Budapest University of Technology and Economics
Department of Networked Systems and Services

Robustness Against Strategic Attacks

Collection of Ph.D. Theses

of

Áron Lászka

Supervisor:

Levente Buttyán, Ph.D.

Budapest, 2014

1 Introduction

Nowadays, both individuals and organizations are becoming more and more dependent on computing resources and networks. However, the adoption of these technologies does not only provide benefits to their users, but it also makes them more vulnerable to strategic attacks. For example, many critical infrastructure sectors, such as the electricity and the water sectors, rely on computer networks, which are susceptible to various attacks. As another example, cyber-espionage activities, which threaten both the trade secrets of private organizations and the security of nations, are on a steady rise.

Traditionally, security research has primarily been focused on preventing adversaries from carrying out successful attacks; however, in many situations, attaining this goal is either economically infeasible or impossible. For example, physical networks are inherently vulnerable to denial-of-service type attacks, such as physical node destruction and wireless jamming. Thwarting all of these attacks would entail protecting every single element of a network, requiring substantial investments from a defender, which is economically infeasible in many situations. As another example, consider recent events from the world of cyber-warfare, which have shown that even secluded and highly protected computer systems can be penetrated by a determined and resourceful attacker. For instance, the Stuxnet worm was able to penetrate highly protected computer systems that were not connected to the Internet, such as nuclear facilities.

When perfect protection is not an attainable goal, a defender has to resort to mitigating the effects of successful attacks. In other words, the defender's goal in these scenarios needs to be ensuring that the system or network will sustain only tolerable losses in the event of a successful attack. This goal can be achieved either proactively by designing the network or systems to be robust (i.e., resilient) to attacks, or reactively by using it in an attack-resilient manner. In my dissertation, I study four problems related to mitigating the effects of strategic attacks.

Robustness of Network Topologies First, I study the robustness of network topologies against strategic attacks. The main motivation for this research is that, in order to design robust networks, one first has to be able to quantify robustness. Although one can find a number of metrics in the literature that can be used to quantify robustness, most of the previous metrics are not based on specific attacker and network models or disregard the strategic nature of the interactions between an attacker and a defender. In contrast, I adopt a game-theoretic approach recently proposed in [12], which derives metrics from given attacker and network communication models.

Designing Robust WSN Topologies Second, I study the design of robust wireless sensor networks. A sensor network consists of a large number of spatially distributed sensor nodes, which measure their environment and forward measurement

data through the network to a data collection center, called the sink node. Sensor networks are envisioned to have many applications, including military applications, such as battlefield surveillance, and critical infrastructure protection, such as surveillance of electric power networks. However, wireless sensor networks (WSNs) are usually assumed to consist of physically unprotected nodes and links, which makes them easy targets for denial-of-service type attacks. One of the key elements of designing networks that are resilient to attacks is designing the topology of the network to be robust.

Mitigating Covert Compromises Third, I study mitigation strategies against covert compromises. Attackers of computing resources often aim to keep security compromises hidden from the defenders in order to extract more value over a longer period of time. If detecting or preventing these covert compromises is too expensive for the defender, the effects of the compromises need to be mitigated by moving the resource into a known secure state (e.g., by changing the password of a potentially compromised account). However, since the attacks are stealthy, the defender has to schedule mitigation moves without knowing when a move will actually be useful, which presents an interesting challenge.

Secure Team Composition Fourth, I study the problem of bribe-resilient team composition in organizations. In cyber-espionage, an adversary can try to sidestep the technical security mechanisms of an organization (or a company) by having an employee bribed or compromised using social-engineering. However, if the secret sought by the adversary needs to be shared only with a subset of the employees, a manager can limit the success probability of the attacks by using a randomized sharing strategy. Hence, a manager can mitigate the effects of attacks sidestepping technical security by using randomized team composition, which forces the adversary to attack blindly.

1.1 Research Objectives

In the dissertation, my primary research objective is to find robust (i.e., attack-resilient) designs and defense strategies for each of the four problems. However, robustness often comes at a price. For an example, consider the third problem, where a defender faces covert attacks, against which she can defend herself only by making mitigation moves. In this case, the more often the defender makes a mitigation move, the more resilient her strategy is; however, these mitigation moves entail some cost. Hence, an economically rational defender must strike the right balance between minimizing mitigation costs and maximizing robustness. Generally, wherever it is possible in the dissertation, I will consider finding the optimal design or strategy to be a trade-off problem between minimizing cost and maximizing robustness.

In the first problem, my goal is to find realistic and efficiently computable robustness metrics for network topologies using network blocking games (NBG) [12]. As we

will see, one of the main challenges posed by NBGs is computational intractability. I will first address this question in general by proving that NBGs are generally computationally intractable, and then I will show that there exists a subclass of games that are efficiently computable. I will propose novel communications models, which will allow us to apply NBGs to a wider range of networks than previously, and show that these new models are also efficiently computable. Finally, I will generalize network blocking games by considering additional technical and economic constraints on the network, which will enable finding the optimal trade-off between cost and security.

In the second problem, my goal is to enable the design of robust wireless sensor network topologies. In wireless sensor networks, the topology of a network is determined by the placement of the nodes. Since the placement of the sensor nodes is usually given by the application (see, e.g., [21] for some supporting arguments), I focus on the problem of robust sink node placement, that is, the problem of finding a sink node placement that results in a robust topology. I will first study a constrained version of the problem, where the sink nodes can be placed only at the locations of the sensor nodes. Again, we will see that this problem is computationally challenging. Consequently, I will propose efficient heuristic and meta-heuristic algorithms to solve it. Finally, I will study the general problem, and show how it can be reduced to the constrained version using an efficient search-space reduction technique.

In the third problem, my goal is to find attack-resilient mitigation strategies against covert compromises. As I have discussed above, finding the optimal rate of the mitigation moves is essentially a trade-off problem between cost and security. I will study a broad class of mitigation strategies (i.e., schedules for the mitigation moves) and show which strategies are optimal against both strategic and non-strategic attacks.

In the fourth problem, my goal is to find bribe-resilient team composition (i.e., secret sharing) strategies. First, I will present an abstract model of this problem, which – as I will discuss in Section 3 – can be applied to problems other than team composition. I will present necessary conditions of the optimal strategies, and I will show one can compute a strategy using these conditions. Finally, I will consider an interesting special case of the problem, and I will show that there is a closed-form solution for this case.

1.2 Methodology

One of the key challenges presented by strategic attacks is that the adversary can anticipate the actions of the defender. This strategic nature of the conflict between a defender and a strategic attacker is modeled most naturally using the game theory nomenclature. Game theory is the mathematical study of conflict and cooperation between strategic decision-makers [18], who are called the players of a game. Resilience against strategic attacks can be studied using attacker-defender games, where one or more players take the role of strategic adversaries, and one player takes the role of the defender. In my dissertation, I model the first problem as a two-player game between a network operator and a strategic adversary capable of

removing elements of the network; the third problem as a game between a defender capable of performing mitigation moves and a stealthy strategic attacker; and the fourth problem as a game between a manager responsible for team composition and a spy who can bribe employees. The analysis of the resulting games will allow us to gain insight into each of these resilience problems.

Another challenge presented by strategic attacks is the complexity of finding an optimal defense. While non-strategic attacks and random faults can usually be modeled by a priori given probabilities of failures, strategic attacks depend on the defense, which results in more complex optimization problems. Furthermore, in the four problems studied in my dissertation, the cardinalities of the sets of strategies or possible designs are generally exponential (or even greater than that) in the size of the input. Hence, these problems are potentially intractable. To show which problems can be solved efficiently and which problems are actually intractable, I use the theory of computational complexity, which classifies computational problems based on their inherent difficulty [8].

2 Results

2.1 Robustness of Network Topologies

THESES 1: *I study the robustness of network topologies using network blocking games. First, I show that solving network blocking games is generally NP-hard, but can be performed in polynomial-time for some communication models. I propose two novel communication models, called the All-to-One model and the All-to-All with linear usage model. I prove that the game can be solved efficiently in these models, and I show that the resulting metrics are closely related to previous graph-theoretic metrics. Finally, I generalize blocking games by introducing a cost model and budget constraints for the operator.*

In order to be able to design robust network topologies, which are resilient to strategic attacks, one must first be able to quantify the robustness of topologies. The robustness – or equivalently, the vulnerability – of network topologies has been extensively studied, for example, in [7, 9, 15]. However, the simultaneous and strategic decision making of the network operator and the adversary, which is of key importance when modeling strategic attacks, has received only little attention. Recently, Gueye et al. proposed another approach for quantifying the robustness of network topologies in a series of papers [10–13]. In this approach, the strategic interaction between an adversary and the operator of a network are modeled as an attacker-defender game, called a *network blocking game* (NBG).

A network blocking game is a simultaneous, two-player, one-shot game between an operator and an adversary, played on a network topology given by a graph $G = (\mathcal{V}, \mathcal{E})$. The operator's pure strategies are the feasible collections T of network elements that can be used for communications. The adversary's pure strategies are the network elements e that can be attacked (i.e., removed from the network). The set of all feasible collections $\mathcal{T}$ and the set of network elements $\mathcal{E}$ are given by the *communication model*. When the operator uses collection $T \in \mathcal{T}$ and the adversary attacks element $e \in \mathcal{E}$, the network sustains $\lambda(T, e)$ usage loss, where the usage (or loss) function λ is again given by the communication model. The operator's and the adversary's pure-strategy payoffs are $-\lambda(T, e)$ and $\lambda(T, e) - \mu_e$ respectively, where μ_e is the cost of attacking e. For a mixed operator strategy $\boldsymbol{\alpha}$ and mixed adversarial strategy $\boldsymbol{\beta}$, the expected payoffs are $\sum_{T\in\mathcal{T}} \sum_{e\in\mathcal{E}} \alpha_T \beta_e \lambda(T, e)$ and $\sum_{T\in\mathcal{T}} \sum_{e\in\mathcal{E}} \alpha_T \beta_e (\lambda(T, e) - \mu_e)$.

Let $\theta_{max}(G)$ be the attacker's expected equilibrium payoff for a given network G. If the network is vulnerable, then the adversary can cause severe damage at little expense, and θ_{max} has to be high. On the other hand, if the network is robust against attacks, the adversary has to spend a lot of effort to cause some damage, and θ_{max} has to be low. Thus, we can use θ_{max} to quantify the vulnerability of a network.

THESIS 1.1: *I show that solving a network blocking game is an NP-hard problem in general, but for the class of communication models whose polyhedra can be characterized using a polynomial number of linear equations, the game can be solved efficiently.*

I begin my analysis with formulating the computational problem of solving a network blocking game as follows.

Definition 1 (Equilibrium Problem [EP])**.** Given a set of elements $\mathcal{E}$, a polynomial-time function $I_{T\in\mathcal{T}}$ for testing $T \in \mathcal{T}$, a polynomial-time usage function $\lambda(T, e)$, a vector of attack costs $\boldsymbol{\mu} \in \mathbb{R}^{|\mathcal{E}|}_{\geq 0}$, and a payoff value p, is the adversary's equilibrium payoff less than or equal to p?

The following theorem shows that the problem is NP-hard.

Theorem 1. *The Equilibrium Problem is NP-hard.*

While solving network blocking games is NP-hard in general, there exists a number of communication models for which the adversary's equilibrium payoff (and, for some models, even an equilibrium strategy profile) can be computed efficiently. Next, I discuss the computational complexity of those models for which the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities, and prove that these models can be solved efficiently. In Section 2.3.2 of the dissertation, I show that the adversary's equilibrium payoff in these models can be expressed as the solution of a linear program, which can be solved efficiently. Furthermore, in the dissertation, I show that an equilibrium strategy profile can also be found in polynomial-time.

THESIS 1.2: *I propose a novel communication model, called the All-to-One model. I show that the game can be solved efficiently in this model and that the resulting robustness metric is closely related to a previous metric, the directed strength of a graph.*

Many access and sensor networks are inherently vulnerable to physical attacks, such as the jamming of wireless signals or the destruction of nodes and links. From a topological point of view, the common characteristic of these networks is that the primary goal of the nodes is to communicate with a (set of) designated nodes; for example, in a sensor network, the goal of the network is to collect the sensed data at a designated central node.

For such networks, I introduce the All-to-One communication model as follows. Note that I discuss a more general version of the model in the dissertation. Let the network topology be represented by a directed graph G, let the set of feasible collections (i.e., the operator's pure-strategy set) be the set of spanning reverse arborescences rooted at r, and the adversary's pure-strategy set be the set of links $\mathcal{E}$. For a given reverse arborescence T and link e, let the usage $\lambda(T, e)$ be the number nodes that are disconnected from r in $G[T \setminus \{e\}]$ (i.e., number of nodes from which the path to r in T contains e).

To prove that this model can be solved efficiently, I show that the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities in this model.

Theorem 2 (See Theorem 3 of the dissertation for a formal version.)**.** *Let $G = (\mathcal{V}, \mathcal{E})$ be a directed graph with designated node r, and let $\mathbf{\Lambda}$ be the usage (or loss) matrix of the All-to-One communication model. Then, the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities.*

Next, I present an intuitive, closed-form expression of the vulnerability metric. Based on Theorem 5 of the dissertation, the vulnerability $\theta_{max}(G)$ of a graph G can be expressed as

$$\theta_{max}(G) = \max_{C \subseteq \mathcal{E} : C \text{ is a minimal cut of } G} \frac{\lambda_r(C)}{|C|} - \sum_{e \in C} \frac{\mu_e}{|C|} \ . \tag{1}$$

Intuitively, this closed-form expression says that an attacker should focus her attack on (combinations of) minimal cuts that maximize the ratio between the weight of disconnected nodes and the number of edges removed and – at the same time – minimize her average attack cost.

Finally, I focus on a special case of the All-to-One network blocking game, where the attack costs μ_e are all zero. This special case is particularly interesting because, in this case, our game-theoretic robustness metric is equivalent to directed graph strength, a metric previously proposed in [7] based on purely graph-theoretical considerations. The directed strength of a graph is defined as follows.

Definition 2 (Directed Graph Strength)**.** Let G be a directed graph with a designated node r. Then, the *directed strength* of G, denoted by $\pi(G)$, is

$$\pi(G) = \min_{F \subseteq \mathcal{E}} \frac{\sum_{e \in F} s(e)}{\lambda_r(F)} \ , \tag{2}$$

where $s(e)$ measures the cost of attacking edge e.

It is fairly easy to see that the above maximum is attained for some minimal cut [7]. Hence, when $s(e) \equiv 1$, we have $\theta_{max}^{-1}(G) = \pi(G)$.

THESIS 1.3: *I propose a novel communication model, called the All-to-All with linear usage model, and show that the game can be solved efficiently in this model. I express the resulting robustness metric as the solution of a graph partitioning problem and show that it is closely related to a previous metric, the Cheeger constant.*

The All-to-One communication model is suitable for modeling a wide range of networks, where the nodes have to remain connected to a (set of) designated nodes, such as sensor or access networks. However, there are many networks where such designated nodes do not exist. For instance, in a local area network whose purpose

is to enable the nodes to communicate with each other, the nodes have to remain connected to each other.

For such networks, I introduce the All-to-All with linear usage model as follows. Let the set of feasible collections $\mathcal{T}$ (i.e., the operator's pure-strategy set) be the set of all spanning trees and the adversary's pure-strategy set be the set of edges $\mathcal{E}$. Then, for a given spanning tree T and edge e, let the usage (or loss) $\lambda(T, e)$ be the number of nodes in the smaller component of $G[T \setminus \{e\}]$ (i.e., the number of nodes separated from the majority). The rationale behind this definition is that, the more nodes become separated due to an attack, the higher the network's loss is.

To prove that this model can be solved efficiently, I show that the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities in this model.

Theorem 3 (See Theorem 6 of the dissertation for a formal version.)**.** *Let $G = (\mathcal{V}, \mathcal{E})$ be an undirected graph, and let $\mathbf{\Lambda}$ be the usage (or loss) matrix of the All-to-All model with linear usage. Then, the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities.*

For the All-to-One model, I have shown that the vulnerability $\theta_{max}(G)$ of a network is closely related to its directed strength $\pi(G)$. Now, I show a similar property for the All-to-All with linear loss model.

In graph theory, the Cheeger constant [5,6] (also called the edge expansion coefficient [2,3] or the isoperimetric number [16,17]) of a graph is a measure of "bottleneckedness", and it is defined as follows.

Definition 3 (Cheeger constant)**.** The *Cheeger constant* of a graph G, denoted by $h(G)$, is

$$h(G) = \min \left\{ \frac{|E(U, \mathcal{V} \setminus U)|}{|U|} : U \subset \mathcal{V}, 0 < |U| \leq \frac{|\mathcal{V}|}{2} \right\} \ , \tag{3}$$

where $E(U, \mathcal{V} \setminus U)$ is the set of all edges between U and $\mathcal{V} \setminus U$.

The following theorem shows that our robustness metric in the All-to-All model with linear loss is closely related to the Cheeger constant.

Theorem 4. *Let $G = (\mathcal{V}, \mathcal{E})$ be an undirected graph, assume that $\boldsymbol{\mu} = \mathbf{0}$, and let $\theta_{max}(G)$ be the vulnerability of G in the All-to-All model with linear usage. Then, for every graph G,*

$$\theta_{max}^{-1}(G) \leq h(G) \ . \tag{4}$$

Furthermore,

- *there exists a graph G such that $\theta_{max}^{-1}(G) < h(G)$,*
- *and there exist an infinite number of graphs such that $\theta_{max}^{-1}(G) = h(G)$.*

THESIS 1.4: *I generalize network blocking games by introducing a usage-based cost model and budget constraints for the operator. I propose two budget-constraint formulations, called the Maximum Cost Constraint and the Expected Cost Constraint. For the communication models that can be solved efficiently in the unconstrained game, I show that solving the game under the Maximum Cost Constraint is NP-hard. Finally, I show that the class of communication models whose polyhedra can be characterized using a polynomial number of linear equations can be solved efficiently under the Expected Cost Constraint.*

So far, the operator was assumed to be interested solely in maximizing security, disregarding other economic and technical factors, such as her operating costs or the quality of the service she provides. In practice, however, network operators are not indifferent to such factors, which are actually an integral part of their decision making.

Recall that $\lambda(T, e)$ was defined to be the usage of link e when the operator selects collection T, which can measure, for example, the amount of traffic or the number of paths that traverse the link. Now, assume that each link e has some *unit usage cost* w_e, so that the network operator incurs $w_e\lambda(T, e)$ cost for using link e when she selects collection T. This abstract unit cost w_e can model various economic and technical factors, including:

- direct financial costs (e.g., leasing a link),
- quality of service (e.g., jitter or delay on a link),
- random faults and reliability (e.g., random failure probability of a link), and
- resource usage (e.g., electric energy consumption of a link).

We can incorporate this cost model into the game in multiple ways. Here, I assume that the operator has a fixed *budget* $b \in \mathbb{R}_{\geq 0}$ to spend, and her goal is to minimize her expected loss by choosing the most secure strategy whose cost does not exceed her budget. This constraint on her strategy choice can again be formulated in multiple ways. Here, I introduce two straightforward formulations.

Maximum Cost Budget Constraint Under the *maximum cost constraint* (MCC), the operator can use only those feasible collections whose cumulative costs are less than or equal to her budget b. Formally, the operator's pure-strategy set is restricted to

$$\mathcal{T}^{(b)} := \{T \in \mathcal{T} \mid w(T) \leq b\} \ , \tag{5}$$

where $w(T) = \sum_{e \in \mathcal{E}} \lambda(T, e) w_e$.

From Theorem 1, we have that the unconstrained game, which is the special case of $b \to \infty$, is NP-hard in general. Hence, the maximum cost constrained game is also NP-hard in general. Consequently, I focus on the communication models which were efficiently computable in the unconstrained game. I first formulate the computational problem and then show that it is NP-hard.

Definition 4 (Equilibrium Problem with Maximum Cost Constraint [EPMAX])**.** Given a network G, a budget limit b, and a payoff threshold p, is the adversary's equilibrium payoff less than or equal to p?

Theorem 5. *The Equilibrium Problem with Maximum Cost Constraint is NP-hard in the (a) Supply-Demand, the (b) All-to-All, and the (c) All-to-One communication models.*

Expected Cost Budget Constraint Under the *expected cost constraint*, the operator can use a mixed strategy only if its expected cost is less than or equal to her budget b. Formally, the set of mixed strategies available to the operator is

$$\mathcal{A}^{(b)} := \left\{ \boldsymbol{\alpha} \in \mathbb{R}_{\geq 0}^{|\mathcal{T}|} \;\middle|\; w(\boldsymbol{\alpha}) \leq b \;\wedge\; \boldsymbol{\alpha}'\mathbf{1} = 1 \right\} , \tag{6}$$

where $w(\boldsymbol{\alpha}) = \sum_{T \in \mathcal{T}} \alpha_T \sum_{e \in \mathcal{E}} \lambda(T, e) w_e$.

Again, I study those communication models which are efficiently computable in the unconstrained game. However, instead of providing specific algorithms for particular communication models, I focus on the class of models for which the usage value combinations attainable by the operator can be characterized using a polynomial number of linear inequalities. To prove that these models remain efficiently computable, I show that for each expected cost constrained game, there exists an equivalent unconstrained game that is efficiently computable.

Definition 5 (Equivalent Unconstrained Game)**.** Let $\boldsymbol{\Lambda}$ be the usage (or loss) matrix of a blocking game, let $\mathcal{T}$ and $\mathcal{E}$ be the operator's and the adversary's pure-strategy sets respectively, let $\boldsymbol{\mu}$ and $\boldsymbol{w}$ be the attack and usage costs respectively, and let $b \in \mathbb{R}_{\geq 0}$ be a budget value. Then, the *equivalent unconstrained game* is defined as follows. Let the operator's pure-strategies be the extreme points of the set $\{\boldsymbol{\alpha} \in \mathbb{R}_{\geq 0}^{|\mathcal{T}|} \mid \boldsymbol{\alpha}'\mathbf{1} = 1 \;\wedge\; \boldsymbol{\alpha}\boldsymbol{\Lambda}\boldsymbol{w} \leq b\}$, let the adversary's pure-strategy set be $\mathcal{E}$, and for a pure-strategy profile $(\boldsymbol{\alpha}, e)$, let the operator's loss be $\sum_{T \in \mathcal{T}} \alpha_T \lambda(T, e)$ and the adversary's payoff be the operator's loss minus μ_e.

The following theorem shows that the equivalent game is indeed equivalent to the original game with respect to the adversary's equilibrium payoff and her set of equilibrium strategies. Consequently, it suffices to find an efficient algorithm for solving the equivalent game.

Theorem 6. *For any blocking game, the adversary's equilibrium payoff and her set of equilibrium strategies*[1] *are the same in the original game under the expected cost constraint and in the equivalent unconstrained game.*

It remains to show that the equivalent game can be solved efficiently. I prove this by showing that usage value combinations attainable by the operator can be

[1] A mixed adversarial strategy is an equilibrium strategy if there exists a mixed operator strategy such that the two form an equilibrium.

characterized using a polynomial number of linear inequalities in the equivalent game. The details of the proof can be found in Section 2.6.4 of the dissertation.

The related publications are [C3–C5, C10].

2.2 Designing Robust WSN Topologies

THESES 2: *I study the problem of finding sink node placements in wireless sensor networks that maximize the robustness of the resulting network topology. I first formulate a constrained version of the problem, called sink selection problem, show that it is NP-hard, and propose heuristic and meta-heuristic algorithms for solving it. Then, I formulate the general version of the problem, show that it is also NP-hard, and propose an efficient search-space reduction technique, which can be used to reduce the problem to the constrained version.*

In many applications, wireless sensor networks consist of resource constrained and physically unprotected devices, which makes them vulnerable to denial-of-service type attacks, such as physical node destruction or wireless jamming. Robustness against such attacks can be attained at multiple levels of the system architecture; here, I study the problem of deploying nodes so that the resulting network topology is robust against attacks. More specifically, as the locations of the sensor nodes are usually pre-determined by the application (see, e.g., [21] for some supporting arguments), I study the problem of robust sink node (i.e., gateway node) placement.

To compare the robustness of different network topologies, I use the notion of *graph persistence*, a generalization of directed graph strength [7]. Formally, the persistence $\pi(G)$ of a graph $G = (\mathcal{V}, \mathcal{E})$ is

$$\pi(G) = \min \left\{ \frac{\sum_{e \in A} s(e)}{\lambda(A)} : \; A \subseteq (\mathcal{E}(G) \cup \mathcal{V}(G)) \,, \; \lambda(A) > 0 \right\} \,, \tag{7}$$

where $s(e)$ is the cost of attacking and removing e from the graph and $\lambda(A)$ is the sum value of the nodes that are disconnected from the sinks if A is removed from the graph. Intuitively, persistence is defined as the minimum ratio between the cost of an attack and the gain of the attacker, where the cost of the attack is the sum cost of removing the targeted links or nodes, and the gain of the attacker is determined by the sum value of the nodes that get disconnected from the sinks as a result of the attack.

I begin my analysis with a constrained variant of the sink placement problem, called the robust sink selection problem, where sinks can only be placed at the locations of the sensor nodes. Then, based on the results for this constrained variant of the problem, I study the general problem of robust sink node placement.

THESIS 2.1: *I formulate the problem of robust sink node selection in sensor networks using persistence as a robustness metric, and show that the problem is NP-hard. To solve the problem in practice, I propose greedy heuristic and genetic meta-heuristic algorithms, and show – by means of simulations – that their performance is reasonably close to the optimum.*

I assume that assigning the sink role to a node v entails a selection cost of $c(v)$, which can model, for example, the cost of establishing an external connection with the node, regularly visiting the node for data collection, etc. Then, I formulate the problem of robust sink node selection as follows.

Definition 6 (Sink Selection with Required Persistence)**.**

INSTANCE: Directed graph G, edge weights $s : \mathcal{E}(G) \to \mathbb{R}^+$, node weights $d : \mathcal{V}(G) \to \mathbb{R}^+$, sink selection costs $c : \mathcal{V}(G) \to \mathbb{R}^+$, and required persistence $\pi_0 \in \mathbb{R}^+$.

SOLUTION: A subset $R \subseteq \mathcal{V}(G)$ such that the persistence $\pi(G)$ of G is at least π_0 with R as its sink nodes.

MINIMIZE: Selection cost of subset R, i.e., $\sum_{v \in R} c(v)$.

The following theorem shows that the sink selection problem is NP-hard.

Theorem 7. *The Sink Selection with Required Persistence problem is NP-hard.*

The proof of the above theorem is based on reducing a well-known NP-hard problem, the Set Cover problem, to the problem of sink selection. Based on the inapproximability of the Set Cover problem, I provide inapproximability results on the sink selection problem.

Theorem 8. *Assuming that $P \neq NP$, there exists a constant $c > 0$ such that there is no polynomial-time algorithm that finds a sink selection of total cost at most $c \log\log|\mathcal{V}| \cdot OPT$, where OPT denotes the minimum total cost of a sink selection.*

To find an optimal solution to the sink selection problem, I first formulate the problem as an integer problem.

$$\text{Minimize} \sum_{v \in \mathcal{V}(G)} c(v) r(v) \tag{8}$$

subject to

$$\forall v \in \mathcal{V}(G): \quad f((v, t^*)) \leq bignum \cdot r(v) \tag{9}$$

$$\forall e \in \mathcal{E}(G): \quad f(e) \geq 0 \tag{10}$$

$$\forall e \in \mathcal{E}(G): \quad f(e) \leq s(e) \tag{11}$$

$$\forall v \in \mathcal{V}(G): \quad \sum_{(u,v) \in \mathcal{E}(G^*)} f((u, v)) = \sum_{(v,u) \in \mathcal{E}(G^*)} f((v, u)) \tag{12}$$

$$\forall v \in \mathcal{V}(G): \quad f((s^*, v)) \geq \pi_0 \cdot d(v)\ , \tag{13}$$

where $r(v) \in \{0,1\}$ for all $v \in \mathcal{V}(G)$, $f(e) \in \mathbb{R}$ for all $e \in \mathcal{E}(G^*)$, *bignum* is a sufficiently large number, $s((u,v))$ is the weight of edge (u,v), $d(v)$ is the weight of node v, $c(v)$ is the selection cost of node v, and π_0 is the required persistence.

Obviously, the worst-case running time of the above algorithm is exponential. To solve the sink selection problem in practice, I propose greedy heuristic and genetic meta-heuristic algorithms. The proposed greedy algorithm is the following.

1. Let $R := \emptyset$.
2. Let $v \in \mathcal{V}(G) \setminus R$ be a vertex for which the maximum

$$\max_{v \in \mathcal{V}(G) \setminus R} \frac{\pi(G, R \cup \{v\}) - \pi(G, R)}{c(v)}$$

   is attained, and let $R := R \cup \{v\}$.
3. If $\pi(G,R) \geq \pi_0$, then return R; otherwise, continue from Step 2.

The description of the genetic algorithm can be found in the dissertation.

Finally, I present numerical results on the proposed sink selection algorithms. To obtain these results, I generated a large number of networks using the unit disk graph model, which is widely used in the literature on wireless sensor networks. Then, I ran each algorithm on all networks of a given size, and plotted the average values. The exact numerical parameters can be found in the dissertation.

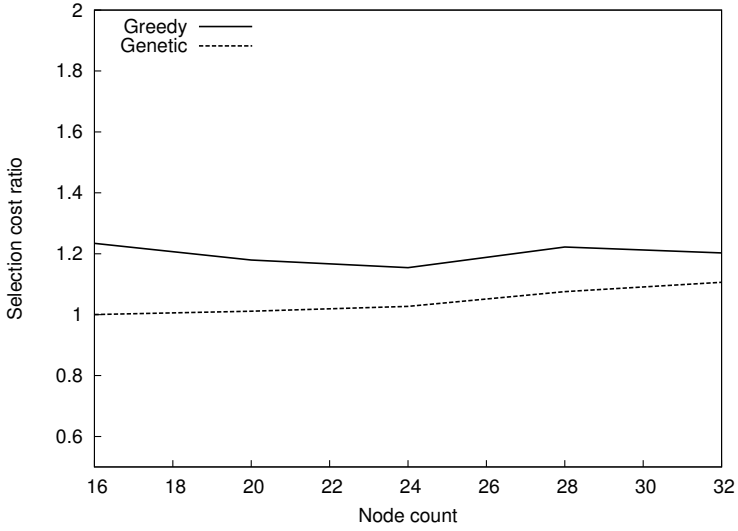


Figure 1: Ratios between the sink selection costs of the heuristic algorithms and the cost of the optimal solution.

Figure 1 shows the ratios between the sink selection costs of the heuristic algorithms and the cost of the optimal solution as a function of the node count. In the case of the greedy algorithm, the excess cost fluctuates around 20%, and it seems

to be quite stable with respect to the number of nodes. The solutions found by the genetic algorithm, on the other hand, are almost optimal if the number of nodes is low, and still a little better than those of the greedy algorithm for higher node counts.

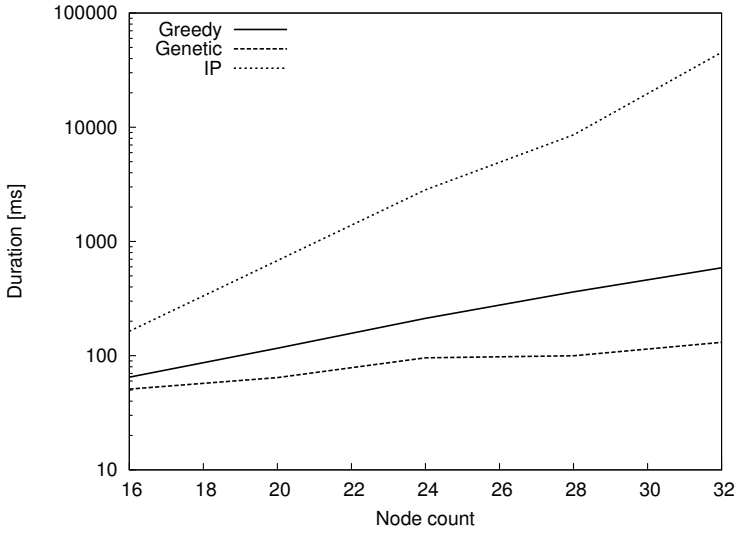


Figure 2: Average running times for different sink selection algorithms.

Figure 2 shows the average running times of the greedy algorithm, the genetic algorithm, and an integer programming solver as a function of the node count. As expected, the running time of the integer programming solver is exponential, and grows faster than those of the heuristic algorithms. Of the two proposed heuristics, the genetic algorithm is faster than the greedy algorithm by an order of magnitude.

THESIS 2.2: *I formulate the problem of robust sink node placement in wireless sensor networks, and show that the problem is NP-hard. To solve the problem, I propose an optimal search-space reduction technique, and show that it is efficient both theoretically and using simulations.*

Now, I relax some of the previous restrictions on the design of the deployment configuration, and allow sinks to be placed anywhere. However, I still consider the placement of non-sink nodes and the links between them to be given.

Definition 7 (Persistence of a Placement)**.** Let G be a directed geometric graph, where $\mathcal{V}(G)$ is a set of points in the Euclidean plane and $\mathcal{E}(G)$ is an arbitrary subset of $V^2(G)$. Let $s : \mathcal{E}(G) \to \mathbb{R}^+$ be edge weights, let $d : \mathcal{V}(G) \to \mathbb{R}^+$ be node weights, and let $D \in \mathbb{R}^+$ be a fixed sink transmission radius. The *persistence of a placement* R, where R is a set of points in the Euclidean plane, for graph G, denoted by $\pi_p(G, R)$, is the persistence of the graph G' with R as its sinks, where

1. $\mathcal{V}(G') = \mathcal{V}(G) \cup R$,
2. $\mathcal{E}(G') = \mathcal{E}(G) \cup \{(v, r) \ : \ v \in \mathcal{V}(G) \wedge r \in R \wedge \mathit{distance}(v, r) \leq D\}$,
3. $\forall_{(v,r) \ \in \ \mathcal{V}(G) \times R} : \ s(v, r) = 1$,
4. $\forall_{r \in R} : \ d(r) = 0$.

Using the above definition, I formulate the robust sink node placement problem as follows.

Definition 8 (Sink Placement with Required Persistence)**.**
INSTANCE: Directed graph G, where $\mathcal{V}(G)$ is a set of points in the Euclidean plane, edge weights $s : \mathcal{E}(G) \to \mathbb{R}^+$, node weights $d : \mathcal{V}(G) \to \mathbb{R}^+$, sink transmission radius D, and required persistence $\pi_0 \in \mathbb{R}^+$.
SOLUTION: A set of points R in the Euclidean plane such that $\pi_p(G, R) \geq \pi_0$.
MINIMIZE: The number of sinks required by the placement, i.e., $|R|$.

Next, I show that the problem defined above is NP-hard.

Theorem 9. *The Sink Placement with Required Persistence problem is NP-hard.*

To solve the placement problem, I propose a technique for reducing the infinite search space of possible placements to a finite set, which always includes an optimal solution. I begin with introducing the concept of single sink coverable sets.

Definition 9 (Single Sink Coverable Set)**.** A set of points W in the Euclidean plane is *single sink coverable* for a transmission radius D, if there exists a point r in the plane such that $\mathit{distance}(w, r) \leq D$ for every $w \in W$ (i.e., the points can be covered by a disk of radius D).

I reduce the infinite search space of possible placements by restricting the positions of the sink nodes to a set of candidate locations. This set of candidate location is given by the following definition.

Definition 10 (Optimal Set of Candidate Locations)**.** Given a geometric graph G and a sink transmission radius D, an *optimal set of candidate locations* $R_{\text{candidate}}$ is a set of positions which includes exactly one position covering every inclusion-maximal single sink coverable subset of $\mathcal{V}(G)$ for D (i.e., includes a location for every single sink coverable set of node positions that is not a subset of a larger single sink coverable set).

The following theorem shows that the above defined set of candidate locations is indeed optimal.

Theorem 10. *The subsets of an optimal set of candidate locations include an optimal placement for every persistence requirement.*

In order for this technique to be practical, the cardinality of the candidate location set has to be sufficiently low. The following theorem shows that the cardinality is polynomial in the size of the network. Later, I will also provide numerical results, which demonstrate that the cardinality is typically much lower in practice.

Theorem 11. *There exists an optimal set of candidate locations with cardinality less than or equal to* $|\mathcal{V}(G)|^3$.

Based on the ideas behind the proof of the above theorem, I provide a polynomial-time algorithm in the dissertation for finding an optimal set of candidate locations. Using the proposed search-space reduction technique, one can easily find a placement: first, find an optimal set of candidate locations using the proposed technique; then, construct a graph from the input network and the candidate locations similarly to Definition 7; and finally, compute a sink selection in the resulting network.

Furthermore, the proposed search-space reduction technique can also be applied to placement problems based on metrics other than persistence. See Section 6.3.6 of the dissertation for a few examples from the literature where the proposed technique could be used as an improvement.

Finally, I provide numerical results on the proposed search-space reduction technique. The networks used for evaluation were generated in a manner similar to the ones used to compare different sink selection algorithms.

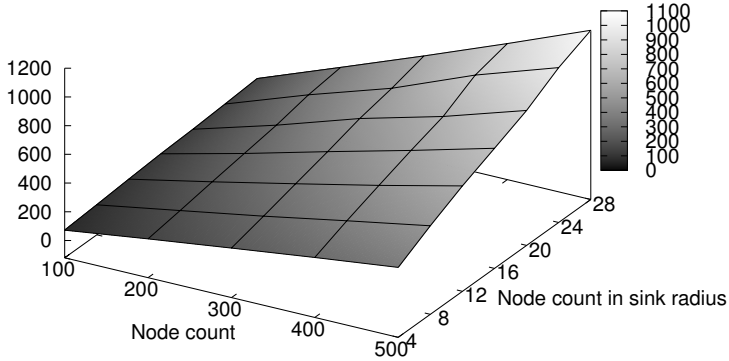


Figure 3: Average number of candidate locations for various node counts and sink radii.

Figure 3 shows the average number of candidate locations. As the exact value of the sink radius is not very informative, the expected average number of nodes on a disk of a given radius (i.e., the average number of nodes covered by a randomly placed sink) is displayed instead. The figure shows that the number of candidate locations grows linearly with the number of nodes, which means that the proposed technique is scalable.

Figure 4 compares different search-space reduction techniques (i.e., different sets of candidate locations): using the positions of the sensor nodes ("*selection*"), sampling the points of a uniform *grid*, choosing positions uniformly at random, and the proposed technique. The figure clearly shows that the proposed technique is superior with respect to the average cost resulting from using a given candidate location set.

The related publications are [C2, J1].

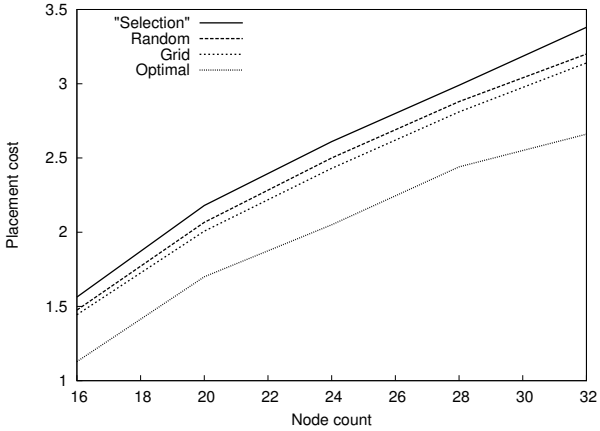


Figure 4: Average sink placement costs for various search-space reduction techniques.

2.3 Mitigating Covert Compromises

THESES 3: *I introduce a game-theoretic model for analyzing mitigation strategies against targeted and non-targeted covert compromises, and I characterize the best-response and equilibrium strategies in this model. I also formulate a variant of this model, where the defender makes her strategy publicly known, and show that this can lead to much higher payoffs for the defender.*

Many attackers prey upon opportunities to keep successful security compromises covert. The goal is to benefit from defenders' lack of awareness by exploiting resources and extracting credentials and company secrets for as long as possible. In contrast to non-covert attacks and compromises that focus on short-term benefits, these long-lasting and (for typical organizations) undetectable attacks pose specific challenges to system administrators and creators of security policies.

Covert (and non-covert) attacks can be distinguished in another dimension, by the extent to which the attack is targeted (or customized) for a particular organization [4, 14]. Approaches related to cyber-espionage are important examples of targeted attacks, and require a high effort level customized to a specific target. A typical example of a non-targeted covert attack is the recruitment of a computer into a botnet via drive-by-download. Such attacks are relatively low effort, and do not require a specific target.

The above examples highlight the importance of developing mitigation strategies to minimize the expected losses resulting from covert compromises. Potentially effective mitigation approaches include resetting of passwords, changing cryptographic private keys, reinstalling servers, or reinstantiating virtual servers.

THESIS 3.1: *I formulate the covert compromise scenario as a two-player game between a defender and a targeting attacker. I characterize the players' best-response strategies and the game's equilibrium strategy profiles.*

I model the covert compromise scenario as a two-player, one-shot, non-zero-sum game. For a list of the symbols used in the model, see Table 1.

Table 1: List of Symbols

C_D	move cost for the defender
C_A	move cost for the targeting attacker
B_A	benefit received per unit of time for the targeting attacker
B_N	benefit received per unit of time for the non-targeting attackers
F_A	cumulative distribution function of the attack time for the targeting attacker
λ_N	rate of the non-targeted attacks' arrival

Let D, A, and N denote the defender, the targeting attacker, and the non-targeting attackers, respectively. At any time instance, player i may make a move, which costs her C_i. When the defender makes a move, the resource becomes uncompromised immediately for every attacker. When the targeting attacker makes a move, she starts her attack, which takes some random amount of time. If the defender makes a move while an attack is in progress, the attack fails. The amount of time required by a targeted attack to succeed is assumed to follow the same distribution every time, and this attack time distribution's cumulative function is denoted by F_A.

The attackers' moves are stealthy; i.e., the defender does not know when the resource became compromised or if it is compromised at all. On the other hand, the defender's moves are non-stealthy. In other words, the attackers learn immediately when the defender has made a move.

The cost rate for player i up to time t, denoted by $c_i(t)$, is the number of moves per unit of time made by player i up to time t, multiplied by the cost per move C_i. For attacker $i \in \{A, N\}$, the benefit rate $b_i(t)$ up to time t is the fraction of time up to t that the resource has been compromised by i, multiplied by B_i. For the defender D, the benefit rate $b_D(t)$ up to time t is $-\sum_{i\in\{A,N\}} b_i(t)$. Player i's payoff is defined as

$$\liminf_{t\to\infty} \; b_i(t) - c_i(t) \; . \tag{14}$$

In my analysis, I consider the following strategy classes.

- Not Moving: A player can choose to *never move*.
- Adaptive Strategies for the Targeting Attacker: The targeting attacker computes an optimal waiting time before her attack based on the defender's previous moves. I model such *adaptive strategies* with a non-deterministic function W, which takes the defender's previous moves as input.

- Renewal Strategies: A player uses a *renewal strategy* if the time intervals between consecutive moves are identically distributed independent random variables.

- Periodic Strategies: A player uses a *periodic strategy* if the time intervals between her consecutive moves are identical.

Finally, I model the arrival of successful non-targeted attacks as a Poisson process. See the dissertation for arguments supporting this modeling assumption.

I begin the analysis with finding the defender's best-response strategies.

Lemma 1. *Suppose that the non-targeted attacks arrive according to a Poisson process with rate λ_N, and the targeting attacker uses an adaptive strategy with a fixed wait time distribution F_W. Then,*

- *not moving is the only best response if $C_D = \mathcal{D}(l)$ has no solution for $l > 0$, where*

$$\mathcal{D}(l) = B_A \left(l F_S(l) - \int_{s=0}^{l} F_S(s)\ ds \right) + B_N \left(-l e^{-\lambda_N l} + \frac{1 - e^{-\lambda_N l}}{\lambda_N} \right)\ ; \quad (15)$$

- *the periodic strategy whose period is the unique solution to $C_D = \mathcal{D}(l)$ is the only best response otherwise.*

Even though we cannot express the solution of $C_D = \mathcal{D}(l)$ in closed form, it (and those of the subequent formulae in this thesis group) can be easily found using numerical methods, as the right hand side is continuous and increasing.

I continue the analysis with finding the attacker's best-response strategy.

Lemma 2. *Against a defender who uses a periodic strategy with period δ_D,*

- *never attacking is the only best response if $C_A > \mathcal{A}(\delta_D)$, where*

$$\mathcal{A}(\delta) = B_A \int_{a=0}^{\delta} F_A(a) da\ ; \quad (16)$$

- *attacking immediately after the defender has moved is the only best response if $C_A < \mathcal{A}(\delta_D)$;*

- *both not attacking and attacking immediately are best responses otherwise.*

Based on the previous lemmas, I characterize the equilibria of the game (if there are any) as follows.

Theorem 12. *Suppose that the defender uses a renewal strategy, the targeting attacker uses an adaptive strategy, and the non-targeted attacks arrive according to a Poisson process. Then, the equilibria of the game can be characterized as follows.*

1. *If $C_D = \mathcal{D}^A(l)$ does not have a solution for l, then there is a unique equilibrium in which the defender does not move and in which the targeting attacker moves once at the beginning of the game.*

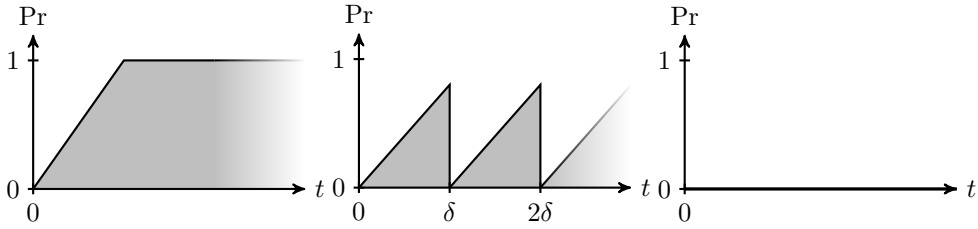
2. *If $C_D = \mathcal{D}^A(l)$ does have a solution δ_D for l:*

   (a) *If $C_A \leq \mathcal{A}(\delta_D)$, then there is a unique equilibrium in which the defender plays a periodic strategy with period δ_D, and the targeting attacker moves immediately after the defender's each move.*

   (b) *If $C_A > \mathcal{A}(\delta_D)$,*

      i. *if $C_D = \mathcal{D}^N(l)$ has a solution δ'_D for l, and $C_A \geq \mathcal{A}(\delta'_D)$, then there is a unique equilibrium in which the defender plays a periodic strategy with period δ'_D, and the targeting attacker never moves;*

      ii. *otherwise, there is no equilibrium.*



(a) Case 1. (b) Case 2. (a) (c) Case 2. (b) i.

Figure 5: The probability that the targeting attacker has compromised the resource (vertical axis) as a function of time (horizontal axis) in various equilibria (see Theorem 12 for each case). Note that these are just examples, the actual shapes of the function depend on F_A.

In the first case (Case 1.), the attacker is at an overwhelming advantage, and the defender simply "gives up" (see Figure 5 for an illustration). In the second case (Case 2. (a)), no player is at an overwhelming advantage. Both players are actively moving, and the resource gets compromised and uncompromised from time to time. In the third and fourth cases (Cases 2. (b) i. and ii.), the defender is at an overwhelming advantage. However, this does not necessarily lead to an equilibrium, only in Case 2. (b) i.

THESIS 3.2: *I formulate a sequential variant of the game and characterize its equilibria. Using numerical results, I show that the defender's payoff can be much higher in the sequential variant than in the simultaneous one.*

So far, I have modeled the mitigation of covert compromises as a simultaneous game. This is realistic for scenarios where neither the defender nor the targeting

attacker can learn her opponent's strategy choice in advance. However, in practice, the defender can easily let the targeting attacker know about the defender's strategy by publicly announcing it.

Now, I model the conflict as a sequential game, where the defender chooses her strategy before the targeting attacker does. I assume that the defender announces her strategy (e.g., publicly commits herself to a certain cryptographic-key update policy) and the targeting attacker chooses her best response based on this knowledge. The following theorem describes the defender's subgame-perfect equilibrium strategies.

Theorem 13. *Let δ_1 be the solution of $C_D = \mathcal{D}^A(\delta)$ (if it exists), δ_2 be the maximal period δ for which $C_A = \mathcal{A}(\delta)$, and δ_3 be the solution of $C_D = \mathcal{D}^N(\delta)$ (if it exists). In a subgame-perfect equilibrium, the defender's strategy is one of the following:*

- *not moving,*
- *periodic strategies with periods $\{\delta_1, \delta_2, \delta_3\}$.*

Based on the above theorem, one can easily find all subgame-perfect equilibria by iterating over the above strategies and, for each strategy, computing the targeting attacker's best response using Lemma 2, and finally comparing the defender's payoffs to find her equilibrium strategy (or strategies).

For the illustrations, I instantiate the model with the *exponential distribution* as the distribution F_A of the attack time. Unless indicated otherwise, the parameters of the game are $C_D = C_A = B_A = \lambda_A = \lambda_N = 1$ and $B_N = 0.1$. I will refer to simultaneous-game Nash equilibria simply as equilibria, and to the defender's subgame-perfect equilibrium strategies as optimal strategies.

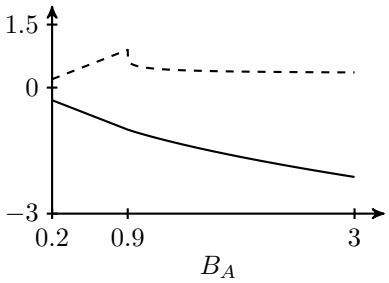
First, in Figure 6, I study the effects of varying how valuable the resource is, that is, varying the unit benefit B_A of the targeting attacker. The key observation from comparing Figures 6a and 6b is that the defender's optimal payoff is much higher than her equilibrium payoff.

Second, in Figure 7, I study the effects of varying the defender's move cost C_D. We see again that the defender's optimal payoff is much higher than her equilibrium payoff. However, for higher move costs ($C_D > 1.93$), she must give up defending the resource, as in her equilibrium strategy for that range.

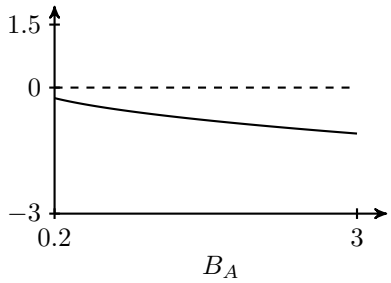
The related publications are [C9, C11].

2.4 Secure Team Composition

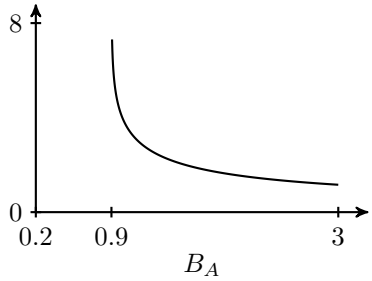
THESES 4: *I study the bribe-resilient team composition problem in a game-theoretic model. I describe the players' best-response and equilibrium strategies, and provide results on the existence and uniqueness of the equilibria and equilibrium payoffs. Finally, I characterize a special case of the model.*



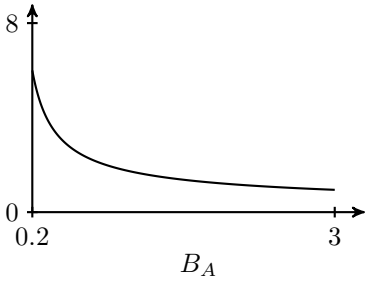
(a) The defender's and the targeting attacker's payoffs (solid and dashed lines, respectively) in equilibria as functions of B_A.



(b) The defender's and the targeting attacker's payoffs for the defender's optimal strategy as functions of B_A.



(c) The defender's equilibrium period as a function of B_A.

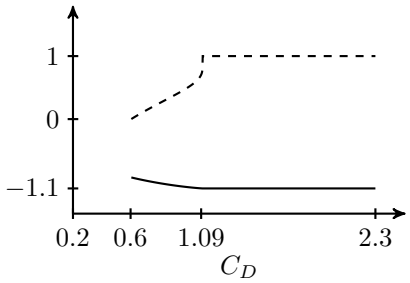


(d) The defender's optimal period as a function of B_A.

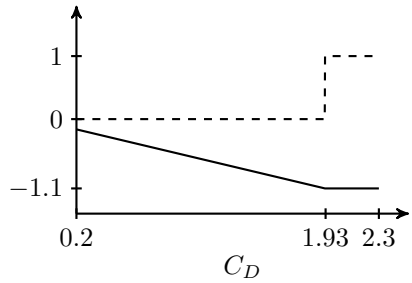
Figure 6: The effects of varying the unit benefit B_A of the targeting attacker.

In information security, selectively restricting individuals' access to information is achieved using access control features and techniques. However, such technical solutions cannot prevent employees from abusing the trust placed in them. Data theft by trusted employees covers a significant share of insider attacks. For example, a CERT investigation of 23 attacks showed that "in 78% of the incidents, the insiders were authorized users with active computer accounts at the time of the incident. In 43% of the cases, the insider used his or her own username and password to carry out the incident" [19].

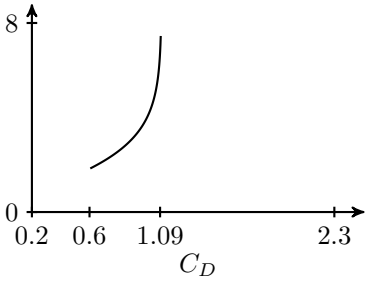
I study the problem faced by a project manager who has a secret she wants to protect but must share with a team of individuals selected from within her organization. The challenge arises from the presence of an attacker who wants to learn the secret (for example, a business competitor trying to steal a trade secret) and tries to sidestep technical security mechanisms by offering a bribe to an employee. Note that a more general interpretation of the model presented here is discussed briefly in Section 3.4.



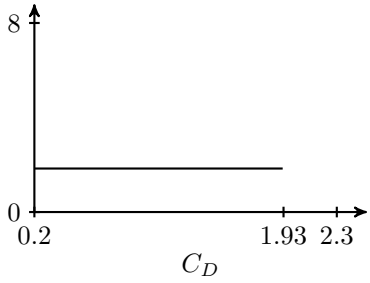
(a) The defender's and the targeting attacker's payoffs (solid and dashed lines, respectively) in equilibria as functions of C_D.



(b) The defender's and the targeting attacker's payoffs for the defender's optimal strategy as functions of C_D.



(c) The defender's equilibrium period as a function of C_D.



(d) The defender's optimal period as a function of C_D.

Figure 7: The effects of varying the defender's move cost C_D.

THESIS 4.1: *I formulate the bribe-resilient team composition problem as a two-player game, and give necessary conditions on the players' best-response and equilibrium strategies.*

I model the team-composition scenario as a two-player, non-zero-sum, non-deterministic game. For a simple illustration of the game's setup, see Figure 8.

An organization (or a company) with a secret of value S has N employees who are qualified to work on a project that requires knowledge of the secret. The project manager, called Alice, has to share the secret with at least k employees in order to enable the project. Formally, Alice's pure strategies are k-subsets of $\{1, \ldots, N\}$. Meanwhile, an attacker, called Eve, wants to learn the secret and has the resources to bribe or eavesdrop on one of the employees. Eve's pure-strategy choice is to select one employee and an amount to bribe with (or spend on eavesdropping). Formally,

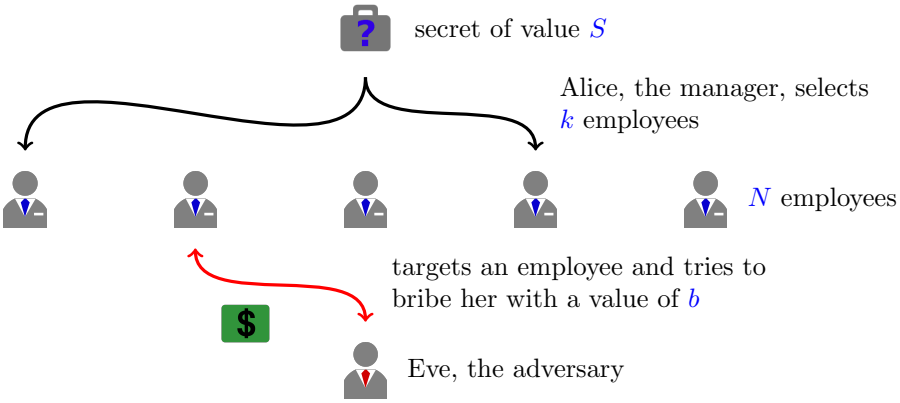


Figure 8: Illustration for the model with $N = 5$ and $k = 2$.

her pure strategies are pairs (i, b) consisting of an employee index $i \in \{1, \ldots, N\}$ and a bribe value $b \in \mathbb{R}_{\geq 0}$. Note that the players do not know which pure strategy their opponent has chosen.

The employees have varying levels of trustworthiness, which can only be estimated. For an employee i, this uncertain trustworthiness level is modeled as a random variable T_i, whose distribution $\mathcal{T}_i$ is known to all players. If $T_i = t_i$, then employee i will reveal what she knows whenever she is bribed with an amount greater than or equal to t_i, but she will never reveal the secret for less than t_i.

Suppose that Alice plays a pure strategy I, and Eve plays a pure strategy (i, b). If $i \in I$ and $T_i \leq b$, then Eve receives the value of the secret S minus the amount of the bribe b, and Alice loses the value of the secret S. In all other cases, Eve loses the amount of the bribe b, and Alice loses nothing.

A mixed strategy for a player is a probability distribution over the set of her pure strategies. Since the pure-strategy sets of both players in the above model are relatively complex, I introduce simpler representations for the players' mixed strategies, which are "payoff equivalent" to the canonical ones. First, I let Alice's mixed strategies be represented by vectors $\boldsymbol{a}$ of probabilities, where a_i is the probability that the secret is shared with employee i. Clearly, for every mixed strategy, there exists a corresponding vector. I prove in the following theorem that this is also true vice versa.

Theorem 14. *For any vector of probabilities $\boldsymbol{a}$ that satisfies $\sum_i a_i = k$, there exists a mixed strategy $\boldsymbol{\alpha}$ for Alice such that, for every i, the probability of sharing the secret with employee i is a_i. Furthermore, there is such a mixed strategy whose support consists of at most N sets.*

Second, I let Eve's mixed strategies be represented by pairs $(\boldsymbol{e}, \boldsymbol{\mathcal{B}})$, where each e_i is the probability that Eve bribes employee i, and each $\mathcal{B}_i$ is a distribution over

bribe values, conditioned on the assumption that Eve chooses employee i. Finally, let $\text{MaxUE}(\mathcal{T}_i, a_i)$ denote the maximum payoff that Eve can attain from targeting employee i, and let $\text{ArgMaxBE}(\mathcal{T}_i, x)$ denote the set of bribes that give Eve her maximum payoff for employee i.

Next, I derive analytical results on the players' best-response and equilibrium strategies in the above model. For the best-response conditions, please see the dissertation. The equilibrium conditions are the following.

Theorem 15. *In any Nash equilibrium, Alice's strategy satisfies the following constraints.*

1. *For any pair of employees i and j, if $a_i, a_j < 1$, then* $\text{MaxUE}(\mathcal{T}_i, a_i) = \text{MaxUE}(\mathcal{T}_j, a_j)$.
2. *For any pair of employees i and j, if $a_j < a_i = 1$, then* $\text{MaxUE}(\mathcal{T}_i, a_i) \leq \text{MaxUE}(\mathcal{T}_j, a_j)$.

It follows from Theorem 15 that Alice's equilibrium strategy $\boldsymbol{a}$ may have some employees with whom she shares the secret with certainty, but for all other employees, her secret-sharing distribution is only constrained by a smoothness constraint on the quantities $\text{MaxUE}(\mathcal{T}_i, a_i)$. From Theorem 15, we also have the following readily.

Corollary 1. *In any Nash equilibrium,*

- *Alice is either perfectly secure, that is, Eve has no strategy against her with a positive payoff, or else Alice shares the secret with every employee with a non-zero probability. Formally, either* $\text{MaxUE}(\mathcal{T}_i, a_i) = 0$ *for every employee i, or $a_i > 0$ for every employee i.*
- *The employees with whom Alice shares the secret with certainty are at most as likely to be targeted by Eve as the other employees, with whom Alice is less likely to share the secret.*

Finally, I provide a necessary condition on Eve's equilibrium strategies.

Theorem 16. *In a Nash equilibrium, if $a_i, a_j < 1$ for a pair of employees i and j, then $e_i \cdot \Pr[T_i \leq B_i] = e_j \cdot \Pr[T_j \leq B_j]$.*

THESIS 4.2: *I show that the game always has at least one equilibrium strategy profile using a constructive proof, and prove that the defender's strategy and the attacker's payoff are unique.*

I begin with showing that there always exists at least on equilibrium strategy profile.

Theorem 17. *The game always has at least one Nash equilibrium.*

The proof is constructive, and it is based on the following algorithm, whose correctness is proved in the dissertation.

1. *Find an equilibrium strategy $\boldsymbol{a}^*$ for Alice*:
   Find a mixed-strategy $\boldsymbol{a}^*$ that satisfies Theorem 15.

2. *Find an equilibrium strategy $(\boldsymbol{e}^*, \boldsymbol{\mathcal{B}}^*)$ for Eve*:
   Let $MaxUE^* = \max_i \mathrm{MaxUE}(\mathcal{T}_i, a_i^*)$ and let I^* be the set of employees for whom the maximum is attained. If $MaxUE^* = 0$, then there is no strategy with a positive expected payoff for Eve, so let $B_i^* \equiv 0$ for every i. Otherwise,

   (a) for every $i \notin I^*$, let $e_i^* = 0$;

   (b) for every $i \in I^*$, choose an arbitrary bribe value from $\mathrm{ArgMaxBE}(\mathcal{T}_i, a_i^*)$ and let B_i^* always take this value; finally, let

$$e_i^* = \frac{\frac{1}{\Pr[T_i \le B_i^*]}}{\sum_j \frac{1}{\Pr[T_j \le B_j^*]}} \ . \tag{17}$$

The next theorem shows that Alice's equilibrium strategy is essentially unique.

Theorem 18. *If Alice has no perfectly secure strategy, then the projection representation $\boldsymbol{a}$ of her equilibrium strategies is unique.*

Finally, based on the above theorem, I show the uniqueness of Eve's equilibrium payoff.

Corollary 2. *Eve's equilibrium payoff is always unique.*

THESIS 4.3: *I characterize the equilibria of the game for the special case of uniform trustworthiness level distributions.*

In this case, the trustworthiness level of each employee i is assumed to be generated by a uniform random variable $T_i \sim \mathcal{U}(l_i, h_i)$, $0 < l_i < h_i < S$. Note that I allow a different distribution, i.e., different l_i and h_i, for each employee.

I begin the analysis with computing Eve's optimal bribe values for a given mixed strategy $\boldsymbol{a}$ of Alice.

Lemma 3. *Eve's optimal bribe values are*

$$\mathrm{ArgMaxBE}(\mathcal{T}_i, a_i) = \begin{cases} \{0\} & \text{if } a_i < \frac{h_i}{S} \\ \{0, h_i\} & \text{if } a_i = \frac{h_i}{S} \\ \{h_i\} & \text{otherwise.} \end{cases} \tag{18}$$

For uniform trustworthiness level distributions, the following theorem characterizes the equilibria of the game.

Theorem 19. *If the trustworthiness level of each employee i is generated according to a uniform distribution $\mathcal{U}(l_i, h_i)$, $0 < l_i < h_i < S$, the equilibria of the game can be characterized as follows.*

- *If* $k < \frac{\sum_i h_i}{S}$*, then Alice is* perfectly secure*: in any equilibrium,* $a_i \leq \frac{h_i}{S}$ *for every* i*, Eve never bribes any of the employees, and both players' payoffs are zero.*

- *If* $k = \frac{\sum_i h_i}{S}$*, then in any equilibrium of the game,* $a_i = \frac{h_i}{S}$ *for every* i*, and Eve's payoff is zero.*

- *If* $k > \frac{\sum_i h_i}{S}$*, then in any equilibrium of the game,* $a_i > \frac{h_i}{S}$ *and* $B_i \equiv h_i$ *for every* i*, and Eve's payoff is strictly positive while Alice's payoff is strictly negative.*

The related publication is [C7].

3 Application of New Results

In this section, I discuss the potential applications of the new results for each of the four problems.

3.1 Robustness of Network Topologies

The primary goal of studying the robustness of network topologies was to find metrics for quantifying robustness, which is a prerequisite for designing attack-resilient networks. While one can find a large number of robustness metrics in the literature, most of these are either not based on attacker and network models, or they disregard the strategic nature of the conflict between a network operator and a strategic adversary. In this dissertation, I followed a game-theoretic approach, whose advantage is that one can find the right metric by formulating one's assumptions on the adversary's capabilities and the constraints on the operation of the network as attacker and network models, respectively. This makes it easier to identify and reason about which robustness metric to choose for a given application.

Furthermore, some of the results can be applied more directly to robust design. For example, the equilibrium adversarial strategies can be used to identify the edges that are most likely to be attacked. These critical edges are the "weakest links" in the network with respect to strategic attacks. Thus, in order to make a topology more robust, these are the edges that need be strengthened first.

3.2 Designing Robust Wireless Sensor Network Topologies

Wireless sensor networks have many applications, including military, environmental, and health applications [1]. For example, WSNs can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance, and targeting (C4ISRT) systems. In many of these applications, the network is likely to be threatened by strategic attacks, against which it must be resilient.

Even though my primary goal was to study the problem of attack-resilient design, the results can be applied to other topology-design problems as well. Firstly, persistence can be used to estimate the lifetime of a network under certain assumptions (see Section 3.2.2 of the dissertation). Secondly, the proposed search-space reduction technique can be used for an even wider-range of design problems (see Section 3.6.3 of the dissertation).

3.3 Mitigating Covert Compromises

The primary application of these results is finding optimal password and cryptographic-key renewal strategies. For example, many online services require – for security reasons – that users change their passwords from time to time. The timing of these mandatory changes is decided by the security policy makers of the service, who have

to minimize both the security risks arising due to compromised accounts and the effort required from the users due to password changes. Note that the model applies to a wider range of problems; for example, the resource could also model a private cryptographic key or a (virtual) machine.

One of the key implications of the results is that the optimal strategy for the defender is to move periodically. While this justifies the prevalent practice of periodic renewal of passwords and cryptographic keys, it contradicts the lesson learned from the very similar `FlipIt` model [20]. This contradiction between the implications of the two models highlights the importance of finding the right modeling assumptions.

The other key implication of the presented results is that the defender can achieve much higher payoffs in a sequential game, where she moves first and the attacker moves second. In practice, this means that the defender should not try to keep her strategy a secret, but should rather publicly announce it, allowing the attacker to play her best-response strategy.

3.4 Secure Team Composition

Even though I formalized the problem faced by a manager who has to assemble a team of employees whom an adversary might try to bribe, the presented results apply to a much wider range of secret-sharing problems. Firstly, even tough I use the term "bribe", the adversary's bribing move can actually model all sorts of attacks that sidestep technical security, such as social-engineering or eavesdropping on a person. Secondly, the results can be applied more generally than the problem of composing a team of employees. In fact, an "employee" can model any entity with whom information can be shared, such as a subcontractor, a computer system, or a facility (see Section 6.2 of the dissertation).

The results allow us to compute an economically optimal strategy for various secret-sharing scenarios. Moreover, they have a number of important implications regarding the problem in general, which – quite interestingly – contradict some very intuitive naïve ideas. For example, one might think that the secret should be shared with only the most trustworthy employees, while the results show that the optimal strategy for the defender is actually to share the secret with every single employee with a non-zero probability, unless she has a perfectly secure strategy.

4 Peer-Reviewed Publications

4.1 Journal Papers

[J2] Aron Laszka and Ádám Máté Földes. Modeling content-adaptive steganography with detection costs as a quasi-zero-sum game. *Infocommunications Journal*, 5:33–43, 2013.

[J1] Aron Laszka, Levente Buttyán, and Dávid Szeszlér. Designing robust network topologies for wireless sensor networks in adversarial environments. *Pervasive and Mobile Computing*, 9(4):546–563, 2013.

4.2 Conference and Workshop Papers

[C15] Benjamin Johnson, Aron Laszka, and Jens Grossklags. The complexity of estimating systematic risk in networks. In *Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF)*, July 2014.

[C14] Benjamin Johnson, Aron Laszka, and Jens Grossklags. How many down? Toward understanding systematic risk in networks. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, June 2014.

[C13] Aron Laszka, Benjamin Johnson, Jens Grossklags, and Mark Felegyhazi. Estimating systematic risk in real-world networks. In *Proceedings of the 18th International Conference on Financial Cryptography and Data Security (FC)*, March 2014.

[C12] Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. Game-theoretic analysis of ddos attacks against big and small mining pools. In *Proceedings of the 1st Workshop on Bitcoin Research, in association with FC 2014 (BITCOIN)*, March 2014.

[C11] Aron Laszka, Benjamin Johnson, and Jens Grossklags. Mitigating covert compromises: A game-theoretic model of targeted and non-targeted covert attacks. In *Proceedings of the 9th Conference on Web and Internet Economics (WINE)*, pages 319–332, 2013.

[C10] Aron Laszka and Assane Gueye. Quantifying network topology robustness under budget constraints: General model and computational complexity. In *Proceedings of the 4th Conference on Decision and Game Theory for Security (GameSec)*, pages 154–174, November 2013.

[C9] Aron Laszka, Benjamin Johnson, and Jens Grossklags. Mitigation of targeted and non-targeted covert attacks as a timing game. In *Proceedings of the 4th Conference on Decision and Game Theory for Security (GameSec)*, pages 175–191, 2013.

[C8] Pascal Schöttle, Benjamin Johnson, Aron Laszka, Jens Grossklags, and Rainer Böhme. Bitspotting: Detecting optimal adaptive steganography. In *Proceedings of the 12th International Workshop on Digital-Forensics and Watermarking (IWDW)*, October 2013.

[C7] Aron Laszka, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. Managing the weakest link: A game-theoretic approach for the mitigation of insider threats. In *Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS)*, pages 273–290, September 2013.

[C6] Pascal Schöttle, Aron Laszka, Benjamin Johnson, Jens Grossklags, and Rainer Böhme. A game-theoretic analysis of content-adaptive steganography with independent embedding. In *Proceedings of the 21st European Signal Processing Conference (EUSIPCO)*, September 2013.

[C5] Aron Laszka and Assane Gueye. Quantifying All-to-One network topology robustness under budget constraints. In *Proceedings of the joint Workshop on Pricing and Incentives in Networks and Systems (W-PIN+NetEcon)*. ACM, June 2013.

[C4] Aron Laszka, Dávid Szeszlér, and Levente Buttyán. Linear loss function for the network blocking game: An efficient model for measuring network robustness and link criticality. In *Proceedings of the 3rd Conference on Decision and Game Theory for Security (GameSec)*, pages 152–170, 2012.

[C3] Aron Laszka, Dávid Szeszlér, and Levente Buttyán. Game-theoretic robustness of many-to-one networks. In *Proceedings of the 3rd International ICST Conference on Game Theory for Networks (GameNets)*, pages 88–98, 2012.

[C2] Aron Laszka, Levente Buttyán, and Dávid Szeszlér. Optimal selection of sink nodes in wireless sensor networks in adversarial environments. In *Proceedings of the 2nd IEEE International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*, pages 1–6, 2011.

[C1] Aron Laszka, Annamaria R. Varkonyi-Koczy, Gábor Pék, and Peter Varlaki. Universal autonomous robot navigation using quasi optimal path generation. In *Proceedings of the 4th IEEE International Conference on Autonomous Robots and Agents (ICARA)*, pages 458–463, February 2009.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002.

[2] Noga Alon. On the edge-expansion of graphs. *Combinatorics, Probability and Computing*, 6(2):145–152, 1997.

[3] Noga Alon. Spectral techniques in graph algorithms. In *Proceedings of the 3rd Latin American Symposium on Theoretical Informatics (LATIN)*, pages 206–215, Campinas, Brazil, April 1998.

[4] Eoghan Casey. Determining intent - opportunistic vs targeted attacks. *Computer Fraud & Security*, 2003(4):8–11, 2003.

[5] Fan Chung. Laplacians and the Cheeger inequality for directed graphs. *Annals of Combinatorics*, 9(1):1–19, 2005.

[6] Fan R. K. Chung. *Spectral graph theory*, volume 92. American Mathematical Society, 1997.

[7] William H. Cunningham. Optimal attack and reinforcement of a network. *Journal of the ACM*, 32(3):549–561, 1985.

[8] Michael R Garey and David S Johnson. *Computer and intractability: A Guide to the NP-Completeness*. W. H. Freeman and Company, 1979.

[9] Tony H. Grubesic, Timothy C. Matisziw, Alan T. Murray, and Diane Snediker. Comparative approaches for assessing network vulnerability. *International Regional Science Review*, 31(1):88–112, 2008.

[10] Assane Gueye and Vladimir Marbukh. A game-theoretic framework for network security vulnerability assessment and mitigation. In *Proceedings of the 3rd Conference on Decision and Game Theory for Security (GameSec)*. Springer, November 2012.

[11] Assane Gueye, Vladimir Marbukh, and Jean C. Walrand. Toward a metric for communication network vulnerability to attacks: A game theoretic approach. In *Proceedings of the 3rd International ICST Conference on Game Theory for Networks (GameNets)*, May 2012.

[12] Assane Gueye, Jean C. Walrand, and Venkat Anantharam. Design of network topology in an adversarial environment. In *Proceedings of the 1st Conference on Decision and Game Theory for Security (GameSec)*, 2010.

[13] Assane Gueye, Jean C. Walrand, and Venkat Anantharam. A network topology design game: How to choose communication links in an adversarial environment? In *Proceedings of the 2nd International ICST Conference on Game Theory for Networks (GameNets)*, 2011.

[14] Cormac Herley. The plight of the targeted attacker in a world of scale. In *Proceedings of the 9th Workshop on the Economics of Information Security (WEIS)*, 2010.

[15] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.

[16] Bojan Mohar. Isoperimetric inequalities, growth, and the spectrum of graphs. *Linear Algebra and Its Applications*, 103:119–131, 1988.

[17] Bojan Mohar. Isoperimetric numbers of graphs. *Journal of Combinatorial Theory, Series B*, 47(3):274–291, 1989.

[18] Roger B Myerson. *Game theory: Analysis of conflict*. Harvard University Press, 1991.

[19] Marisa Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore. Insider threat study: Illicit cyber activity in the banking and finance sector. Technical Report CMU/SEI-2004-TR-021, Carnegie Mellon University, June 2005.

[20] Marten van Dijk, Ari Juels, Alina Oprea, and Ronald Rivest. FlipIt: The game of "stealthy takeover". *Journal of Cryptology*, 26:655–713, October 2013.

[21] M. Welsh. Sensor networks for the sciences. *Communications of the ACM*, 53(11):36–39, November 2010.