Game Theoretic Characterization of Collusive Behavior among Attackers

Abhishek Roy*, Charles A. Kamhoua†, and Prasant Mohapatra‡
*Department of Electrical and Computer Engineering, University of California, Davis, USA,
‡Department of Computer Science, University of California, Davis, USA,
†CIV US Army RDECOM ARL (US)
Email: { abroy, pmohapatra }@ucdavis.edu, charles.a.kamhoua.civ@mail.mil

Abstract – **Recent observations have shown that most of the attacks are fruits of collaboration among attackers. In this work we have developed a coalition formation game to model the collusive behavior among attackers. The novelty of this work is that we are the first to investigate the coalition formation dynamics among attackers with different efficiency. Most of the related works have modeled the attacker as a single entity. We define a new parameter called friction to represent the unwillingness of an attacker to collude. We have shown that the proportion of attackers in the Maximum Average Payoff Coalition (MAPC) decreases with efficiency. We have also shown that as the friction increases, size and heterogeneity of MAPC decrease. We show, using text analysis on a hacker web forum chat data, that the hacker collaboration network shows a strong small-world characteristics. We identify the leaders in these coalitions. The cluster compositions of the hacker collaboration network agree with our model. We also develop method to estimate the friction parameters for the attackers to decide optimal coalition to join. As this model provides insight into coalition formation among attackers, e.g., leaders, composition, and homogeneity, this model will be helpful to develop better defender strategies.**

I. INTRODUCTION

Most security games concentrate on abstracted scenarios where a single defender is up against a single attacker. But now-a-days most of the attacks are fruits of collaboration among attackers. We want to emphasize that collaboration does not necessarily be towards a single attack, and hence, it is not possible to model the collaborating attackers as a metaphorical single attacker. It has been observed that attackers sharing resources among themselves can have totally different objectives and attack targets. For example, in many cybercrimes insider information is needed [1]. While the insider may not be involved in the attack directly, without his/her help the attack may not be possible. Similarly, while launching an attack, a hacker often seeks help from other hackers. This collaboration needs to be understood as the helping hackers are indirectly partaking in the attack. Therefore, identifying attackers who can be potential members of a coalition for a successful attack will be useful to take precaution against imminent attacks. So, we need to understand the coalition formation dynamics among attackers to develop better defender strategy.

There are numerous examples of collusive attackers in real life. For example, in the underground market an ATM card pin code sells at $0.40 – $20.00 and a bank account sells at $10 – $100. The price for an individual's identity, i.e., name, social security number, and birth day is $1 - $15 [2]. Higher level attackers like terrorist organizations can exploit this information to pull off a bigger heist which provides an incentive for the attackers to work together. In these cases finding a suitable strategy against a single attacker may not be useful. Attacks can also be politically motivated, e.g., the Stuxnet attack on Iran's nuclear program in 2010 [3]. Most of the hacker communities have reputation score to represent the efficiency and reliability of a hacker. The hacker may also launch an attack to increase its reputation score. Gang of hackers also compete among themselves for cyberspace resources to establish their dominance [4]. These online crimes, while motivating the existence of communities among the attackers also bear evidence of competition among themselves.

Even though in this work we have tested our model against the data of a hacker web-forum, this model will be applicable to any crime where the attackers can benefit from collusion. Examples include cyber-crime, poaching, drug trafficking [5], and terrorism. In 1993 Mumbai bomb blast, it was reported that the main perpetrator D-company allied with several other mafia groups to execute the attack [6]. Many well-known terrorist groups have well established alliances with other terrorist groups [7]. Our model is applicable to these scenarios as well.

The objective of this work is to explore the reasons of collusive behavior among the attackers. We study the characteristics of coalitions among an infinite population of attackers with different efficiency and infer their implications.

Understanding of collusive behavior among attackers will help to improve defense mechanisms. For example, say a defender is in a hacker web-forum in disguise. If a group of hackers is observed sharing resources on similar topics then the defender can boost up its security measures according to the resources being shared. In another scenario, many attackers consulting a particular attacker repeatedly indicates that he is an expert. A defender may develop strategy to block the formation of groups which includes that expert to prevent imminent attacks. There can be two parallel attacks where the smaller one is just a decoy to divert attention from the bigger one. But observing the types of attackers collaborating and resources being shared within attacker coalitions the defender can be prepared against both the attacks.

Understanding of group dynamics among attackers demands attention to some observed characteristics of them. As we show in the data analysis section, highly efficient attackers do not team up with attackers of similar ranks. The reasons are:

i) Unavailability: One trivial reason is large number of highly efficient attackers may not be available.

ii) Tragedy of commons: Cyberspace is limited resource economy, e.g., only 0.00001% of the population responds to a phishing mail [2, 8]. In a limited resource economy, *tragedy of*

commons means that if a single player overexploits the resources then the whole coalition of players suffer. More efficient attackers are capable of dominating an attack depriving other efficient attackers of their expected profit. This leads to an unstable group dynamics.

iii) Efficiency of the attacker: A very efficient attacker is capable of launching an attack alone. He uses small attackers at a small cost to increase the scale of the attack. An extreme example of this is the Distributed Denial of Service (DDoS) attack where only one attacker controls the attack and uses millions of machines across internet to scale up the attack.

In our proposed model, we introduce a new parameter, *friction* between two attackers, which represents their reluctance to collude. Friction is defined as the fractional loss of efficiency for each attacker due to collusion. Qualitatively, if the friction between two attackers is high then they are less prone to collude with each other and vice versa. The less efficient the attacker is, the less is his/her friction with others. So large number of highly efficient attackers cannot collude as that will decrease their effective efficiency. The facts that a highly efficient attacker is not easily available, and can lead to the problem of *tragedy of commons* are explained by his/her high friction with other highly efficient attackers. But more efficient attackers can still form collusions with less efficient attackers due to small friction. Apart from the above mentioned coalition dynamics observed among attackers, friction also explains other commonly observed traits of coalition formation in a limited resource economy. For example, as the coalition size increases the cost of monitoring increases which is a key factor behind the existence of a stable group [9]. Similarly, as coalition size increases, the loss from friction increases among the players which is analogous to increased monitoring cost and this leads to a bounded coalition size. In any stable coalition, if a member is not following the rules, that member is banned temporarily or permanently. Likewise, these members can be modelled as having very high friction with others which ensures that he will be undesired in any stable collusion.

The contributions of this work are as follows:

- We have proposed a game explaining the observed collusive behavior among attackers of different efficiency levels.
- We have examined the model quite thoroughly establishing several characteristics of the attacker coalitions along with proving the existence of core.
- We have verified the behavior predicted by the model against real life collusive behavior among hackers. Absence of analysis on real data was a major drawback of the previous works very of which were there.
- To the best of our knowledge, our game theoretic model is the first one to investigate the mechanism and characteristics of coalition formation among attackers.
- We quantify the strength of collusion and identify the leaders in a coalition.

The rest of the paper is organized as follows. Related work is presented in Section II. Section III presents the proposed mathematical model and analysis of coalition characteristics. We explain the model through a toy example in Section IV. Estimation of friction parameters are discussed in Section V. Simulation and data analysis results are shown in Section VI. We conclude the paper in Section VII.

II. RELATED WORK

Previous research in this area models attackers as individual entities or groups operating independently [10 – 14]. A few recent works models the scenario of multiple collusive attackers. The authors of [15] have considered the scenario in which an attacker can attack multiple nodes simultaneously. They have shown that Nash equilibrium for this scenario exists and has interchangeability property, i.e., as long as the defender and the attacker are playing strategies corresponding to any equilibrium, essentially the resulting strategy profile will consist a Nash Equilibrium. Even though Ref. [15] considers multiple attacker resources, they do not consider collusion among multiple attackers. Ref. [16] models the case of multiple attackers and single defender as a Coalitional Skill Game [17]. The network is modeled as a collection of different types of connected targets. A fixed set of skills are needed to attack a particular type of target. Attackers form coalitions to pool their skills together to attack a target. But this work assumes that the graph describing the coalitions of attackers is known which is unrealistic. A more detailed and realistic analysis of collusive attackers vs. single defender can be found in [5]. Ref. [5] obtains the optimal defender strategy by solving a Mixed Integer Linear Program (MILP) given the knowledge of payoff matrices, risks, and probability of success for each target. The attackers are modeled using human behavioral models using the data obtained from a game developed by the authors and played 700 subjects. By far, [5] is the most extensive work on this topic though the exact knowledge of payoff matrices, risks, and probability of success for each target are strong and a little unrealistic assumptions. Ref. [5] does not validate their results through real attacker dataset. To the best of our knowledge, till date there is no work which considers behavioral features, and dynamics of hackers explicitly. Irrational competition among hackers have not been addressed in any work. Also, heterogeneity among attackers have been broadly overlooked.

The heterogeneity and collusive behavior among hackers have been studied in [18 – 20]. Authors of [18] studied the discussions among hackers of USA and China over years on web forums. They have found that there are communities within hackers. Hackers with more diversity and novelty tend to be leaders. Less efficient hackers try to form group with the leaders for code snippets, stolen identities, and fully developed applications. It is stated in [19] that hackers tend to form small world networks with small clustering coefficient. The authors of [20] have discovered clustering based methodology to identify hacker communities and possible leaders among them. These works strongly support that attackers operate in communities, and thereby motivates the need for gaining insight into behavior and dynamics of collusive attackers.

In our proposed work we have used a framework similar to the one in [21] to model the attackers. Ref. [21] describes partnerships among players of various abilities and explains why grand coalition may not form in this case. We extend this framework to incorporate friction among attackers, and explore other relevant properties.

III. MODEL

All the notations used in this paper are defined in Table 1. In our proposed model we assume that attackers can be of M efficiencies $1 \geq e_1 > e_2 \cdots > e_M > 0$. We do not consider efficiency to be task-specific. Efficiency defines the capability of an attacker; a more efficient attacker is more capable to launch and exploit an attack regardless of the resource being attacked. In reality, it is indeed observed that hacker web forums have reputation scores for its users which represent the efficiency of the hacker [19].

Definition 1: The friction between two attackers of efficiency e_i and e_j, f_{ij} is a measure of loss of efficiency for each of them due to collusion, and is defined as,

$$f_{ij} = \frac{e_i - e_i{}'}{e_i e_j} = \frac{e_j - e_j{}'}{e_i e_j}.$$

where $e_{i(j)}{}'$ is the effective efficiency of attacker $i(j)$ after collusion, $e'_{i(j)} = e_{i(j)} - e_i e_j f_{ij}$.

Table 1: List of Parameters

Notation	Meaning
M	Total number of efficiency levels
e_i	Efficiency of i^{th} level
e_i-attacker	An attacker with efficiency e_i
$\bar{e}$	Average efficiency of a coalition
e_i'	Effective efficiency after collusion
$\bar{e}'$	Average effective efficiency after collusion
f_{ij}	Friction between two attackers of efficiency e_i and e_j
F	Friction matrix, $F = [f_{ij}]$
G	A coalition of attackers
$T(\lvert G\rvert)$	Incentive factor in total payoff due to scale
$V(\lvert G\rvert)$	Incentive factor in average payoff due to scale, $T(\lvert G\rvert) = \lvert G\rvert V(\lvert G\rvert)$
n_i	Number of e_i-attacker in a coalition
s_i	Total number of available e_i-attackers
$\boldsymbol{n}$	Composition of a coalition, $\boldsymbol{n} = \{n_i\}$
$a(\boldsymbol{n})$	Average payoff of a coalition with composition $\boldsymbol{n}$
$t(\boldsymbol{n})$	Total payoff of a coalition with composition $\boldsymbol{n}$
$\boldsymbol{n}_{\max}$	Coalition composition maximizing $a(\boldsymbol{n})$
$\boldsymbol{n}_{\mathbf{i},\max}$	i^{th} element of $\boldsymbol{n}_{\max}$
I	$M \times$ M Identity matrix
E	$M \times M$ diagonal matrix with diagonal elements $e_1, e_2, \dots, e_M$
D	$M \times M$ diagonal matrix with diagonal elements $f_{11}, f_{22}, \dots, f_{MM}$
$\mathbf{1}$	$M \times 1$ vector with all elements equal to 1
ϵ	Between Group friction, $\epsilon = f_{ij} \quad i \neq j \quad i,j = 1,2,\dots,M$
δ_i	Difference between Within and Between Group friction, $\delta_i = f_{ii} - \epsilon \quad i = 1,2,\dots,M$
$CI(G)$	Collusion Index of coalition G
$\mathbb{R}^M$	M dimensional real space
F_i	Fraction of efficiency e_i effective in a coalition
$\mathbb{G}(P,a)$	Coalition formation game with player set P, payoff function a
S_i	i^{th} subset of a partition of P corresponding to the core of $\mathbb{G}$
N	Maximum Average Payoff Coalition (MAPC) size, $N = \lvert\boldsymbol{n}_{\max}\rvert$
c_i	Marginal Contribution of attacker i
$a_{-i}(\boldsymbol{n}_{\max})$	Average payoff of the MAPC when attacker i is left out
Δ_i	Decrease in average payoff of MAPC when e_i-attackers leave
L_i	Leadership metric of e_i-attackers, $L_i = \Delta_i/n_i$
$\hat{x}$	Estimate of variable $x, x = \epsilon, \delta, n_i$
S	$S = \sum_{i=1}^{M} \hat{n}_i e_i$
L_e	Sum of squares of residuals while estimating n_i
σ	Small-worldness index
$C_{n(r)}$	Clustering coefficient of a given (random) network
$L_{n(r)}$	Average path length on a given (random) network
G_H	Collaboration graph among hackers
α_i	$\alpha_i = (\hat{n}_i - 0.5)/(S - 0.5e_i)$

Assumption 1.

a) $0 \leq f_{ij} \leq 1$ and the matrix $F = [f_{ij}] \succ 0$.

b) $f_{11} \geq f_{22} \dots \geq f_{MM}$.

c) $f_{ii} \geq f_{ij}\ \forall i,j = 1,2,\dots,M$.

Assumption 1 reflects the facts that friction between similarly efficient attackers is more, and more efficient hackers have more friction. The total payoff of a coalition G of attackers is given by $T(|G|)\sum_{i\in G} e_i{}'$ where $|G|$ is the coalition size. As we show later via real data that attackers do form coalitions, we assume $\frac{\partial T(|G|)}{\partial |G|} > 0$. This is similar to economies of scale [21]. The average income of a coalition is denoted by $\frac{T(|G|)\sum_{i\in G} e_i{}'}{|G|}$. If a coalition G has n_i attackers of efficiency $e_i (i = 1,2,\dots,M)$ then the total payoff of G is given by

$$t(\boldsymbol{n}) = T(n)\sum_{i=1}^{M} n_i e_i{}' = T(n)\sum_{i=1}^{M} n_i e_i\left(1 + f_{ii}e_i - \sum_{j=1}^{M} n_j f_{ij} e_j\right).$$

where $n = n_1 + n_2 + \cdots + n_M$, and $\boldsymbol{n} = [n_1, n_2, \dots, n_M]^T$. The average payoff is given by, $a(\boldsymbol{n}) = t(\boldsymbol{n})/n$.

Assumption 2. $T(|\boldsymbol{n}|) = n$.

In matrix form,

$$a(\boldsymbol{n}) = \mathbf{1}^T E(I + DE)\boldsymbol{n} - \boldsymbol{n}^T EFE\boldsymbol{n}. \qquad (1)$$

Where $E = \text{diag}(e_1, e_2, \dots, e_M), \mathbf{1} = [1,1,\dots,1]^T, I = M \times$ M Identity matrix, and $D = \text{diag}(1 + f_{11}, 1 + f_{22}, \dots, 1 + f_{MM})$. In this paper we assume the payoff of a coalition is divided equally among its members as in [21].

Theorem 1. The maximum coalition size is bounded as,

$$n \leq \frac{e_1(1 + f_{11}e_1)}{e_M^2 f_{MM}}.$$

Proof. $a(\boldsymbol{n}) \geq 0$

$\Rightarrow \sum_{i=1}^{M} n_i e_i(1 + f_{ii}e_i) > \sum_{i=1}^{M}\sum_{j=1}^{M} n_i n_j e_i e_j f_{ij}$

Combining Assumption 1(b) and 1(c) we get,

$\Rightarrow e_1(1 + f_{11}e_1)\sum_{i=1}^{M} n_i > e_M^2 f_{MM}\sum_{i=1}^{M}\sum_{j=1}^{M} n_i n_j$

$\Rightarrow \frac{e_1(1 + f_{11}e_1)}{e_M^2 f_{MM}} \geq n.$ ∎

This shows that the group size cannot increase unboundedly irrespective of what $T(n)$ is.

We solve the following optimization by augmented Lagrangian method to obtain the Maximum Average Payoff Coalition (MAPC).

$$\max_{\substack{n_i \geq 0 \\ i=1,2,\dots,M}} a(\boldsymbol{n}).$$

Theorem 2. $a(\boldsymbol{n})$ has a unique global maxima and the maxima is achieved at $\boldsymbol{n}_{\max} = \frac{1}{2}(E^{-1}F^{-1}E^{-1})(I + ED)E\mathbf{1}$.

Proof. As E is a diagonal matrix with positive elements $E \succ 0$. Under Assumption 1, $F \succ 0 \Rightarrow EFE \succ 0$. Hessian of $a(\boldsymbol{n})$ is $-2(EFE) \prec 0$. So $a(\boldsymbol{n})$ is concave, hence possesses a global optima which is the solution to the following equation:

$$\nabla a(\boldsymbol{n}) = 0$$
$$\Rightarrow \boldsymbol{n}_{\max} = \frac{1}{2}(E^{-1}F^{-1}E^{-1})(I + DE)E\mathbf{1}. \quad (2)\blacksquare$$

Note that we have not restricted $\boldsymbol{n}$ to be an integer vector. In real life an attacker is often part of multiple coalitions among which it divides its resources. This phenomenon manifests itself as fractional presence in our model.

Highly efficient attackers team up with lower level attackers to increase the scale of the attack. If the coalition size increases beyond $\mathbf{1}^T\boldsymbol{n}_{\max}$ then due to equal sharing, advantage of large coalition size is undermined. The total payoff of a coalition is maximized at a larger coalition size than $\mathbf{1}^T\boldsymbol{n}_{\max}$.

Theorem 3. $t(\boldsymbol{n})$ has a unique maxima with coalition size greater than or equal to $\mathbf{1}^T\boldsymbol{n}_{\max}$.

Proof. Say, $t(\boldsymbol{n})$ has a maxima at $\boldsymbol{n}'_{\max}$ where coalition size $m = \mathbf{1}^T\boldsymbol{n}'_{\max} < \mathbf{1}^T\boldsymbol{n}_{\max}$. As $a(\boldsymbol{n})$ is strictly concave,

$$a(\boldsymbol{n}'_{\max}) < a(\boldsymbol{n}_{\max})$$

and, $m < \mathbf{1}^T\boldsymbol{n}_{\max}$. So

$$t(\boldsymbol{n}'_{\max}) = ma(\boldsymbol{n}'_{\max}) < \mathbf{1}^T\boldsymbol{n}_{\max}a(\boldsymbol{n}_{\max}) = t(\boldsymbol{n}_{\max}).$$

But this is a contradiction as $t(\boldsymbol{n})$ has a maxima at $\boldsymbol{n}'_{\max}$. So, $m \geq \mathbf{1}^T\boldsymbol{n}_{\max}$. As $\boldsymbol{n}$ is non-negative and due to Theorem 1, $\boldsymbol{n}$ is closed and bounded in $\mathbb{R}^n$. $t(\boldsymbol{n})$, a real-valued continuous function in a closed and bounded interval, by extreme value theorem, has at least one maxima and one minima. As $t(\boldsymbol{n})$ is cubic function of $\boldsymbol{n}$, there will be a unique maxima. ■

Now, for better interpretability, let us introduce two types of friction: *Within Groups* (WG) and *Between Groups* (BG).

Assumption 3. The friction matrix is of the following form:

a) BG friction $f_{ij} = \epsilon, 0 \leq \epsilon < 1 \ \forall i, j = 1,2,\dots,M \text{ and } i \neq j.$

b) WG friction $f_{ii} = \epsilon + \delta_i \ \forall i = 1,2,\dots,M \ \ 0 < \delta_i \leq 1 - \epsilon.$

This structure also ensures that F is a positive definite matrix. To see this, F can be written as:

$$F = \begin{bmatrix} \epsilon & \cdots & \epsilon \\ \vdots & \ddots & \vdots \\ \epsilon & \cdots & \epsilon \end{bmatrix} + \begin{bmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_M \end{bmatrix} = A + B.$$

$\boldsymbol{y}^T A\boldsymbol{y} = \epsilon(\mathbf{1}^T\boldsymbol{y})^2 \geq 0, \forall \boldsymbol{y} \in \mathbb{R}^M$. All eigen values of B are positive. So $\boldsymbol{y}^T B\boldsymbol{y} > 0, \forall \boldsymbol{y} \in \mathbb{R}^M$. So, $\boldsymbol{y}^T F\boldsymbol{y} > 0, \forall \boldsymbol{y} \in \mathbb{R}^M$. Note that F still ensures that the loss of efficiency due to friction is more for more efficient hackers because the loss of efficiency between two players of efficiency e_i and e_j is given by $e_i e_j f_{ij}$, i.e. the loss is proportional to efficiency.

We should look more closely at the relationship between friction and the extent of collusion among the attackers.

Definition 2: We define the Collusion Index (CI) as the effective normalized efficiency of a coalition. Quantitatively, if a coalition G has n_i attackers of efficiency $e_i (i = 1,2,\dots,M)$, and the friction matrix is $F = [f_{ij}]$,

$$CI(G) = \frac{a(\boldsymbol{n})}{\sum_{i=1}^{M} n_i e_i} = \frac{\sum_{i=1}^{M} n_i e_i F_i}{\sum_{i=1}^{M} n_i e_i} = \frac{\bar{e'}}{\bar{e}}.$$

where $F_i = 1 - \sum_{j=1}^{M} n_j e_j f_{ij} + f_{ii} e_i$, $\bar{e'}$ is the effective average efficiency of G, and $\bar{e}$ is the average efficiency of G. F_i represents the fraction of efficiency e_i which is effective in G. When all the friction coefficients are 0, $\bar{e'} = \bar{e}$ and $CI(G) = 1$ implying full collusion, i.e., the attackers are collaborating towards a single attack. When $a(\boldsymbol{n}) = 0$, $CI(G) = 0$ implying no attacker can benefit from this coalition and the coalition will disintegrate. When, $0 < CI(G) < 1$, it means that attackers collaborate to maximize their profit but with their own, and possibly different attack plans.

Let us consider the game $\mathbb{G}\big(P, a(.)\big)$ being played by $s_1, s_2, \dots, s_M$ players of efficiency $e_1, e_2, \dots, e_M$ respectively, and P is the set of these players. The friction matrix is F. The payoff of a player belonging to a coalition consisting of $n_1, n_2, \dots, n_M$ players of efficiency $e_1, e_2, \dots, e_M$ respectively is given by $a(n_1, n_2, \dots, n_M)$. In a cooperative game the *core* is an imputation which cannot be improved by any other coalition structure. A coalition structure is *individually stable* if there is no player who can improve his/her payoff by joining another coalition and that coalition welcomes that player. A coalition structure is *Nash stable* if there is no player who can improve his/her payoff by joining another coalition.

Theorem 4. (*Existence of core*) Under Assumption 3, the core of the game $\mathbb{G}$ is non-empty.

Proof. As F is a positive definite matrix, according to Theorem 2, $a(\mathbf{n})$ is maximized at $\boldsymbol{n}_{\max} = \big(n_{1,\max}, n_{2,\max}, \dots n_{M,\max}\big)$. If $s_i < n_{i,\max}, i = 1,2,\dots,M$, then all the attackers form a coalition to maximize payoff and the grand coalition is in the core. Else, a subset of attackers form a coalition S_1 to maximize payoff. If we eliminate this attackers, as the friction matrix is still positive definite, a subset of the rest of the attackers $(P - S_1)$ form a coalition S_2 to maximize their payoff and so on. Here we assume that ties are broken randomly. These set of coalitions $\{S_1, S_2, \dots\}$ construct the core of $\mathbb{G}$. ■

Proposition 1 (*Stability properties*). The coalition structure formed as in Theorem 4 is strict core stable but not necessarily Nash stable.

Proof. Observe that the coalition structure developed in Theorem 4 consists of unique MAPC among the available attackers at various stages. So a player cannot join a coalition with higher payoff than him as that coalition is a MAPC and admitting the new player will decrease the payoff for all the players in that coalition. Similarly, no player will join a coalition with lower payoff as he already is in a MAPC and joining a MAPC with lower payoff will reduce his/her payoff. So the solution is strict core stable.

We will prove that the solution is not necessarily Nash stable through an example. We take $\epsilon = 0$. Without any restriction on the number of available attackers, the MAPC consists of $n_{i,\max}$ attackers of efficiency e_i $(i = 1,2,\dots,M)$ where $n_{i,\max} = \frac{1}{2} + \frac{1}{2\delta e_i}$ $i = 1,2,\dots,M$. Let us assume, $1 \geq e_1 > e_2 \cdots > e_M > 0$. Consider an example that, before any coalition formation, in total there were $2n_{1,\max} - 1, 2n_{2,\max}, \dots, 2n_{M,\max}$ attackers of efficiency $e_1, e_2, \dots, e_M$. After the first MAPC has formed with $n_{i,\max}$ attackers of efficiency e_i, the second MAPC will contain rest of the attackers. Let the average payoffs of two MAPCs be a_1, and a_2. Then $a_2 = a_1 - e_1\big[1 - 2\big(n_{1,\max} - 1\big)e_1\delta\big]$. Now if

an attacker with efficiency e_2 joins the first MAPC from the second, then his/her new payoff, $a_2' = a_1 + e_2(1 - 2n_{2,\max}e_2\delta)$.

$$a_2' - a_2 = e_2(1 - 2n_{2,\max}e_2\delta) + e_1[1 - 2(n_{1,\max} - 1)e_1\delta]$$

Replacing $n_{i,\max} = \frac{1}{2} + \frac{1}{2\delta e_i}$ $(i = 1,2)$,

$a_2' - a_2 = \delta(e_1^2 - e_2^2) > 0 \quad \Rightarrow a_2' > a_2$.

This shows that one attacker can improve his/her payoff by joining another coalition showing that the coalition structure in Theorem 4 is not necessarily Nash Stable. ■

By properties of strict core stability, the coalition structure in Theorem 4 is strongly individually stable, and hence individually stable, and hence individually rational.

The marginal contribution of attacker i to the MAPC is measured by $c_i = a(\boldsymbol{n}_{\max}) - a_{-i}(\boldsymbol{n}_{\max})$ where $a_{-i}(\boldsymbol{n}_{\max})$ is the average payoff of the MAPC when attacker i is left out.

Proposition 2. Marginal contribution of an attacker is proportional to efficiency as well as WG friction.

Proof. Let there be a MAPC with $n_i (i = 1,2)$ attackers of efficiency e_i, where $e_1 > e_2$. The BG friction is ϵ, and WG friction of e_i-attacker is $(\epsilon + \delta_i)$. We assume $n_1, n_2 \geq 1$. The marginal contribution of an e_k-attacker is given by –

$$c_k = e_k(1 + 2e_k f_{kk}) - 2\sum_{i=1}^{2} n_i f_{ik} e_i e_k \qquad k = 1,2. \tag{3}$$

In a MAPC,

$$n_1 = \frac{(\epsilon+\delta_1)(\epsilon+\delta_2) + \frac{\delta_2}{e_1} - \frac{e_2}{e_1}\epsilon(\epsilon+\delta_2)}{2[\delta_1\delta_2 + \epsilon(\delta_1+\delta_2)]}, \; n_2 = \frac{(\epsilon+\delta_1)(\epsilon+\delta_2) + \frac{\delta_1}{e_2} - \frac{e_1}{e_2}\epsilon(\epsilon+\delta_1)}{2[\delta_1\delta_2 + \epsilon(\delta_1+\delta_2)]}. \tag{4}$$

From (3) and (4),

$$c_i = e_i^2(\epsilon + \delta_i) \quad i = 1,2. \tag{5}$$ ■

Observe that the marginal contribution of an attacker is proportional to efficiency, and, a little counterintuitively, also to WG friction. This is because, if WG friction is high then there will be less number of attackers in the coalition, in turn increasing their marginal contribution.

Marginal contribution is not a good measure to decide the leader of a coalition because to qualify as a leader, besides contributing to the coalition, the leader should also be able to be part of a large coalition. A leader group should be a small fraction of the MAPC but relatively contribute more. As marginal contribution can be maximized by increasing friction, i.e., by decreasing the coalition size, it is not a good representative value of leadership. Let us consider that the MAPC contains $n_1, n_2, \dots, n_M$ attackers of efficiency $e_1, e_2, \dots, e_M$ respectively and the average payoff is a. If all the e_i-attackers $(i = 1,2, \dots, M)$ leave the MAPC, the average payoff reduces to $a - \Delta_i$ $(\Delta_i \geq 0)$.

Definition 2: The *leader* group of a MAPC is defined to be the attacker(s) with maximum leadership metric, $L_i = \Delta_i / n_i$.

$$L_i = e_i\left[1 - (n_i - 1)e_i f_{ii} - 2\sum_{\substack{j=1 \\ j\neq i}}^{M} n_j e_j f_{ij}\right] i = 1,2, \dots M. \tag{6}$$

A group of attackers with less efficiency can be leader because they have lower friction than more efficient attackers. To see this, under Assumption 3, set $M = 2$, $\delta_1 = \epsilon = 0.001$, $e_1 = 1$, and $e_2 = 0.5$ in (6). Figure 1 shows that when $0 < \delta_2 < 0.33\delta_1$, $L_2 > L_1$, i.e., the e_2-attackers are leaders even though their efficiency is lesser than e_1-attackers.

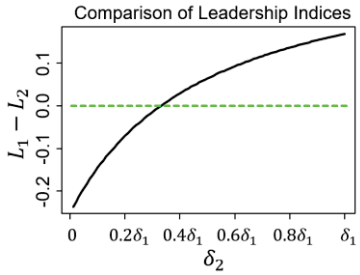


Fig. 1. Leadership index of less efficient attackers can be more than more efficient hackers.

Homogeneity of a group is another interesting aspect of a coalition. We measure the homogeneity of a group by the variance of efficiency, V_E of attackers in a coalition. We present the analysis for attackers of two possible efficiency levels here deferring the results for multiple efficiency levels to Section VI. Let there be attackers of two efficiency levels e_1, and $e_2 (e_1 > e_2)$. As long as there is only one type of attackers in the MAPC, $V_E = 0$. V_E increases when MAPC has attackers of the other efficiency level. So we restrict our analysis only to the case when MAPC includes attackers of all levels of efficiency. With a given friction matrix F as in Assumption 3, in a MAPC, n_1, and n_2 are given by (4). Then,

$$V_E = \frac{n_1 n_2}{n_1 + n_2}(e_1 - e_2)^2. \tag{7}$$

If there is no BG friction, i.e. $\epsilon = 0$,

$$\frac{1}{n_1} + \frac{1}{n_2} = \frac{2\delta}{\delta + \frac{1}{e_1}} + \frac{2\delta}{\delta + \frac{1}{e_2}}. \tag{8}$$

Right hand side of (8) is an increasing function of δ implying V_E is a decreasing function of δ. Observe that V_E is an increasing function of coalition size when proportion of attackers are constant. When $\epsilon > 0$, V_E takes a complicated form. We have shown the results in Section VI.

It will be interesting to see how the collusive behavior is affected by heterogeneity. We take MAPC size as the strength of collusion. Two effciency-levels case is presented here for better interpretability while deferring the multiplayer scenario to Section VI. Say, there is one type of attacker of efficiency e_1 with WG friction $\epsilon + \delta_1$. From (2), the MAPC size is given by $N = \frac{(1+e_1(\epsilon+\delta_1))}{2(\epsilon+\delta_1)e_1}$. Now, another set of attackers of efficiency e_2 becomes available. Let F be as in Assumption 3,

$$F = \begin{bmatrix} \epsilon + \delta_1 & \epsilon \\ \epsilon & \epsilon + \delta_2 \end{bmatrix}$$

Here we ignore the trivial case where the friction of e_2-attackers is so much that they are not included in the MAPC. The MAPC size is

$$N' = 1 + \frac{2\epsilon^2 + \frac{\delta_1}{e_2} + \frac{\delta_2}{e_1} - \frac{e_1}{e_2}\epsilon(\epsilon + \delta_1) - \frac{e_2}{e_1}\epsilon(\epsilon + \delta_2)}{2\left(\delta_2\delta_1 + \epsilon(\delta_2 + \delta_1)\right)}.$$

Proposition 3. If $\delta_1 = 0$, the MAPC size increases when,

$e_2 \in \left[\frac{e_1\epsilon}{\epsilon+\delta_2}, e_1\sqrt{\frac{\epsilon}{\epsilon+\delta_2}}\right]$ and decreases otherwise.

Proof.

$$N' - N = \frac{1}{2} + \frac{2\epsilon^2 e_1 e_2 - e_1^2\epsilon^2 - e_2^2\epsilon(\epsilon+\delta_2)}{2\epsilon\delta_2 e_1 e_2}.$$

$$N' - N > 0 \Rightarrow \frac{1}{2} + \frac{2\epsilon^2 e_1 e_2 - e_1^2\epsilon^2 - e_2^2\epsilon(\epsilon+\delta_2)}{2\epsilon\delta_2 e_1 e_2} > 0$$
$$\Rightarrow \frac{e_1\epsilon}{\epsilon+\delta_2} < e_2 < e_1. \quad (9)$$

As $e_2 < e_1$, so the loss from WG friction among e_2-attackers must be less than e_1-attackers, i.e., $e_2^2(\epsilon+\delta_2) < e_1^2\epsilon \Rightarrow e_2 < e_1\sqrt{\frac{\epsilon}{\epsilon+\delta_2}}$ which, combined with (3) imply, the group size increases when $e_2 \in \left[\frac{e_1\epsilon}{\epsilon+\delta_2}, e_1\sqrt{\frac{\epsilon}{\epsilon+\delta_2}}\right]$. ■

When $\epsilon < \frac{1}{4}$, the interval of Proposition 3 increases with δ_2 when $\delta_2 \in [0, 3\epsilon]$ and decreases with δ_2 when $\delta_2 \in [3\epsilon, 1-\epsilon]$. For $\epsilon \geq \frac{1}{4}$, the interval always increases with δ_2. When $e_2 > e_1$, the MAPC size always decreases which means that average payoff can be maximized with a smaller group size as attackers with higher efficiency are available.

IV. TOY EXAMPLE

We have an infinite population of attackers who can be of two efficiencies, e_1 and e_2. $n_i (i = 1,2)$ denotes the number of e_i-attacker in a coalition. The friction matrix is –

$$F = \begin{bmatrix} 0.15 & 0.10 \\ 0.10 & 0.15 \end{bmatrix}$$

Table 2: Average pay-off for the toy example

n_1 \ n_2	0	1	2	3	4
0	0.00	0.50	0.92	1.28	1.55
1	1.00	1.40	1.72	1.98	2.15
2	1.70	2.00	2.22	2.38	2.45
3	2.10	2.30	2.42	**2.48**	2.45
4	2.20	2.30	2.32	2.28	2.15

Table 3: Total pay-off for the toy example

n_1 \ n_2	0	1	2	3	4	5	6	7
0	0.00	0.50	1.85	3.83	6.20	8.75	11.25	13.48
1	1.00	2.80	5.18	7.90	10.75	13.50	15.93	17.80
2	3.40	6.00	8.90	11.88	14.70	17.15	19.00	**20.03**

Table 2, and Table 3 show average payoff per player, and total payoff for the coalitions of different sizes and compositions. It can be seen that the MAP is achieved at $n_1 = 3$, and $n_2 = 3$. The maximum total payoff is achieved at $n_1 = 2$, and $n_2 = 7$. Note that total payoff is maximized at a larger group size. Even though the e_1-attackers are more efficient than the e_2-attackers, the proportion of them is lower in the MAPC due to high friction. As the coalition size increases average payoff becomes negative meaning those coalitions will never form. Figure 2a, and 2b show that the average and total payoffs are concave functions of $[n_1, n_2]^T$ and hence both possess global maxima.

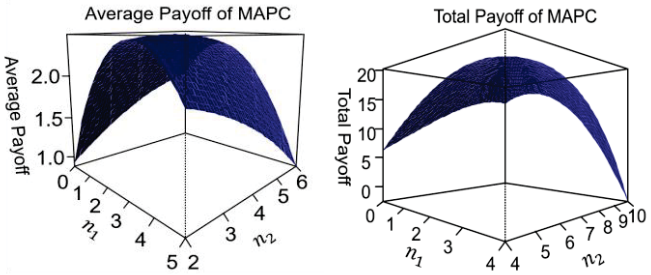
V. ESTIMATION OF FRICTION PARAMETERS

So far we have assumed the friction matrix to be known. But unless mandated by a protocol followed by a set of attackers, the friction matrix is unknown. So an outside attacker needs to estimate the friction parameters to decide which coalition to join. In this section, we provide an optimization framework to estimate the friction parameters by observing the equilibrium coalition compositions. Assume that the observed MAPC has $n_i (i = 1,2,\dots,M)$ e_i-attackers. There is an unknown friction matrix of the form in Assumption 3, controlling the dynamics of the coalition formation. We also assume that $\delta_i = \delta, i = 1,2,\dots,M$. According to our proposed model in Section III, the MAPC should have $\hat{n}_i (i = 1,2,\dots,M)$ e_i-attackers where, according to (2),

$$\hat{n}_i = \frac{\epsilon+\delta}{2\delta} + \frac{1}{2e_i}\left[\frac{1}{\delta} - \frac{M\epsilon + \epsilon(\epsilon+\delta)\sum_{i=1}^{M} e_i}{\delta(\delta + M\epsilon)}\right] \quad i = 1,2,\dots,M.$$

To estimate ϵ and δ, we minimize the least square error –

$$\min \; L_e = \sum_{i=1}^{M} (n_i - \hat{n}_i)^2$$
$$s.t. \quad \epsilon \geq 0$$
$$\delta > 0$$
$$\epsilon + \delta \leq 1.$$



(a) (b)

Fig. 2. Average payoff, and Total payoff for the toy example.

Proposition 4. L_e, as a function of ϵ, and δ, has a unique global minima.

Proof. Let us assume that there are two distinct pairs of friction parameters (ϵ_1, δ_1), and (ϵ_2, δ_2) which lead to the same MAPC. From (2),

$$\delta_i \hat{n}_1 e_1 + \epsilon_i S = \frac{1}{2} + \frac{e_1}{2}(\epsilon_i + \delta_i) \qquad i = 1,2. \quad (10)$$

where $S = \sum_{i=1}^{M} \hat{n}_i e_i$. From (10),

$$\hat{n}_1 e_1(\delta_1 - \delta_2) + S(\epsilon_1 - \epsilon_2) = \frac{e_1}{2}(\epsilon_1 - \epsilon_2 + \delta_1 - \delta_2)$$
$$\Rightarrow (\epsilon_1 - \epsilon_2) + (\delta_1 - \delta_2)\alpha_1 = 0.$$

where $\alpha_1 = \frac{e_1\left(\hat{n}_1 - \frac{1}{2}\right)}{S - \frac{e_1}{2}}$. Similarly,

$$(\epsilon_1 - \epsilon_2) + (\delta_1 - \delta_2)\alpha_i = 0 \;\; i = 1,2,\dots,M. \quad (11)$$

If for some i, $\alpha_i = 0$, i.e., $\hat{n}_i = 0$, then $\epsilon_1 = \epsilon_2$. But $\forall i$, α_i cannot be 0 as that requires all $\hat{n}_i$ to be same. This is impossible when at least one e_i is different from the others. So $\delta_1 = \delta_2$. If $\alpha_i \neq 0 \; \forall i$, then solving (11) for $i = 1,2$ we obtain, $\epsilon_1 = \epsilon_2$, and $\delta_1 = \delta_2$. But this is a contradiction as (ϵ_1, δ_1), and (ϵ_2, δ_2) are distinct pairs. This completes the proof. ■

We solve the above optimization using NOWPAC (Nonlinear Optimization With Path-Augmented Constraints) algorithm

which is convergent to a stationary point of the objective function [22]. We run the algorithm with multiple initial values to increase the chance of finding global maxima. In Section VI, we show numerically, and through data that the estimation is satisfactory. After estimation, an attacker can join a coalition which maximizes its payoff according to (1).

VI. RESULTS

In this section we present the results on the characteristics of coalitions among attackers using simulations and real data.

A. Simulation

We first present the result on the variation of characteristics of MAPCs with given friction matrix as in Assumption 3.

- Scenario 1: Here we study the MAPC characteristics against WG friction when BG friction is fixed. There are $M = 20$ equally spaced efficiency levels between 0.01 and 1. Four levels of BG friction is considered: $f_{ij} = \epsilon = 0.001, 0.005, 0.01,$ and $0.05, i \neq j \;\; i,j = 1,2,\dots,20$. WG friction $(\epsilon + \delta)$ is varied from $(\epsilon + 0.0001)$ to 1. It can be seen from Fig. 3a that the proportion of attackers in the MAPC decreases with efficiency except when WG friction is close to BG friction. When WG friction is small, more highly efficient attackers are present. Less efficient attackers are forced out of MAPC as they cannot withstand large BG friction from more efficient attackers. The composition does not change significantly with WG friction except when BG friction is too high. The number of attackers from all groups decrease in the MAPC with the increase in WG friction (darker to lighter shade). As the BG friction is constant, the loss due to friction from other groups of attackers also decreases with the increase in WG friction leading to almost constant proportion of attackers in the MAPC. The size of MAPC decreases with WG friction except when $\epsilon = 0.005, 0.01,$ and 0.05 as shown in Fig. 3b. For these cases, when BG friction is small only highly efficient attackers are present in MAPC who form small coalition among themselves due to high friction. Once less efficient attackers are part of MAPC, the size increases but then decreases as it should with friction. The heterogeneity of the MAPC decreases with WG friction as shown in Fig. 3c because the proportions remains approximately same but MAPC size decreases as explained before.
- Scenario 2: Here we study the MAPC characteristics against BG friction when WG friction is fixed. There are $M = 20$ equally spaced efficiency levels between 0.01 and 1. Four levels of WG friction is considered: $f_{ii} = \epsilon + \delta = 0.001, 0.005, 0.01,$ and $0.05, \;\; i = 1,2,\dots,20$. BG friction (ϵ) is varied from 0 to $(\epsilon + \delta - 0.0001)$. Figure 4a shows that as the BG friction increases (darker to lighter shade) the proportion of more efficient attackers increases. When $\epsilon + \delta$ is high, and ϵ is close to $\epsilon + \delta$, least efficient attackers disappear from the MAPC as explained in Scenario 1. This implies that more efficient hackers can afford to have large friction whereas less efficient hackers cannot. Figure 4b shows that the MAPC size decreases with BG friction as expected. Figure 4c shows that the homogeneity of the MAPC increases with BG friction as explained in Scenario 1.

B. Estimation of friction parameters

We set true ϵ, and δ as $\epsilon = 0.004$, and $\delta = 0.02$. We solve the optimization problem described in Section V with the MAPC composition as input. The estimates of ϵ, and δ were: $\hat{\epsilon} = 0.00397$, and, $\hat{\delta} = 0.01812$.

Figure 5 shows the fitted, and observed MAPC composition. The estimation errors of ϵ, and δ are 0.75%, and 9.4%.

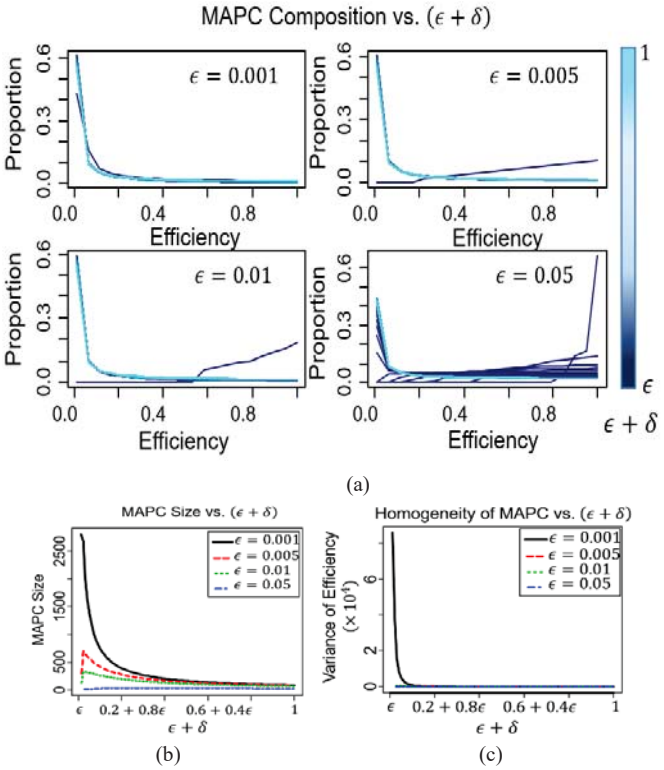


Fig. 3. MAPC Composition vs. WG Friction. The composition does not change with WG Friction. Number of attackers decrease in the MAPC with efficiency.

C. Data Application

We analyze the dataset in [23], containing details on posts from a hacker web-forum, to explore collaborations among the hackers, and verify our model. We use the following features of this dataset: post index, thread index, author index, author name, date and time of the post, content of the post, and user status of the hacker. This dataset contains 4242 posts by 794 hackers over three years from 10/12/2012 to 9/20/2015.

To draw meaningful inference we eliminate all the hackers who just posted once in the span of 3 years leaving 370 hackers to analyze. The hackers in this dataset belong to 16 efficiency levels. The number of messages posted by a hacker is a significant predictor of a hacker's efficiency [18]. Following that we quantify the efficiency of a hacker as

$$\text{efficiency} = \frac{\#\text{posts by hackers of an efficiency level}}{\#\text{hackers at the corresponding level}}.$$

In the set of the normalized efficiencies, some of the efficiencies were same up to five decimal places which were set

to the same value to avoid undesired noise. Hackers with non-unique efficiency values were discarded from the study.

We need to identify the comments which contain useful information to establish connections among the hackers. We divide the hackers into 3 levels to identify the key words in the comments. The boundaries between the levels are defined by the 0.67 and 0.33 quantiles of efficiencies. We create a corpora containing 3 documents consisting of the comments corresponding to these 3 levels. We used $term\ frequency - inverse\ document\ frequency\ (tf - idf)$ index to identify the keywords [24]. tf is the frequency of a particular term in a document. idf of a term is defined as:

$$idf = \ln\left(\frac{\#\text{documents}}{\#\text{documents containing term}}\right).$$

$tf - idf$ is defined as:

$$tf - idf = tf \times idf.$$

We consider the words with $tf - idf$ value 0 useless. The comments without any useful word were discarded.

We construct the collaboration graph G_H among the hackers as follows: the hackers commenting on a status are considered as connected by edges to the hacker who initiated the post. G_H had 3 small components with 3 nodes each, disconnected with the giant component. We restricted our analysis to the giant component which will be called G_H from now on. The observed characteristics on G_H are:

Small-worldness: A network is defined to be *small-world* if $\sigma > 1$; The small-world index σ is given by:

$$\sigma = \frac{C_n/C_r}{L_n/L_r}$$

where L_n and L_r are the average path lengths between two nodes on the given network and a random graph respectively; C_n and C_r are the clustering coefficients of the given network and a random graph respectively [25]. For G_H, $\sigma = 167.75$ which suggests strong small-worldness among the hackers.

Composition of clusters: We performed cluster analysis on G_H using hierarchical agglomerative clustering. The suitable number of clusters was set to 32 as decided by Dunn index. Dunn index is the ratio of the minimum inter-cluster distance to maximum intra-cluster distance [26]. Figure 6a, and 6b show the composition of the largest cluster, and other clusters with more than 10 members respectively.

Figure 6 shows that the proportion of hackers in the cluster decrease with efficiency except cluster 2 where proportion of hackers increase initially. This is because in real world, quite often, efficiency is subjective. In cluster 2, the hackers having maximum proportion were either very efficient or totally ignorant about some particular topic for which they had communicated more leading to their higher proportion. Except this small anomaly, our model seems to explain the collusive behavior among hackers quite correctly.

Figure 7 shows the estimation of MAPC composition. The estimated friction parameters are $\hat{\epsilon} = 0.0276$, and $\hat{\delta} = 0.9723$. This means that WG friction is greater than BG friction. Figure 8 shows $L_i\ (i = 1,2,..,8)$ increases with efficiency in the biggest cluster according to the estimated friction parameters. The Collusion Index of the biggest cluster is 0.7538 meaning that the hackers are not aiming for a single attack.

D. Discussion

- We have shown, both theoretically and through data that, attackers can benefit from collusion.
- We found out that the network among the attackers have strong small-world characteristic.
- We showed that in a coalition, proportion of attackers decrease with efficiency. This, combined with small-worldness, indicates that attacker communities have recognized leaders.
- We have identified leaders of a coalition, and quantified the strength of a collusion.
- We have theoretically shown, that as friction increases homogeneity of attacker coalitions increases.

We have developed a method to estimate unknown friction parameters.

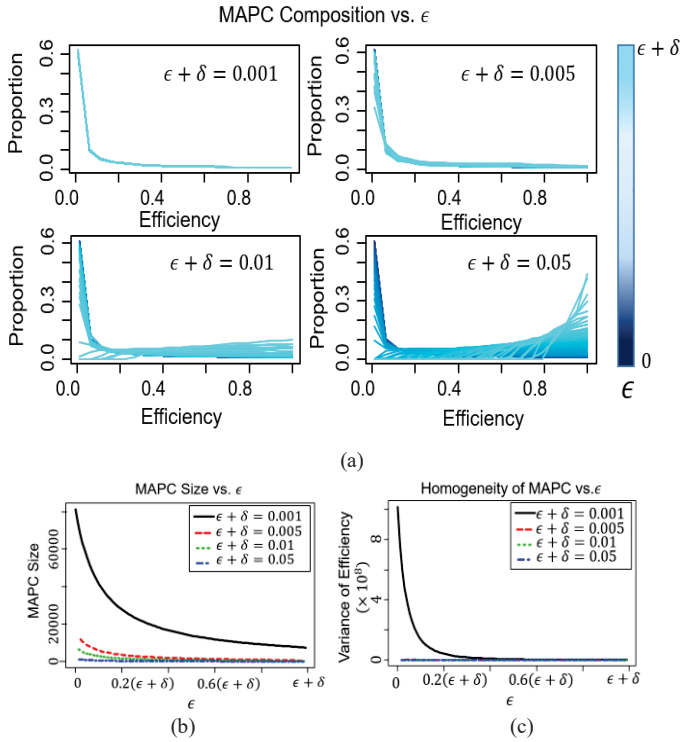


Fig. 4. MAPC Composition vs BG Friction. Increase in BG friction increases (decreases) proportion of highly (less) efficient attackers. Number of attackers and heterogeneity decrease in the MAPC with BG friction.

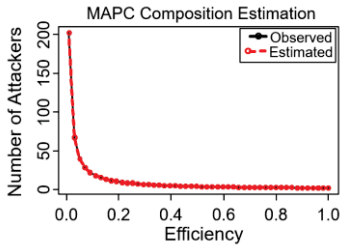
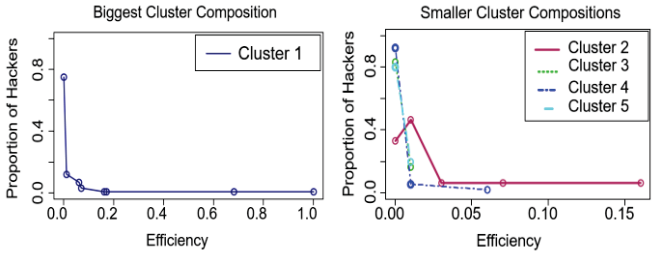


Fig.5. Observed vs. Estimated MAPC Composition

VII. CONCLUSION AND FUTURE WORK

In this work we have shown that attackers form coalitions to pool skills, and launch a bigger attack. The novelty of this work lies in the fact that, we are the first to develop a coalition formation game among attackers to explain the observed characteristics in real data. We have shown that the proportion of attackers in the MAPC decreases with efficiency.

We have theoretically shown that a less efficient attacker can have more leadership quality than a more efficient one. This shows that less efficient hackers can also play a key role in the coalition. We have quantified the strength of a collusion. Our solution to coalition formation game has been shown to be core stable but not Nash stable. We have shown how the coalition characteristics vary with homogeneity. We have developed a method to estimate friction parameters for an attacker to determine which coalition to join. As this model provides information about the driving forces of coalition formation among attackers, e.g., leaders, composition, and homogeneity, this model will be helpful to predict imminent attacks.



(a) (b)

Fig. 6. Compositions of clusters show that the proportion of hackers in the cluster decrease with efficiency (except cluster 2). Separate plots for cluster 1 and other clusters were necessary to show the composition clearly.

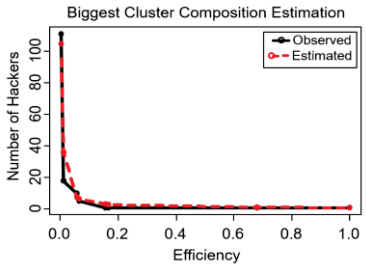


Fig.7. Observed vs. Estimated MAPC Composition.

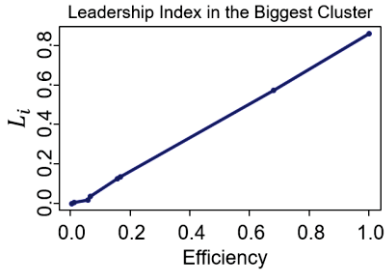


Fig.8. Leadership Index vs. Efficiency in the Biggest Cluster.

As future work, we plan to develop defender strategy which exploits the collusive behavior of attackers to the benefit of the defender. The game where multiple defenders are up against multiple attackers will be interesting to explore. We have only considered maximizing average and total payoff of a coalition. We plan to look at other types of payoff functions and corresponding equilibria in future.

VIII. ACKNOWLEDGEMENT

The effort described in this article was partially sponsored by the U.S. Army Research Laboratory Cyber Security Collaborative Research Alliance under Contract Number W911NF-13-2-0045. The views and conclusions contained in this document are those of the authors, and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright notation hereon.

REFERENCES

[1] "2014 US State of Cybercrime Survey," http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml.
[2] T. Moore, R. Clayton, and R. Anderson, "The Economics of Online Crime." *Journal of Economic Perspectives* 23, no. 3 (2009): 3-20.
[3] D. Kushner, "The real story of stuxnet." *IEEE Spectrum* 50, no. 3 (2013): 48-53.
[4] https://www.wired.com/1994/12/hacker-4/
[5] N. Sintov, and M. Tambe. "Divide to Defend: Collusive Security Games." In *Proceedings of 7th International Conference on Decision and Game Theory for Security,* 2016.
[6] https://en.wikipedia.org/wiki/1993_Bombay_bombings
[7] A. Moghadam, "Terrorist Affiliations in Context: A Typology of Terrorist Inter-Group Cooperation." *CTC Sentinel* 8, no. 3 (2015): 22-25.
[8] C. Herley and D. Florencio, "A profitless endeavor: phishing as tragedy of the commons," In *Proceedings of the 2008 Workshop on New security Paradigms*, 2009.
[9] S. Afroz, V. Garg, D. McCoy, and R. Greenstadt, "Honor among thieves: A common's analysis of cybercrime economies." In *eCrime Researchers Summit (eCRS),* 2013.
[10] Z. Wang, Y. Yin, and B. An, "Computing optimal monitoring strategy for detecting terrorist plots." In *Proceedings of the 30th Conference on Artificial Intelligence* (*AAAI*), 2016.
[11] M. Zhao, B. An, and C. Kiekintveld, "Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks." In *Proceedings of the 30th Conference on Artificial Intelligence (AAAI)*, 2016.
[12] Y. Yin, B. An, and M. Jain, "Game-theoretic resource allocation for protecting large public events." In *Proceedings of the 28th Conference on Artificial Intelligence (AAAI)*, 2014.
[13] Y. Yin, H. Xu, J. Gan, B. An, and A. X. Jiang, "Computing optimal mixed strategies for security games with dynamic payoffs." In *Proceedings of the 24th International Joint Conference on Artificial Intelligence* (*IJCAI*), 2015.
[14] Y. Vorobeychik, B. An, M. Tambe, and S. P. Singh, "Computing solutions in infinite-horizon discounted adversarial patrolling games." In *Proceedings of the 24th International Conference on Automated Planning and Scheduling* (*ICAPS*), 2014.
[15] D. Korzhyk, V. Conitzer, and R. Parr, "Security games with multiple attacker resources." In *Proceedings-International Joint Conference on Artificial Intelligence* (*IJCAI*), 2011.
[16] Q. Guo, B. An, Y. Vorobeychik, L. Tran-Thanh, J. Gan, and C. Miao, "Coalitional security games." In *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems*, 2016.
[17] Y. Bachrach, and J. S. Rosenschein, "Coalitional skill games." In *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems*, 2008.
[18] V. Benjamin, and H. Chen, "Securing cyberspace: Identifying key actors in hacker communities." In *Proceedings of the International Conference on Intelligence and Security Informatics (ISI), 2012.*
[19] S. Afroz, V. Garg, D. McCoy, and R. Greenstadt, "Honor among thieves: A common's analysis of cybercrime economies." In *eCrime Researchers Summit (eCRS), 2013*,
[20] H. Du, and J. Y. Shanchieh, "Discovering Collaborative Cyber Attack Patterns Using Social Network Analysis." In *SBP*, 2011.
[21] J. Farrell, and S. Scotchmer. "Partnerships." *The Quarterly Journal of Economics* 103.2 (1988): 279-297.
[22] Augustin, F., and Y. M. Marzouk, "NOWPAC: a provably convergent derivative-free nonlinear optimizer with path-augmented constraints." *arXiv preprint arXiv:1403.1931* (2014).
[23] S. Samtani. Hacker Web Forum Collection: Hackhound Forum Dataset. University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen. Available http://www.azsecure-data.org/ [3 June 2016].
[24] https://cran.r-project.org/web/packages/tidytext/vignettes/tf_idf.html.
[25] M. D. Humphries, and K. Gurney, "Network 'small-world-ness': a quantitative method for determining canonical network equivalence." *PloS one* 3, no. 4 (2008): e0002051.
[26] J. C. Dunn, "Well-separated clusters and optimal fuzzy partitions." *Journal of cybernetics* 4, no. 1 (1974): 95-104.