Fifty-fourth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 27 - 30, 2016

Game Theoretic Defense Approach to Wireless Networks Against Stealthy Decoy Attacks

Ahmed H. Anwar[1], George Atia[1], and Mina Guirguis[2]

[1]Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816
[2]Department of Computer Science, Texas State University, San Marcos, TX 78666
a.h.anwar@knights.ucf.edu, george.atia@ucf.edu, msg@txstate.edu

***Abstract*—Wireless networks implementing dynamic channel assignment mechanisms are vulnerable to stealthy decoy attacks that aim to disrupt natural network operation by creating cascading channel conflicts. This paper develops a game-theoretic defense strategy in which a network administrator makes judicious adjustments of the transmission footprint of the various nodes, thereby continuously adapting the underlying network topology. The defense strategy is a mixed-strategy Nash equilibrium of a formulated 2-player zero-sum game between the admin and the attacker. As the space of strategies of the admin grows exponentially with the size of the network, a scalable decomposition-based approach is developed yielding a defense strategy whose performance is shown to closely approach the Nash equilibrium of the non-decomposed game. Numerical results demonstrate the effectiveness of the proposed strategies against various attack policies under different attack costs and initial conflict sizes.**

I. Introduction

Motivation and scope: In 2015, more than half a billion devices were added and mobile data traffic grew 74% to reach 3.7 exabytes per month [1]. The deployment of wireless-enabled devices (e.g., Internet of Things, wearables, etc.) has made our networks larger and more dense. To accommodate such growth under spectrum constraints, significant research efforts focused on developing spectrum management techniques through the use of Software Defined Networks (SDN) and Cognitive Radios (CR) to improve the spectrum utilization [2],[3]. These techniques rely on sensing the current conditions (e.g., channels used, transmission power, interference levels, etc.) and dynamically making the appropriate decisions. Current Access Points (APs) can dynamically select their channels and their transmission ranges to minimize interference with surrounding APs in wireless mesh networks (e.g., Cisco's Transmit Power Control [4]). The shared nature of wireless communication, however, has made many of the above techniques susceptible to attacks.

Various types of attacks have emerged that target such adaptation employed in SDN and CR at different layers [5], [6]. Jamming attacks, in particular, have been shown to cause significant degradation through exploiting dynamic channel allocation and power transmission techniques (e.g., [7], [8], [9], [10]). In these attacks, the attacker creates interference on a given channel causing surrounding nodes to switch to other channels. Depending on the topology of the network, the effect of the attack can ripple through the network causing further nodes to switch channels. Once (and if) the network converges, the attacker can repeat the attack. Attacks on the control channel can also cause a similar outcome. Defense against jamming attacks has focused on the physical layer through frequency/channel hopping/selection techniques – including the control channels – (e.g., [11], [12], [13], [14]), as well as power allocation methods (e.g., [15], [16]).

To study the interactions between attackers and defenders, game theory has provided a rigorous framework to model the strategies of each player and has been instrumental in advancing the state-of-the-art in various security areas [17], [18]. Due to the inherent complexity of the space of strategies, however, obtaining optimal policies is computationally hard. Many studies have looked at different techniques to make the problem more tractable, [19],[20]. In this project, we propose a novel decomposition-based approach whereby the combinatorial game is effectively decoupled into a number of simpler sub-games, – one per node – capturing local node interactions. The local strategies corresponding to these sub-games are combined to yield a global tractable and scalable mixed-strategy Nash equilibrium that well approximates the optimal best response strategy based on the non-decomposed game.

Approach and contributions: In this paper, we make the following contributions:

- Formulate the game as a zero-sum game between the attacker and the defender focusing on defense strategies that minimize the reward for the attacker.
- Parameterize our proposed game with different performance metrics that capture the cost of jamming to the attacker (e.g., the level of exposure risk that the attacker is willing to take) and the damage inflicted in the network (e.g., areas with uncovered wireless services).
- Identify a Nash equilibrium yielding a best response defense strategy for the defender against decoy attacks.
- Due to the exponential complexity of the strategy space for the defender, we develop a scalable decomposition-based approach solving smaller sub-problems to identify an effective approximation to the optimal best response strategy.
- Assess the interactions of the players on different network topologies and show that our decomposition and approximation approach yields near optimal strategies.

978-1-5090-4550-1/16/$31.00 ©2016 IEEE

II. Related Work

This work is related to two research areas: security in wireless channel allocation techniques and security games formulations.

A. Security in Wireless Channel Allocation Techniques

There is a large body of research on the security of channel assignment algorithms exposing attacks and developing defense mechanisms (e.g., [10], [7], [21], [9], [8], [14], [13]). The work in [10] exposes three types of attacks against channel assignment algorithms that capitalize on attacking the highest loaded channels. One of those attacks is the Low-Cost Ripple Effect Attack (LORA) that aims to force the network in quasi-stable state by continuously inducing channel conflicts. In [21] the authors show a number of vulnerabilities in MAC protocols due to selfish cognitive radio users that seek to gain more than their fair share of resources. The authors in [7] expose three types of attacks against channel assignment mechanisms through creating utilization-based conflicts, link breakage and Denial of Service. The attacks above, however, were not studied from an optimization/game theoretic standpoint and thus the attack strategies were rather arbitrary. Our recent work in [9], [8] exposed attacks on dynamic channel allocation methods through Markov Decision Process (MDP) problems in which the attacker seeks to maximize the damage inflicted (captured by the interference level in the network) subject to an attack cost (e.g., risk of being detected). These attacks, however, did not consider the defense strategies and this paper considers the impact of the defender through a game-theoretic formulation. On the defense front, the authors in [14], [13], [15] address the control-channel jamming attacks and propose a randomized distributed scheme in which nodes can reestablish the control channel using frequency hopping techniques. Furthermore, in [13] the authors propose two methods for identifying the jammers whether acting independently or colluding. The work in [15] is related to our work here, in which the author considers power control to improve the chances of successful transmission. Our work, however, considers power control through a game-theoretic formulation with an attacker deciding which node to attack and what channel to induce.

B. Game Theoretic Formulations in Security games

There has been some studies that focused on the game-theoretic aspect of jamming attacks as in [22], [16], [11]. In [22] the authors consider a game in which the attacker aims to maximize the corrupted communication links through jamming while the defender aims to detect the presence of the attacker based on the percentage of collisions. The authors in [16] consider a jamming attack against a secondary user in cognitive radio setups in which a secondary user allocates different transmission powers to the fallow bands available. In [11] the authors consider a stochastic game between a jamming attacker and a secondary user. In this game, multiple channels are reserved for control messages and are dynamically switched with data channels by the secondary user based on the attacker's strategy. This work is also related to Stackelberg games [23] that have been applied in various settings for physical security [18], [17]. In this game, the defender is allowed to play first and the attacker is allowed to observe the defender before taking his/her action. Our approach here is different as we allow both players to choose their actions simultaneously. If we were to allow the defender to choose first, then the attacker's actions would resemble those that we studied earlier through the MDP framework [9], [8]. Another important difference is that in Stackelberg games considered in [18], [17], the payoff of attacking a certain node is independent of the state of the other nodes, whereas here we do not consider this assumption.

To the best of our knowledge, this work is the first to look at controlling the transmission power as a defense mechanism against jamming attacks through a game-theoretic formalism. It builds on our previous work by considering the defender's strategies. Moreover, our decomposition approach to solve the game provides a very good approximation to the optimal policies which are computationally prohibitive to obtain due to the exponential complexity of the strategy space.

III. System Model

We consider a wireless network represented by a graph, $G(\mathbb{V}, \mathbb{E})$, where $\mathbb{V}$ is the set of nodes with cardinality N, and $\mathbb{E}$ is the set of edges. Any pair of nodes $u, v \in \mathbb{V}$ are connected with an edge, $e_{u,v} \in \mathbb{E}$, if they are within each other's interference radius. Hence, $e_{u,v} \in \mathbb{E}$ iff $r_u + r_v > d_{u,v}$, where r_u is the transmission radius of node u, and $d_{u,v}$ is the distance between the two nodes. If $e_{u,v} \in \mathbb{E}$, u and v are called neighbors. In this setting each node represents an access point. Ideally, all access points transmit simultaneously using non-interfering frequency channels. Every node v is assigned a frequency channel $c_v \in \mathbb{C}$. Herein, we consider $\mathbb{C} = \{1, 2, 3, ..., 11\}$, the set of usable frequency channels in the United States for the 2.4 GHz band in the 802.11n specification. If a node experiences any type of interference it automatically switches to another non-interfering channel, if any are available. This switching process leads to delay overhead in the network causing performance degradation.

A. Channel Assignment

Assigning channels to nodes in a non-interfering manner is similar to the well-known graph coloring problem. Corresponding to each node v, we define a set ψ_v of all the neighboring nodes of v. We also define an interference set, I_v, of all channels that can interfere with node v as follows

$$I_v = \{c_v - x, ..., c_v, ..., c_v + x\}, \tag{1}$$

where x is a separation index that determines the channels that incur adjacent channel interference (ACI) with c_v. Hence, the set of non-interfering channels available to node v is

$$A_v = \mathbb{C} \setminus \cup_{u \in \psi_v} I_u \quad ; \forall v \in \mathbb{V}, \tag{2}$$

B. Transmission Power Levels

Due to the limitation of usable frequency channels, access points adapt their broadcasting power levels to reduce

their interference footprint, and therefore the overall network interference, [4].

In our system, we assume that the network administrator can reduce the power of an AP to a level that guarantees absolutely no interference with any other neighboring AP. This power level is denoted by '*low*'. On the other hand, to avoid loss in coverage, aka coverage holes, the network admin can set the transmitting power level to '*high*', which guarantees no loss in coverage for this AP. Without loss of generality, we consider only 2 power levels, however, our approach can be directly extended to any number of levels.

C. Stealthy Attacker

An outsider stealthy attacker can transmit power near an AP in the network at an interfering frequency to create a state that forces the admin to reassign the frequencies of the nodes as well as their transmit power levels. This effect can be more drastic in settings wherein channel switching is automated on the software level. Therefore, while Software Defined Networks (SDNs) and Network Function Virtualization (NFV) can increase network performance and stability [24], the network becomes more susceptible to the type of attacks described above.

In our previous work, we studied this type of attacks – termed decoy attacks – from the attacker's side [9], [8] as a Markov decision process (MDP) problem where the attacker decides at each time step which AP to attack and at which frequency in a static topology. An MDP problem is a single-player stochastic game. In sharp contrast, this paper considers a 2-player game between an attacker and a defender (the network admin). We focus on a static version of this game (i.e., game played only once). A dynamic version of a 2-player single controller stochastic game is deferred to an extended version of this work.

IV. Game Formulation

The defender (i.e., the admin) aims to mitigate the conflicts in the network, as well as avoid coverage holes. On the other hand, the attacker attempts to create more conflicts in order to increase the interference level within the network, and hence cause unnecessary channel switching. The reward of the attacker is proportional to the number of nodes transmitting at low level (hence coverage holes), and the number of conflicts in the network. However, the attacker also incurs a cost proportional to the power transmitted to cause interference and the risk of exposure.

The game, $\mathcal{G}$, can be defined as a tuple $\mathcal{G}(\mathcal{N}, \mathcal{A}, \mathcal{R})$ as follows:

- $\mathcal{N}$ is the set of players. $\mathcal{N}$= $\{1, 2\}$, denotes the admin and the attacker, respectively.
- $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ is the action space.
- $\mathcal{R} = \{R_1, R_2\}$ is the reward function, $\mathcal{R} : \mathcal{A} \rightarrow \mathbb{R}^2$ mapping actions to rewards for both players. Since we consider a zero-sum game, $R_1 = -R_2 = R$.

A. Player 1: The Admin

The admin defends the network by changing the topology through adapting the power levels of the APs, hence their interference footprints. Without loss of generality, we assume that each node can transmit at one of two levels, either high or low. Hence, $\mathcal{A}_1 = \left\{a_1^1, a_1^2, \ldots, a_1^{2^N}\right\}$. Each element is a pure strategy $a_1^i = (a_1^i(v)) \in \{0,1\}^N, \ \forall\ v \in \mathbb{V}, i = 1, \ldots, 2^N$. If $a_1^i(v) = 0$, then the power level of node v is set '*low*', and if $a_1^i(v) = 1$ its power level is set '*high*'. There are 2^N pure strategies for a network of N nodes, thus the dimensionality of the action space grows exponentially with the graph size. The admin may choose to play any of these actions, where an action represents a pure strategy, or a combination of these strategies through a mixed strategy as explained later.

B. Player 2: The Attacker

The attacker's action space is $\mathcal{A}_2 = \left\{a_2^1, a_2^2, ..., a_2^{N+1}\right\}$. The pure strategies are $a_2^j = (a_2^j(v)) \in \{0,1\}^N, \ \forall\ v \in \mathbb{V}, j = 1, \ldots, N+1$, where $a_2^j(v) = 0$ if the attacker decides not to attack node v, and $a_2^j(v) = 1$ if the attacker decides to attack node v. We assume that a single attacker can attack at most one node at a time, while a pure strategy vector $a_2^j \in \mathcal{A}_2$ of all zeros corresponds to a no-attack action. The attacker may choose not to attack thereby avoiding the cost of exposure. There is a fundamental tradeoff in attacking high degree nodes since attacking dense areas of the wireless network could increase the risk of exposure, but could also lead to a larger number of conflicts.

Let 1_A denote an indicator function associated with event A. We define the reward of the admin as a function of the admin's and the attacker's actions as follows,

$$R_1(a_1^i, a_2^j) = \sum_v h_v^j \ \frac{\delta_v^{i,j} + \gamma_j}{2} - \sum_v 1_{\left\{a_1^i(v)=0\right\}} - \sum_v \beta_v^{i,j} \left(1_{\left\{a_1^i(v)=1\right\}} + 1_{\left\{a_1^i(v)=0\right\}} 1_{\left\{a_2^j(v)=1\right\}}\right), \tag{3}$$

where,

$$h_v^j = h \cdot 1_{\left\{a_2^j(v)=1\right\}}, \tag{4}$$

$$\gamma_j = \delta_v \cdot 1_{\left\{a_2^j(v)=1\right\}} \tag{5}$$

$$\delta_v^{i,j} = \begin{cases} \sum_{u \in \psi_v} 1_{\left\{a_1^i(v)=1\right\}} 1_{\left\{a_1^i(u)=1\right\}} & \text{if } a_2^j(v) = 1 \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

$$\beta_v^{i,j} = \sum_{u \in \psi_v, c_u \in I_v} \left(1_{\left\{a_1^i(u)=1\right\}} + 1_{\left\{a_1^i(u)=0\right\}} 1_{\left\{a_2^j(u)=1\right\}}\right) \tag{7}$$

The first term on the RHS of (3) is the cost incured by the attacker (reward for the admin). Recall that the topology varies from its original state depending on the selected power transmission profile of the nodes. The degrees for nodes $v \in \mathbb{V}$ are δ_v and $\delta_v^{i,j}$ prior and after playing the game, respectively, and h denotes the attack cost. Hence, considering any node $v \in \mathbb{V}$, the attacker incurs a cost $h \cdot \delta_v^{i,j}/2$ capturing the node degree after the game is played, plus another cost $h \cdot \delta_v/2$, which is a constant penalty

reflecting the original importance of the attacked node and the power used by the attacker. The second term in the summand is a cost incurred by the admin for the coverage holes. This is captured by the number of nodes transmitting at '*low*' power level. The third term captures the conflicts in the network, calculated by summing the number of nodes in conflict, each weighted by the number of neighbors it conflicts with.

C. Mixed Strategy

We have defined the actions available to each player in the game, i.e, $\mathcal{A}_1$ and $\mathcal{A}_2$. A pure strategy is a strategy that selects one of these actions. Alternatively, a player may choose to use a randomized (mixed) strategy defined through a probability distribution over these actions. Given the set of actions of player 1, $\mathcal{A}_1$, let $\Pi(\mathcal{A}_1)$ denote the set of all probability distributions over $\mathcal{A}_1$. Then, the set of mixed strategies for player 1 is $\Pi(\mathcal{A}_1)$, denoted by $\mathcal{X}_1$. Therefore, in a mixed strategy $\mathbf{X} \in \mathcal{X}_1$, action a_1^i is played with probability x_i such that,

$$\mathbf{X} = \left[x_1, x_2, \ldots, x_{2^N}\right]^T. \tag{8}$$

Similarly, the attacker may also play a randomized strategy, $\mathbf{Y} = \left[y_1, y_2, \ldots, y_{N+1}\right]^T$. Hence, the expected admin reward, denoted U_1, can be expressed as

$$U_1 = \mathbf{X}^T \mathbf{R_1} \mathbf{Y} = \sum_{i=1}^{2^N} \sum_{j=1}^{N+1} x_i y_j R_1(a_1^i, a_2^j). \tag{9}$$

Each player aims to maximize his own reward. In a zero-sum game, this implies the expected utility for player 1 in equilibrium, $U_1 = -U_2$. The minimax theorem implies that U_1 holds constant in all equilibria and is the same value that player 1 achieves under a minimax strategy by player 2. Using this result, we can construct the optimization problem of player 1 as a linear program (LP) as follows,

$$\begin{aligned} \underset{\mathbf{X}}{\text{maximize}} \quad & U_1 \\ \text{subject to} \quad & \sum_{i=1}^{2^N} R_1(a_1^i, a_2^j) x_i \geq U_1, \qquad \forall j = 1, \ldots, N+1. \\ & \sum_{i=1}^{2^N} x_i = 1, \\ & x_i \geq 0, \qquad i = 1, \ldots, 2^N. \end{aligned} \tag{10}$$

The first constraint follows from the definition of the Nash Equilibrium. Therefore, the expected reward is greater than the value of the game. Since the value of the game depends on the mixed strategy played by player 2 (the attacker), the admin should constrain his response to the best response set that guarantees a higher reward. The remaining two constraints ensure that $\mathbf{X}$ is a valid probability distribution.

The complexity of this LP grows exponentially with the number of nodes as it searches a very large space of admissible strategies given that the number of pure strategies for the admin is $O(2^N)$. To reduce complexity and derive a scalable solution, we propose an efficient decomposition of the problem in which one solves N simpler sub-problems (one per node) in lieu of one large optimization problem.

D. Proposed Decomposition Approach

We define a game per node, aka sub-game. Hence, we define N sub-games solved by the admin to decide on the transmission power of each node. Each sub-game is associated with a subgraph consisiting of a given node and its neighbors. Along the same lines used above, let $\mathcal{G}_v(\mathcal{N}_v, \mathcal{A}_v, \mathcal{R}_v)$ define the sub-game played at node v. $\mathcal{N}_v$ is the same set of players as $\mathcal{N}$. The action space $\mathcal{A}_v$ is the set of all possible actions by both players, i.e.,

$$\mathcal{A}_v = \{(a_1, a_2)\}, a_1, a_2 \in \{0, 1\},$$

and $\mathcal{R}_v = \{r_1, r_2\}$. We use small letters to indicate the action and reward per node.

In solving the sub-game corresponding to node v to determine its power level, the admin has to make some assumptions about the unknwon power profiles of the neighbors of v. This uncertainty is the result of seeking a decoupling scalable strategy versus a joint solution of all the power profiles as in the optimal LP (10). To tackle this difficulty, we assume that all the neighboring nodes of v will be transmitting at '*high*'. This is a worst case assumption in case conflicts exist between node v and any of its neighbors. We can readily express the reward of the admin for this sub-game as,

$$\begin{aligned} r_1(a_1, a_2) = h_{a_2} \frac{\delta_v^{a_1,a_2} + \gamma_{a_2}}{2} - 1_{\{a_1=0\}} \\ -\beta_v^{a_1,a_2} \left(1_{\{a_1=1\}} + 1_{\{a_1=0\}} 1_{\{a_2=1\}}\right), \end{aligned} \tag{11}$$

where all parameters are defined as before but with the subgraph of node v and the reduced action space.

The decomposed approach is now formulated as a 2×2 matrix game. The payoff matrix of the admin has entries $r_{ij} \triangleq r_1(a_1 = i, a_2 = j), i, j \in \{0, 1\}$.

A maximin (mixed) strategy for the sub-game leads to a Nash Equilibrium, which is the solution to the following LP,

$$\begin{aligned} \underset{p_v}{\text{maximize}} \quad & u_v \\ \text{subject to} \quad & r_{10}.p_v + r_{00}.(1 - p_v) \geq u_v, \\ & r_{11}.p_v + r_{01}.(1 - p_v) \geq u_v, \\ & 1 \geq p_v \geq 0, \end{aligned} \tag{12}$$

where p_v is the probability of playing action $a_1 = 1$, i.e, assign '*high*' power level to node v. Also, let ρ_v denote the probability of attacking node v. Hence, the sub-game value can be expressed as

$$u_v = \begin{bmatrix} 1 - p_v & p_v \end{bmatrix} \begin{bmatrix} r_{00} & r_{01} \\ r_{10} & r_{11} \end{bmatrix} \begin{bmatrix} 1 - \rho_v \\ \rho_v \end{bmatrix}. \tag{13}$$

It is worth mentioning that after obtaining the attacker's minimax strategy $\rho_v, v \in \mathbb{V}$ for the N sub-games, it should be appropriately normalized since only one node can be attacked at a time.

In the next section, we present numerical results that illustrate the performance of the proposed defense mechanism. Remarkably, the performance of the decomposition-based

method is shown to closely approach the optimal solution. Hence, we can often obtain a scalable suboptimal strategy with a very small performance gap.

V. Experimental Results

In this section, we present numerical results for the proposed defense mechanism when both the admin and the attacker play a mixed-strategy Nash equilibrium. The reward of the admin – as defined in (9) – is evaluated under different attack cost values and initial number of conflicts. We also evaluate the performance of the proposed decomposition-based approach and provide comparisons with the defender's best response strategy against different attack strategies. Each time, we present results from both theory and simulation, which are shown to perfectly match. The theoretical performance without and with decomposition is obtained by solving the LPs in (10) and (12), respectively. Simulations are obtained by actually playing the game using actions sampled from the computed randomized strategies, and averaging over 1000 runs of the game. In addition, we compare the run time of the mixed-strategy Nash-equilibrium (without decomposition) and the strategy obtained through decomposition as we increase the network size. The former is obtained for relatively small network sizes given its exponential complexity. However, with decomposition, the mixed startegy is perfectly scalable, hence we readily present results for a 64-node network topology later in the section.

For the tree network topology shown in Fig. 1, the game is played at different attack cost values. The mixed-strategy Nash equilibrium based on the decomposition-based approach performs closely to the Nash equilibrium when solving jointly for the power profiles (without decomposition) as shown in Fig. 2. The decomposition-based approach is shown to yield a slightly lower reward for the admin – equivalently a higher reward for the attacker – particularly in the low attack cost regime owing to the high power transmission assumption (for all the neighbors) in solving the sub-games, which in turn motivates the admin to play more conservatively when attacks are emboldened by the lower attacking cost. When the attack cost is sufficiently high, both strategies converge to the same value of the game as the attacker chooses to back-off.

In Fig. 2, we also show the performance as the defender continues to play his best response against a random attack strategy in which attacks are launched at randomly picked nodes regardless of the cost the attack. Since the attacker is unilaterally changing its strategy, the reward of the defender increases in agreement with the definition of the Nash equilibrium. In addition, we compare the performance of the defender's strategy against an attacker that consistently targets the node with the highest degree – termed maximum connected node (MCN) attack. MCN performs fairly close to the Nash Equilibrium strategy for an attack cost that is less than 1 as attacking nodes with high-degree when attack is fairly uncostly can conceivably induce a large number of conflicts. As the cost of the attack increases, however, attacking the MCN shows to be very expensive from the attacker's perspective.

The initial number of conflicts in the network is another important factor that impacts the performance of the strategies of both players. Fig. 3 shows the admin's reward with and without decomposition at attack cost, $h = 1$. For this cost value, the gap between both approaches is negligible. In a network with a small number of initial conflicts, the attacker's task is harder, hence the larger reward for the admin. In such a setting, the admin is able to play less conservatively and safely assign '*high*' power levels to a larger number of nodes. Interestingly, the gap between both strategies diminishes in the low conflict regime – recall the high-power assignment assumption utilized in solving the decoupled sub-games. A detailed mathematical analysis of the gap between both approaches, as well as additional simulations are deferred to an extended version of this paper.

Complexity reduction: A fundamental contribution of this work is the significant complexity reduction brought about through the decomposition-based approach, whose performance was shown to often closely approach that of the optimal mixed-strategy. Decoupling the initial game – which has combinatorial complexity – into smaller and scalable sub-games effectively addresses the so-called curse of dimensionality. Instead of solving one optimization problem of size $2^N \times (N+1)$, we solve N sub-problems, each of size 2×2. To illustrate the significant complexity reduction of the decomposed problem, we compared the experimental run time to solve for the maximin strategy with the number of nodes. It has been observed to grow exponentially for the full scale problem. On the other hand, the run time increases only linearly with the proposed decomposed approach.

Fig. 4 shows the admin's reward against the attack cost for a 64-node network topology in comparison to the random attack strategy. This underscores the scalability of the proposed decomposition-based approach since obtaining a mixed strategy Nash equilibrium for a network of this size without decomposition is computationally prohibitive.

VI. Conclusion and Future Work

In this paper, we proposed a defense mechanism whereby a network admin defends the network against stealthy decoy attacks through adapting the transmission profiles of the wireless access points in a game-theoretic framework. Given the combinatorial complexity of the best response strategy, we also proposed a scalable decomposition-based defense approach in which the defender solves multiple, yet simple, sub-games instead of one large combinatorial game. The decoupled approach was shown to yield a mixed strategy Nash equilibrium whose performance closely matches that of the full-scale Nash equilibrium, particularly for sufficiently large attack cost. The defender can achieve a larger reward should the attacker opt to adopt a different strategy, including launching a random attack or one that targets networks hubs (high-degree nodes). Future research directions include analytically investigating the gap between the proposed mixed-strategies with and without decomposition, as well as explor-

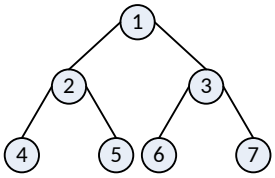

Fig. 1: Tree network topology.

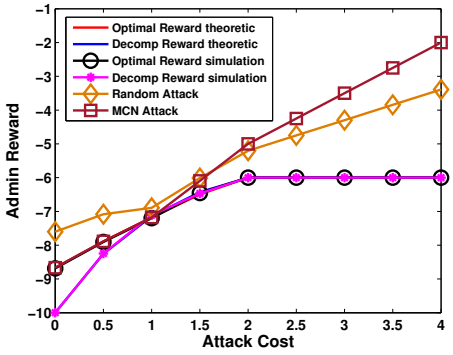

Fig. 2: Admin reward versus attack costs.

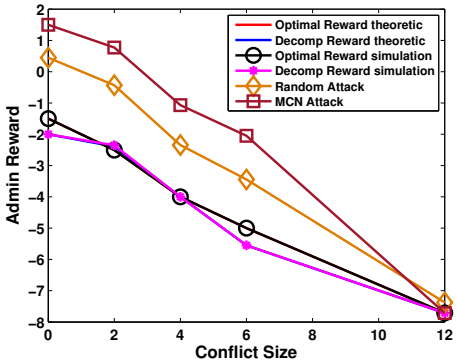

Fig. 3: Admin reward versus size of conflict.

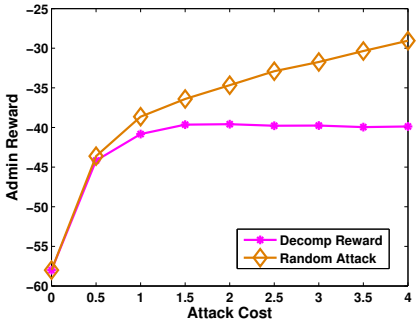

Fig. 4: Admin reward for a 64-node network.

ing stochastic game formulations capturing the dynamics of such attack and defense mechanisms.

ACKNOWLEDGMENT

This work was supported by NSF CAREER Award CCF-1552497, NSF grant No. CCF-1320547 and NSF CAREER Award CNS-1149397.

REFERENCES

[1] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 20152020 white paper," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, 2016.

[2] J. Mitola III and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, 1999.

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[4] Cisco, "Radio resource management white paper: Chapter: Transmit power control (tpc) algorithm," http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0101.html, 2016.

[5] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Gódor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 2, pp. 355–379, 2012.

[6] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, pp. 1–7.

[7] Q. Gu, M. Yu, W. Zang, and P. Liu, "Lightweight attacks against channel assignment protocols in MIMC wireless networks," in *IEEE Int. Conf. on Communications (ICC)*, 2011, pp. 1–6.

[8] J. Kelly, M. Guirguis, and G. Atia, "Pinball attacks: Exploiting channel allocation in wireless networks," in *Proceedings of the IEEE ICC*, Kuala Lumpur, Malaysia, 2016.

[9] A. H. Anwar, J. Kelly, G. Atia, and M. Guirguis, "Stealthy edge decoy attacks against dynamic channel assignment in wireless networks," in *IEEE Military Comm. Conf. (MILCOM)*, 2015, pp. 671–676.

[10] A. Naveed and S. Kanhere, "Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks," in *IEEE Global Telecommunications Conference*. IEEE, 2006, pp. 1–5.

[11] B. Wang, Y. Wu, K. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 877–889, 2011.

[12] M. Ihmig and P. Steenkiste, "Distributed dynamic channel selection in chaotic wireless networks," in *13th European Wireless Conference, Paris, France*, 2007.

[13] S. Liu, L. Lazos, and M. Krunz, "Thwarting Control-channel Jamming Attacks from Inside Jammers," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, 2012.

[14] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-channel Jamming Attacks in Multi-channel Ad hoc Networks," in *WiSec*, 2009.

[15] W. Xu, "On adjusting power to defend wireless networks from jamming," in *4th Int. Conf. on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*. IEEE, 2007, pp. 1–6.

[16] Y. Wu, B. Wang, and K. R. Liu, "Optimal power allocation strategy against jamming attacks using the colonel blotto game," in *IEEE Global Telecommunications Conference (GLOBECOM)*, 2009, pp. 1–5.

[17] A. Sinha, T. Nguyen, D. Kar, M. Brown, M. Tambe, and A. X. Jiang, "From physical security to cyber security," *J. of Cybersecurity*, 2015.

[18] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proc. of The 8th Int. Conf. on Autonomous Agents and Multiagent Systems-Volume 1*, 2009, pp. 689–696.

[19] M. Jain, E. Kardes, C. Kiekintveld, F. Ordónez, and M. Tambe, "Security games with arbitrary schedules: A branch and price approach." in *Proceedings of AAAI*, 2010.

[20] M. Jain, D. Korzhyk, O. Vaněk, V. Conitzer, M. Pěchouček, and M. Tambe, "A double oracle algorithm for zero-sum security games on graphs," in *The 10th Int. Conf. on Autonomous Agents and Multiagent Systems-Volume 1*, 2011, pp. 327–334.

[21] Y. Zhang and L. Lazos, "Vulnerabilities of Cognitive Radio MAC Protocols and Countermeasures," *IEEE Networks*, vol. 27, no. 3, 2013.

[22] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *26th IEEE Int. Conf. on Computer Comms (INFOCOM)*, 2007, pp. 1307–1315.

[23] H. Von Stackelberg, *Marktform und gleichgewicht*. J. springer, 1934.

[24] C. Monsanto, J. Reich, N. Foster, J. Rexford, and D. Walker, "Composing software defined networks," in *10th USENIX Symp. on Networked Systems Design and Implementation (NSDI 13)*, 2013, pp. 1–13.