2015-02

Designing interference-robust wireless mesh network using a defender-attacker-defender model

Nicholas, Paul J.

Monterey, California. Naval Postgraduate School

NPS-OR-15-002

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DESIGNING INTERFERENCE-ROBUST WIRELESS MESH NETWORKS USING A DEFENDER-ATTACKER-DEFENDER MODEL

by

Paul J. Nicholas
David L. Alderson

February 2015

Prepared for: Office of Naval Research,
875 N. Randolph Street,
Arlington, VA 22203

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
28-02-2015	Technical Report	17-07-2011 – 17-07-2014

4. TITLE AND SUBTITLE
Designing Interference-robust Wireless Mesh Network using a Defender-Attacker-Defender Model

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Paul J. Nicholas
David L. Alderson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Operations Research Department
Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-OR-15-002

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research, 875 N. Randolph Street, Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

14. ABSTRACT

Wireless mesh networks (WMNs) are interconnected systems of wireless access points (APs) that provide untethered network connectivity for a group of users who require data, voice, and/or video communication. The wireless access medium of a WMN makes it particularly vulnerable to attack and exploitation. We seek a method for quickly designing WMN physical topologies (i.e., the placement of APs) that are robust to the effects of electromagnetic jamming.

The conflicting interests of a network designer and attacker in respectively maximizing and minimizing network performance make this problem a natural candidate for the use of game theory. We apply the game theoretic defender-attacker-defender (**DAD**) methodology to the simultaneous routing, resource allocation, and coverage (SRRA+C) model of WMN performance to simulate the design, attack, and operation of a WMN. Our algorithm and associated decision-support tool can quickly prescribe jamming-robust WMN topologies that minimize the worst possible damage that an adversary can inflict. Our approach considers radio-operating characteristics, the relative importance of client coverage and network flow, and the effects of radio propagation over terrain. To our knowledge, we are the first to use an algorithm with proven global convergence to design jamming-robust WMNs, and the first to apply the **DAD** framework to the problem of WMN design.

15. SUBJECT TERMS
Wireless mesh networks, interference, jamming, game theory, defender-attacker-defender (DAD) model, SRRA+C, optimization, Dividing Rectangles (DIRECT) algorithm

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			David L. Alderson
Unclassified	Unclassified	Unclassified	Unclassified	71	**19b. TELEPHONE NUMBER** *(include area code)* (831) 656-1814

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Douglas Hensler
Provost

The report entitled "*Designing Interference-Robust Wireless Mesh Network Using a Defender-Attacker-Defender Model"* was prepared for and funded by the Office of Naval Research, 875 N. Randolph Street, Arlington, VA 22203.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Paul J. Nicholas
Operations Research Analyst

David L. Alderson
Associate Professor of Operations Research

Reviewed by:

Johannes O. Royset
Associate Chairman for Research
Department of Operations Research

Released by:

Robert F. Dell
Chairman
Department of Operations Research

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Wireless mesh networks (WMNs) are interconnected systems of wireless access points (APs) that provide untethered network connectivity for a group of users who require data, voice, and/or video communication. The wireless access medium of a WMN makes it particularly vulnerable to attack and exploitation. We seek a method for quickly designing WMN physical topologies (i.e., the placement of APs) that are robust to the effects of electromagnetic jamming.

The conflicting interests of a network designer and attacker in respectively maximizing and minimizing network performance make this problem a natural candidate for the use of game theory. We apply the game theoretic defender-attacker-defender (**DAD**) methodology to the simultaneous routing, resource allocation, and coverage (SRRA+C) model of WMN performance to simulate the design, attack, and operation of a WMN. Our algorithm and associated decision-support tool can quickly prescribe jamming-robust WMN topologies that minimize the worst possible damage that an adversary can inflict. Our approach considers radio-operating characteristics, the relative importance of client coverage and network flow, and the effects of radio propagation over terrain. To our knowledge, we are the first to use an algorithm with proven global convergence to design jamming-robust WMNs, and the first to apply the **DAD** framework to the problem of WMN design.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Wireless mesh networks (*WMNs*) are interconnected systems of wireless *access points* (*APs*) that provide untethered network connectivity for a group of users that require data, voice, and/or video communication. Each AP has two radio devices: the first connects to local *client devices*, such as laptops and portable digital assistants (PDAs); the second connects to other APs to create a *backhaul network*. Communication between users on a WMN passes from a source client through one or more APs before reaching a destination client. To function, APs require only a local power source, such as a battery or portable generator. This property of WMNs make them well-suited to operations in austere environments, such as combat and humanitarian assistance disaster relief (HA/DR) operations. See Nicholas (2009) for an introduction to WMNs.

The wireless access medium of a WMN makes it particularly vulnerable to attack and exploitation (Pelechrinis, Iliofotou, and Krishnamurthy 2011; Mpitziopoulous, Gavalas, Konstantopoulos, and Pantziou, 2009). Such actions may include passive eavesdropping and packet capture, spoofing trusted identities to gain unauthorized access to the network, injecting malicious code, or denial of service (DoS) attacks (Xu, Wood, Trappe, and Zhang, 2004). Designers of WMNs employ various strategies to defend against such threats, including frequency hopping and spread spectrum techniques, filtering noisy connections, adjusting the signal-to-noise ratio (SNR) threshold, implementing intrusion detection systems (IDSs) and access control lists (ACLs), data encryption, and various other security protocols (Ståhlberg, 2000; Zhang, Zheng, and Hu, 2009, pp. 115-118; Poisel, 2011, pp. 3-7).

In this report, we consider a simple, but often very effective, method for a DoS attack. In *physical-layer denial jamming*, *constant jamming*, or simply *noise jamming*, an attacker constantly broadcasts random noise on the same radio frequency (RF) *channel* used by the WMN in an attempt to overpower the friendly signal, thus degrading or denying use of the channel (Vakin, Shustov, and Dunwell, 2001; Xu, Trappe, Zhang, and Wood, 2005; Poisel, 2011; Pelechrinis et al., 2011). Powerful commercial and military jamming systems are readily available, but this type of attack can be conducted with inexpensive equipment and little technological prowess, and can be very challenging to

defend against (Wood, Stankovic, and Son, 2003; Xu et al., 2004; Mpitziopoulous et al., 2009, The Economist, 2011; The Institute for Engineering and Technology, 2013). Even unintentional interference can be as harmful as an intentional attack (see, e.g., Cox, 2007); hence, it is of increasing concern in both civilian and military operating environments (Caro, 2007).

We seek a method for quickly designing WMN physical topologies (i.e., the placement of APs) that are robust to the effects of deliberate jamming or other *electromagnetic interference* (*EMI*) emanating from point sources. We refer to the point sources of both intentional jamming and unintentional EMI as *jammers*. Although we focus on the effects of brute physical-layer jamming, our technique can be generalized to any form of WMN interference in which network performance is a function of the distance between interference sources and WMN APs.

The conflicting interests of a network *designer* and *attacker* in, respectively, maximizing and minimizing network performance, make this problem a natural candidate for the use of *game theory*, a mathematical representation of conflict between rational opponents (Myerson, 1991). We adopt the game theoretic *defender-attacker-defender* (**DAD**) methodology of Brown, Carlyle, Salmeron, and Wood (2006), Alderson, Brown, Carlyle, and Wood (2011), and Alderson, Brown, and Carlyle (2014) to model the design, attack, and operation of a WMN. We seek AP locations that minimize the disruption to client coverage caused by jammers, subject to constraints on network service and considering the effects of radio propagation over terrain.

A. RELATED WORK

Wood et al. (2003) describe a method of mapping the areas affected by physical-layer jamming to avoid placing sensors in these denied areas. However, they do not mention how a network engineer should minimize the effects of jamming if sensors are placed within a denied area. Xu et al. (2005) observe, based on empirical evidence they gather, that common measurements, such as signal strength, may not be able to conclusively identify the presence of a jamming attack. However, they find that devices that constantly jam (which we assume) are more prone to detection, and they develop

algorithms to improve the classification rate of jamming attacks. The methods of both Wood et al. (2003) and Xu et al. (2005) could provide useful input to our problem.

Ståhlberg (2000) and Lazos and Krunz (2011) each recommend several methods of increasing the robustness of wireless networks to attacks, including the use of directional antennae, frequency hopping and spread spectrum technology, lower data rates, fiber-optic backhaul networks, encryption and error correction, and frequency-agile control channels. Neither specifically consider defensive placement of APs. Xu (2008) examines the effectiveness of adjusting transmission power to avoid jamming; however, she assumes that jammers will operate at a fixed transmission power less than that of the Aps, while we make no such assumption. Wood, Stankovic, and Zhou (2007) assume jammers will have the same capabilities as APs, but do not consider AP mobility.

Xu et al. (2004) examine *spatial retreats*, i.e., moving APs physically away from the sources of interference, as a form of defense against a jamming attack. Their model assumes that jammers are stationary; they minimize the damage done by this fixed attack by coordinating the retreat of APs from the effective range of the adversary's jammers. Ma, Zhang, and Trappe (2005) create a network dynamics model based on Newtonian equations to describe the attractive and repulsive forces between mobile nodes in wireless networks. Building on Xu et al. (2004), they examine spatial retreats as a method of avoiding the effects of jamming. Their algorithm moves nodes away from the sources of jamming in such a way as to reconstruct a working network. However, neither they nor Xu et al. (2004) consider jammers that could then move and attack the newly-configured network. As Mpitziopoulous et al. (2009) observe, this type of defense is ineffective against an adversary that can again move jammers. Our approach to building a robust WMN topology is similar to a spatial retreat in that the only defensive method we consider to minimize the effects of jamming is to place an AP somewhere else. However, unlike any of this previous work that focuses on static or random jamming, we consider WMN network design in the presence of an intelligent adversary who observes our network and then places the jammer(s) to maximally disrupt network performance. In this way, we seek network designs that will maximize robustness to the *worst possible* jamming attack, rather than defending against a specific one.

Thamilarasu and Sridhar (2009) also consider the use of game theory in modeling optimal jamming attack and detection strategies. However, they do not consider the actions taken by a network designer or defender, and both they and Srivastava et al. (2005) consider only *strategic-form* games (wherein players move simultaneously), vice *extensive form* games (wherein players move sequentially) that we consider (Fudenberg & Tirole, 1991, pp. 3-4, 67-68).

In our previous work (Nicholas & Alderson, 2012), we consider the task of a network designer who must quickly determine good locations for APs to maximize client coverage and delivered backhaul network flow, considering the effects of radio propagation over terrain. That work adopts and modifies He et al.'s (2004) concept of power coverage to calculate client coverage, and builds on the Simultaneous Routing and Resource Allocation (SRRA) problem of Xiao et al. (2004) to calculate the value of network flow. Our resulting model of WMN performance is the SRRA+Coverage or *SRRA+C* problem. We use the DIviding RECTangles (DIRECT) sampling algorithm of Jones, Perttunen, and Stuckman (1993) to quickly find good solutions to SRRA+C (i.e., AP locations).

Shankar (2008) similarly considers the deliberate placement of jammers by an intelligent adversary (called the *attacker*) to maximally disrupt network operation, which in turn is also solved using SRRA. He solves the *attacker's problem* by considering a fixed number of candidate locations for jammers and then exhaustively enumerating them to find the location(s) that maximally disrupt network performance. In contrast, we consider a continuous space for jammer placement (and therefore an infinite number of possible locations).

Our work can be viewed as a merger of the *attacker-operator* formulation of Shankar (2008) and the *designer-operator* formulation of Nicholas and Alderson (2012). As noted in Wood et al. (2003), overcoming the effects of jamming can quickly escalate into a costly game of one-upmanship, where the network designer and adversary are constantly trying to outmaneuver each other. The application of the defender-attacker-defender **DAD** game theoretic framework to our model can identify WMN topologies that minimize the worst possible damage that an adversary can inflict, avoiding such endless competition. To our knowledge, we are the first to use an algorithm with proven

global convergence to design EMI-robust WMNs, and the first to apply the **DAD** framework to the problem of WMN design.

In the next part, we describe our new jammer-cognizant SRRA+C model of WMN performance and our application of the **DAD** framework. In Part III, we describe our method for solving the **DAD**-SRRA+C problem. In Part IV, we run our model to explore its behavior under various conditions. We conclude by describing areas of future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PROBLEM FORMULATION

We apply the **DA<u>D</u>** methodology of Brown et al. (2006), Alderson et al. (2011), and Alderson et al. (2014) to model the design, attack, and operation of a WMN. In our version of this three-stage, sequential Stackelberg game (von Stackelberg, 1952), the *defender-as-designer*, or simply *designer* **D**, places a defined number of APs. In the second stage, the *attacker* **A**, cognizant of the AP topology, places a defined number of jammers to disrupt client coverage and total delivered flow. In the final stage, the *defender-as-operator*, or simply *operator* **<u>D,</u>** calculates client coverage and flow across the backhaul network (in reality, the operator is a routing algorithm computed by the APs). We repeat this game over many rounds, allowing the designer to learn the best AP topologies. The optimal solution to our **DA<u>D</u>** problem identifies the locations of APs to create a WMN that is the most robust to the worst possible jamming attack. Such an attack could represent the actions of a rational human opponent, or the worst-case positioning of unintentional interference sources such as civilian radios, other RF devices, or high-voltage electrical devices.

A. THE OPERATOR'S PROBLEM: CALCULATING THE VALUE OF A WMN TOPOLOGY

We begin by describing the *operator's problem*, a method of calculating the value of a WMN physical topology given fixed AP and jammer locations. Building on the notation of Nicholas and Alderson (2012), we define N to be the set of all AP nodes, indexed by i = 1, 2,…, n, where $n = |N|$. We define M to be the set of all jammer nodes, indexed by k = 1, 2,…, m, where $m = |M|$. Let $\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)$ represent the locations of the APs, and let $\chi = (\chi_1, \chi_2, ..., \chi_m)$ represent the locations of the jamming sources. We define the *operating area* as the topographic area where an AP i or jamming source k may be physically located. A two-dimensional coordinate (x, y) is associated with each location λ_i and with each χ_k; these coordinates represent the northing and easting for AP node i and each jammer node k, respectively. We assume that APs and jammers, once placed, remain stationary. We divide the operating area into a set of discrete *coverage*

regions R, indexed by $r = 1, 2, \ldots |R|$. Although our formulation allows the use of any discretization scheme, our implementation assumes rectangular regions arranged in a grid (see Figure 1). Each coverage region $r \in R$ has an associated elevation that we assume is uniform throughout the region. This assumption is not true in practice, but is consistent with much of the available elevation data.

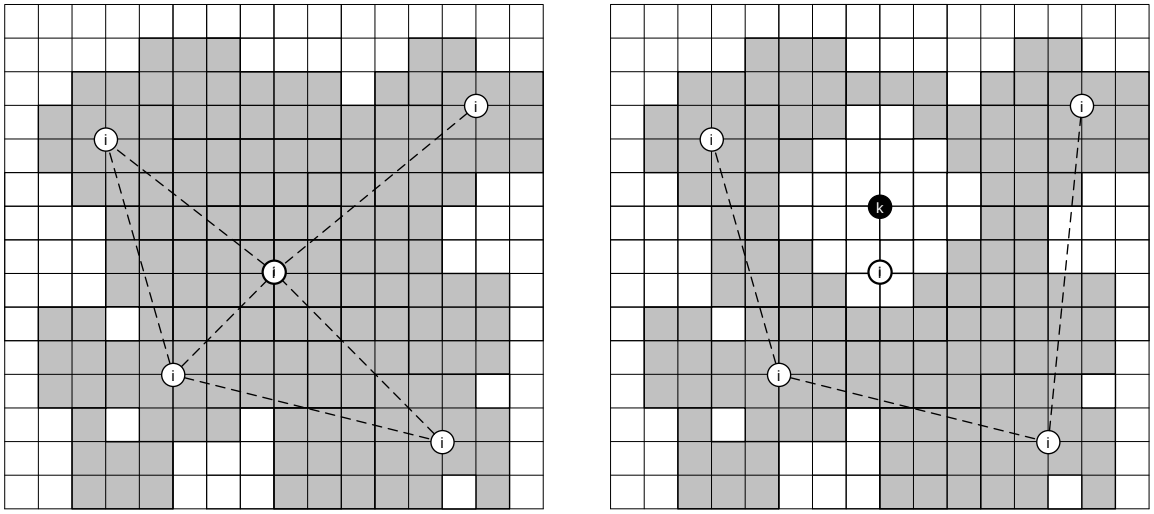


Figure 1. A representative discretized operating area and wireless mesh network without a jammer (left) and with a jammer (right). White circles denote the location of access points, shaded regions denote the areas with sufficient client coverage (i.e., zero coverage shortfall), and dashed lines denote links in the backhaul network. The placement of a jammer, denoted by a black circle, decreases client coverage and disrupts backhaul network connectivity.

Figure 1 (left) depicts a typical WMN in the absence of jamming. AP nodes are illustrated as white circles, and shaded grid elements represent locations that receive sufficient client coverage from the APs. The coverage obtained at each grid location depends on several factors including the local terrain, AP and client radio characteristics, and EMI. The dashed lines in Figure 1 represent the backhaul network used to communicate between AP nodes.

Figure 1 (right) depicts a WMN in the presence of jamming. Each jammer node $k \in M$ (illustrated as a black circle) may have two active transmitters: one interfering with nearby AP client coverage radios and the other interfering with nearby AP backhaul network radios. Without loss of generality, we assume APs are not subject to

self-jamming or interference from other APs, and jammers emit signals consisting of random noise perfectly matched in frequency, phase, and polarization to AP transmissions (i.e., perfect physical-layer interference) (Pelechrinis et al., 2011).

Each AP node $i \in N$ may serve as a source of network traffic. We identify sink or *destination nodes* $d \in N$ as the sinks for all network traffic. As presented by Shankar (2008), in the case where the number of destinations is less than the number of jammers, the optimal jamming solution is to simply jam each destination, cutting off all delivered network flow. To avoid such results, here we assume all APs serve as destination nodes, as is common in peer-to-peer networks (Schollmeier, 2001).

We assume the physical location of one destination node, designated the *headquarters* (*HQ*) *node*, is known in advance and fixed. This node may serve as the network gateway and/or location of domain controllers and servers. This is consistent with reality, where network designers must place an AP at their headquarters, satellite gateway, or Internet point of presence (PoP). While there is no hard constraint requiring the HQ node to connect to other APs, in realistic problems we find it is always connected. The placement of this node within the operating area greatly influences the resulting topologies.

Building on the SRRA+C formulation of Nicholas and Alderson (2012), we quantify the value of a particular WMN topology in the presence of EMI by calculating two subproblems. First, we calculate the value of coverage provided to client devices $Z_{coverage}$, and then calculate the value of delivered backhaul network flow Z_{flow}. We use a linear combination to obtain a value of the given WMN topology:

$$Z\left(\hat{\lambda},\hat{\chi}\right) \equiv Z_{coverage}\left(\hat{\lambda},\hat{\chi}\right) - w\,Z_{flow}\left(\hat{\lambda},\hat{\chi}\right), \tag{1}$$

where w is a positive scalar representing the relative importance of network flow (see Appendix for complete derivation), and the ^ symbol denotes that the locations λ and χ are fixed.

Given fixed AP locations $\hat{\lambda}$ and fixed jammer locations $\hat{\chi}$, the operator **D** aims to minimize client coverage shortfall and minimize negative network flow (i.e., maximize positive network flow) by choice of flow variables S, F, T, and P. For clarity, we

explicitly state the variables being minimized by the operator **D** in the operator's problem:

$$Z_{\underline{\mathbf{D}}}\left(\hat{\lambda},\hat{\chi}\right)=\min_{S,F,T,P}\left(Z_{coverage}\left(\hat{\lambda},\hat{\chi}\right)-wZ_{flow}\left(\hat{\lambda},\hat{\chi},S,F,T,P\right)\right). \qquad (2)$$

B. THE ATTACKER'S PROBLEM: PLACING JAMMERS

The attacker **A**, given fixed AP node locations $\hat{\lambda}$, wishes to maximize disruption to the WMN by placing jammer nodes at locations χ:

$$\mathbf{DA\underline{D}}\left(\hat{\lambda},\cdot,\cdot\right)\mathbf{:}\quad Z_{\mathbf{A\underline{D}}}\left(\hat{\lambda}\right)=\max_{\chi}\min_{S,F,T,P}\left(Z_{coverage}\left(\hat{\lambda},\chi\right)-wZ_{flow}\left(\hat{\lambda},\chi,S,F,T,P\right)\right). \qquad (3)$$

The attacker's objective is to maximize coverage shortfall and minimize delivered backhaul network flow.

C. THE DESIGNER'S PROBLEM: PLACING ACCESS POINTS

The network designer **D**, given fixed jammer node locations $\hat{\chi}$, wishes to maximize WMN performance by placing AP nodes at locations λ:

$$Z_{\mathbf{D\underline{D}}}\left(\hat{\chi}\right)=\min_{\lambda}\min_{S,F,T,P}\left(Z_{coverage}\left(\lambda,\hat{\chi}\right)-wZ_{flow}\left(\lambda,\hat{\chi},S,F,T,P\right)\right). \qquad (4)$$

The designer's objective is to minimize coverage shortfall and maximize delivered backhaul network flow. The SRRA+C problem presented in Nicholas and Alderson (2012) is a special case of the designer's problem with no jammer nodes.

D. THE DA<u>D</u> PROBLEM

By nesting the problems of the operator, attacker, and designer, we obtain the overall **SRRA+C DA<u>D</u>** formulation:

$$Z_{\mathbf{DA\underline{D}}}=\min_{\lambda}\max_{\chi}\min_{S,F,T,P}\left(Z_{\boldsymbol{coverage}}\left(\lambda,\chi\right)-wZ_{flow}\left(\lambda,\chi,S,F,T,P\right)\right). \qquad (5)$$

The designer **D** first chooses AP locations λ, which the attacker **A** then aims to maximally disrupt by placing jammers at locations χ. The operator **<u>D</u>** calculates client coverage and determines how to route traffic given AP and jammer locations. By allowing the designer to move first in this sequential Stackelberg game, we assume the designer is operating in an area that will subsequently be subject to jamming. Had we allowed the

attacker to move first (i.e., **ADD**), we would assume the designer is being forced to operate in an area already being jammed.

The solution to the **DAD** problem indicates where the network designer should place APs to minimize the worst-case disruption possible by EMI. That is, when solved to optimality, the obtained AP network topology *is completely immune* to greater degradation, as the attacker cannot possibly do more damage. Note that the converse is not true. Because we assume the designer (with *perfect information* of the worst possible attack) places his APs first, it is possible (indeed, likely) that the designer could improve upon this design *given fixed jammers*. Likewise, if we allow the attacker to move first (**ADD**), it is likely he could improve upon his attack *given fixed APs*. In other words, we find a *Stackelberg equilibrium*, but not a *Nash equilibrium* (Cruz, 1975; Fudenberg & Tirole, 1991), as the designer could likely unilaterally improve his/her strategy after the opponent's move.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SOLUTION METHOD

A. SOLVING THE OPERATOR'S PROBLEM

We solve the operator's problems by calculating the two components of the overall objective function $\boldsymbol{Z}_{\underline{\mathbf{D}}}$ (2) separately. Calculating client coverage $Z_{coverage}$ is a straightforward series of calculations based on input data. Calculating the value of network flow Z_{flow} via the SRRA problem is more challenging. Xiao et al. (2004) observe that the SRRA problem has special structure that allows it to be solved using dual decomposition. We use the same approach to solve the problem using the subgradient method (Bertsekas, 1999), stopping after a given number of iterations. See Nicholas and Alderson (2012) and Nicholas (2009) for further details on our SRRA solution technique.

B. SOLVING THE ATTACKER AND THE DESIGNER'S PROBLEMS

The attacker and designer's problems (like the SRRA+C problem) are nondifferentiable, nonconvex, nonlinear optimization problems. The difficulty of finding exact solutions to such problems increases the desirability of using heuristic computational techniques, such as genetic or simulated annealing algorithms, and sampling algorithms, such as mesh adaptive direct search (MADS) (Audet, 2004). In our previous work, we use the DIviding RECTangles (DIRECT) algorithm of Jones et al. (1993) to sample the SRRA+C solution space (i.e., the designer's problem with no jammers) to quickly find solutions. This same approach will work for the attacker's problem $\boldsymbol{Z}_{\mathbf{A}\underline{\mathbf{D}}}$ (given fixed AP nodes), and for the designer's problem $\boldsymbol{Z}_{\mathbf{D}\underline{\mathbf{D}}}$ (given fixed jammers).

DIRECT is a sampling optimization algorithm based on Lipschitzian optimization (Horst & Hoang, 1996, pp. 43-46). The algorithm iteratively samples from the solution space, where the number of dimensions is $2m$ (attacker's problem) or $2(n-1)$ (designer's problem), the length of each dimension is proportional to the operating area length or width, and a single point in the solution space represents the locations of all the nodes being placed (whether AP locations λ in the designer's problem, or jammer locations χ in the attacker's problem). The algorithm progressively samples from and

divides the space into smaller hyper-rectangles. At each step, it chooses to explore a particular sub-hyper-rectangle based on both the solution value of the center point and the total volume of the given shape, where larger volumes are more desirable because they indicate greater unexplored territory and hence greater potential for an improved incumbent solution. The DIRECT algorithm is continuous, i.e., it can place APs or jammers at any location within the user-specified operating area. The DIRECT algorithm is guaranteed to eventually converge to the optimum solution, as it will eventually sample within an arbitrary distance of any point in the solution space (Jones et al., 1993).

We observe DIRECT suffers problems symptomatic of the *curse of dimensionality* (Bellman, 1961). First, as the number of nodes (and thus dimensions) increases, the portion of a dimension needed to capture a given fraction of the solution space increases logarithmically. That is, at higher dimensions (i.e., when placing more APs or jammers), DIRECT requires an increasing number of iterations in order to sufficiently search the solution space. Also, at higher dimensions, an increasing percentage of solutions are near the solution space boundary (i.e., the physical boundary of the operating area). This makes sampling for good AP and jammer locations near the operating area boundaries increasingly difficult (Hastie, Tibshirani, and Friedman, 2001, pp. 22-24). We find that the DIRECT algorithm running on a laptop computer quickly finds good solutions to the attacker and designer's problems for networks consisting of up to 10 APs where the operating area is discretized into r = 6,000 regions. Future research could consider avoiding the problem of sampling near the operating area boundary via parallelization of the algorithm: dividing the original solution space into subspaces, exploring each, and then comparing the best solutions found.

C. SOLVING THE DA<u>D</u> PROBLEM

To solve the **SRRA+C DA<u>D</u>** problem, we cannot simply use one large instance of DIRECT to search concurrently for good AP locations λ and jammer locations χ, as the attacker and designer are playing against each other and have opposing (i.e., maximization and minimization) goals. Instead, we follow Alderson et al. (2011) and decompose the **DA<u>D</u>** problem into a designer **D** *master problem* with separate attacker **A** *subproblems*. We solve using different instances of DIRECT, each with its

own objective function. In the master problem, DIRECT chooses AP locations λ_u for each iteration u = 1,2,…, *max_master_iterations*. For those given AP locations, another instance of DIRECT is initialized to solve the associated subproblem, choosing jammer locations χ_v for each iteration v = 1,2,…, *max_sub_iterations*. Given AP locations λ_u and jammer locations χ_v, the overall objective value is then obtained via solving the operator's problem (2). After *max_sub_iterations*, the subproblem returns the jammer locations $\chi^{\wedge}$ yielding the best attack found (i.e., the highest overall objective value). The master problem continues searching for the best AP locations λ^* to minimize the damage caused by the worst attack found until *max_master_iterations*. The following pseudo-code details our nested DIRECT algorithm:

Algorithm DIRECT for SRRA+C DA<u>D</u>

Input: Full SRRA problem data (number and operating characteristics of APs and jammers, HQ node location, and elevation and coverage requirements for each $r \in R$) and desired number of iterations *max_master_iterations* and *max_sub_iterations*.

Output: Best estimate of optimal AP locations $\lambda^* = (\lambda_1^*, \lambda_2^*, ..., \lambda_n^*)$ and $\chi^* = (\chi_1^*, \chi_2^*, ..., \chi_m^*)$, and operator solution $Z_{\underline{\mathbf{D}}}(\lambda^*, \chi^*)$.

begin
Store map data
Initialize $u \leftarrow 1$
***Master problem* (*Designer*)**
while ($u <$ *max_master_iterations*) **do**
Calculate AP locations λ_u using DIRECT
Initialize $v \leftarrow 1$
***Subproblem* (*Attacker*)**
while ($v <$ *max_sub_iterations*) **do**
Calculate EMI locations χ_v using DIRECT
Solve operator's problem $Z_{\underline{\mathbf{D}}}$ for λ_u and χ_v
if $Z_{\underline{\mathbf{D}}}(\lambda_u, \chi_v) > Z_{\underline{\mathbf{D}}}(\lambda_u, \chi^{\wedge})$ /* If this is the best attack yet, store as incumbent */
$\chi^{\wedge} \leftarrow \chi^k$
$Z_{\underline{\mathbf{D}}}(\lambda_u, \chi^{\wedge}) \leftarrow Z_{\underline{\mathbf{D}}}(\lambda_u, \chi_v)$
endif;
$v \leftarrow v + 1$
end;
if $Z_{\underline{\mathbf{D}}}(\lambda_u, \chi^{\wedge}) < Z_{\underline{\mathbf{D}}}(\lambda^*, \chi^*)$ /* If this is the best design yet, store as incumbent */
$\lambda^* \leftarrow \lambda_u$
$\chi^* \leftarrow \chi^{\wedge}$
$Z_{\underline{\mathbf{D}}}(\lambda^*, \chi^*) \leftarrow Z_{\underline{\mathbf{D}}}(\lambda_u, \chi^{\wedge})$
endif;
$u \leftarrow u + 1$
end;
Return best AP locations λ^*, EMI locations χ^*, and operator's solution $Z_{\underline{\mathbf{D}}}(\lambda^*, \chi^*)$
end;

For given AP locations λ_u and given enough iterations, DIRECT will eventually find a solution within an arbitrary distance of the solution space point defining the optimal jamming attack. In practice, we are constrained by the computational limits of our computer implementation (specifically, double-precision, floating-point arithmetic), and cannot divide any hyper-rectangle more than 32 or 33 times.

Our algorithm to solve the attacker and designer's problems using DIRECT runs in polynomial time, is specifically:

$$O\left(\left(u|R|n^2+un^2+u^3\right)\left(v|R|n^2+vn^2+v^3\right)\right)$$

time, where *u* and *v* are, respectively, the current number of DIRECT algorithm iterations for the master and subproblems, $|R|$ is the total number of coverage regions, and *n* is the number of APs, assuming $n < m$, the number of jammers. Though the algorithm runs in polynomial time, the problem grows very quickly in the number of nodes being placed and the number of DIRECT iterations.

In Nicholas (2009) and Nicholas and Alderson (2012), we calculate a theoretical lower bound for the SRRA+C problem based on the *best possible* AP topology that provides zero coverage shortfall and maximum possible delivered network flow. (Such results are achievable only in unrealistic circumstances, where APs provide complete client coverage to the operating area, yet are located directly next to one another to provide maximum backhaul flow.) The optimality gap for any SRRA+C solution is the difference between the obtained objective value $Z_{\mathbf{DD}}(\lambda)$ (4) and this theoretical lower bound. In the SRRA+C **DAD** problem, a theoretical upper bound can be calculated as the difference between the *worst possible* jamming attack (i.e., complete client coverage shortfall and zero network flow) and the obtained objective value $Z_{\mathbf{DAD}}$ (5). Such attacks are possible with powerful and plentiful jammers. However, as we use a log utility function to quantify the value of network flow, a total flow of zero would obtain a penalty of negative infinity, so this theoretical upper bound is of limited practical use. Though we have no feasible method of precisely calculating the optimality gap of any particular solution, we do not have the need, considering our intended user is conducting time-sensitive network design in support of HA/DR or combat operations.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

Building on the software we initially developed for Nicholas (2009), we implement our algorithm for solving the SRRA+C **DAD** problem using Microsoft Visual C++. Our decision support tool runs on a laptop, does not require commercial solvers or other add-ins, and can use terrain information freely downloaded from the Internet.

Many different factors affect the shape of the SRRA+C solution space, including the technical characteristics of the APs and jammers, their relative numbers and signal strengths, the type and effectiveness of jamming, the amount of overlap in client coverage, the effects of terrain on electromagnetic propagation, and the assignment of traffic destination nodes. An exhaustive exploration of all these factors is beyond the scope of this report. We focus on those factors that have the greatest effect on model outcome. In the following analyses, and unless otherwise noted, we follow Wood et al. (2007) and assume each radio in each AP and the associated radio in each jammer are identical, transmitting with the same output power and similar antennae. The scalar w is set to one, thereby weighting client coverage and backhaul network flow equally. In previous field testing, we have found this value to yield realistic network topologies (Nicholas & Alderson, 2012). We begin with simple analyses on flat "tabletop" terrain to gain intuition on optimal jamming and defense strategies, and then consider realistic case studies using actual terrain data. We also provide analysis of the performance of our method.

We consider two types of jamming. In *narrowband noise jamming*, *spot jamming*, or simply *single-channel jamming*, a jammer places all its energy on a single channel (Mpitziopoulous et al., 2009; Poisel, 2011). We assume each AP is assigned its own channel, so single-channel jamming will only affect the AP using that channel (and its associated client devices) at that time. This may be a preferred jamming strategy when maximum energy must be directed at a single AP in order to overpower the signal of the AP, or when energy must be conserved by the jammer. Good attack strategies using single-channel jamming in our model are quite trivial: place the jammer as close as possible to, or on top of, an AP on the same channel. This is because jamming affects only the receiver of a radio, not the transmitter. While our SRRA+C formulation

considers client devices, the optimal targets are APs because they require two-way connections with both other APs and their connected client devices, and so are *single points of failure* for both backhaul network traffic and client coverage. An attacker should assign additional jammers to other APs until the network is sufficiently degraded. The defensive strategy under single-channel jamming reduces to determining where to place redundant APs to build maximum robustness. This, in turn, is determined by the relative values of network flow and client coverage (the two competing terms in our objective function).

We also consider *broadband noise jamming* or *barrage jamming*, where the EMI produced by a jammer is spread across the entire targeted spectrum (Mpitziopoulous et al., 2009; Poisel, 2011, p. 470). Barrage jamming affects all APs and client devices operating in that spectrum; we assume the effects of multiple jammers are perfectly additive at the respective receivers. Such jammers provide lower power spectral densities (i.e., power per EM wave) than an equivalent single-channel jammer because transmission power is spread over a larger frequency range (Poisel, 2011). They are very cheaply acquired or built (Ståhlberg, 2000) and are, hence, increasingly prevalent. Additionally, such barrage jamming cannot be overcome by simply placing an additional, redundant AP (as in single-channel jamming), as all APs are subject to the same interference. Shankar (2008) uses the SRRA formulation and attacks a network using barrage jammers. His optimal attack strategy is the same as ours for single-channel jamming: place the jammer as close as possible to, or on top of, an AP. However, Shankar does not consider client coverage. As we will demonstrate, the optimal attack strategy in our SRRA+C model using barrage jamming is often to attack more than one AP (and its associated client devices) concurrently, while the optimal defensive strategy involves finding AP locations that minimize the ability of jammers to conduct concurrent attacks.

A. EXPLORING THE ATTACKER'S PROBLEM

1. Attacking a Network of Two APs

We first explore the attacker's problem (3) by finding the optimal single jammer attack against a network of two fixed APs. Consider a one square kilometer operating

area (gridded into 100 x 100 regions) with flat terrain, with an AP placed near the top and bottom of the region (left side of Figure 2). With no jammer present, these two APs (depicted as open circles) will provide the client coverage shown in white and deliver network traffic to each other at a maximum rate of 419 kilobits per second (kbps). Our formulation penalizes solutions based on the degree of insufficient client coverage, depicted in Figure 2 as darker areas.

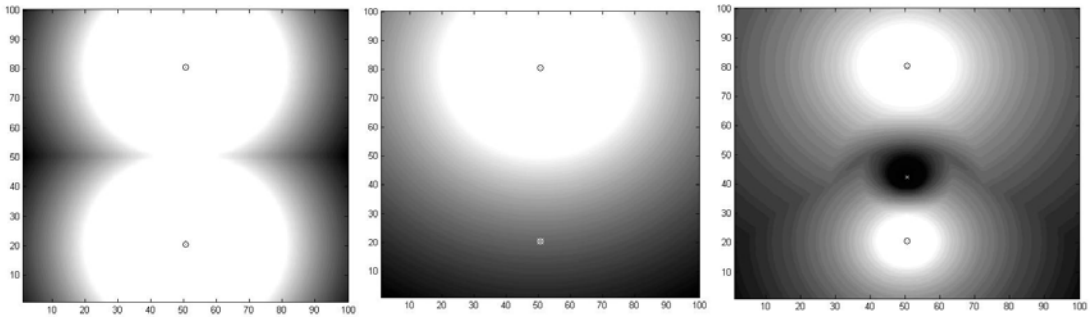


Figure 2. Client coverage provided by two APs (indicated by black circles) on flat terrain without jammers (a), during optimal single-channel jamming attack (b), and barrage jamming attack (c). White areas indicate sufficient client coverage where client devices are able to connect to APs. Darker areas indicate progressively worse client coverage shortfall.

In a single-channel jamming attack, the optimal attack is to simply place the single jammer directly on top of either AP, depicted as an "X" on the bottom AP in Figure 2(b). This *direct-AP attack* eliminates the client coverage by the bottom AP, and reduces network traffic flow between the APs to essentially zero. In barrage jamming, the optimal attack is to place the jammer in between the two APs in a *between-AP attack* (Figure 2(c)). In such a location, the barrage jammer is able to significantly reduce the client coverage provided by both APs, and reduce the delivered network traffic flow to both devices to essentially zero.

The between-AP attack may at first seem counterintuitive, as the horizontal centerline of the scenario without jammers (Figure 2(a)) receives less coverage than that area immediately surrounding each AP at the bottom and top; it may seem this center area has "less to lose" than an attack directly on each AP. However, recall that our formulation penalizes the degree of coverage shortfall. By placing the jammer in between each AP, the jammer maximizes this penalty by making the centerline region

receive worse client coverage than would be provided if the jammer was placed directly on top of either AP. Likewise, network flow is maximally disrupted in a barrage jamming attack by placing the jammer between each AP because this reduces delivered flow to both APs, as our model assumes user datagram protocol (UDP)-like traffic transmission without handshake dialogues (Postel, 1980). Figures 3(a) and (b) are contour plots, respectively, depicting the client coverage value and network flow value provided by two APs in the presence of a single barrage jammer placed at each of 10^4 locations enumerated in the Cartesian plane. The plots show that the worst (i.e., higher) objective values are obtained when the barrage jammer is used in a between-AP attack.

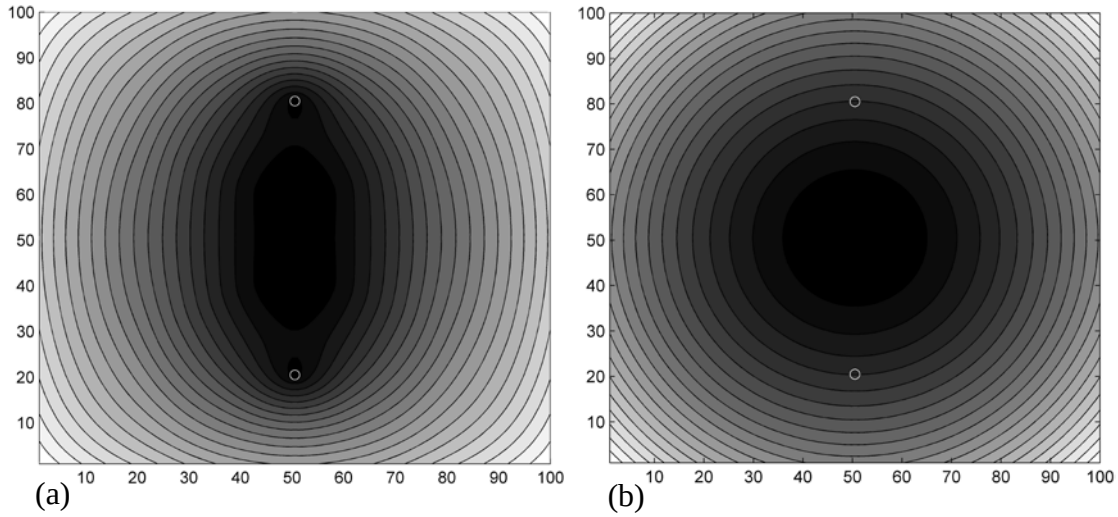
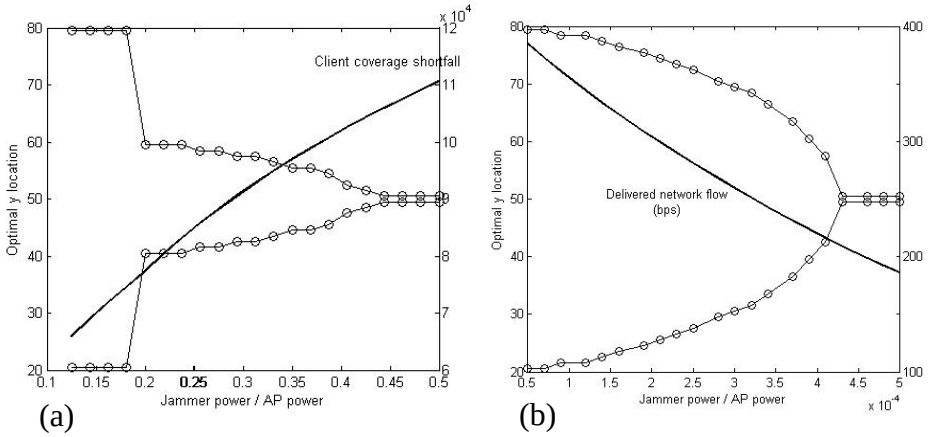


Figure 3. Contour plot of client coverage values (a) and network flow values (b) provided by two fixed APs (open circles) in the presence of one barrage jammer. The shade at each (*x*,*y*) location indicates the client coverage or network flow value when a jammer is placed at that location (worse jamming attacks are indicated by darker areas).

Note that in this simple example, the two unjammed APs provide overlapping client coverage (i.e., the overlap in white coverage areas in Figure 2). This is a function of AP placement and radio characteristics. When trying to maximize client coverage (even at the expense of network flow), such overlap may be wasteful, but does accurately reflect real-world AP placement that attempts to provide uninterrupted coverage to mobile clients. We find that modifying radio characteristics to change the size of this overlap alone generally doesn't affect the optimal barrage jamming strategy. The best attack may still be the between-AP attack because coverage isn't binary (adequate or not

adequate): we penalize the degree of insufficiency. If there is little or no coverage between two APs, the optimal attack location may still be between APs because a jamming attack makes *inadequate coverage that much worse*. However, if the area in between the two APs is already at the maximum penalty limit, then a jammer will not be able to penalize it. In this case, a direct-AP attack may be more effective.

We next examine the optimal jamming strategy as a function of relative AP and jammer transmission powers. Figure 4(a) shows the optimal *y* location(s) for one barrage jammer placed between two APs at locations (50, 20) and (50, 80) to minimize client coverage, as a function of jammer transmission power relative to client device power. Figure 4(b) presents the same analysis for a barrage jammer to minimize backhaul network flow. Equivalent solutions in each figure are shown by two points at a given power ratio. We observe that when jamming power relative to AP and client transmission power is low enough, the optimal barrage jamming strategy may become the direct-AP attack.



(a) (b)

Figure 4. Optimal *y* location for a single barrage jammer to minimize client coverage (a) and network flow (b) provided by two APs placed at $y = 20$ and $y = 80$, as a function of jammer transmission power relative to AP transmission power. The solid line indicates client coverage shortfall (a) or delivered network flow (b). Two points at a given power ratio indicate solutions with the same objective value.

Note the sudden jump in Figure 4(a). This is an artifact of continuous client service—which, on perfectly flat terrain, is essentially a circle around each AP—being discretized into the gridded operating area. As the relative transmission power of an AP changes, the "circle" of client coverage around each AP will change in a discontinuous

fashion, occasionally jumping in value. In this case, it occurs when the area receiving adequate client service no longer overlaps the upper and lower boundaries of the operating area. The calculation of network flow (i.e., Figure 4(b)) is not affected by the discretization of the operating area, so these jumps are not present.

We observe that the optimal jamming strategy (i.e., direct-AP or between-AP attack) for attacking client coverage and network flow occurs at different power ratio levels. That is, the best location to place a jammer to maximize client coverage shortfall may not always be the best place to minimize network flow. The best overall location will be a function of *w*, the positive scalar indicating the value of network flow in the SRRA+C objective function (6).

2. One Jammer, Four APs

We next consider the optimal barrage jamming attack in the presence of four APs. Figures 5(a) and (b) are contour plots, respectively depicting the client coverage value and network flow value provided by four APs in the presence of a single barrage jammer placed at each of 10^4 Cartesian locations. As in the two AP example, the optimal attack against client coverage remains between the four APs in a smooth, continuous pattern. The pattern of optimal network flow attack strategies is more complex, however. The most damaging attacks occur not when the jammer is placed directly in the middle, but around the middle in a small ring. This complex pattern emerges for two reasons. First, as noted above, we assume all nodes are destinations for network traffic and hence form a peer-to-peer network. Whereas client coverage grid squares connect only to that single AP providing the best service, APs can exchange traffic simultaneously with multiple APs. In this example, each of the APs is able to connect with the other three APs. Placing a single jammer at various locations among the four APs degrades network communication between each of these AP-to-AP connections in a nonlinear, but symmetric fashion. Second, nonlinearity also results from running the subgradient method on the SRRA problem only for a fixed number of iterations (as opposed to solving to optimality). We find these slight numerical irregularities to be worth the benefit of greatly reduced computation time.

This simple example illustrates how quickly this problem grows in complexity. The number and respective locations of each AP and jammer have a significant impact on the optimal offensive and defensive design strategies. The effects of terrain and different radio characteristics only magnify this complexity, making a quick method of finding relatively good solutions valuable to a network designer.

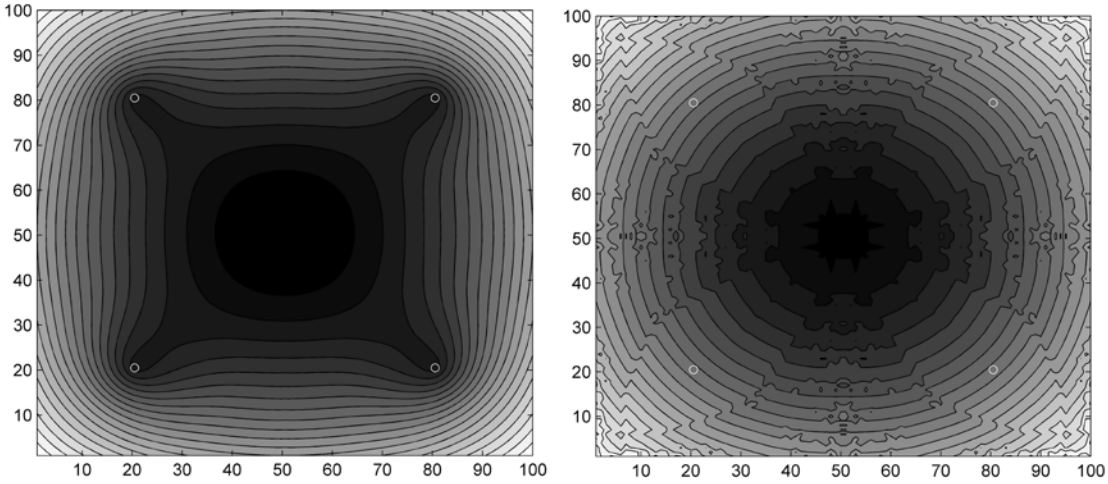


Figure 5. Contour plot of client coverage values (a) and network flow values (b) provided by four fixed APs (open circles) in the presence of one barrage jammer on flat terrain. The shade at each (*x*,*y*) location indicates the overall client coverage value (a) or network flow value (b) when a jammer is placed at that location (worse jamming attacks are indicated by darker areas).

3. Two Jammers, Four APs

We next place two jammers among four fixed APs. This is a four-dimensional problem (since each jammer has a corresponding *x* and *y* location) and difficult to present in two dimensions. We find that the most effective jamming strategy in this particular scenario is a "symmetric" jamming attack, where, for each jamming attack, the location of the second jammer is across the positive diagonal axis from the first jammer. That is, if the first jammer is located at point (*x*,*y*), the second jammer is located at point (*y*,*x*). For the sake of clarity, we present the objective values of only these symmetric attacks for client coverage and network flow, respectively depicted in Figures 6(a) and (b). In each, the color at each point represents the value of client coverage or network flow (respectively), when one jammer is placed at that point and the other jammer is placed immediately across the positive diagonal axis. The best location for the jammers is the

area immediately in front of two diagonally-positioned APs. Clearly, these results are greatly affected by the relative locations of each radio device.

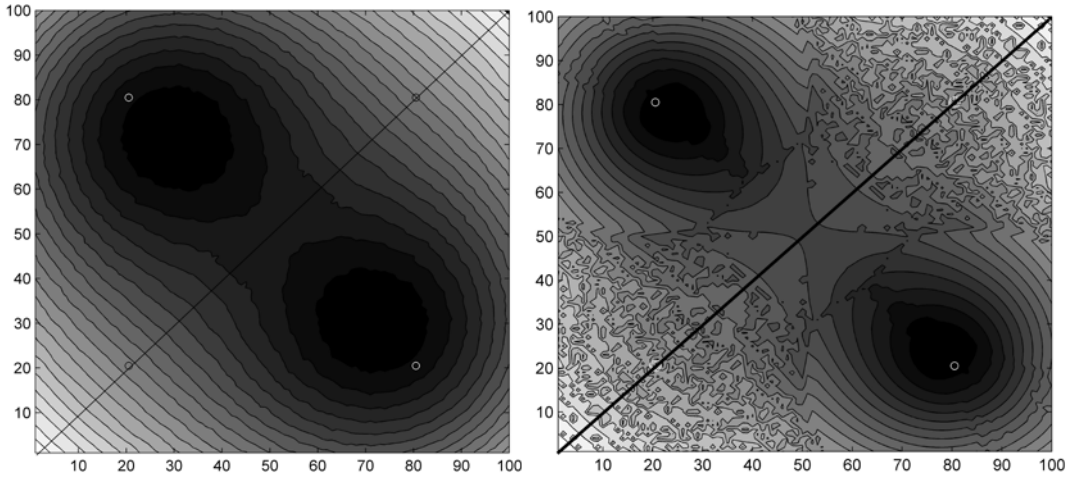


Figure 6. Contour plot of client coverage values (a) and network flow values (b) provided by four fixed APs (open circles) in the presence of two barrage jammers on flat terrain. The color at each (x,y) location indicates the overall client coverage value (a) or network flow value (b) when one jammer is placed at that location and the other jammer is placed immediately across the positive diagonal axis. Worse jamming attacks are indicated by darker areas.

B. EXPLORING THE DESIGNER'S PROBLEM

We briefly explore the designer's problem (4) of finding optimal locations for APs with jammers at fixed locations. While attempting to minimize the effects of jamming, the designer must consider the competing objectives of client coverage and network flow: network flow can be maximized by simply placing the APs as far as possible from the jammers (i.e., on the farthest border of the operating area), but such placement will likely provide very little client coverage. The optimal solution to the designer's problem balances these competing concerns.

We consider a scenario with one fixed jammer located in the center of the 100 x 100 operating area. The designer places two APs to minimize the damage incurred by the jammer. This problem is too large to enumerate within a reasonable amount of time (roughly 35 days with our computer), so we sample 10,000 random solutions; Figures 7 and 8 show the 25 best solutions, using a single-channel and barrage jammer, respectively. Individual solutions (consisting of a pair of AP locations) are depicted as

dots connected by a line. With a single-channel jammer (Figure 7), the best strategy in this scenario is to place the jammed AP far from the jammer and place the unjammed AP near the jammer, maximizing the utility of providing client coverage in the unjammed area. With a barrage jammer (Figure 8), the best strategy is to move the APs away from the jammer to a point that maximizes client coverage while balancing the competing requirement of network flow. In this scenario, these locations are in the corners of the operating area.

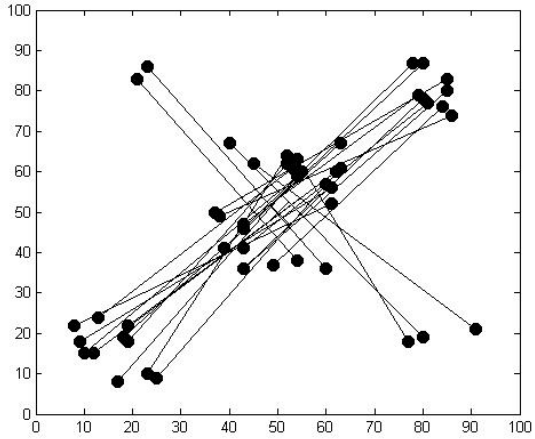


Figure 7. The 25 best of 10,000 randomly-sampled solutions for placing two APs in an operating area, with one single-client jammer in the center. Each solution is depicted by a line and two dots denoting the location of the APs.

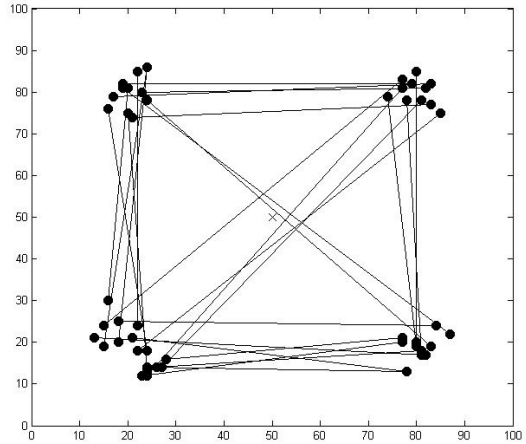


Figure 8. The 25 best of 10,000 randomly-sampled solutions for placing two APs in an operating area, with one barrage in the center. Each solution is depicted by a line and two dots denoting the location of the APs.

C. EXPLORING THE DAD PROBLEM

We now consider the full **DAD** problem, where the network designer determines the optimal strategy for minimizing the damage caused by the optimal jamming attack. Many variables affect the optimal solution to the operator's, attacker's, and designer's problems; an exhaustive analysis of these variables is beyond the scope of this report. We focus on interesting examples that are likely to occur in realistic conditions. We model our AP and jammer radio characteristics on the Cisco Aironet 1550 WMN AP, and our client devices on a generic internal 802.11n wireless interface card. We examine increasingly complex examples, gradually adding devices and eventually considering the effects of terrain. The results are presented in a tri-panel format, where the left panel depicts the best *unjammed solution* found (i.e., the designer's problem without jammers); the middle panel depicts the best *undefended solution* found when the attacker now jams the unjammed solution (i.e., the solution to the attacker's problem (3)); and the right panel depicts the best *defended solution* found when the designer chooses that network topology which minimizes the effects of the best jamming attack found (i.e., the **DAD** solution (5)). (Note that these panels represent the net results of our nested DIRECT optimization, which samples many different jamming attacks for many different network designs.) For each solution panel, the thickness of the lines between APs is directly proportional to delivered network flow. We run DIRECT until the solution objective values have not changed significantly for more than 10 function evaluations, or 20 master and subproblem iterations of DIRECT (whichever occurs first).

We first consider a network of four APs being attacked by one barrage jammer (see Figure 9), with the fixed HQ node located in the lower left of the operating area. In Figure 9(a), the designer places his four APs to cover most of the operating area. Given this fixed design, in Figure 9(b), the attacker places his barrage jammer in the middle of the operating area, greatly increasing client coverage shortfall and decreasing total delivered network flow. Finally, in Figure 9(c), the designer chooses a more dispersed network topology that minimizes the damage of the worst attack, generating reduced client coverage shortfall. In this case, the **DAD** solution does not provide more network flow than the undefended attacker's solution. (However, our tool stores alternate, runner-up solutions that often provide both increased client coverage and network flow.)

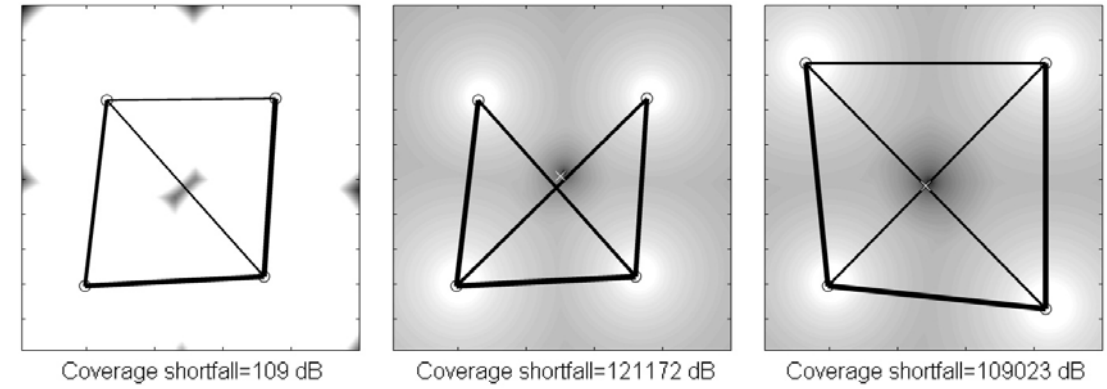


Figure 9. SRRA+C, attacker, and DA**D** solutions for a network of four APs and one barrage jammer on flat terrain.

In Figure 10, we add a second other jammer. The attacker now places each near an AP, rather than directly between the APs. In the **DA<u>D</u>** solution, the designer again chooses an AP topology that minimizes the effectiveness of a between-AP attack, but of course cannot overcome a direct-AP attack from a barrage jammer. Note that because the jammers have the same operating characteristics as the APs, the only way to completely eliminate client coverage is to place a jammer directly on top of an AP. In the **DA<u>D</u>** solution, this occurs in the upper-left, but the algorithm chooses a between-AP attack in the lower-right. The **DA<u>D</u>** solution decreases coverage shortfall and increases network flow over the undefended solution.

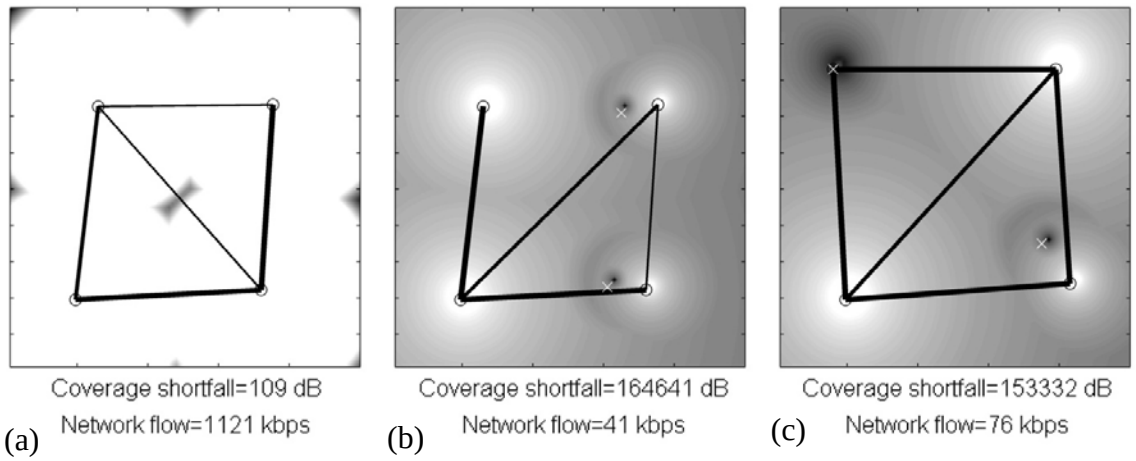


Figure 10. SRRA+C, designer, attacker, and DA**D** solutions for a network of four APs and two barrage jammers on flat terrain.

We next consider five APs in the presence of two barrage jammers in Figure 11, and five APs with three barrage jammers in Figure 12. With two jammers, the attacker

favors between-AP attacks, but with three jammers, he favors the direct-AP attack. As detailed earlier, there is a tension when placing barrage jammers: as a jammer gets nearer an AP, it more effectively jams that AP, but less effectively jams distant APs. As the ratio of jammers to APs increases, the direct-AP attack becomes more attractive because this tension slackens: distant APs are more likely to already be effectively jammed.

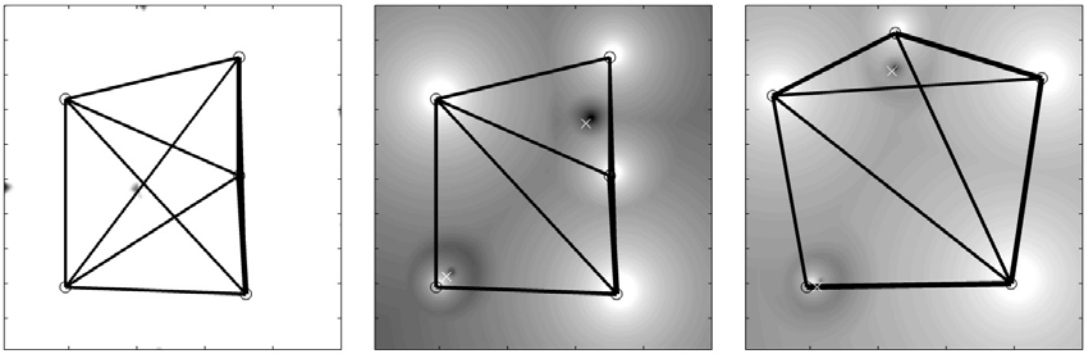


Figure 11. SRRA+C, designer, attacker, and DA<u>D</u> solutions for a network of five APs and two barrage jammers on flat terrain.

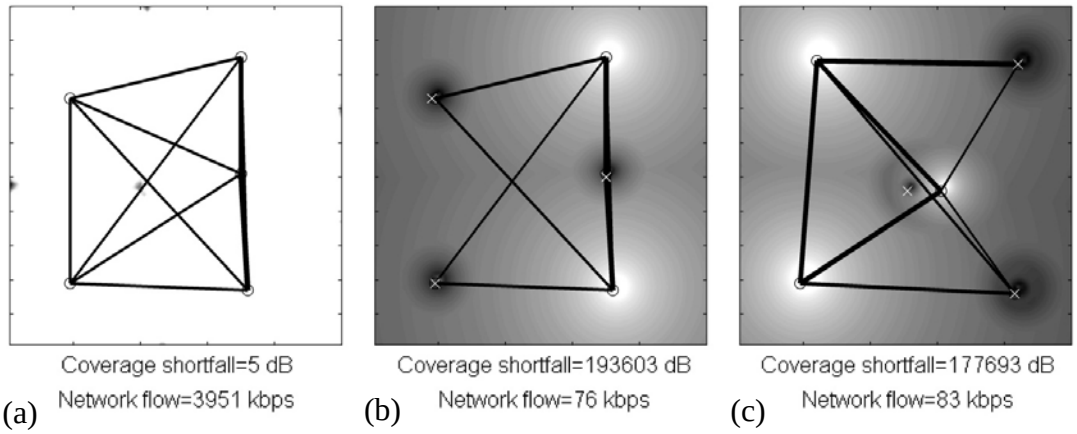


Figure 12. SRRA+C, designer, attacker, and DA<u>D</u> solutions for a network of five APs and three barrage jammers on flat terrain.

In Figure 13, we consider six APs in the presence of two barrage jammers. Rather than distributing the first five APs in the pattern depicted in Figures 11 and 12, the DIRECT algorithm finds a better overall solution can be obtained by placing APs in each corner, and placing the sixth AP in the lower right corner, directly next to another AP. This allows the algorithm to concurrently provide very good client coverage and delivered backhaul network flow, and may be reasonable in situations with many client

devices at that location. In the **DA<u>D</u>** solution, the designer chooses to avoid a potentially damaging double direct-AP attack by moving the sixth AP away from the corner. In Figure 14, we observe the same behavior in a network with six APs and three jammers.

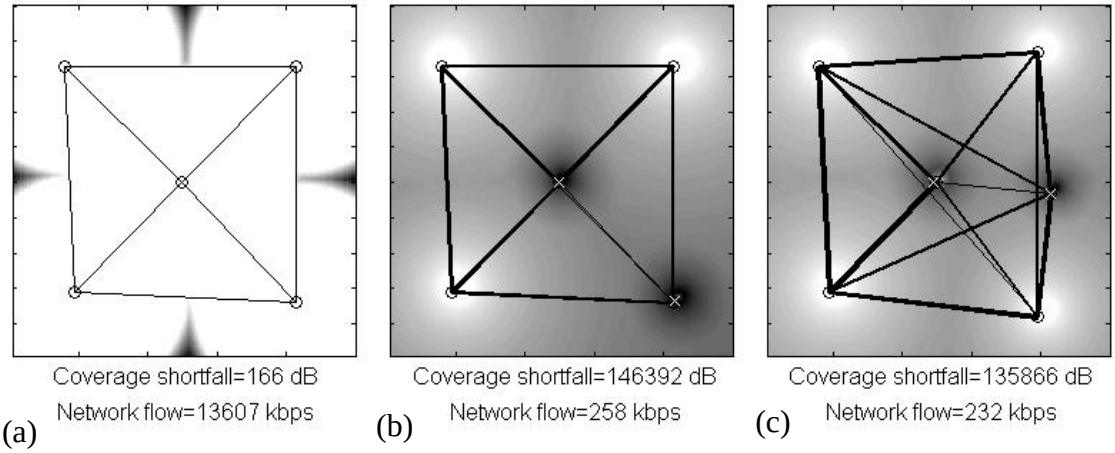


Figure 13. SRRA+C, designer, attacker, and DA<u>D</u> solutions for a network of six APs and two barrage jammers on flat terrain.

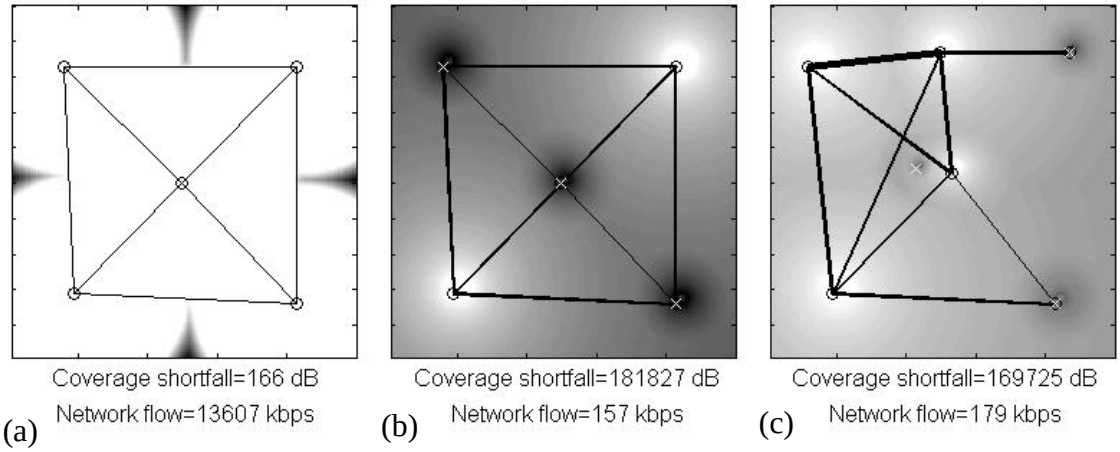


Figure 14. SRRA+C, designer, attacker, and DA<u>D</u> solutions for a network of six APs and three barrage jammers on flat terrain.

D. PERFORMANCE ANALYSIS

Using our tool, we compare the performance of our algorithm to exhaustive enumeration. Our algorithm places n-1 APs (i.e., the HQ node is assumed fixed in place) and m jammers in a continuous space. We can discretize this space by limiting feasible AP and jammer locations to a finite set. Using the same discretization scheme as that used to define the set of coverage regions R within the operating region, the number of

possible AP topologies is $\binom{|R|}{n-1}$, and for each AP topology there are $\binom{|R|}{m}$ possible jammer topologies, yielding $\binom{|R|}{n-1}\binom{|R|}{m}$ solutions to this discretized variant of the SRRA+C **DA<u>D</u>** problem. The exponential increase in the number of solutions as *n*, *m*, and $|R|$ grow restricts the use of this enumeration method to trivially small problems, but we provide a few examples to demonstrate the performance of the DIRECT algorithm.

It is not valid to compare the **DA<u>D</u>** solutions found using DIRECT and exhaustive enumeration by simply determining which produces a lower overall objective value. If our goal was simply to find the lowest overall value, we could set DIRECT to run with very few subproblem iterations. This would prevent DIRECT from finding good jamming attacks and yield a low overall objective value; however, our goal is to find those WMN designs that are most robust to jamming attacks. To demonstrate the performance of DIRECT in finding such designs, we use DIRECT to attack the best (i.e., most interference-robust) AP design found using enumeration. We then use enumeration to attack the best AP design found using DIRECT.

Consider a small, flat, operating region discretized into $10 \times 10 = 100$ coverage regions. Using the described discretization scheme, we first enumerate all possible discrete solutions for WMNs consisting of two APs and one jammer, three APs and one jammer, and two APs and two jammers. We then use DIRECT to attack the fixed AP topology of the best **DA<u>D</u>** solution found using enumeration, and present the results in Table 1. Bold values indicate that the DIRECT method obtains a worse jamming attack than enumeration. DIRECT does this in each case, and does so in less than a second of processing time.

		DA<u>D</u> Solved Using Enumeration			DIRECT Attack		
n	*m*	Function Evaluations	Overall Value	Runtime (hr:min:sec)	Function Evaluations	Overall Value	Runtime (hr:min:sec)
2	1	4,950	642.73	0:00:49	123	**703.78**	0:00:0.7
3	1	495,000	472.317	1:40:56	101	**502.74**	0:00:1
2	2	495,000	5268.58	0:41:37	167	**6087.93**	0:00:1
3	2	24,502,500	933.43	53:54:27	103	**1019.68**	0:00:1

Table 1. DIRECT barrage jamming attacks on designs obtained using discrete enumeration. In each case, DIRECT is able to find an attack that provides greater damage than that found using enumeration.

In Table 2, we do the opposite: we use DIRECT to find **DAD** solutions and then use enumeration to attack the fixed AP topology of the best one. Bold values indicate that the DIRECT method found worse jamming attacks than the enumeration method. In no case does the enumeration method yield an attack more damaging than that found using DIRECT. While these results demonstrate instances where DIRECT is more effective and efficient than discrete enumeration in quickly finding interference-robust WMN topologies, this is not a fair comparison. DIRECT is a continuous algorithm, able to place APs and jammers anywhere within the operating region, whereas discrete enumeration is limited to placing these nodes at fixed, finite locations. Hence, DIRECT is guaranteed to eventually find a solution at least as good as discrete enumeration. Future research could compare the use of DIRECT to other algorithms, such as genetic or simulated annealing algorithms (see, e.g., Serafino, Liuzzi, Piccialli, Riccio, and Toraldo, 2011).

		DAD Solved Using DIRECT			Enumerated Attack		
n	*m*	Function Evaluations	Overall Value	Runtime (hr:min:sec)	Function Evaluations	Overall Value	Runtime (hr:min:sec)
2	1	11,249	**703.52**	0:00:41	100	701.52	0:00:1.0
3	1	5,591	**561.98**	0:00:50	100	539.94	0:00:1.0
2	2	6,447	**3909.00**	0:00:27	4,950	2003.40	0:00:27
3	2	33,963	**1387.69**	0:09:22	4,950	945.59	0:01:2.0

Table 2. Enumerated barrage jamming attacks on designs obtained using DIRECT. In no case is the enumeration method able to find an attack that provides greater damage than that found using DIRECT.

We next analyze the performance of our algorithm using the 50-node network considered by Xiao et al. (2004) and Shankar (2008) on the same $10 \times 10 = 100$ flat coverage region. We denote five nodes as destinations for traffic (indicated by large black circles in Figure 15), but unlike these authors, we allow any node to serve as a source for network traffic. (This follows from our assumption that each AP will be servicing client devices in the surrounding area.) Shankar uses enumeration to calculate the damage incurred by iteratively placing jammers at locations defined by a fixed grid. Using our SRRA+C formulation with one and two jammers, we compare attacks generated using Shankar's enumeration method to those generated using our DIRECT method. The results are presented in Table 3. In both cases, DIRECT is able to find a

more damaging attack than the enumeration method, and does so in considerably less time.

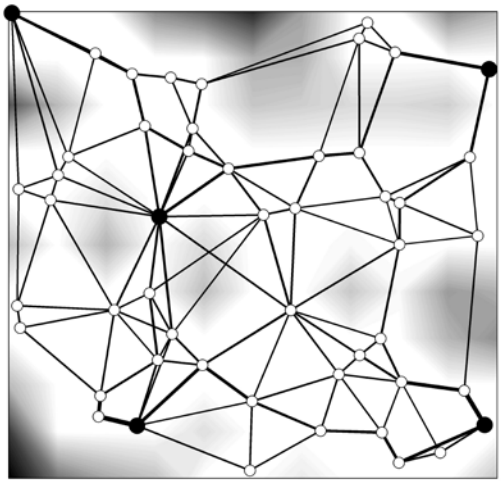


Figure 15. SRRA+C analysis of the 50-node network considered by Xiao et al. (2004) without jammers. The large black nodes denote traffic destinations. Client coverage shortfall is indicated by shaded areas. Line thickness is proportional to the traffic flow along each respective link.

	Enumerated Attack			DIRECT Attack		
m	Function Evaluations	Overall Value	Runtime (hr:min:sec)	Function Evaluations	Overall Value	Runtime (hr:min:sec)
1	100	376.16	0:51:55	7	**421.96**	0:03:36
2	4,950	871.15	55:02:7	25	**963.45**	0:25:45

Table 3. Comparison of enumerated and DIRECT attacks using one and two jammers against the 50-node network considered by Xiao et al. (2004) and Shankar (2008). In each case, DIRECT is able to find a more damaging attack in considerably less time.

E. THE COMPLICATING EFFECTS OF TERRAIN

While simple rules-of-thumb such as "Place barrage jammers between APs" may be useful when designing WMNs for flat surfaces, the effects of terrain greatly complicate the problem. We conduct a case study using our algorithm to consider the effects of terrain. Our operating area is a 116-acre section on Ft. Ord, California, gridded into a $73 \times 73 = 5,329$ coverage region. The area has gently rolling hills, a large parking lot, a stadium, and several roads. We use elevation data from the National Elevation Dataset (NED) provided by the United States Geological Survey (USGS, 2013) via MapMart (2009). Elevation in the operating area varies from 98 to 226 feet.

Figure 16(a) is a contour plot of the elevation, and Figure 16(b) is a Google Maps (2013) image of the area.

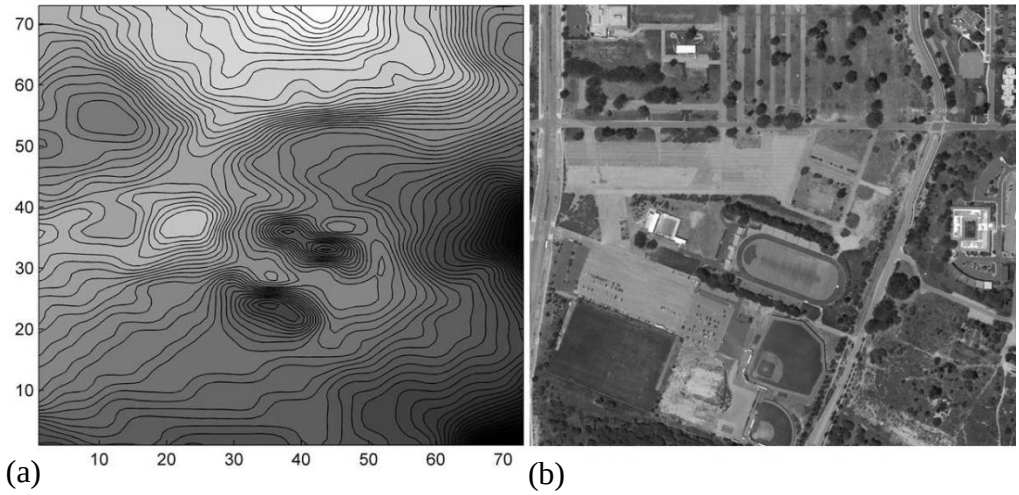


Figure 16. Elevation contour map (a) and Google Maps (2013) image (b) of the 116 acre operating area on Ft. Ord, CA.

Modeling the same Cisco Aironet WMN APs as before, we first consider the optimal placement for one barrage jammer among four APs at fixed locations. Figure 17 depicts the client coverage provided by four APs arranged in a square about 160 meters across. As in Figure 5, we fix the four APs and place one barrage jammer at each of the 5,329 regions *r*. Figure 17(a) depicts the client coverage and Figure 17(b) depicts network flow values when the jammer is placed at each location. Unlike the results on flat terrain, the results here are highly nonlinear and cannot be prescribed using simple rules-of-thumb. Placing a barrage jammer at each of the four fixed APs results in very different outcomes. For example, placing the jammer at the lower-left AP location provides only moderate client coverage jamming, but provides the worst backhaul jamming among the four AP locations. Our algorithm and tool can help network designers quickly find good solutions to such nonlinear problems.

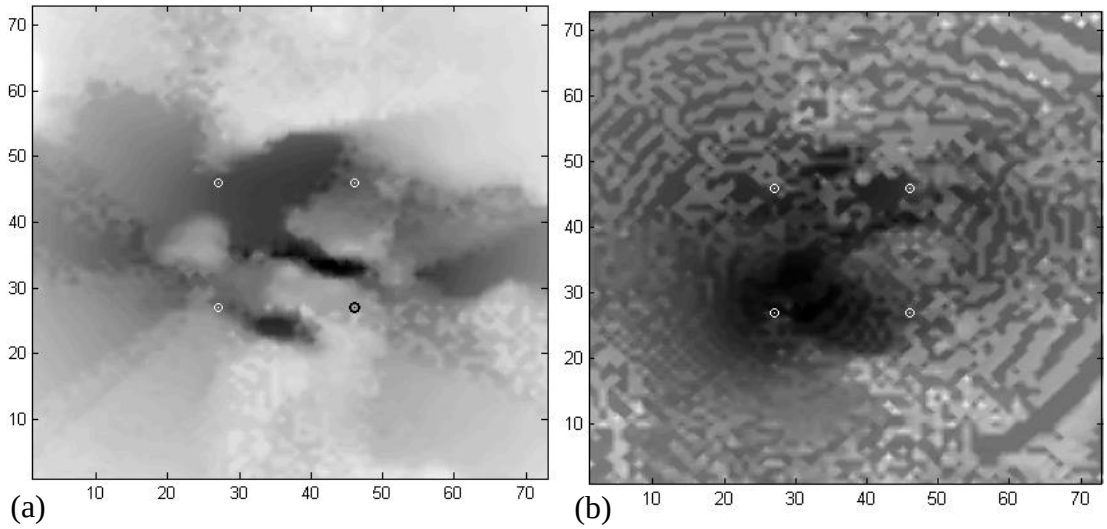
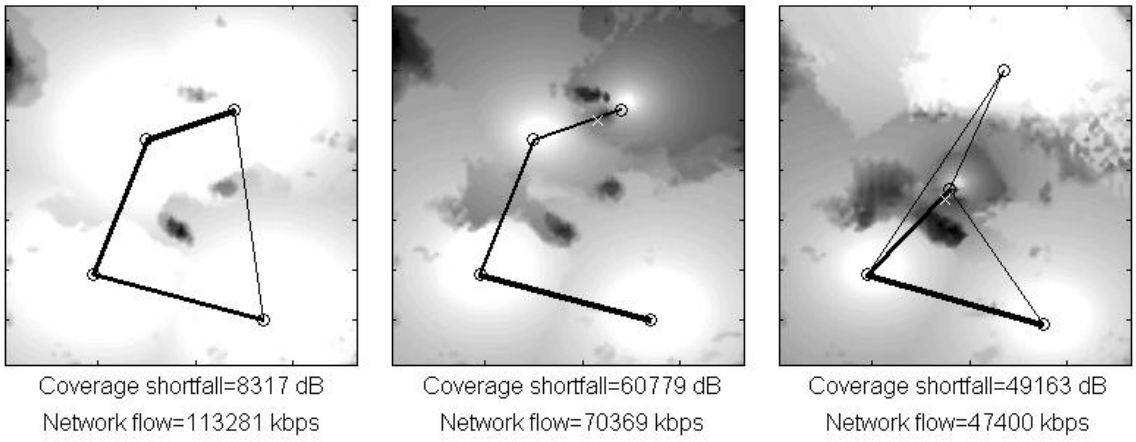


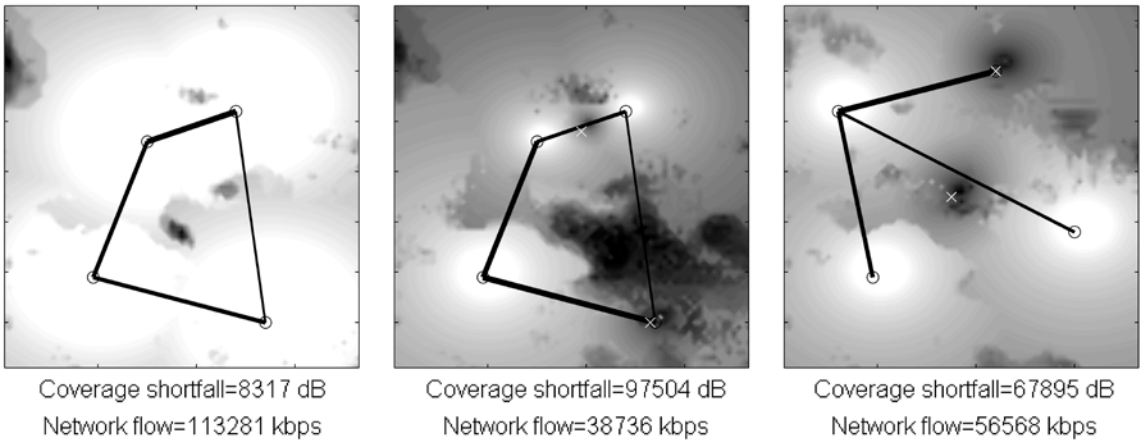
Figure 17. Contour plot of client coverage values (a) and network flow values (b) provided by four fixed APs (open circles) in the presence of one barrage jammer on real terrain. The color at each (*x*,*y*) location indicates the overall client coverage value (a) or network flow value (b) when a jammer is placed at that location (worse jamming attacks are indicated by darker areas).

As in the previous section, we now examine the unjammed (i.e., SRRA+C), undefended, and defended solution in tri-panel format. The results of four APs and one barrage jammer are depicted in Figure 18. By placing the barrage jammer between two APs in the undefended solution, the attacker does considerable damage to the network. In the defended solution, the attacker again chooses a between-AP attack, but the designer chooses locations for the APs that reduce the damage done to client coverage. With two barrage jammers (Figure 19), the attacker places the first jammer in a position near that chosen in the two-jammer scenario, and places the second jammer in a direct-AP attack. By varying the value of *w* (here set to one), our algorithm will find AP topologies that both decrease client coverage shortfall and increase delivered network flow over the undefended solution.



(a) (b) (c)

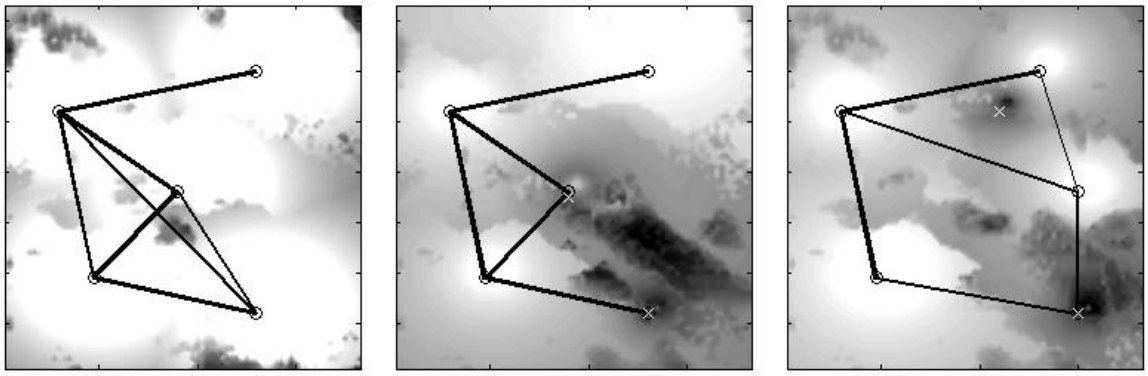
Figure 18. SRRA+C designer, attacker, and DA<u>D</u> solutions for a network of four APs and one barrage jammer on Ft. Ord terrain.



(a) (b) (c)

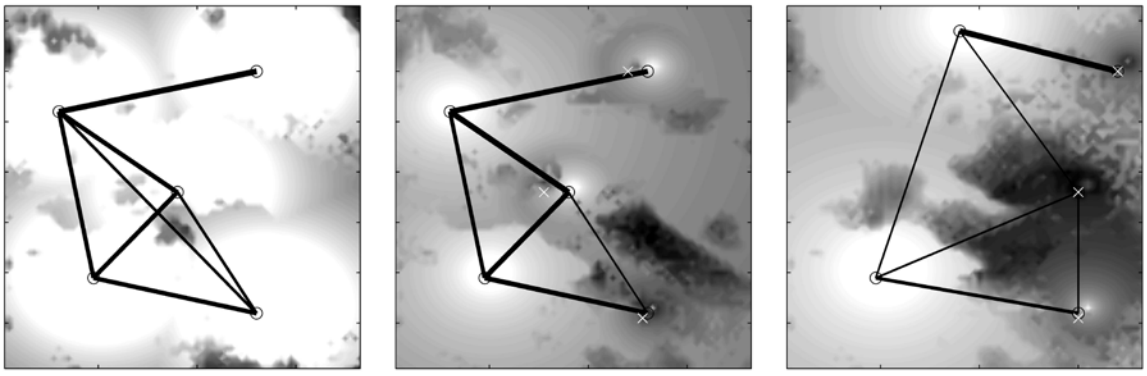
Figure 19. SRRA+C designer, attacker, and DA<u>D</u> solutions for a network of four APs and two barrage jammers on Ft. Ord terrain.

In Figures 20 and 21, we consider networks of five APs and, respectively, two and three barrage jammers. In each undefended solution, the attack chooses direct-AP attacks for each jammer. In the **DA<u>D</u>** solution, the designer places the APs farther apart.



(a) (b) (c)

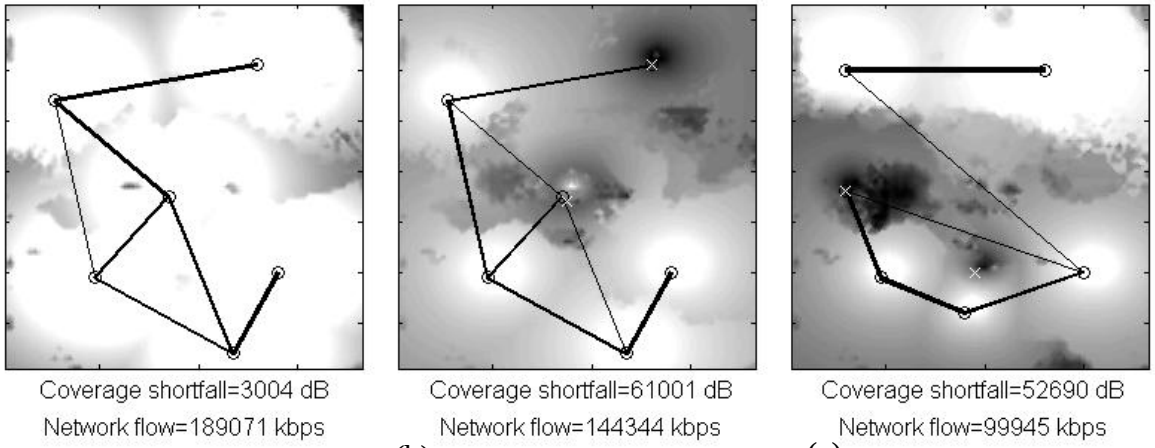
Figure 20. SRRA+C designer, attacker, and DA<u>D</u> solutions for a network of five APs and two barrage jammers on Ft. Ord terrain.



(a) (b) (c)

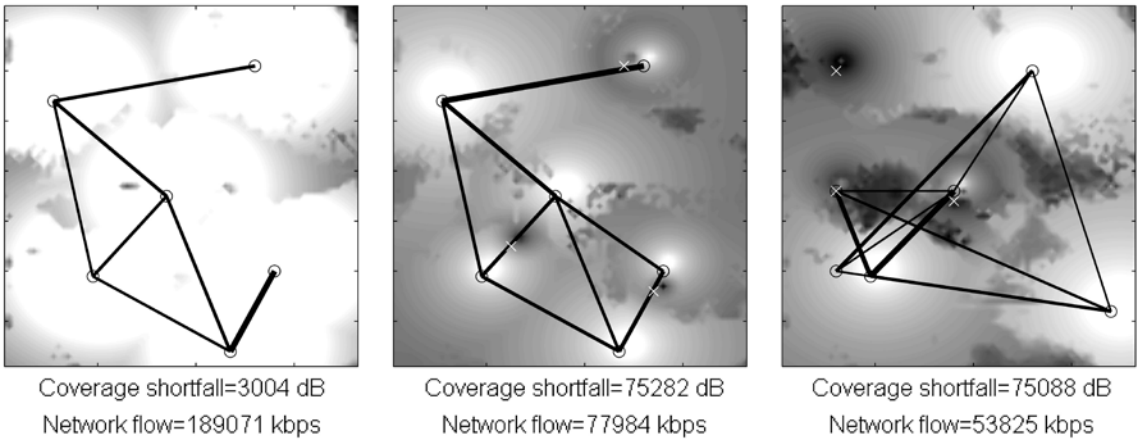
Figure 21. SRRA+C designer, attacker, and DA<u>D</u> solutions for a network of five APs and three barrage jammers on Ft. Ord terrain.

In Figure 22 (six APs and two jammers), the attacker again chooses direct-AP attacks in the undefended solution. In the **DA<u>D</u>** solution, the attacker nearly severs the top two APs from the rest of the network: traffic between these two segments is less than 8 kbps. As noted, our formulation disincentives complete disconnection because SRRA (see Appendix) provides an infinite penalty if a destination node does not receive any network flow. In Figure 23, we consider six APs and three barrage jammers. In this case, the attacker essentially denies the use of the upper-left portion of the operating area. This forces the designer to place his APs close together in the lower-right portion of the operating area and causing considerable damage to client coverage.



(a) (b) (c)

Figure 22. SRRA+C designer, attacker, and DAD solutions for a network of six APs and two barrage jammers on Ft. Ord terrain.



(a) (b) (c)

Figure 23. SRRA+C designer, attacker, and DAD solutions for a network of six APs and three barrage jammers on Ft. Ord terrain.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

The vast number and complex interactions of factors affecting the performance of WMNs require that any model of WMNs must incorporate simplifying assumptions to be computationally feasible. In this work, our model of WMN performance is based on arguably the most fundamental factor in wireless communications: the transmission and reception of EM energy over terrain (Molish, 2011). Using the game theoretic **DAD** framework, and based on our SRRA+C model of WMN performance, we develop a method for quickly designing WMNs that are robust to the effects of EMI. While our approach specifically considers avoiding the damage caused by the use of simple noise jammers, our approach can be generalized to any form of EMI where network degradation is a function of distance from the jamming source.

Within the context of our model, we find that the optimal attack strategy using single-channel jammers is a simple direct-AP attack, placing the jammer directly atop an AP operating on the same channel. The optimal defensive strategy against such an attack is to place redundant devices nearby, operating on separate channels. (In reality, such inefficient use of resources is often avoided through the use of spread spectrum or frequency-hopping technology, not considered in this work.) The optimal attack strategy using barrage jammers is generally a between-AP attack, placing jammers between APs to concurrently degrade the service provided by two or more APs. Defensive strategies include moving APs farther apart to minimize concurrent damage, and finding terrain locations negating the impact of between-AP attacks.

As we have demonstrated, however, the relative number and location of devices, their positions, and the effects of terrain greatly complicate WMN design strategy. Our decision-support tool quickly prescribes good WMN topologies, considering radio operating characteristics, the relative importance of client coverage and network flow, and the effects of radio propagation over terrain. Our tool provides reasonably good approximations of network performance, and does so quickly and without guesswork.

A. OTHER INTERPRETATIONS OF SRRA+C

The **DAD** SRRA+C formulation may be useful in modeling the interactions of other, similar systems where areas (whether physical or logical) need to be serviced by a fixed number of interconnected entities and need to be robust to worst-case disruption. For instance, the formulation could be applied to a logistics network or facility location problem (e.g., Church, Scaparra, and Middleton, 2004), where warehouses (i.e., APs) need to distribute goods to customers in known locations (i.e., client coverage areas). Overlapping warehouse coverage may be inefficient, increasing the incentive to place warehouses far apart, but greater distances between warehouses may incur additional transportation costs or time lags. Road construction, traffic jams, or natural disasters (i.e., jammers) could be modeled to create a disruption-robust warehouse topology.

Another application area may be electrical distribution systems, where substations (i.e., APs) need to service client areas. While some overlap in client coverage may be beneficial in minimizing the effects of local outages, too much overlap is financially inefficient. Further, increased distances between substations incur greater transmission losses. Blown transformers, fallen trees, and intentional attacks (i.e., jammers) could be modeled to increase the robustness of the electrical network to worst-case attack.

B. FUTURE WORK

Our model of WMN performance makes many simplifying assumptions. Future research could consider the effects of electromagnetic phase or use a more accurate method of calculating channel capacity to increase model fidelity. The modular nature of our formulation allows essentially any WMN model to be substituted, including high-fidelity simulators like OPNET (Riverbed Technology, 2013), but increased fidelity will incur increased runtimes and possibly less tractability.

We consider only one type of defense to jamming: placing APs in jamming-robust locations. Future research could consider other defenses, such as the use of directional antennae as recommended by Ståhlberg (2000). Antenna direction could be modeled as a continuous decision variable, allowing the use of the DIRECT algorithm. Directionality would affect both backhaul network performance and client coverage, introducing interesting new tensions to the model.

As noted, our approach finds the Stackelberg equilibrium, but not the Nash equilibrium. Glicksberg (1952) proves the existence of a mixed strategy Nash equilibrium in a game with continuous payouts and *compact* strategy spaces. Our problem satisfies both of these conditions if the operator's variables *S*, *F*, *T*, and *P* (see Appendix) are bounded. Future research could consider methods of determining the Nash equilibrium of our problem.

Another area of interest is the use of our formulation in creating much larger networks (i.e., 100 or more APs). Due to the curse of dimensionality and the high rate of growth in computing time as a function of the number of objects being placed, we may examine the iterative use of DIRECT to design small networks and then combine them into larger networks.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX: DERIVATION OF JAMMER-COGNIZANT SRRA+C FORMULATION

We quantify the value of a particular WMN topology in the presence of EMI by building on the SRRA+C formulation of Nicholas and Alderson (2012). We first calculate the value of coverage provided to client devices $Z_{coverage}$, and then calculate the value of delivered backhaul network flow Z_{flow}.

A. CALCULATING CLIENT COVERAGE

The client coverage provided by a WMN topology is a function of its AP and jammer locations. Given these locations, we adopt the approach of Nicholas and Alderson (2012) and quantify the value of client coverage by first calculating the *received signal strength* (*RSS*) in Decibel-milliwatts (dBm from each discrete coverage region $r \in R$ from each AP node i or jammer node k (and the reverse path) using the standard link budget formula (Olexa, 2005):

$$RSS = power_{tx} + g_{tx} - l_{tx} - l_{path} - l_{misc} + g_{rx} - l_{rx},$$

where $power_{tx}$ is transmission power in dBm, g_{tx} and g_{rx} are, respectively, the gains of the transmitter and receiver in dBi, l_{tx} and l_{rx} are, respectively, the losses (i.e., from cables, connectors, etc.) of the transmitter and receiver in dB, l_{path} is the total path loss in Decibels (dB), and l_{misc} is the miscellaneous loss (such as fade margin) in dB. Using Equation (1), we define ρ_{ir} (ρ_{ri}) as the received signal strength from (to) a transmitting AP node i to (from) coverage region r, and η_{kr} (η_{ki}) as the received signal strength from a transmitting jammer node k to coverage region r (AP i). All of the terms in Equation (1) are input data, determined by the equipment technical characteristics, except for the total path loss l_{path}, which depends on the position of the transmitting device (a client device, AP node λ_i, or jammer node χ_k).

We can use any method for computing l_{path}, such as a simple inverse-square calculation, the Irregular Terrain Model (ITM) (Longley & Rice, 1968), or Hata-COST 231 (COST, 1999). We prefer the Terrain Integrated Rough Earth Model (TIREM) of Alion Science & Technology Corporation (Alion, 2013). This model computes path loss

by sampling terrain elevation at fixed points between transmitter and receiver. It considers the effects of free space loss, diffraction, and atmospheric absorption and reflection, but does not consider foliage, buildings, or other nonterrain obstructions. While TIREM is computationally more expensive than simpler models, it provides fairly accurate results. For line-of-sight propagation in commonly-used frequency ranges, Eppink and Kuebler (1994) compare TIREM predictions and actual measurements. They find a difference with a mean of –2.8 dB and a standard deviation of 8.9 dB, which is very accurate considering the relative simplicity of the model. In previous work (Nicholas & Alderson, 2012), we find TIREM reasonably predicts Cisco Aironet WMN AP (Cisco, 2013) performance during field testing.

We adopt and modify the technique of Nicholas and Alderson (2012) to quantify the value of client coverage. We first calculate in dBm the total *interference* received at region $r \in R$ and AP node $i \in N$. Following Ståhlberg (2000), we assume the cumulative effects of jamming sources on the same channel are additive (in watts) at each receiver. We thus obtain:

$$Interference_r \equiv 10\log_{10}\left(1000\sum_{k\in M}\frac{10^{\eta_{kr}/10}}{1000}\right) = 10\log_{10}\sum_{k\in M}10^{\eta_{kr}/10} \qquad \forall r \in R$$

$$Interference_i \equiv 10\log_{10}\left(1000\sum_{k\in M}\frac{10^{\eta_{ki}/10}}{1000}\right) = 10\log_{10}\sum_{k\in M}10^{\eta_{ki}/10} \qquad \forall i \in N.$$

Next, we calculate in dB the *signal-to-interference ratio* (*SIR*) σ between each region $r \in R$ and AP node $i \in N$. SIR is arguably the most important measure of how well a signal is received (Poisel, 2011). We calculate this quantity in both directions (*i* to *r* and *r* to *i*), as two-way communication is necessary for a client device to successfully exchange traffic with an AP, and terrain, obstructions, and the effects of EMI may cause these quantities to be very different (Freeman, 2006).

$$\left(Signal\ to\ Interference\ Ratio\right)_{ir} = \sigma_{ir} \equiv \rho_{ir} - interference_r \qquad \forall i \in N, \forall r \in R$$

$$\left(Signal\ to\ Interference\ Ratio\right)_{ri} = \sigma_{ri} \equiv \rho_{ri} - interference_i \qquad \forall r \in R, \forall i \in N.$$

We define τ as the minimum allowable SIR or *sensitivity threshold* in dB for each region $r \in R$ and AP node $i \in N$. Higher τ values indicate a higher priority or a requirement for a higher quality signal and thus greater data transfer rates (we typically

use a value of 10 dB). A positive difference of τ and σ indicates insufficient signal quality. We calculate this *client coverage shortfall* between region *r* and AP node *i*. We penalize the weakest component of the bidirectional link between the AP and region (i.e., the link with the greatest coverage shortfall):

$$\left(Coverage\ Shortfall\right)_{ir} \equiv \max_{i\in N, r\in R}\left(\left(\tau_r - \sigma_{ir}\right)_+, \left(\tau_i - \sigma_{ri}\right)_+\right),$$

where $()_+$ denotes the projection onto the nonnegative real line. Because a positive difference represents inadequate client coverage, we wish to minimize this quantity. We need consider only the minimum coverage shortfall from each AP node $i \in N$, as we assume each client device will connect only to that AP with the strongest available σ_{ir}. We sum over all $r \in R$ to calculate *total coverage shortfall*, denoted $Z_{coverage}$:

$$Z_{coverage}\left(\lambda, \chi\right) = \left(Total\ Coverage\ Shortfall\right) \equiv \sum_{r\in R} \min_{i\in N}\left\{\max\left(\left(\tau_r - \sigma_{ir}\right)_+, \left(\tau_i - \sigma_{ri}\right)_+\right)\right\}.$$

The total coverage shortfall is a function of AP node locations λ and EMI node locations χ. By allowing only positive terms, we disallow the benefit of transmitting received power to any given coverage region.

B. CALCULATING NETWORK FLOW

To assess the value of network flow, we first calculate arc capacities between each node using the Shannon capacity formula (1949), which establishes a theoretical upper bound on transmission capacity in bits per second (bps). Following Xiao et al. (2004), the capacity from AP node *i* to *j* in bps is:

$$\left(Capacity\right)_{ij} = bandwidth \log_2\left(1 + \frac{gain_{ij}}{interference_j loss_{ij}} P_{ij}\right) \quad \forall\left(i, j\right) \in A,$$

where *bandwidth* is channel bandwidth in Hertz and $gain_{ij}$ is the sum of the antilog gain terms (g_{tx} and g_{rx}). $Loss_{ij}$ is the sum of the antilog loss terms (l_{tx}, l_{rx}, l_{path}, and l_{misc}) from AP node *i* to *j*. Note $interference_j$ is converted to watts; we simplify the notation for clarity. These input data are calculated by the known locations of AP node locations λ and jammer node locations χ. We assume each AP has limited total transmission power denoted p_i (in watts), and we define P_{ij} to be the fraction of p_i used to transmit from *i* to *j*.

Thus, each AP is additionally constrained by

$$\sum_{j:(i,j)\in A} P_{ij} \leq p_i.$$

Here, P_{ij} is a decision variable representing the AP-to-AP transmission power from node *i* to node *j*, whereas the transmission powers for AP-to-client, jammer-to-client, and jammer-to-AP $power_{tx}$ is a (constant) input parameter. By calculating the capacity of each arc separately and not considering the effects of handshake dialogues or error correction, our model roughly approximates user datagram protocol (UDP) traffic transmission (Postel, 1980).

We measure each individual traffic flow in bps. We adopt the approach of Xiao et al. (2004) to quantify the value of total network flow according to a log-utility function that places a zero value on unit flow, positive values on flows greater than one, and negative values on flows less than one. Note that a zero flow has an infinite penalty, and therefore there is strong incentive to ensure that each source-destination pair receives some flow. Defining S_i^d to be the total flow originating at node *i* and destined for node *d*, we have

$$\left(Utility\ of\ Total\ Network\ Flow\right) \equiv \sum_d \sum_{i \neq d} \log_2\left(S_i^d\right). \tag{6}$$

Collectively, we obtain our version of the Xiao et al. (2004) SRRA problem to calculate the value of network flow, denoted Z_{flow}:

Formulation **SRRA**

Index Use

$i \in N$	AP node (*alias j*)	
$k \in M$	jammer node	
$(i, j) \in A$	directed arc (*link*)	
$d \in D \subseteq N$	destination node	

Input Data

$\hat{\lambda}_i$	locations of AP nodes, $\hat{\lambda} = \left\{ \hat{\lambda}_i, i \in N \right\}$	[none]
$\hat{\chi}_k$	locations of jammer nodes, $\hat{\chi} = \left\{ \hat{\chi}_k, k \in M \right\}$	[none]
p_i	maximum total transmission power per AP node, $i \in N$	[watts]
bandwidth	channel bandwidth	[hertz]

Calculated Data

$gain_{ij}$	product of antilog gain terms from $i \in N$ to $j \in N$	[none]
$loss_{ij}$	product of antilog loss terms from $i \in N$ to $j \in N$	[none]
$interference_j$	Total received EMI and background noise power at $j \in N$	[watts]

Decision Variables

S_i^d	total flow of traffic from origin $i \in N$ to destination $d \in D$	[bps]
F_{ij}^d	traffic flow along arc $(i, j) \in A$ to destination $d \in D$	[bps]
T_{ij}	total flow along arc $(i, j) \in A$	[bps]
P_{ij}	total transmission power along arc $(i, j) \in A$	[watts]

Formulation

$$Z_{flow}\left(\hat{\lambda}, \hat{\chi}\right) = \max_{S,F,T,P} \sum_d \sum_{i \neq d} \log_2\left(S_i^d\right) \qquad (S0)$$

s.t.

$$\sum_{i:(j,i)\in A} F_{ji}^d - \sum_{i:(i,j)\in A} F_{ij}^d = S_j^d \qquad \forall j \in N,\ \forall d \in D \qquad (S1)$$

$$T_{ij} = \sum_d F_{ij}^d \qquad \forall (i,j) \in A \qquad (S2)$$

$$T_{ij} - bandwidth \log_2\left(1 + \frac{gain_{ij}}{interference_j loss_{ij}} P_{ij}\right) \leq 0 \qquad \forall (i,j) \in A \qquad (S3)$$

$$\sum_{j:(i,j)\in A} P_{ij} \leq p_i \qquad \forall i \in N \qquad (S4)$$

$$S_i^d \geq 0 \qquad i \neq d \qquad (S5)$$

$$F_{ij}^d \geq 0 \qquad \forall (i,j) \in A,\ \forall d \in D \qquad (S6)$$

$$T_{ij} \geq 0 \qquad \forall (i,j) \in A \qquad (S7)$$

$$P_{ij} \geq 0 \qquad \forall (i,j) \in A \qquad (S8)$$

Given AP locations $\hat{\lambda}$ and jammer locations $\hat{\chi}$, this is a multicommodity network flow problem. The objective function (S0) maximizes the total utility of traffic flow between each source-destination pair. Constraints (S1) ensure balance of flow at each AP node. Constraints (S2) define the total flow along any arc as the sum of all traffic flows along that arc. Constraints (S3) ensure that total flow along any arc is less than or equal to the arc capacity. Constraints (S4) restrict total transmission power at each AP. Constraints (S5-S8) ensure nonnegativity.

C. OVERALL OBJECTIVE FUNCTION

The overall jammer-cognizant SRRA+C objective function is obtained using a linear combination of client coverage (calculated as client coverage shortfall) and network flow (calculated via the SRRA problem):

$$Z\left(\hat{\lambda},\hat{\chi}\right) \equiv Z_{coverage}\left(\hat{\lambda},\hat{\chi}\right) - wZ_{flow}\left(\hat{\lambda},\hat{\chi}\right).$$

Combining the value of network coverage with the value of network flow as an *elastic constraint* (Bazaraa, Sherali, and Shetty, 2006, p. 28) in the objective function ensures the problem is continuous, a requirement for the DIRECT algorithm (described below). We use w as a positive scalar representing the relative importance of network flow. Larger values of w indicate network flow is of greater importance and, in general, increase network flow by valuing more compact network topologies. See Nicholas (2009) for a detailed sensitivity analysis of w.

SRRA+C is our simplified model of WMN operations. There are many higher-fidelity models available, but with an increase in modeling fidelity, generally comes an increase in computational complexity and runtime. Heeding the warning of Alderson et al. (2011) against the use of untested surrogate models for real-world infrastructure analysis, in Nicholas and Alderson (2012) we conduct field-testing with SRRA+C (without jammers) and find it can provide results that fairly approximate real WMNs.

LIST OF REFERENCES

Alderson, D.L., Brown, G.G., & Carlyle, W.M. (2014). Assessing and improving operational resilience of critical infrastructures and other systems. In A. Newman & J. Leung (Eds.), *Tutorials in Operations Research: Bridging Data and Decision* (pp. 180–215). Hanover, MD: Institute for Operations Research and Management Science.

Alderson, D.L., Brown, G.G., Carlyle, W.M., & Wood, R.K. (2011). Solving defender-attacker-defender models for infrastructure defense. In R.K. Wood & R.F. Dell (Eds.), *Operations Research, Computing, and Homeland Defense* (pp. 28–49). Hanover, MD: INFORMS.

Alion Science and Technology Corporation. (2013). TIREM details. Retrieved from http://www.alionscience.com/en/Technologies/Wireless-Spectrum-Management/TIREM.

Audet, C. (2004). Mesh adaptive direct search algorithms for constrained optimization. *SIAM Journal on Optimization*, *17*(1), 188–217.

Bazaraa, M.S., Sherali, H.D., & Shetty, C.M. (2006). *Nonlinear programming: Theory and algorithms*. Hoboken, NJ: John Wiley and Sons.

Bellman, R.E. (1961). *Adaptive control processes: A guided tour*. Princeton, NJ: Princeton University Press.

Bertsekas, D. (1999). *Nonlinear programming*. Belmont, MA: Athena Scientific.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces*, *36*(6), 530–544.

Caro, D. (2007). Users fear wireless networks for control. *InTech Magazine*, 1 May 2007. Retrieved from http://lists.jammed.com/ISN/2007/05/0122.html.

Church, R., Scaparra, M., & Middleton, R. (2004). Identifying critical infrastructure: The median and covering facility interdiction problems. *Annals of the Association of American Geographers*, *94*(3), 491–502.

COST (European Cooperation in the Field of Scientific and Technical Research). (1999). Digital mobile radio towards future generation systems: COST 231 Final Report.

Cox, J. (2007). Xbox accused of jamming WLANs. *Network World*, 14 December 2007. Retrieved from http://news.techworld.com/mobile-wireless/10941/xbox-accused-of-jamming-wlans/.

Cruz, J.B. (1975). Survey of Nash and Stackelberg equilibrium strategies in dynamic games. *Annals of Economic and Social Measurement*, *4*(2), 339–344.

Economist, The. (2011). GPS jamming: No jam tomorrow. 10 March 2011.

Eppink, D., & Kuebler, W. (1994). *TIREM/SEM handbook*. Electromagnetic Compatibility Analysis Center, Annapolis, MD: Department of Defense.

Freeman, R. (2006). *Radio systems design for telecommunication*. New York, NY: Wiley-IEEE.

Fudenberg, D., & Tirole, J. (1991). *Game theory*. Cambridge, MA: MIT.

Glicksberg, I.L. (1952). A further generalization of the Kakutani Fixed Point Theorem, with application to Nash equilibrium. *Proceedings of the American Mathematical Society*, *3*(1), 170–174.

Google Maps. (2013). Retrieved from http://maps.google.com/.

Hastie, T., Tibshirani, R., & Friedman, J. (2001). *The elements of statistical learning: Data Mining, inference, and prediction*. New York, NY: Springer Series in Statistics.

He, J., Verstak, A., Watson, L., Stinson, C., Ramakrishnan, N., Shaffer, C., . . . Tranter, W. (2004). Globally optimal transmitter placement for indoor wireless mesh networks. *IEEE Transactions on Wireless Communications*, *3*(6), 1906–1911.

Horst, R., & Hoang, T. (1996). *Global optimization: Deterministic Approaches*. Springer.

Institute for Engineering and Technology, The. (2013). Jamming & radio interference: Understanding the impact. *IET Sector Insights*. Retrieved from http://www.theiet.org/sectors/information-communications/.

Jones, D.R., Perttunen, C.D., & Stuckman, B.E. (1993). Lipschitzian optimization without the Lipschitz constant. *Journal of Optimization Theory and Applications*, *79*(1), 157–181.

Lazos, L., & Krunz, M. (2011). Selective jamming/dropping insider attacks in wireless mesh networks. *IEEE Network*, *25*(1), 30–34.

Longley, A.G., & Rice, P.L. (1968). *Prediction of tropospheric radio transmission loss over irregular terrain. A computer method-1968*. Boulder, CO: Institute for Telecommunications Sciences.

Ma, K., Zhang, Y., & Trappe, W. (2005). Mobile network management and robust spatial retreats via network dynamics. Presented at the IEEE Conference Mobile Ad-hoc and Sensor Systems, pp. 235–242.

MapMart. (2009). MapMart global mapping solutions. Retrieved from http://www.mapmart.com/.

Molish, A. (2011). *Wireless communications*. United Kingdom: Wiley.

Mpitziopoulos, A. Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, *11*(4), 42–56.

Myerson, R. (1991). *Game theory: Analysis of conflict*. Cambridge, MA: Harvard University Press.

Naveed, A., Kanhere, S.S., & Jha, S.K. (2009). Attacks and security mechanisms. In Y. Zhang, Jun. Zheng, & Honglin Hu, (Eds.), *Security in wireless mesh networks*, (pp. 111–144). Boca Raton, FL: Auerbach Publications.

Nicholas, P. (2009). *Optimal transmitter placement in wireless mesh networks* (Master's Thesis). Monterey, CA: Naval Postgraduate School.

Nicholas, P., & Alderson, D. (2012). Fast, effective transmitter placement in wireless mesh networks. *Military Operations Research*, *17*(4), 69–84.

Olexa, R. (2005). *Implementing 802.11, 802.16, and 802.20 wireless networks: Planning, troubleshooting and operations*. Burlington, MA: Elsevier.

Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, *13*(2), 245–257.

Poisel, R. (2011). *Modern communications jamming: Principles and techniques*. Norwood, MA: Artech House.

Postel, J. (1980). User datagram protocol. Internet Engineering Task Force, Request for Comment 768.

Riverbed Technology. 2013. Network simulation: OPNET modeler suite. Retrieved from http://www.riverbed.com/products-solutions/products/network-planning-simulation/Network-Simulation.html.

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *IEEE Proceedings of the First International Conference on Peer-to-Peer Computing*, 101–102.

Serafino, D., Liuzzi, G., Piccialli, V., Riccio, F., & Toraldo, G. (2011). A modified DIviding RECTangles algorithm for a problem in astrophysics. *Journal of Optimization Theory and Applications, 151*(1), 175–190.

Shankar, A. (2008). *Optimal jammer placement to interdict wireless network services* (Master's Thesis). Monterey, CA: Naval Postgraduate School.

Shannon, C. (1949). Communication in the presence of noise. *Proceedings of the IRE*, *37*, 10–21.

Srivastava, V., Neel, J., Mackenzie, A., Menon, R., Dasilva, L. Hicks, J., . . . Gilles, R. (2005). Using game theory to analyze wireless ad hoc networks. *IEEE Communications Surveys*, *7*(4), 46–56.

Ståhlberg, M. (2000). Radio jamming attacks against two popular mobile networks. Seminar on Network Security, Helsinki University of Technology, Helsinki, Finland.

Thamilarasu, G., & Sridhar, R. (2009). Game theoretic modeling of jamming attacks in ad hoc networks. *Proceedings Of the 18th International Conference on Computer Communications and Networks*, 1–6.

United States Geological Survey. (2013). National elevation dataset. Retrieved from http://ned.usgs.gov/.

Vakin, S., Shustov, L., & Dunwell, R. (2001). *Fundamentals of electronic warfare*. Norwood, MA: Artech House.

von Stackelberg, H. (1952). *The theory of the market economy*. London: William Hodge.

Wood, A.D., Stankovic, J.A., & Son, S.H. (2003). JAM: A jammed-area mapping service for sensor networks. *IEEE Real-time System Symposium*, conference publications, 286–297.

Wood, A.D., Stankovic, J.A., & Zhou, G. (2007). DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. *4th Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks*, 60–69.

Xiao, L., Johansson, M., & Boyd, S. (2004). Simultaneous routing and resource allocation via dual decomposition. *IEEE Transactions on Communications*, *52*(7), 1136–1144.

Xu, W. (2008). On adjusting power to defend wireless networks from jamming. *Proceedings of the 1st ACM Conference on Wireless Security*, 203–213.

Xu, W., Wood, T., Trappe, W., & Zhang, Y. (2004). Channel surfing and spatial retreats: defenses against wireless denial of service. *Proceedings of 3rd ACM Workshop on Wireless Security*, 80–89.

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. MobiHoc 05, Urbana-Champaign, IL, pp. 46–57.

Zhang, Y., Zheng, Jun., & Hu, Honglin (editors). (2009). "*Security in wireless mesh networks*" (book name). "Attacks and security mechanisms" (article) by Naveed, A., Kanhere, S.S., and Jha, S.K., pp. 111–144. Boca Raton, FL: Auerbach Publications.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, California

4. Richard Mastowski (Technical Editor).....1
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, California