Perverse Incentives in Security Contracts: A Case Study in the Colombian Power Grid

Carlos Barreto and Alvaro A. Cárdenas

Abstract

In 2008 security forces in Colombia found that one of the companies hired to repair electric transmission towers from guerrilla attacks had hired guerrilla members to demolish towers in their contracted area of service. As a result, their business boomed as they were called often to repair electric towers. We model this problem as a game between contractors and the power transmission company, we show how misaligned incentives enabled contractors to profit by hiring guerrilla groups, and then model the changes to contracts that the transmission company implemented in order to minimize the incentives for future contractors to collude with guerrilla members in destroying electric towers.

I. Introduction

In the last four decades, Colombia has suffered one of the longest periods of sustained internal conflict; during this period, most of its critical infrastructures have been systematically targeted by guerrilla groups. According to data compiled by the National Memorial Institute for the Prevention of Terrorism, among all terrorist attacks to the electricity infrastructure between 1994 and 2004, 67% of attacks occurred in Colombia and the rest of the countries accounted for less than 7% each [1]. An example of a destroyed transmission tower in Colombia can found in Figure 1.

Fig. 1: Transmission tower destroyed by attack. Photo courtesy of ISA.

The experience of government and private sectors in Colombia operating such critical infrastructures under constant attacks can provide insights into the strategic and adversarial nature of defender-attacker games in a variety of settings, including cyber-security and critical infrastructure protection.

An interesting case study of the incentives of different parties participating in the protection and operation of the power grid is the bizarre case where Electroservicios (a contractor in charge of repairing transmission towers damaged by guerrilla attacks) was found to be paying guerrilla groups to destroy more towers than they usually would. As a result, the guerrilla attacked approximately 215 electric towers between 2005-2008 in the region of operation of Electroservicios [2], [3]. Electroservicios paid guerrilla members $8,000,000 pesos (approximately $4,000 USD according to the exchange rate in 2008) to bring

Carlos Barreto and Alvaro A. Cárdenas are with the Computer Science Department, University of Texas at Dallas (e-mail: {carlos.barretosuarez},{alvaro.cardenas}@utdallas.edu)

down each tower, and in return ISA, a transmission company in Colombia would pay Electroservicios $150,000,000 pesos (approximately $75,000 USD in 2008) to repair a tower. They even asked the guerrilla to bomb towers only during working days, so that Electroservicios would not have to pay weekend or holiday-hours to their workers [2].

In this paper we provide an analysis of the contracts between the transmission company and the contractor in charge of repairing towers. In particular, we show how the original model for assigning repair contracts was exploited by contractors, and how the electric transmission company changed the way it awarded contracts in order to minimize incentives for misbehavior. We believe the lessons learned from this experience are important for computer security researchers because cyber-attacks are even harder to attribute than physical attacks, and therefore the risks and barriers for would-be attackers to consider similar strategies to the ones used by the contractor of our analysis might be lower.

II. Model

A. Background

The role the contractor was playing in the attacks against the power grid was discovered because 93% of all attacks took place in the same region. After more than 100 towers were attacked, the police started an investigation in 2007 and found that the attacks had the following characteristics:

- All towers belonged to the same transmission company (ISA),
- Explosives were deployed in the same place,
- The modus operandi was the same,
- Repairs were made by the same contractor.

Repair costs per tower were between $50 and $150 million pesos. The estimated loses for ISA (the electricity transmission company) were approximately $16000 million pesos (around $8 million dollars at the time).

The authorities infiltrated the contractor and obtained a confession from one of the executives. They found out that the contractor business was booming thanks to the frequent tower repairs. The contractor did not attack the electric towers directly, instead, they hired four guerrilla militants and paid each one of them $2 million pesos. The contractor used the following criteria to attack towers.

- Easy access to facilitate the escape of militants and the arrival of contractors, so they could arrive fast to the site of the repair,
- Towers were partially damaged to allow both cheap and fast repairs,
- The attacks were made only on weekdays to avoid paying their employees for overtime.

Because of these conditions, the contractor was able to maximize the difference between the average payment p they received and their costs c of these repairs.

B. Lawful Contractors

To start modeling this problem we first consider the ideal scenario where contractors who repair electric towers do not sponsor attacks. We later introduce the case where they can pay the guerrilla to attack more towers. In the original setting, a repair contract of a region was awarded to one contractor, and this contractor was required to repair all the attacked towers in their assigned region.

The transmission company assigns contracts using an auction, in which the contractors send offers (or bids) of repair costs. Some auctions guarantee that with enough participants, the contract is assigned to the contractor with the lowest bid. Specifically, according to the Colombian contracting code of public administration [4], [5], a public bidding is made using reverse auctions. In a reverse auction the buyer is the transmission company who wants to buy a service (tower repair). Multiple sellers (who must satisfy the contract specifications) are then able to offer bids on the contract. The i^{th} contractor is a seller who offers repair services with a value $c_i \geq 0$. Without loss of generality we can assume that $c_1 \leq c_2 \leq \cdots \leq c_m$.

The reverse auction might have many stages in which bidders make offers using closed envelopes. At each stage the bids should be lower than the lowest bid of the previous stage. Thus, the sellers compete decreasing their bids and the contract is awarded to the seller that bids the lower price.

We assume that the contract is awarded to the contractor with the lowest repair costs; therefore, the transmission company has to pay $p = c_{min}$ (per tower repaired), where $c_{min} = \min_{i\in\{1,\dots,m\}} c_i$. We assume that the repair cost c_i guarantees a minimum benefit $U_i \geq 0$ for the contractor.

Attacks on electric transmission towers can interrupt the electricity flow to some regions that need to be served by the transmission company. While the Colombian regulations do not impose liabilities for failures to deliver electricity due to guerrilla attacks, they still need to purchase more expensive sources of electricity (if available) such as carbon-based fuels (more than 70% of the electricity in Colombia is generated by hydropower, and when attacks limit the transmission of this type of energy, the transmission company needs to satisfy the demand with more expensive carbon-based power).

Therefore, each time that a tower is attacked, the transmission company deals with repairs and additional operational costs to supply energy in the affected regions. We generalize the additional operational costs with the parameter $o \geq 0$. Therefore, the total expenses for the transmission company are

$$\theta(p + o),$$

where θ is the total number of attacks.

In summary, with honest contractors, $p = c_1$ and the cost of attacks for the transmission company is $\theta(c_1 + o)$. On the other hand, the benefit for the contractor is θU_1.

C. Modeling the Electroservicios Case

Here a contractor sees the opportunity to hire militants to commit attacks on specific towers and thus increase the use of their repair services.

Let $\tilde{\theta}_i \in \mathbb{Z}^*$ be the number of attacks sponsored by the i^{th} contractor and $b(\cdot)$ be the bribe or cost function of sponsoring attacks. We assume that the number the attacks $\tilde{\theta}_i$ increases the bribe b (guerrillas also have other opportunities and if they are asked to spend more time attacking electric towers, they will ask for more money to do so). Hence, the bribe is defined as convex function $b : \mathbb{Z}^* \to \mathbb{R}_+$.

The benefit of the contractor per sponsored attack $\tilde{U}_i$ is greater than the benefit of generic (non-sponsored) infrastructure attacks, because sponsored attacks are made carefully to reduce the repair expenses, that is, $\tilde{U}_i \geq U_i$. A contractor might use this additional benefit of sponsored-attacks to lower its bid, so it can compete for a contract. Let us denote the excess benefit with sponsored-attacks as $L_i = \tilde{U}_i - U_i$.

We now parameterize the way a contractor can change their bids with the knowledge that it can sponsor attacks (the goal of the contractor is to select a bid low enough to get the repair contract, even if it does not let the contractor get the full benefit of the lower costs of sponsored attacks). If a contractor decides to accept a benefit per tower of $\tilde{U}_i - \gamma L_i$ instead of $\tilde{U}_i$, with parameter $\gamma \in [0, 1]$, then the total cost of $\theta + \tilde{\theta}_i$ attacks for the contractor becomes

$$(\theta + \tilde{\theta}_i)\tilde{c}_i(\gamma) = \theta c_i + \tilde{\theta}_i(c_i - \gamma L_i),$$

where $\tilde{c}_i(\gamma)$ is the new cost per tower as a function of the benefit reduction γ. From the previous expression we have

$$\tilde{c}_i = c_i - \frac{\tilde{\theta}_i}{\theta + \tilde{\theta}_i}\gamma L_i$$

On the other hand, the profit function of the contractor with sponsored attacks $\tilde{\theta}_i$ is

$$\theta U_i + \tilde{\theta}_i(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i). \tag{1}$$

Thus, if $\gamma = 0$ the contractor does not offer reduced prices as bids, and its benefit per sponsored-attack is $\tilde{U}_i$. On the other hand, if $\gamma = 1$, then the bid can be reduced to its lowest value and the contractor accepts the typical benefit U_i (instead of $\tilde{U}_i$).

The optimal number of attacks, denoted by $\tilde{\theta}_i^{*1}$, can be found solving the following maximization problem

$$\begin{aligned} \underset{\tilde{\theta}_i}{\text{maximize}} \quad & \theta U_i + \tilde{\theta}_i(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i) \\ \text{subject to} \quad & \tilde{\theta}_i \in \mathbb{Z}^*, \end{aligned} \tag{2}$$

We assume that attacks are feasible if the benefit per sponsored attack is greater than zero, that is

$$\tilde{\theta}_i^*(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i^*) > 0.$$

From the point of view of the transmission company, the payments are reduced because $c_i \geq \tilde{c}_i(\gamma)$. However, the number of attacks might increase if the contractor can have some benefit. Therefore, the objectives of both transmission company and contractor might not be aligned. For this reason, it is necessary to design the contract rules to avoid incentives of contractors to increase the number of attacks.

1) Example: Let us consider a base bribe $b_0 + \lambda$ to launch only one attack. A second attack might be more difficult to launch, because unlawful activities count with scarce resources.

Therefore, the bribe for an additional attack is modeled as $b_0 + \lambda(1 + \alpha)$, where $\lambda\alpha$, with $\alpha > 0$, is the increased bribe cost for a second attack.

Let us define the additional cost for the k^{th} attack with the recursion $\lambda_k = \lambda_{k-1}(1 + \alpha)$, where $k = \{1, \ldots, \tilde{\theta}_i\}$ and $\lambda_1 = \lambda$. Now we can define the total bribe for $\tilde{\theta}_i$ attacks with the following function:

$$b(\tilde{\theta}_i) = \sum_{j=1}^{\tilde{\theta}_i} b_0 + \lambda_j = \tilde{\theta}_i b_0 + \lambda + \lambda(1 + \alpha) + \cdots + \lambda(1 + \alpha)^{\tilde{\theta}_i - 1}$$

The right hand side function is a geometric series is equivalent to

$$b(\tilde{\theta}_i) = \sum_{j=1}^{\tilde{\theta}_i} b_0 + \lambda_j = \tilde{\theta}_i b_0 + \lambda \frac{(1 + \alpha)^{\tilde{\theta}_i} - 1}{\alpha} \tag{3}$$

Since $\alpha > 0$, then $b(\tilde{\theta}_i)$ is a strictly increasing convex function as required by our assumptions.

We can use Eq. (3) to find the optimal number of sponsored attacks $\tilde{\theta}_i^*$ that solves the optimization problem in Eq. (2). Since $b(\tilde{\theta}_i)$ is convex, then the objective function in Eq. (2) is a concave function, and the solution satisfies the following First Order Condition (FOC):

$$\frac{\partial}{\partial \tilde{\theta}_i} \left(\tilde{\theta}_i(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i) \right) \Big|_{\tilde{\theta}_i = \tilde{\theta}_i^{*1}} = 0.$$

Solving the previous equation we have

$$\tilde{\theta}_i^{*1} = \ln \left(\frac{\alpha(\tilde{U}_i - \gamma L_i - b_0)}{\lambda \ln(1 + \alpha)} \right) \Big/ \ln(1 + \alpha) \tag{4}$$

In this case the number of optimal attacks is a convex function with respect to the benefit of the attacks $\tilde{U}_i - \gamma L_i$. Since $\tilde{\theta}_i^{*1}$ must be an integer, the attacks are unprofitable if $\tilde{\theta}_i^{*1} < 1$. We can use Eq. (4) to obtain the following condition for unprofitability:

$$\frac{\lambda}{\alpha}(1 + \alpha)\ln(1 + \alpha) + b_0 > \tilde{U}_i - \gamma L_i \geq U_i.$$

In general, the previous inequality is not satisfied if 1) the bribe b_0 is lower than the benefit of the contractor U_i; and 2) the term $\frac{\lambda}{\alpha}(1 + \alpha)\ln(1 + \alpha)$ is small. Particularly, the parameters that determine the

profitability of attacks cannot be manipulated directly by the transmission company.

III. Designing Contracts to Disincentivize Attacks by Contractors

We now discuss a model designed to reduce the incentives of contractors for attacking the power system infrastructure. The basic idea of the new contract structure is to guarantee contracts for a population n of contractors and award them specific repairs at random. That way even if a contractor sponsors an attack, they might actually be helping their competition. These new contracts would be vulnerable if a large set of contractors collude in attacks, but as far as we are aware, that level of corruption hasn't been encountered in Colombia.

The model we present in this section is based on our discussions with the transmission company of Colombia and how they changed the way they awarded contracts after the case of Electroservicios came to light. The technical details of the contracts are more involved and they deal with incentives as they relate to specific municipalities and incentives of the local populations (as it has been found that some of the local population who gets hired as temporary workers to help the contractor repair the tower are also involved in attacks, so contractors are also required in the revised contracts to bring all temporary workers from outside of the affected municipality, and they are not allowed to hire the local population). We are entering a confidentiality agreement with ISA, and XM (The Colombian Independent System Operator) to discuss these finer points, but in this section we model the impact of the main modification done in the way they awarded contracts.

Let us consider a mechanism in which the transmission company assigns individual repair tasks to contractors at random; that way a contractor will not know in advance if a repair service will be assigned to them or not. Similar to the previous case, the contractors in charge of repairs are selected using some auction; however, this time the transmission company selects only the n contractors with the lowest bids. With the new contract the expected profit function of contractors considering sponsored attacks is

$$\frac{\theta U_i + \tilde{\theta}_i(\tilde{U}_i - \gamma L_i)}{n} - b(\tilde{\theta}_i). \tag{5}$$

The optimal number of sponsored attacks $\tilde{\theta}_i^{*2}(n)$ can be found by solving the following maximization problem:

$$\begin{aligned} \underset{\tilde{\theta}_i}{\text{maximize}} \quad & \frac{\theta U_i + \tilde{\theta}_i(\tilde{U}_i - \gamma L_i)}{n} - b(\tilde{\theta}_i) \\ \text{subject to} \quad & \tilde{\theta}_i \in \mathbb{Z}^*. \end{aligned} \tag{6}$$

The optimal number of sponsored attacks $\tilde{\theta}_i^{*2}(n)$ is a function of the number of contractors n, which in this case is the decision variable of the transmission company. In particular, the optimal number of attacks in the first game is larger than the optimal number of attacks in this second game, that is: $\tilde{\theta}_i^{*1} \geq \tilde{\theta}_i^{*2}(n)$.

In this case, the expected benefits of contractors decrease fast. For instance, with $n = 2$ the contractor's benefits decrease in a half. The reduction in benefits will be greater for small values of n, and less significant as n increases.

In this new game, attacks are profitable if the benefit of sponsored attacks is positive, that is,

$$\frac{\tilde{\theta}_i(\tilde{U}_i - \gamma L_i)}{n} - b(\tilde{\theta}_i) > 0.$$

Therefore, sponsored attacks can be made unprofitable if the electricity transmission company selects n large enough to guarantee

$$\frac{\tilde{\theta}_i^{*2}(n)}{n}(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i^{*2}(n)) < 0 \tag{7}$$

On the other hand, selecting n contractors (instead of just one with the lowest bid) is more expensive for the electric transmission operator. In particular, the payment for individual repairs is larger in this

second game because it is defined as $\hat{p} = \max_{i\in\{1,\dots,n\}} c_i$ (we assume that the contractors report truthfully their bids). Thus, the payment is large enough to cover the repair expenses of all contractors. Specifically, the value of the payment is

$$\hat{p} = c_n,$$

where the additional cost with respect to the original game is

$$p_r(n) = \hat{p} - p = c_n - c_1.$$

The expected cost for the transmission company becomes $\theta_T(n)(p + p_r(n) + o)$. The transmission company would choose n companies to make attacks unprofitable with minimum expenses. This can be expressed as

$$\begin{aligned} \underset{n}{\text{minimize}} \quad & \theta_T(n)(p + p_r(n) + o) \\ \text{subject to} \quad & n \geq 1, \\ & Eq.(7), \end{aligned} \tag{8}$$

where $\theta_T(n) = \theta + \tilde{\theta}_i^{*2}(n)$. The objective function in Eq. (8) is a concave. Therefore, the optimal number of attacks $\tilde{\theta}_i^{*2}$ satisfies the following FOC:

$$\frac{\partial}{\partial\tilde{\theta}_i}\left(\frac{\tilde{\theta}_i}{n}(\tilde{U}_i - \gamma L_i) - b(\tilde{\theta}_i)\right)\bigg|_{\tilde{\theta}_i^{*2}} = 0.$$

Solving the previous equation we have

$$\tilde{\theta}_i^{*2}(n) = \ln\left(\frac{\alpha}{\lambda\ln(1+\alpha)}\left(\frac{\tilde{U}_i - \gamma L_i}{n} - b_0\right)\right)\Big/\ln(1+\alpha) \tag{9}$$

In this case, the number of optimal attacks decreases with n. Since $\tilde{\theta}_i^{*2}(n)$ must be an integer, then attacks are unprofitable if $\tilde{\theta}_i^{*2} < 1$. From Eq. (9) we obtain the following condition of unprofitability:

$$\left(\frac{\lambda}{\alpha}(1+\alpha)\ln(1+\alpha) + b_0\right) n > \tilde{U}_i \geq \tilde{U}_i - \gamma L_i.$$

Hence, the attacks are unprofitable if

$$n > \tilde{U}_i \Big/ \left(\frac{\lambda}{\alpha}(1+\alpha)\ln(1+\alpha) + b_0\right)$$

IV. Numerical Example

There is not enough information to estimate all the parameters of the model, therefore, we extract some parameters from news reports and make further assumptions to give values to other parameters of the model. We hope that once our confidentiality agreement with ISA is approved, we will be able to use more detailed estimates in future work.

The news report by Caracol [3] mentions that approximately 215 attacks on energy towers were sponsored in 3 years. The report mentions that the transmission company paid about $\$150$ million pesos ($\$83333$ USD) to repair each tower (labor costs are less expensive in Colombia than in the US or Europe). Let us assume that

$$c_1 = p = \$83333,$$

where c_1 includes both net repair expenses and the expected benefit U_1, such that

$$c_1 = E + U_1.$$

If we assume a rate of return of 10%, then the contractor might expect that an investment of capital E would give a benefit of $0.1E$. In other words, the benefit is $U_1 = 0.1E$ and the cost might be $c_1 = 11U_1$. Hence, the benefit of the contractor with terrorist attacks would be

$$U_1 = c_1/11 \approx \$7576.$$

On the other hand, we assume that careful attacks can lower the damage of the towers. The report from Semana Magazine [6] mentions that the minimum repair payment was $\$50$ million pesos ($\$27778$ USD). Therefore, let us assume that the attacks can be made reducing repair costs to the minimum. If we denote the minimum repair cost as $\underline{c_1} = 27778$, then the benefit in this case is $\underline{U_1} = \underline{c_1}/11 \approx \$2525$ and the minimum expenses are $\underline{E} = \$25253$. Because the transmission company does not know the exact damage of the tower, then it will make the usual payment p, leaving the contractor with a benefit per tower of

$$\tilde{U}_1 = p - \underline{E} = \$58081.$$

Here the benefit with sponsored attacks $\tilde{U}_1$ is more than seven times the benefit received by contractors when they repair electric towers with "regular" (i.e. not sponsored) attacks.

Now, let us define the bribe required to attack one tower as $b(1) = \$4444$ (recall that the attacks were made by 4 militants, whose fee was $\$1111$ USD). Let us assume that $b(1) = b_0 + \lambda$, with a variable cost equal to the 20% of the constant cost, that is, $\lambda = 0.2b_0$. Consequently, $b(1) = 1.2b_0$ and $b_0 = \$3704$.

If we assume that the number of sponsored attacks was optimal, then we can estimate the average number of attacks during one year as $\tilde{\theta}_i^{*1} = 215/3 \approx 72$. Besides, in a competitive auction the contractor would have to reduce its bid the most it can to increase its chances to get the contract. Hence, we can assume that $\gamma = 1$. Finally, the only parameter that remains is α, which can be estimated from Eq. (4) as $\alpha = 0.0234$.

Now we are interested in observing the change in the number of attacks with different values of γ. Figure 2 shows that as γ decreases, the number of attacks increases, because with larger γ the contractor has more benefits per tower, so it does not need to attack as many; however, more benefits per tower might prevent them from offering a competing bid in the first place, so this is something the attacker needs to balance when submitting the bids.

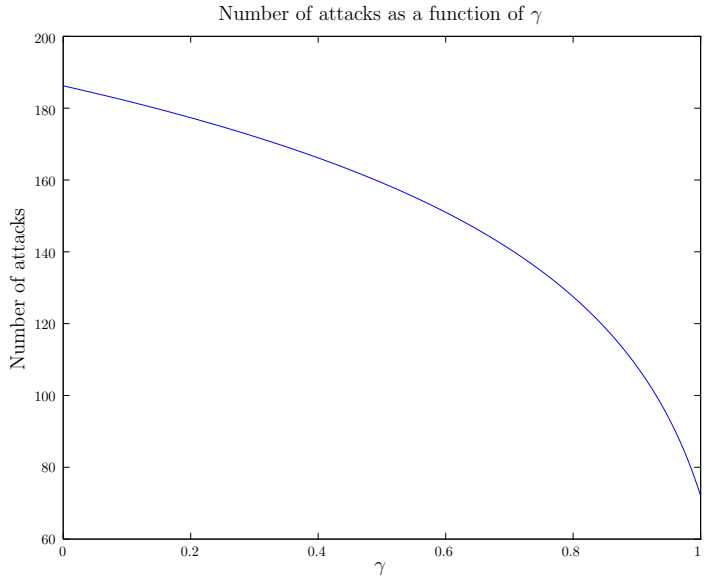

Fig. 2: Number of attacks as a function of the bid reduction established with γ.

We now investigate the change in the number of attacks with the mechanism the transmission company implemented for trying to reduce the perverse incentives of contractors to attack the towers they are

supposed to repair. Figure 3 shows the optimal number of attacks (see Eq. (9)) in a contract with the proposed mechanism. In this case we assume that $\gamma = 0$, which results in the best scenario for the contractor. In this experiment the number of attacks is greater than one if $n \leq 13$.

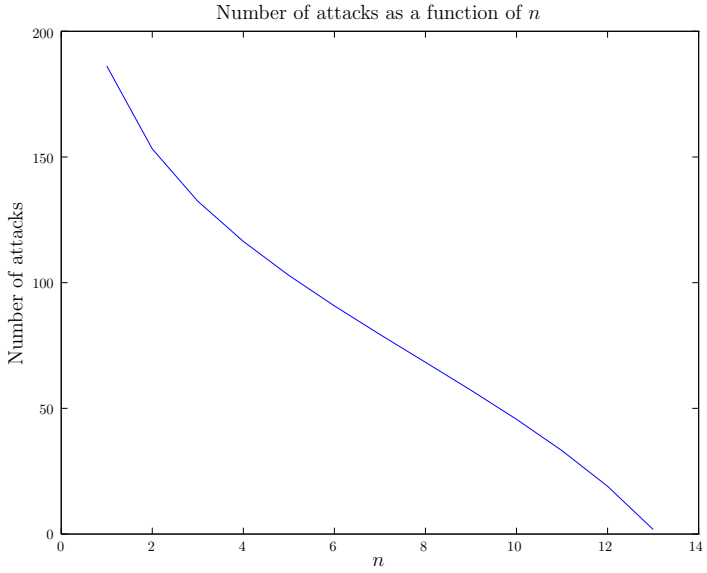

Fig. 3: Number of attacks as a function of the number of companies n.

Finally, Figure 4 shows the maximum profit of a contractor (e.g., when $\gamma = 0$) as a function of the number of attacks $\tilde{\theta}_i$ in both the original contract and the new contracts designed to prevent incentives for attacking (see Eqs. (1) and (5) respectively). The optimal number of attacks for the original contract (or a contract with $n = 1$) is $\tilde{\theta}_i^{*1} = 186$. However, if the transmission company implements a contract with $n = 14$ contractors, then the optimal number of attacks is $\tilde{\theta}_i^{*2} = 0$. Thus, random selection of contractors reduces the incentives for sponsored attacks.

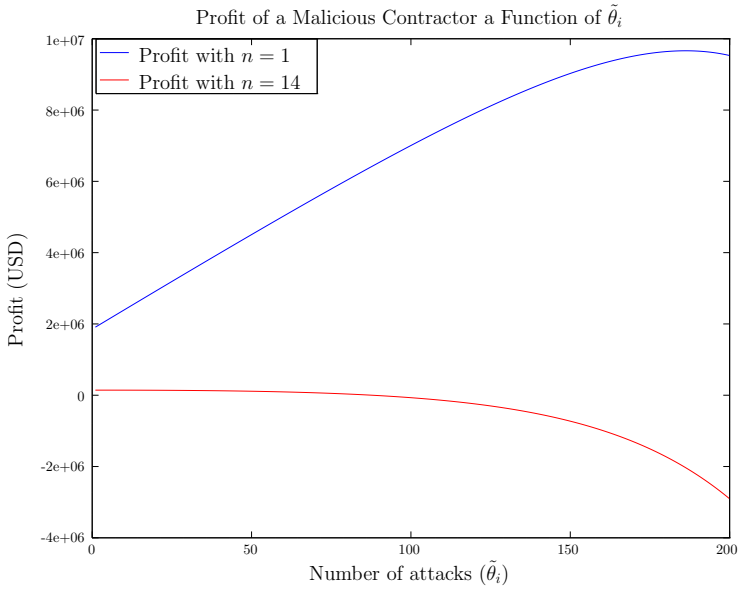

Fig. 4: Profit of a contractor in contracts with either 1 or 14 contractors. The inclusion of more contractors decrease the optimal number of attacks.

V. Conclusions

In this paper we provide a model of a series of attacks that happened in the Colombian power system, and the actions the electric transmission company took to minimize future contractors from launching similar attacks. In future work we will introduce more detailed models incorporating details of population incentives and the other parties in the larger internal conflict in Colombia.

Before we talked to the transmission company of Colombia we were thinking that a way to modify the contracts awarded to contractors could be based on paying the contractors a fix amount every year to fix as many towers as necessary. We thought the only challenge of this scheme would be for contractors to estimate the expected number of attacks, similar to what insurance companies do in their risk assessments. However, after talking with the transmission company in Colombia they mentioned that this approach has some drawbacks because the prices can be manipulated by malicious contractors. First, contractors who anticipate this type of contract might try to increase the number of attacks to increase the contract's payments (or to cause the bankruptcy of competing firms).

Yardstick competition is an alternative regulation mechanism that sets prices comparing costs of multiple similar firms [7]. This mechanism might help identify suspicious contractors bidding at a rate much lower than similar contractors in other regions. A malicious contractor can however offer bids that are consistent with Yardstick competition while still being δ smaller to bids from competing contractors.

We believe that the strategic nature of attackers, defenders, and the ecosystem of industries and other agents in the protection of large critical infrastructures in Colombia can serve to find analogies for the protection of critical infrastructures against cyber-attacks. While we are not aware of these attacks happening, we can imagine an anti-DDoS service contractor sponsoring DDoS attack so they get paid to help the afflicted company survive these incidents. Similar to the case studied in this paper, to prevent these types of attacks companies might require to hire the services of multiple anti-DDoS companies, so each of them wouldn't know in advance if they are going to get hired as a response to a particular incident or not. We will pursue more concrete analogies in future work.

Acknowledgments

This work is supported by NSF CNS-1547502 and NSF CMMI-1541199. We thank Ross Baldick for helpful feedback on a previous version of this paper.

References

[1] R. Zimmerman, C. E. Restrepo, N. Dooskin, J. Fraissinet, R. Hartwell, J. Miller, and W. Remington, "Diagnostic tools to estimate consequences of terrorism attacks against critical infrastructure," in *Proceedings of the U.S. Department of Homeland Security conference, Working Together: Research and Development Partnerships in Homeland Security, Boston, MA*.

[2] Semana, "Negocio redondo," August 2008. [Online]. Available: http://www.semana.com/nacion/articulo/negocio-redondo/94315-3

[3] Caracol radio, "Capturan a funcionarios de una empresa que atentaba contra las torres eléctricas de ISA," http://caracol.com.co/radio/2009/06/15/judicial/1245050340_829038.html, 2009.

[4] C. de Colombia, "Ley 80 de 1993," http://www2.igac.gov.co/igac_web/UserFiles/File/web%202008%20/ley%2080-93.pdf, 1993.

[5] ——, "Decreto 1510 de 2013," http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53776#163, 2013.

[6] Semana, "Negocio redondo," http://www.semana.com/nacion/articulo/negocio-redondo/94315-3, 2008.

[7] A. Shleifer, "A theory of yardstick competition," *The RAND Journal of Economics*, pp. 319–327, 1985.