrm{b}} \end{pmatrix} \tag{4}$$

where $\mathbf{G}$ and $\mathbf{H}$ are defined in Eq. (3). As is well-known [16], the "hitting" probabilities of a random walk from an unobserved vertex to an observed vertex are given by the matrix $\mathbf{U} = (\mathbf{I} - \mathbf{G})^{-1}\mathbf{H}$; therefore, an equivalent definition of threat probability θ_v from Eq. (4) is the probability that a random walk emanating from v terminates at an observed vertex, conditioned on the probability of threat over all observed vertices:

$$\theta_v = \sum\nolimits_c P(\text{walk}_{v \to v_{b_c}}) P(\Theta_{v_{b_c}}). \tag{5}$$

The existence of a positive solution to Eq. (4) follows from a generalization of the Perron-Frobenius theorem for a special class of *reducible* nonnegative matrices [20].

2.1.2. Probabilistic Approach

The probabilistic equation for threat propagation from the neighbors of a vertex v follows immediately its definition by first-step analysis, yielding the *threat propagation equation:*

$$\theta_v = \psi_v \sum\nolimits_{u \in N(v)} t_{vu}\theta_u \quad \text{and} \quad \theta_v = \frac{\psi_v}{d_v} \sum\nolimits_{u \in N(v)} \theta_u \tag{6}$$

in which $N(v) = \{ u : (v,u) \in E \}$ denotes the neighborhood of vertices adjacent to v. The first equation of Eq. (6) is a general case of space-time threat propagation [19, 21] and equivalent to the stochastic approach described above. The second equation arises for the simplest case of uniform transition probabilities, $\mathbf{T} = \mathbf{D}^{-1}\mathbf{A}$. Expressed in matrix-vector notation, Eq. (6) becomes

$$\boldsymbol{\theta} = \boldsymbol{\Psi}\mathbf{T}\boldsymbol{\theta} \quad \text{and} \quad \boldsymbol{\theta} = \boldsymbol{\Psi}\mathbf{D}^{-1}\mathbf{A}\boldsymbol{\theta}, \tag{7}$$

where $(\boldsymbol{\theta})_v = \theta_v$. The threat probabilities at the observed vertices $v_{b_1}, \ldots, v_{b_C}$ are determined by the observation model. Threat probabilities at all other vertices are determined by solving Eq. (6), as with all Laplacian boundary value problems.

The threat propagation equation Eq. (7) written as

$$\boldsymbol{Ł}^{\psi}\boldsymbol{\theta} = \mathbf{0}, \tag{8}$$

in which $\boldsymbol{Ł}^{\psi} \stackrel{\text{def}}{=} \mathbf{I} - \boldsymbol{\Psi}\mathbf{D}^{-1}\mathbf{A}$ is the generalized Laplacian operator, connects the generalized asymmetric Laplacian matrix of with threat propagation, the solution of which itself may be viewed as a boundary value problem with the harmonic operator $\boldsymbol{Ł}^{\psi}$. Given observations at vertices $v_{b_1}, \ldots, v_{b_C}$, the *harmonic threat propagation equation* is

$$\begin{pmatrix} \boldsymbol{Ł}^{\psi}_{\mathrm{ii}} & \boldsymbol{Ł}^{\psi}_{\mathrm{ib}} \end{pmatrix} \begin{pmatrix} \boldsymbol{\theta}_{\mathrm{i}} \\ \boldsymbol{\theta}_{\mathrm{b}} \end{pmatrix} = \mathbf{0} \tag{9}$$

where the generalized Laplacian $\boldsymbol{Ł}^{\psi} = \begin{pmatrix} \boldsymbol{Ł}^{\psi}_{\mathrm{ii}} & \boldsymbol{Ł}^{\psi}_{\mathrm{ib}} \\ \boldsymbol{Ł}^{\psi}_{\mathrm{bi}} & \boldsymbol{Ł}^{\psi}_{\mathrm{bb}} \end{pmatrix}$ and the threat vector $\boldsymbol{\theta} = \begin{pmatrix} \boldsymbol{\theta}_{\mathrm{i}} \\ \boldsymbol{\theta}_{\mathrm{b}} \end{pmatrix}$ have been permuted so that observed vertices are in the 'b' blocks (the "boundary"), unobserved vertices are in 'i' blocks (the "interior"), and the observation vector $\boldsymbol{\theta}_{\mathrm{b}}$ is given. The *harmonic threat* is the solution to Eq. (9),

$$\boldsymbol{\theta}_{\mathrm{i}} = -(\boldsymbol{Ł}^{\psi}_{\mathrm{ii}})^{-1}(\boldsymbol{Ł}^{\psi}_{\mathrm{ib}}\boldsymbol{\theta}_{\mathrm{b}}). \tag{10}$$

It can be shown that the vector $\boldsymbol{\theta} = \begin{pmatrix} \boldsymbol{\theta}_{\mathrm{i}} \\ \boldsymbol{\theta}_{\mathrm{b}} \end{pmatrix} \in \mathbb{R}^N$ is a nonnegative solution to the boundary value problem of Eqs. (9)–(10) if and only if the augmented vector $\boldsymbol{\theta}^{\mathrm{a}} = \begin{pmatrix} \boldsymbol{\theta}_{\mathrm{i}} \\ \boldsymbol{\theta}^{\mathrm{a}}_{\mathrm{b}} \end{pmatrix} \in \mathbb{R}^{N+1}$ of Eq. (4) is a stationary vector of the absorbing Markov chain transition matrix $\mathbf{T}$ of Eq. (2) with given values $\boldsymbol{\theta}^{\mathrm{a}}_{\mathrm{b}}$ [20].

A simple model for the a priori probabilities is degree-weighted threat propagation (DWTP), $\psi_v = d_v^{-1}$ in which threat is less likely to propagate through high-degree vertices. Another simple model sets the mean propagation length proportional to the graph's average path length $l(G)$ yields length-weighted threat propagation (LWTP) $\psi_v \equiv 2^{-1/\,l(G)}$. For almost-surely connected Erdős-Rényi graphs with $p = n^{-1}\log n$, $l(G) = (\log n - \gamma)/\log\log n + 1/2$ and $\gamma = 0.5772\ldots$ is Euler's constant [9]. A model akin to breadth-first search (BFS) sets the a priori probabilities to be inversely proportional to the Dijkstra distance from observed vertices, i.e. $\psi_v \propto 1/\operatorname{dist}(v, \{ v_{b_1}, \ldots, v_{b_C} \})$.

2.1.3. Connections with Spectral Detection Methods

Whereas threat propagation involves the harmonic solution to a boundary value problem with the graph Laplacian, spectral methods solve the graph partitioning problem by optimizing various subgraph connectivity properties [4, 7, 8]. Though the optimality criteria for spectral methods and threat propagation are different, all these network detection methods must address the fundamental problem of avoiding the trivial solution of constant harmonic functions on graphs. Fiedler showed that if the eigenvector $\boldsymbol{\xi}_1$ corresponding to the second smallest eigenvalue $\lambda_1(\mathbf{D} - \mathbf{A})$ of the (unnormalized) graph Laplacian is used (the smallest is $\lambda_0 \equiv 0$), then for every nonpositive constant $c \leq 0$, the subgraph whose vertices are defined by the threshold $\boldsymbol{\xi}_1 \geq c$ is necessarily connected [8]. This "relaxation" approach provides an approximate solution to the problem of minimizing the *cut size* of a subgraph—the number of edges necessary to remove to separate the subgraph from the graph, which is equivalent to the quadratic optimization problem $\max_{\mathbf{s}} \mathbf{s}^{\mathrm{T}}\mathbf{Q}\mathbf{s}$, where $\mathbf{s} = (\pm 1, \ldots, \pm 1)^{\mathrm{T}}$ is a ± 1-vector who entries are determined by subgraph membership [17].

Because spectral detection with its implicit assumption of minimizing the cut size oftentimes does not detect intuitively appealing subgraphs, Newman introduced the alternate criterion of subgraph "modularity" for subgraph detection [13]. Rather than minimize the cut size, Newman proposes to maximize the subgraph connectivity relative to background graph connectivity, which yields the quadratic maximization problem $\max_{\mathbf{s}} \mathbf{s}^{\mathrm{T}}\mathbf{M}\mathbf{s}$, where $\mathbf{M} = \mathbf{A} - V^{-1}\mathbf{d}\mathbf{d}^{\mathrm{T}}$ is Newman's *modularity matrix*, $(\mathbf{d})_i = d_i$ is the degree vector, and $V = \mathbf{1}^{\mathrm{T}}\mathbf{d}$ is the graph volume [13]. Newman's modularity-based graph partitioning algorithm, also called community detection, involves thresholding the values of the principal eigenvector of $\mathbf{M}$. Miller et al. [11] also consider thresholding arbitrary eigenvectors of the modularity matrix, which by the Courant minimax principle biases the Newman community detection algorithm to smaller subgraphs, a desirable property for many applications.

As shown below in Section 2.3, the threat propagation algorithm optimizes the probability of detecting a subgraph for a specific Bayesian model, i.e. threat propagation is optimum in the Neyman-Pearson sense. Therefore, both spectral detection methods and threat propagation may be viewed as solutions to different optimization problems involving the graph Laplacian.

2.2. Space-Time Threat Propagation

Many important network detection applications, especially networks based on vehicle tracks and computer communication networks, involve directed graphs in which the edges have departure and arrival times associated with their initial and terminal vertices. Space-Time threat propagation is used compute the time-varying threat across a graph given one or more observations at specific vertices and times [19,21]. In such scenarios, the time-stamped graph $G = (V, E)$ may be viewed as a *space-time graph* $G_T = (V \times T, E_T)$ where T is the set of sample times and $E_T \subset [V \times T]^2$ is an edge set determined by the temporal correlations between vertices at specific times.

The advantage of time-stamped edges is that the times can be used to detected temporally coordinated network activity. According to this model of threat networks, the a priori probability that a threat propagates through vertex v at time t_k is determined by the Poisson process used to model the probability

of threat as a function of time:

$$\psi_v(t_k) = \frac{1}{d_v} \sum_{u,l} k_{vu;kl}, \tag{11}$$

where d_v is the spatial degree of vertex v, i.e. the number of interactions associated with a spatial vertex, and $k_{vu;kl} = (\mathbf{K}_\tau^{uv})_{kl}$ is the discretized space-time kernel [21].

2.3. Neyman-Pearson Network Detection

Network detection of a subgraph within a graph $G = (V, E)$ of order N is treated as N independent binary hypothesis tests to decide which of the graph's N vertices does not belong (null hypothesis H_0) or belongs (hypothesis H_1) to the network. Maximizing the probability of detection (PD) for a fixed probability of false alarm (PFA) yields the Neyman-Pearson test involving the log-likelihood ratio of the competing hypothesis. We will derive this test in the context of network detection, which both illustrates the assumptions that ensure detection optimality, as well as indicates practical methods for computing the log-likelihood ratio test and achieving an optimal network detection algorithm. It will be seen that a few basic assumptions yield an optimum test that is equivalent to the Bayesian threat propagation algorithm. An application of Bayes' theorem to the harmonic threat $\theta_v = f(\Theta_v \mid \mathbf{z})$ provides the optimum Neyman-Pearson detector

$$\frac{f(\mathbf{z} \mid \Theta_v = 1)}{f(\mathbf{z} \mid \Theta_v = 0)} \underset{\mathrm{H}_0(v)}{\overset{\mathrm{H}_1(v)}{\gtrless}} \lambda \tag{12}$$

because

$$\begin{aligned} \frac{f(\mathbf{z} \mid \Theta_v = 1)}{f(\mathbf{z} \mid \Theta_v = 0)} &= \frac{f(\Theta_v = 1 \mid \mathbf{z})}{f(\Theta_v = 0 \mid \mathbf{z})} \cdot \frac{f(\Theta_v = 0)}{f(\Theta_v = 1)} \\ &= \frac{\theta_v}{1 - \theta_v} \cdot \frac{f(\Theta_v = 1)}{f(\Theta_v = 0)} \underset{\mathrm{H}_0(v)}{\overset{\mathrm{H}_1(v)}{\gtrless}} \lambda, \end{aligned} \tag{13}$$

results in a threshold of the harmonic space-time threat propagation vector, $\boldsymbol{\theta} \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}}$ threshold, with the prior ratio $f(\Theta_v = 1)/f(\Theta_v = 0)$ and the monotonic function $\theta_v \mapsto \theta_v/(1 - \theta_v)$ being absorbed into the detection threshold. This establishes the detection optimality of harmonic space-time threat propagation.

Because the probability of detecting threat is maximized at each vertex, the probability of detection for the entire subgraph is also maximized, yielding an optimum Neyman-Pearson test under the simplification of treating the 2^N-ary multiple hypothesis testing problem as a sequence of N binary hypothesis tests. Summarizing, the probability of network detection given an observation $\mathbf{z}$ is maximized by computing $f(\Theta_v \mid \mathbf{z})$ using a Bayesian threat propagation method and applying a simple likelihood ratio test.

3. DETECTION PERFORMANCE

The ROC performance between space-time threat propagation [STTP; Section 2.2], breadth-first search spatial-only threat propagation [BFS], and modularity-based spectral detection [SPEC] [11] are illustrated in Figure 2 for a stochastic blockmodel [22] with varying activity. By the classical result of Erdős-Rényi [5], each community is almost surely connected iff $\mathbf{S}_{kk} > \log N_k/N_k$ in which N_k is the number of vertices in community k. We introduce the activity parameter $r_k \geq 1$ and set $\mathbf{S}_{kk} = r_k \log N_k/N_k$ to adjust a community's density relative to its Erdős-Rényi connectivity threshold. The simulations show that excellent ROC performance is achievable if temporal information is exploited (STTP) with highly coordinated foreground network with sparse to moderate connectivity. Spectral methods, which are designed to detect highly connected networks, perform poorly on sparse foreground networks, and improve as foreground network connectivity increases.

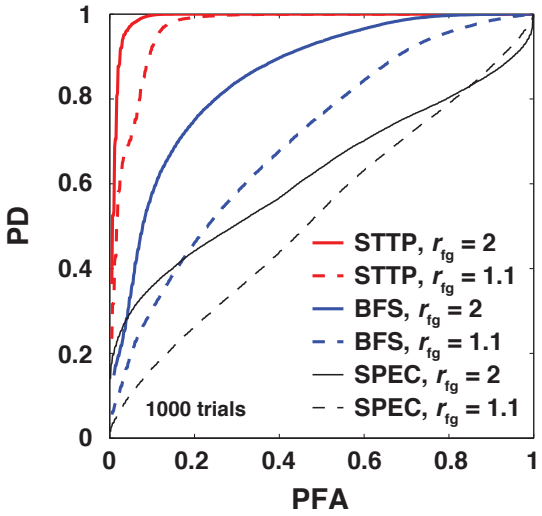

Fig. 2. Detection ROC curves of the three different algorithms at two levels of foreground activity $r_{\mathrm{fg}} = 1.1, 2$ that define its Erdős-Rényi connectivity $r_{\mathrm{fg}} \cdot \log N_{\mathrm{fg}}/N_{\mathrm{fg}}$. Data is simulated using the stochastic blockmodel, $N = 256$, $N_{\mathrm{fg}} = 30$, with 1000 Monte Carlo trials each with an independent draw of the random network and single threat observation.

4. CONCLUSIONS

A Bayesian framework for network detection can be used to unify the different approaches of network detection algorithms based on random walks and algorithms based on spectral properties. Bayesian space-time threat propagation with diffusion is interpreted both as a random walk on a graph and, equivalently, as the solution to a harmonic boundary value problem. Bayes' rule determines the unknown probability of threat on the uncued nodes based on threat observations at cue nodes. In the important situation of low foreground activity with coordination, the examples show the superior detection performance of Bayesian space-time threat propagation compared to other spatial-only and uncued spectral methods.

5. REFERENCES

[1] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. "Epidemic thresholds in real networks," *ACM T. Inform. Syst. Se.*, **10** (4) : 13.1–13.26 (2008).

[2] F. R. K. Chung and W. Zhao. "PageRank and random walks on graphs," in *Fete of Combinatorics and Computer Science*, Bolyai Society Mathematical Studies **20** : 43–62, Vienna: Springer (2010).

[3] R. Diestel. *Graph Theory*. New York: Springer-Verlag, Inc. (2000).

[4] W. E. Donath and A. J. Hoffman. "Lower bounds for the partitioning of graphs," *IBM J. Res. Development* **17** : 420–425 (1973).

[5] P. Erdős and A. Rényi, "On the evolution of random graphs," *Pubs. Mathematical Institute of the Hungarian Academy of Sciences* **5** : 17–61 (1960).

[6] J. P. Ferry, D. Lo, S .T. Ahearn, and A. M. Phillips. "Network detection theory," in *Mathematical Methods in Counterterrorism*, eds. N. Memon et al., pp. 161–181, Vienna: Springer (2009).

[7] M. Fiedler. "Algebraic connectivity of graphs," *Czech. Math. J.* **23** (2) : 298–305 (1973).

[8] M. Fiedler. "A property of eigenvectors of non-negative symmetric matrices and its application to graph theory," *Czech. Math. J.* **25** : 619–633 (1975).

[9] A. Fronczak, P. Fronczak, and J. A. Hołyst. "Average path length in random networks," *Phys. Rev. E* **70** : 056110 (2004).

[10] J. Leskovec, K. J. Lang, and M. Mahoney. "Empirical comparison of algorithms for network community detection," in *Proc. 19th Intl. Conf. World Wide Web (WWW'10)*. Raleigh, NC, pp. 631–640 (2010).

[11] B. A. Miller, N. T. Bliss, and P. J. Wolfe. "Subgraph detection using eigenvector L_1 norms," in *Proc. 2010 Neural Information Processing Systems (NIPS)*. Vancouver, Canada (2010).

[12] R. R. Nadakuditi and M. E. J. Newman. "Graph spectra and the detectability of community structure in networks," *Phys. Rev. Lett.* **108**, 188701 (2012).

[13] M. E. J. Newman. "Finding community structure in networks using the eigenvectors of matrices," *Phys. Rev. E*, **74** (3) (2006).

[14] J.-P. Onnela and N. A. Christakis. "Spreading paths in partially observed social networks," *Phys. Rev. E*, **85** (3) : 036106 (2012).

[15] M. N. Özişik. *Boundary Value Problems of Heat Conduction*. Scranton PA: International Textbook Company, 1968.

[16] M. A. Pinsky and S. Karlin. *An Introduction to Stochastic Modeling*. New York: Academic Press (2010).

[17] A. Pothen, H. Simon, and K.-P. Liou. "Partitioning sparse matrices with eigenvectors of graphs," *SIAM J. Matrix Anal. Appl.* **11** : 430–45 (1990).

[18] K. K. Sabelfeld and N. A. Simonov. *Random Walks on Boundaries for Solving PDEs*. Utrecht, The Netherlands: VSP International Science Publishers, 1994.

[19] S. T. Smith, K. D. Senne, S. Philips, E. K. Kao, and G. Bernstein. "Covert Network Detection," *Lincoln Laboratory J.* **20** (1) : 47–61 (2013).

[20] S. T. Smith, E. K. Kao, K. D. Senne, G. Bernstein, and S. Philips. "Bayesian Discovery of Threat Networks," submitted to *IEEE Trans. Signal Proc.*

[21] S. T. Smith, S. Philips, and E. K. Kao. "Harmonic space-time threat propagation for graph detection," in *Proc. IEEE Intl. Conf. Acoustics, Speech and Signal Processing (ICASSP)*. Kyoto, Japan (2012).

[22] S. Wasserman and K. Faust. *Social Network Analysis*. Cambridge University Press. (1994).