MAINTAINING THROUGHPUT NETWORK CONNECTIVITY IN AD HOC NETWORKS

Ying Liu, Andrey Garnaev, Wade Trappe

WINLAB, Rutgers University, North Brunswick, NJ 08902, USA

ABSTRACT

This paper focuses on the challenge of maintaining reliable connectivity in an ad hoc network, where interference is possible. To cope with such interference, the paper introduces throughput connectivity and weighted throughput connectivity. Throughput connectivity reflects the possibility of establishing communication between nodes for given a signal power level, while weighted throughput connectivity associates the throughput as a weight in the associated network graph. Throughput connectivity is less sensitive to network's parameters than the one based on weighted throughput connectivity. It makes maintaining throughput connectivity protocol less resource consuming (say, by sending less frequently channel state information (CSI)). Whereas, weighted throughput protocol is more efficient in power allocation due to employing a continuous scale in Laplacian matrix. To illustrate these notions, two approaches to maximize connectivity were considered: (a) an adaptive transmission protocol that re-allocates transmission power between nodes, and (b) detecting and eliminating a malicious threat to maintain accumulated connectivity over time slots. The first problem was modeled by a maxmin problem, and solved by Semi-Definite Programming. The second problem was modeled by a stochastic game and solved explicitly.

Index Terms— Connectivity, Throughput Connectivity, Fiedler value, Jamming, Stochastic game

1. INTRODUCTION

In order for networks to be reliable, they must maintain their underlying connectivity, and resist to adversarial attack. An important characteristic of network connectivity is algebraic connectivity, as characterized by the network's Fiedler value, which is the second smallest eigenvalue of the graph's Laplacian. This measures how well-connected the graph is, and has been used to optimize a network's design, and we now survey a few such works. A greedy heuristic algorithm was presented in [1], which adds edges (from a set of candidate edges) to a graph to maximize its algebraic connectivity. A distributed algorithm for the estimation and control of the connectivity of ad hoc networks for random topologies was suggested in [2], while a steepest-descent algorithm was proposed for control of the algebraic connectivity in [3]. The problem of improving network connectivity by adding a set of relays to increase number of links between network's nodes was considered in [4]. Its simplified version was reduced to a semi-definite programming optimization problem. In [5] a genetic algorithm and swarm algorithm were applied for finding the best positions of adding nodes to a network to meet trade off between deployment cost and network's connectivity. A decentralized algorithm to increase the connectivity of a multi-agent system was suggested in [6]. In [7], a problem of finding the best vertex positional configuration to maximize Fiedler value of a weighted graph was studied. Finally note that besides algebraic connectivity the other type of connectivity (such as global message connectivity, worst-case connectivity, network bisection connectivity, and k-connectivity, see [8]) are used in networks depending on characteristics to be maintained and methods used,

.

We note that in all of these papers the possibility of establishing a new communication link in a network did not depend on signal interference. Interference, however, can lead to a significant impact since signals sent to establish new communication links also serve as a noise for all the other links and their signals, thereby reducing the network's capacity for maintaining existing communication links. To deal with this problem, in this paper, two types of connectivity are introduced. First is throughput connectivity, which reflects the possibility of establishing communication between nodes for a given power level. Second is weighted throughput connectivity, which associates with each link a weight corresponding to that link's throughput. To illustrate these notions, two approaches to maximizing connectivity were considered: (a) an adaptive transmission protocol that re-allocates transmission power between nodes, and (b) detecting and eliminating a malicious threat to maintain accumulated connectivity over time slots.

The first problem is modeled by a maxmin problem, and is solved by a generic method. The second problem is modeled by a stochastic game and solved explicitly. Example applications of stochastic games in modeling network security can be found in [9, 10, 11, 12] and [13]. We also note that there is quite an extensive literature on detecting an intruder's signal or its source (see, for example, books [14, 15, 16], papers on the detection of unknown signals [17, 18, 19, 20] and on game-theoretic modeling of spectrum scanning [21, 22]).

The paper is organized as follows. In Section 2, the new notions for a network's connectivity are defined. In Section 3, the problem of designing an optimal transmission protocol to maximize a network's connectivity is considered. In Section 4, an optimal scanning protocol to maintain a network's connectivity is explored.

2. NETWORKS' CONNECTIVITY

We model a wireless network consisting of n nodes in radio range of each other. We denote a node by $v_i = (x_{1i}, x_{2i})$, $i \in [1, n]$, where (x_{1i}, x_{2i}) is the coordinate for node v_i. Let

$V = \{v_i, i \in [1, n]\}$ be the set of all nodes. We assume that, when each node communicates, it emits the same power in all directions. Of course, due to fading gains, pathloss and mutual interference of the signals, not every signal can reach each receiver. Let $\boldsymbol{P} = (P_1, \ldots, P_n)$ be the transmission power allocation where signal P_i is the signal power sent by node i to every other node. Interference between signals could take place, and its effect depends on the distance between the receiver and the sender. Namely, the throughput of received signal by node j is

$$T_{ij,\epsilon}(\boldsymbol{P}) = \begin{cases} 0, & \mathrm{SINR}_{ij}(\boldsymbol{P}) < \epsilon, \\ \ln(1 + \mathrm{SINR}_{ij}(\boldsymbol{P})), & \mathrm{SINR}_{ij}(\boldsymbol{P}) \geq \epsilon, \end{cases}$$

where $\epsilon \geq 0$ is a threshold value for SINR, and $\mathrm{SINR}_{ij}(\boldsymbol{P}) = (h_i P_i / d_{ij}^2)/(\sigma^2 + \sum_{k \neq i, k \neq j} h_k P_k / d_{kj}^2)$ with σ^2 is the background noise, h_i is the fading channel gain, and $d_{ij} = \sqrt{(x_{1i} - x_{1j})^2 + (x_{2i} - x_{2j})^2}$ is the distance between node v_i and node v_j.

To define a communication network's topology beyond the nodes, *links* (edges) between nodes have to be established. Note that due to its communication background this topology has to depend on communication type maintained by the network. In this paper we consider *symmetric* communication, i.e., two nodes (say, node i and node j) are considered to be linked if and only if $T_{ij,\epsilon}(\boldsymbol{P})$ and $T_{ji,\epsilon}(\boldsymbol{P})$ are positive. A link means a possibility to maintain communication. Since communication is symmetric, link is undirected. Denote the link between node v_i and node v_j by e_{ij}. Let $E(\boldsymbol{P})$ be the set of all links. It is clear that the graph $\Gamma(\boldsymbol{P}) = (V, E(\boldsymbol{P}))$ is simple, i.e., there is no self loop for each node and there are not multiple links connecting two nodes.

The graph $\Gamma(\boldsymbol{P})$, associated with a network, can be represented by the Laplacian matrix as

$$L_{ij}(\Gamma(\boldsymbol{P})) = \begin{cases} -1, & i \neq j, \ v_i \text{ and } v_j \text{ are linked}, \\ 0, & i \neq j, \ v_i \text{ and } v_j \text{ are not linked}, \\ -\sum\limits_{k=1, k \neq i}^{n} L_{ik}, & i = j, \end{cases}$$

where $L_{ii}(\Gamma(\boldsymbol{P}))$ equals the number of nodes connected with node v_i. Also, it is possible to consider a weighted network by assigning throughput as weight for each link, in which case the weighted network can be represented by a Laplacian matrix as

$$L_{ij}(\Gamma(\boldsymbol{P})) = \begin{cases} -w_{ij}, & i \neq j, \ v_i \text{ and } v_j \text{ are linked}, \\ 0, & i \neq j, \ v_i \text{ and } v_j \text{ are not linked}, \\ -\sum\limits_{k=1, k \neq i}^{n} L_{ik}, & i = j, \end{cases}$$

where $w_{ij} = T_{ij,\epsilon}(\boldsymbol{P}) + T_{ji,\epsilon}(\boldsymbol{P})$ is total throughput of symmetric communication between node v_i and node v_j, and $L_{ii}(\Gamma(\boldsymbol{P}))$ is the total throughput of symmetric communication between node v_i and others nodes.

Since $L(\Gamma(\boldsymbol{P}))$ is positive semi-definite and symmetric, its eigenvalues are all nonnegative. By ordering the eigenvalues in an increasing way, we have: $0 = \lambda_1(\Gamma(\boldsymbol{P})) \leq \lambda_2(\Gamma(\boldsymbol{P})) \leq \ldots \leq \lambda_n(\Gamma(\boldsymbol{P}))$. The eigenvector corresponding to the first eigenvalue is always $\boldsymbol{e}^T = (1, \ldots, 1)$. The second eigenvalue $\lambda_2(\Gamma(\boldsymbol{P}))$ is the algebraic connectivity of the system, and is an indicator of how connected the graph is, and is also called the Fiedler value. To emphasize that we consider connectivity based on the fact that there is bi-directional throughput (above a threshold value) for a link, we will use the term *throughput connectivity* and *throughput Fiedler value*. For a fixed transmission protocol involving a power assignment $\boldsymbol{P}$, the throughput Fiedler value can be found as solution of the following optimization problem

$$\lambda_2(\Gamma(\boldsymbol{P})) = \min_{\boldsymbol{y}^T \boldsymbol{y} = 1, \boldsymbol{e}^T \boldsymbol{y} = 0} \boldsymbol{y}^T L(\Gamma(\boldsymbol{P})) \boldsymbol{y}.$$

Let us illustrate the behavior of throughput connectivity by the following example. Let the network consist of five nodes $(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$ and $(2, 0.5)$ (Figure 1(a)), and $h = 1$, $\sigma^2 = 2$, $\epsilon = 0.1, 0.25$ and $\boldsymbol{P} = (10, 20, 15, 25, 10)$ and P_5 varies from 0.2 to 40. Of course, increasing ϵ yields a decrease in total throughput (Figure 1(b)). Throughput connectivity is piece-wise constant versus varying of the power (in our case, P_5, see, Figure 1(c)), while weighted throughput connectivity is piece-wise continuous on P_5 (Figure 1(d)). Thus, weighted throughput connectivity is more sensitive than throughput connectivity to a variation of the power. In this example, we can observe that there is a continuum where throughput connectivity obtains its maximum, and the value of this maximum is not too sensitive to the threshold ϵ (in the considered example they coincide for $\epsilon = 0.1$ and $\epsilon = 0.25$, and are equal to 3). Also, we can observe that there is a reduction of the set where the throughput connectivity obtains its maximum on reducing the threshold ϵ, but there is no simple monotonic dependence between throughput connectivity and threshold ϵ, For weighted throughput connectivity, such dependence could be observed, as well as the fact that it obtains its maximum for a unique P_5.

3. OPTIMAL TRANSMISSION PROTOCOL

The network provider might improve the network's connectivity by varying transmission power vector. Let Π be the set of feasible transmission protocols. For example, it could be $\Pi(\overline{P}) = \{\boldsymbol{P} \geq 0 : \sum_{j=1}^{n} P_i = \overline{P}\}$, where $\overline{P}$ is the total power allowed by the network's provider among the nodes. Then, the problem of optimal transmission power assignment is given as the following maxmin problem:

$$\lambda_2(\Gamma(\boldsymbol{P})) = \max_{\boldsymbol{P} \in \Pi(\overline{P})} \min_{\boldsymbol{y}^T \boldsymbol{y} = 1, \boldsymbol{e}^T \boldsymbol{y} = 0} \boldsymbol{y}^T L(\Gamma(\boldsymbol{P})) \boldsymbol{y}. \quad (1)$$

This maximization problem of the second smallest eigenvalue of the Laplacian matrix on its inner parameters is equivalent to the following optimization problem (see, [23]):

$$\begin{aligned} &\max_{\boldsymbol{P}, z} z, \\ &\text{subject to} \\ &L(\Gamma(\boldsymbol{P})) - z\boldsymbol{I} \succ \boldsymbol{0}, \quad \boldsymbol{P} \in \Pi(\overline{P}) \text{ and } z > 0, \end{aligned} \quad (2)$$

where $\boldsymbol{I}$ is the $n \times n$ identity matrix, and "$\succ$" represents positive definiteness. By definition, Laplacian matrix $L(\Gamma(\boldsymbol{P}))$ is symmetric. Thus, $L(\Gamma(\boldsymbol{P})) - z\boldsymbol{I}$ is also symmetric. Therefore, (2) belongs to Semi-Definite Programming (SDP) problems [24]. It can be solved by SDP optimization tools, such as SDPT3 [25, 26], SDPA-M [27, 28] and CSDP [29].

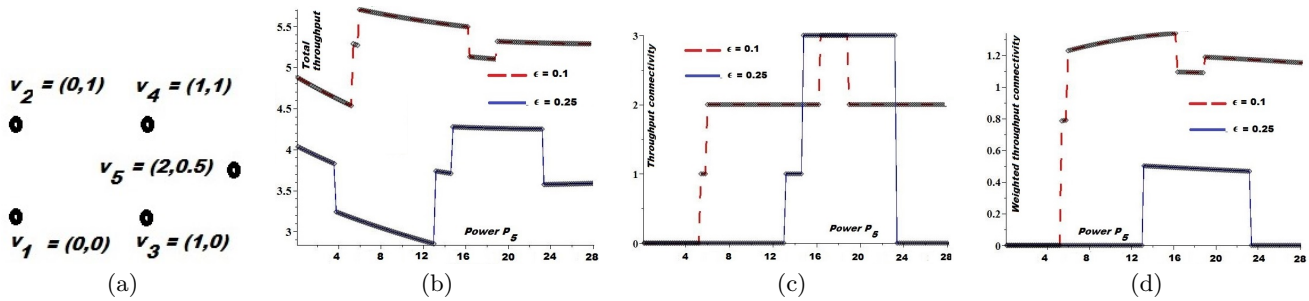

Fig. 1. (a) Nodes of the network,(b) Total throughput, (c) Throughput connectivity and (d) Weighted throughput connectivity as functions on P_5.

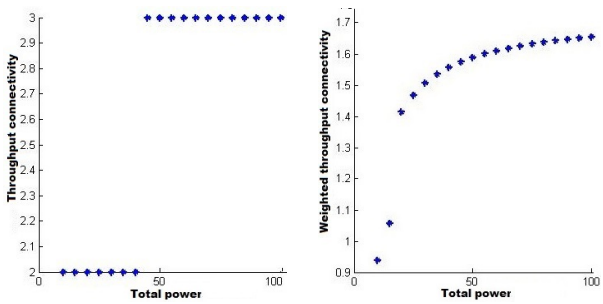

Fig. 2. Throughput connectivity (left) and weighted throughput connectivity (righr) as functions on $\overline{P}$.

Figure 2(a) illustrates dependence of throughput connectivity and weighted throughput connectivity versus total power $\overline{P}$ with $\epsilon = 0.1$. It is interesting that these two forms of connectivity are non-decreasing due to the cooperative re-allocation of transmission power between the nodes. Meanwhile, as it was shown in Figure 1, selfishly increasing transmission power of just one node could lead to decreasing the network's connectivity. Of course, cooperative throughput is larger than selfish throughput.

4. OPTIMAL SCANNING PROTOCOL

In this section, we consider a problem where an adversary wants to damage connectivity of a network Γ by attacking its nodes, while an IDS (Intrusion Detection System), scanning nodes, intends to detect the adversary to stop his malicious activity. We assume that all the actions (scanning by the IDS and attacking by the adversary) are performed in discrete time slots $1, 2, ..., \infty$. At each time slot, the adversary can choose a node to attack, and the IDS can choose a node to scan. If node i is attacked, then connectivity of the undamaged network $\Gamma_i = \Gamma \backslash \{v_i\}$ is C_i. If the rivals choose different nodes then the IDS gets connectivity for an un-jammed network as an instantaneous payoff, and the game moves to the next time slot and is played recursively with discount factor δ. If the rivals choose the same node, then with probability $1-\gamma$ the adversary is detected and eliminated from the network. Then, the network keeps on working, and the IDS gets as instantaneous payoff the discounted connectivity C_0 of the whole network. With probability γ the adversary is not detected, the game moves to the next time slot and is played recursively with discount factor δ. This game can be considered as a two-state (1 and 2) stochastic game $G = (G^1, G^2)$. State 1 represents the malicious state in which the network is vulnerable to an attack by the adversary, while state 2 represents the state in which the adversary is detected and is not a threat to the network anymore. Stochastic game $G = (G^1, G^2)$ can be described in matrix form as follows:

$$G^1 : \begin{array}{c} \\ 1 \\ 2 \\ ... \\ n \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & ... & n \end{array} \\ \begin{pmatrix} C_1|(\gamma, 1-\gamma) & C_2|(1,0) & ... & C_n|(1,0) \\ C_1|(1,0) & C_2|(\gamma, 1-\gamma) & ... & C_n|(1,0) \\ ... & ... & ... & \\ C_1|(1,0) & C_2|(1,0) & ... & C_n|(\gamma, 1-\gamma) \end{pmatrix} \end{array},$$

$$G^2 : \begin{array}{c} \\ 1 \end{array} \begin{array}{c} 1 \\ \big(C_0|(0,1) \big) \end{array},$$

In state 1, matrix notation is used such that each entry corresponds to a pair of nodes (i, j) chosen by the IDS and the adversary. The value in the left part of each entry is the instantaneous payoff (un-jammed connectivity) to the IDS in this zero-sum stochastic game, while the right part gives the probability distribution over the future states. Thus, if $i \neq j$ then the instantaneous payoff to the IDS is C_j, and the next state is state 1. If $i = j$ then the instantaneous payoff to the IDS is C_i, and the next state is state 1 with probability γ, and it is state 2 with probability $1-\gamma$. Note that the payoff at the next epoch is discounted with discount rate δ.

In state 2, the rivals are passive, since the adversary is detected and cannot attack the network anymore. The game cannot leave this safe state. At each time slot the IDS obtains the discounted payoff C_0, which is the connectivity of un-jammed network. Thus, the total accumulated discounted payoff in state 2 is equal to $(1 + \delta + \delta^2 + ...)C_0 = C_0/(1-\delta)$. Thus, the game G is equivalent just to the game G^1 with a single state. The game G^1 has a solution in (mixed) stationary strategies, i.e., the strategies that are independent of history and current time slot. A (mixed) stationary strategy to the IDS is a probability vector $\boldsymbol{p}^T = (p_1, p_2, ..., p_n)$, where p_i is the probability to scan node i and $\boldsymbol{e}^T\boldsymbol{p} = 1$. A (mixed) stationary strategy to the jammer is a probability vector $\boldsymbol{q}^T = (q_1, q_2, \ldots, q_n)$, where q_i is the probability to jam node i, and $\boldsymbol{e}^T\boldsymbol{q} = 1$. Solution of the game G^1 is given as a solution to the Shapley (-Bellmann) equation game [30]:

$$\mathrm{val}(G^1) = \max_{\boldsymbol{p}\geq 0, \boldsymbol{e}^T\boldsymbol{p}=1} \min_{\boldsymbol{q}\geq 0, \boldsymbol{e}^T\boldsymbol{q}=1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}(\mathrm{val}(G^1))p_i q_j,$$

$$= \min_{\boldsymbol{q}\geq 0, \boldsymbol{e}^T\boldsymbol{q}=1} \max_{\boldsymbol{p}\geq 0, \boldsymbol{e}^T\boldsymbol{p}=1} \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}(\mathrm{val}(G^1))p_i q_j,$$

where

$$A_{ij}(G^1) = \begin{cases} C_i + (1-\gamma)C_0/(1-\delta) + \gamma\delta G^1, & i = j, \\ C_i + \delta G^1, & i \neq j, \end{cases}$$

and $V := \mathrm{val}(G^1)$ is the value of the game, i.e., the equilibrium total accumulated payoff to the IDS. This game G^1 is a stochastic discounted game [30], and so, it has the unique solution in stationary strategies. To find the equilibrium strategies explicitly without loss of generality we can assume that the nodes are arranged in non-increasing order by C_i, i.e., $C_1 \leq C_2 \leq \ldots \leq C_n$. Also, connectivity of an un-jammed network is considered larger than connectivity of a damaged network, i.e., $C_0 \geq \max_{1\leq i\leq n} C_i$.

Theorem 1 *The game has a unique equilibrium in stationary strategies. The value of the game and stationary equilibrium strategies are given as follows:*

$$V = \frac{\delta(1-\gamma)C_0/(1-\delta) + \sum_{i=1}^{k} C_i}{k(1-\delta) + \delta(1-\gamma)},$$

$$p_i = \begin{cases} \dfrac{(1-\delta)V - C_i}{\delta(1-\gamma)(C_0/(1-\delta) - V)}, & i \leq k, \\ 0, & i > k, \end{cases}$$

$$q_i = \begin{cases} 1/k, & i \leq k, \\ 0, & i > k, \end{cases}$$

where $k \in \{1, \ldots, n\}$ is an integer given by

$$\varphi_k \leq C_0 < \varphi_{k+1}, \tag{3}$$

and φ_i is such that

$$\varphi_i = \frac{(1-\delta)\sum_{j=1}^{i}(C_i - C_j) + \delta(1-\gamma)C_i}{\delta(1-\gamma)}, \quad i \in \{1, \ldots, n\}$$

and $\varphi_{n+1} = \infty$. Since φ_i is increasing and $\varphi_1 = C_1 < C_0$, the k is uniquely defined by (3).

Figure 3 illustrates the tradeoff for weighted throughput connectivity between detection probability and intention to bring the maximum damage to the network by the jammer with $\delta = 0.6$. Namely, if the detection probability is small, then the jammer could focus his attack on the node which would reduce the connectivity maximally. Responding to this threat, the IDS also focuses its scanning effort on this node. Increasing detection probability makes the jammer consider its safety by applying his attack efforts among a larger number of nodes to reduce its detection probability. Also, this illustrates that the accumulated weighted throughput connectivity is increasing versus discount factor δ (which reflects the reduction in the urgency of maintaining higher connectivity) and detection probability.

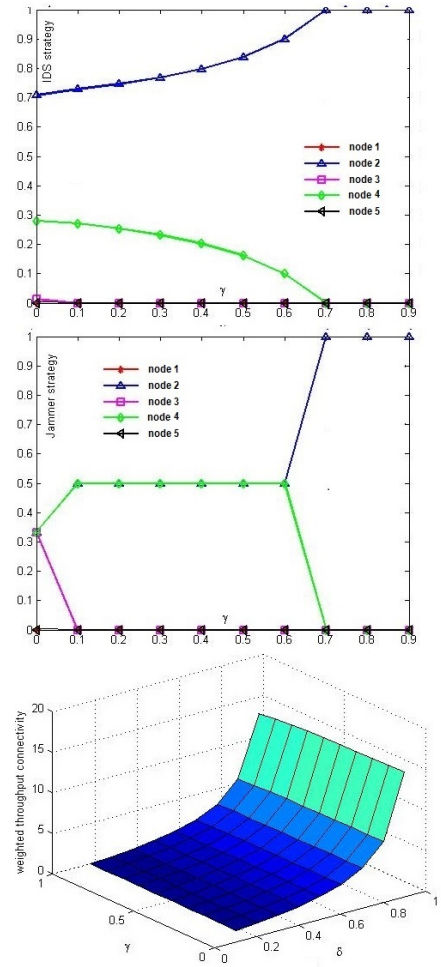

Fig. 3. IDS strategy (top), jammer's strategy (center) and accumulated weighted throughput connectivity (bottom).

5. CONCLUSIONS

In this paper, the concept of throughput connectivity and weighted throughput connectivity was introduced to to describe the reliability of a network's communication in the presence of signal interference due to an adversary. In particular, we have shown a difference between selfish and cooperative power allocation, namely, selfishly increasing power by a node might reduce network connectivity, while cooperative allocation improves the connectivity. Also, we have shown how a repeated jamming attack could impact the accumulated network connectivity, and how to reduce this impact by designing a scanning protocol. Our future work is focused on applying the new connectivity metrics we introduced to other scenarios, including moving nodes in a theater for coordinating network connectivity, and to apply the throughput connectivity to Massive MIMO 5G networks.

6. REFERENCES

[1] A. Ghosh and S. Boyd, "Growing well-connected graphs," in *Proc. 45th IEEE Conference on Decision and Control (CDC)*, 2006, pp. 6605–6611.

[2] P. Di Lorenzo and S. Barbarossa, "Distributed estimation and control of algebraic connectivity over random graphs," *IEEE Transactions on Signal Processing*, vol. 62, no. 21, pp. 5615–5628, 2014.

[3] F. Morbidi, "On the control of the algebraic connectivity and clustering of a mobile robotic network," in *Proc.European Control Conference (ECC)*, 2013, pp. 2801–2806.

[4] A.S. Ibrahim, K.G. Seddik, and K.J.R. Liu, "Improving connectivity via relays deployment in wireless sensor networks," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, 2007, pp. 1159–163.

[5] M. Romoozi and H. Babaei, "Improvement of connectivity in mobile ad-hoc networks by adding static nodes based on a realistic mobility model," *IJCSI International Journal of Computer Science Issues*, vol. 8, no. 4, pp. 76–83, 2011.

[6] M.C. De Gennaro and A. Jadbabaie, "Decentralized control of connectivity for multi-agent systems," in *Proc. IEEE Conference on Decision and Control (CDC)*, 2009, pp. 3628–3633.

[7] Y. Kim and M. Mesbahi, "On maximizing the second smallest eigenvalue of a state-dependent graph laplacian," in *Proc. American Control Conference (ACC)*, 2005, pp. 99–103.

[8] Z. Han, A.L. Swindlehurst, and K.J.R. Liu, "Optimization of MANET connectivity via smart deployment/movement of unmanned air vehicles," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3533–3546, 2009.

[9] K.C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," in *Proc. International Conference on Game Theory for Networks (GameNets)*, 2009, pp. 697–703.

[10] B. Wang, Y. Wu, K.J.R. Liu, and T.C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 877–889, 2011.

[11] A. Garnaev and W. Trappe, "Stationary equilibrium strategies for bandwidth scanning," in *Multiple Access Communcations*, M. Jonsson and et al, Eds. 2013, vol. 8310 of *LNCS*, pp. 168–183, Springer.

[12] A. Garnaev and W. Trappe, "Anti-jamming strategies: a stochastic game approach," in *Mobile Networks and Management*, R. Aguero and et al, Eds. 2015, vol. 141 of *LNICST*, pp. 230–243, Springer.

[13] G. Calinescu, S. Kapoor, K. Qiao, and J. Shin, "Stochastic strategic routing reduces attack effects," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2011, pp. 1–5.

[14] C. Comaniciu, N.B. Mandayam, and H.V. Poor, *Wireless networks multiuser detection in cross-layer design*, Springer, New York, 2005.

[15] S. Verdu, *Multiuser detectiony*, University Press, New York, 1998.

[16] H.L.V. Trees, *Detection, estimation, and modulation theory*, Wiley, New York, 2001.

[17] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, pp. 523–531, 1967.

[18] F.F. Digham, M.S. Alouini, and M.K. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. IEEE International Conference on Communications (ICC)*, 2003, pp. 3575–3579.

[19] Y. Liu and W. Trappe, "Jammer forensics: Localization in peer to peer networks based on q-learning," in *Proc. 40th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1737–1741.

[20] A. Garnaev, Y. Liu, and W. Trappe, "Anti-jamming strategy versus a low-power jamming attack when intelligence of adversary's attack type is unknown," *IEEE Transactions on Signal and Information Processing over Networks*, 2015, DOI: 10.1109/TSIPN.2015.2506038.

[21] A. Garnaev, W. Trappe, and C.-T. Kung, "Dependence of optimal monitoring strategy on the application to be protected," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 1054–1059.

[22] A. Garnaev and W. Trappe, "Bandwidth scanning involving a Bayesian approach to adapting the belief of an adversary's presence," in *Proc. IEEE Conference on Communications and Network Security (CNS)*, 2014, pp. 35–43.

[23] A.M. Blanco and J.A. Bandoni, "Eigenvalue and singular value optimization," *Mecanica Computational*, 2003.

[24] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM review*, vol. 38, no. 1, pp. 49–95, 1996.

[25] R.H. Tutuncu, K.C. Toh, and M.J. Todd, "Solving semidefinite-quadratic-linear programs using SDPT3," *Mathematical programming*, vol. 95, no. 2, pp. 189–217, 2003.

[26] M.J. Todd, K.C. Toh, and R.H. Tutuncu, "A MATLAB software package for semidefinite programming," *Technical report. School of OR and IE, Cornell University. Ithacat NY*, 1996.

[27] A.S. Ibrahim, K.G. Seddik, and K.J.R. Liu, "Improving connectivity via relays deployment in wireless sensor networks," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, 2007, pp. 1159–1163.

[28] K. Fujisawa, Y. Futakata, M. Kojima, S. Matsuyama, S. Nakamura, K. Nakata, and M. Yamashita, "SDPA-M (semidefinite programming algorithm in matlab) user's manual-version 6.2," *Research Reports on Mathematical and Computing Sciences, Series B: Operation Res., Dep. Math. and Computing Sci., Tokyo Institute of Technol., Japan*, vol. 10, 2000.

[29] B. Borchers, "CSDP, AC library for semidefinite programming," *Optimization methods and Software*, vol. 11, no. 1-4, pp. 613–623, 1999.

[30] G. Owen, *Game Theory*, Academic Press, 1982.