A Coalitional Game Theory Approach for Cybersecurity Information Sharing

Iman Vakilinia
Dept. of Computer Science and Eng.
University of Nevada, Reno, NV, USA
ivakilinia@unr.edu

Shamik Sengupta
Dept. of Computer Science and Eng.
University of Nevada, Reno, NV, USA
ssengupta@unr.edu

***Abstract*—As the complexity and number of cybersecurity incidents are growing, the traditional security measures are not sufficient to defend against attackers. In this situation, cyber threat intelligence capability substantially improves the detection and prevention of the sophisticated attacks. Cybersecurity information sharing is a key factor of threat intelligence, allowing organizations to detect and prevent malicious behaviors proactively. However, stimulating organizations to participate and deterring free-riding in such sharing is a big challenge. To this end, the sharing system should be equipped with the rewarding and participation-fee allocation mechanisms to encourage sharing behavior. In this paper, we investigate the rewarding and participation-fee calculation based on profit sharing in coalitional game theory. In particular, we formulate a coalitional game between organizations and analyze the well-known Shapley value and Nucleolus solution concepts in cybersecurity information sharing system.**

***Index Terms*—Coalitional Game, Cybersecurity, Information Sharing, Rewarding, Profit Sharing**

I. Introduction

The frequency and complexity of cyberattacks have increased with the substantial growth of our daily life dependency to the cyberspace. To get ahead of the security threats, it is crucial to have proactive security approach to prevent any dangers before they occur. Cybersecurity information sharing is a key factor of proactively defending against sophisticated cyberattacks [1]. Moreover, such sharing decreases the time and enhances the accuracy of detection and prevention of malicious behaviors in the system. Due to the importance of cybersecurity information sharing, governmental laws/initiatives have been legislated to mandate/encourage the governmental and private organizations to share their cybersecurity information [2]. For instance, the US Senate has passed the Cybersecurity Information Sharing Act (CISA) [3] federal law designed to improve cybersecurity through enhanced sharing of information about cybersecurity threats. The law allows the sharing of Internet traffic information between the US government and private companies. In the UK, Cybersecurity Information Sharing Partnership (CiSP) [4] is an initiative for industry and government that has been set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment to increase situational awareness and reduce the impact on UK business. EU has also launched several cross-sector and intra-sector initiatives to enhance the EU Member States capability for preparedness, cooperation, information exchange, coordination, and response to cyber threats. In the private sector, the organizations act as self-interested rational players and sharing cybersecurity information can be costly for the information possessor. For example, attackers might utilize the shared information for reconnaissance, the competitive organization might take advantage of the shared information which indirectly affects the organization's utility, and sensitive private information (such as names and email addresses) might leak out.

Recently, plenty of research has been done in modeling the benefit and cost for cybersecurity information sharing by applying game theory [5]–[8]. Traditionally the cybersecurity information sharing is modeled as a non-cooperative game where the players are the organizations, and the strategies are choosing between sharing and not-sharing. Then we have the following conditions: if none of the organizations share their information, the organizations' payoffs are zero, if some of the organizations participate in sharing, but the others refuse to reciprocate, then the organizations who refused receive better payoff than the rest of them. Finally, if all of the organizations share, then all of them benefit from sharing. This game resembles the well-known Prisoner's Dilemma game [9]. Although the best payoff is received from mutual sharing, players choose not-sharing as their Nash Equilibrium approach. To change the equilibrium point to the sharing strategy, we need a mechanism which rewards the sharing behavior. Here, choosing the proper rewarding value is a big challenge. To stimulate organizations to share applicable information, the reward should be an increasing function of the total benefits of the other organizations applying the information. On the other hand, as we assume the organizations are the only financial sources of cybersecurity information sharing system, the total rewards are equal to the total amount of organizations' participation-fee. The participation-fee ought to prevent organizations to take advantage of the shared information without participating in sharing. This problem is known as free-riding. Furthermore, the fee should be fair, such that the organizations' payment should be proportional to their benefits from the information.

In this paper, we aim to find the proper rewarding and participation-fee mechanism through applying the coalitional game theory in cybersecurity information sharing system. The

This research is supported by the National Science Foundation (NSF), USA, Award #1528167.

main objective of this mechanism is to stimulate organizations to share more useful information with the goal of increasing the organizations' payoff fairly. To achieve this goal, we investigate the solution concepts of Shapley value and Nucleolus allocations in cybersecurity information sharing game.

The main contributions of this paper are the two parts, as described below.
1-We present a novel coalitional game for rewarding and participation-fee allocation in cybersecurity information sharing.
2-We investigate the fair distribution solution concepts of utility among organizations in cybersecurity information sharing.

II. Related Work

A. Cybersecurity Information Sharing

Cybersecurity information sharing have been studied extensively in [5]–[8], [10]–[14]. Rutkowski et al. [10] has investigated the specification and use case of the cybersecurity information exchange framework. To facilitate sharing the cybersecurity information, various protocols and standards have been proposed such as TAXII, STIX, and CybOX [12], [13]. The security information sharing in competitive environments with the game theory approach has been studied in [7], [8]. Economic analysis of security information sharing and applying incentives for motivation has been studied in [6]. Tosh et al. [5] has formulated a non-cooperative cybersecurity information sharing game and investigated the evolutionary game-theoretic strategy. The role of a social planner to control free-riding in cybersecurity information sharing game has been investigated in [14]. Mandatory security breach reporting through security audits and imposing sanctions have been studied in [11].

However, none of the above works consider the problem of rewarding and participation-fee allocation according to the sharing and benefits obtained from the system. Unlike the above works, we aim to model cybersecurity information sharing as a coalitional game and investigate the solution concepts for fair allocation of utility among the players.

B. Coalitional Game

Coalitional game theory studies the behavior of rational self-interested players in strategic settings where players reach agreements to elevate their payoffs. The main question in coalitional game is how to share the benefits among agents in coalition. The most well-known solution concepts for such sharing are the Shapley value [15] and the Nucleolus [16]. Saad et al. [17] classify the coalitional game into three different groups as canonical coalitional games, coalition formation games, and coalitional graph games. In canonical coalitional games, the grand coalition of all users is an optimal structure and is of major importance and the problem is to stabilize the grand coalition. In coalition formation games, the network structure that forms depends on gains and costs from cooperation and the problem is how to form an appropriate coalitional topology. In coalitional graph games, players' interactions are governed by a communication graph structure and the problem is to stabilize the grand coalition or form a network structure taking into account the communication graph. Since in cybersecurity information sharing system, the goal is to have the grand coalition of the entities to maximize the benefits of sharing information, the problem of proper rewarding and participation-fee allocation falls into canonical coalitional games category. Canonical coalitional games has been studied in wireless network, for instance Singh et al. [18] discuss the profit sharing in coalition base resource allocation in wireless networks, and fair payoff allocation for cooperation in wireless ad-hoc networks using Shapley value is studied in [19]. Muto et al. [20] categorize a set of coalitional games as big boss games. In such games, the coalition value is dependent on the existence of a specific player (namely *big boss*) in the coalition. The coalition of subsets not containing the big boss receives zero value. In the cybersecurity information sharing game if the information possessor does not locate in the coalition then there is no benefit for the coalition, therefore this game is a subset of big boss games.

III. System Model

A. System Architecture

Let $O = \{o_1, ..., o_n\}$ represent the organizations participating in cybersecurity information sharing. Various information can be shared among organizations such as raw network logs, attackers techniques, signature of attacks, and the vulnerabilities' details. In this work, we particularly focus on the sharing discovered security vulnerabilities as in [8]. We consider there is a time slot for each cybersecurity information sharing plan, e.g one month. In each sharing cycle, a set of vulnerabilities $V = \{v_1, ..., v_m\}$ will be detected by the participant organizations. Each vulnerability is associated with a feature set $F_{v_k \in V}$, which is the vulnerability specification. As an example, consider vulnerability CVE-2016-8740. The feature set of this vulnerability[1] is shown in Table I. In this table CVSS[2] (Common Vulnerability Scoring System) is a metric for the calculation of vulnerabilities' impacts, and CWE[3] (Common Weakness Enumeration) represents the weakness category. F_{v_k} allows organizations to calculate the expected cost of vulnerability exploitation.

Let $\pi_i(F_{v_k})$ indicate the expected expenditure cost of exploitation of vulnerability v_k for o_i. Let $\mathcal{P}_i(F_{v_k})$ and $\mathcal{E}_i(F_{v_k})$ denote the probability and the cost of successful exploitation of v_k for o_i respectively. Therefore we have

$$\pi_i(F_{v_k}) = \mathcal{P}_i(F_{v_k}) \times \mathcal{E}_i(F_{v_k}) \tag{1}$$

In the rest of the paper, we will denote $\pi_i(F_{v_k})$ with $\pi_{i,k}$ for simplicity. If o_i patches the vulnerability before exploitation by accessing the shared information, then $\pi_{i,k}$ is the benefit of accessing the shared information for o_i regarding the vulnerability v_k. When an organization o_i shares the information of vulnerability $v_{k'}$, then it receives the reward $r_{i,k'}$. The reward $r_{i,k'}$ is the total payment of the other participant organizations $o_{j \neq i}$ for accessing the vulnerability information $v_{k'}$. Let $x_{j,k'}$

[1] http://www.cvedetails.com/cve/CVE-2016-8740/
[2] https://nvd.nist.gov/vuln-metrics/cvss
[3] https://cwe.mitre.org/

TABLE I: Feature Set of Vulnerability CVE-2016-8740

Feature	***Description***
CVSS	5
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	20
Vendor, Product, Version	Apache, Http Server, 2.4.17-23

denote the o_j's payment for accessing the shared information of the vulnerability $v_{k'}$. Thus we have $x_{j,k'} < \pi_{j,k'}$. In the rest of the paper we use *participation-fee* term for parameter $x_{j,k'}$. The possessor of vulnerability information decides whether to share the vulnerability information or not, based upon the reward value $r_{i,k'} = \sum_{o_j \in O} x_{j,k'}$. Let f_i denote the membership-fee of o_i at the end of cybersecurity information sharing, then f_i is computed as

$$f_i = \sum_{v_k \in V} (x_{i,k} - r_{i,k}) \tag{2}$$

The vulnerability information is stored at the server $\mathcal{S}$. Moreover, we assume $\mathcal{S}$ is a trusted third party computing the participation-fee and reward for players.

The steps of information sharing are as follows. At the first step, organizations register into the system by providing the certificates and their platform information to $\mathcal{S}$. When a new vulnerability has been detected by one of the members, $\mathcal{S}$ calculates the patching benefit and participation-fee for the organizations getting advantage of such information. Based on the total participation-fee, $\mathcal{S}$ computes the reward value for the information possessor. When a cybersecurity information sharing cycle ends, $\mathcal{S}$ calculates the membership-fee f_i. If f_i is negative, then $\mathcal{S}$ pays corresponding amount to o_i, and if f_i is positive, then o_i pays corresponding amount to $\mathcal{S}$.

Figure 1 displays the general process of cybersecurity information sharing system, and Figure 2 depicts the overall picture of participation-fee and reward calculation.

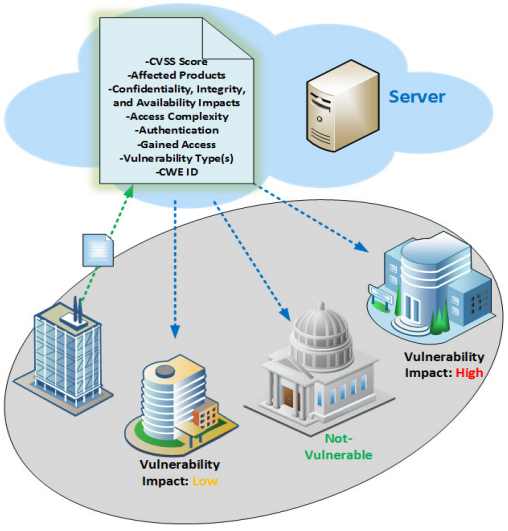


Fig. 1: The cybersecurity information sharing process

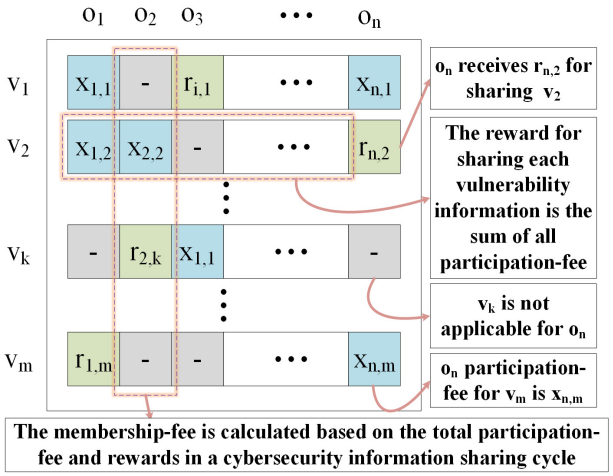


Fig. 2: The calculation of reward and participation-fee

IV. Rewarding and Participation-fee Allocation in Cybersecurity Information Sharing System

In this section, first, we investigate the requirements of participation-fee and reward calculation for cyebrsecurity information sharing system. Second, we analyze the solution concepts for the coalitional formation of cybersecurity information sharing game.

A. Rewarding

As pointed out earlier, typically organizations are not willing to share their cybersecurity information because of the sharing cost. Let $\tau_{i,k}$ denote the sharing cost of v_k for o_i, then o_i would share v_k if and only if $\tau_{i,k} < r_{i,k}$. Besides that, the impacts of vulnerabilities are not equal and other organizations $o_{j \neq i}$, would pay $x_{j,k}$ to access v_k to patch their systems as long as the patching benefit outweighs the participation-fee. If $x_{j,k}$ is small, then the reward may not be motivative for o_i, and as a result o_i will not share the information, resulting in risk of vulnerability exploitation for o_j. On the other hand, if $x_{j,k}$ is large, then the margin of profit for o_j is small. Thus, in this setting, we are interested in fair distribution of the utilities among organizations to satisfy all of them. To achieve this goal, first, we define the following features for the rewarding mechanism in cybersecurity information sharing.

Definition 1. The rewarding mechanism of the cybersecurity information sharing is *dynamic* if it calculates the reward based on the overall benefits to the system. In the dynamic rewarding mechanism, the participants are motivated to share more useful information since the reward is an increasing function of the

benefits achieved by the other organizations exploiting the shared information.

Definition 2. The rewarding mechanism of the cybersecurity information sharing is *fair* if the participation-fee for beneficiary organizations calculated based on their advantages from accessing the information. If the rewarding mechanism is not fair, organizations may not contribute to the reward value (since their benefits may not outweigh the payment cost). In this case, the reward may not be motivative for the information possessor and as a result, the information will not be shared in the system.

Definition 3. The rewarding mechanism of the cybersecurity information sharing is *stable* if it is dynamic and fair.

We are interested in finding the stable rewarding mechanism. To this end, in the next section, we investigate the profit sharing in the coalition formation of cybersecurity information sharing.

B. Profit Sharing

In coalitional game with transferable utility, an n-person game is given by the pair $G(N, \mathrm{v})$, where $N = \{1, 2, ..., n\}$ is the set of players and v is a real-valued payoff that the coalitions members can distribute among themselves. v is also called the characteristic function of the game, which returns a value for each subset of N. In other words $\mathrm{v} : 2^N \rightarrow \mathbb{R}$. *Superadditivity* and *Convexity* of the game are defined as follows.

Superadditivity- A game $G(N, \mathrm{v})$ is superadditive, if for all $S, T \subset N$ and $(S \cap T = \emptyset)$, then $\mathrm{v}(S) + \mathrm{v}(T) \leq \mathrm{v}(S \cup T)$.

Convexity- A game $G(N, \mathrm{v})$ is convex if for all $S, T \subset N$, then $\mathrm{v}(S \cup T) \geq \mathrm{v}(S) + \mathrm{v}(T) - \mathrm{v}(S \cap T)$.

While the characteristic function describes the payoff available to coalitions, it does not prescribe a way of distributing these payoffs. An allocation is a vector $x = (z_1, ..., x_n)$ assigning payoff to each player. In the cybersecurity information sharing game, we are looking for an allocation which stimulate organizations to make the largest coalition. Formally we are looking for an allocation which is located in the *Core*.

Core- An allocation x is in the core of $G(N, \mathrm{v})$ iff $x(N) = \mathrm{v}(N)$ and for any $S \subseteq N$ we have $x(S) \geq \mathrm{v}(S)$. In words, core is the set of x payoff allocations with the property that no coalition of agents can guarantee all of its members a payoff higher than to what they currently receive under x.

We investigate two most widely used fair allocation methods in this paper which are *Shapley Value* [15] and *Nucleolus* [16].

Shapley Value- The Shapley value deals with dividing the surplus among players in a coalition. The Shapley value is calculated as:

$$\phi_i(\mathrm{v}) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n - |S| - 1)!}{n!} [\mathrm{v}(S \cup \{i\}) - \mathrm{v}(S)] \quad (3)$$

Nucleolus- Nucleolus searches for the allocation which minimizes the worst inequity. As an inequity measure of an allocation x, it uses *excess* value as

$$e(x, S) = (S) - \sum_{j \in S} x_j \quad (4)$$

Both Shapley Value and the Nucleolus prescribe a unique solution in all cases.

C. Coalition Formation

In this section, we model the cybersecurity information sharing as a multi-stage coalitional game. The game players are the organizations. The information possessor o_i strategy is to decide whether to share or not to share the information. If o_i decides to share the vulnerability information v_k, then its utility is $u_{i,k} = r_{i,k}$, and otherwise its utility is 0. On the other side, when the vulnerability gets shared then the utility of $o_{j \neq i}$ players are $u_{j,k} = \pi_{j,k} - x_{j,k}$. This game has m stages where m represent the number of vulnerabilities which are being detected in the cybersecurity information sharing cycle. Thus, the characteristic function of this game for each stage is

$$\mathrm{v}(S) = \begin{cases} 0 & |S| = 1 \text{ or } i \notin S \\ \sum_{j \in S} \pi_{j,k} & i \in S \end{cases} \quad (5)$$

Here, the value of single coalition is equal to 0, this is due to the fact that no information is getting shared between entities. If the information possessor belongs to the coalition, then the value of coalition is equal to the total benefit of organizations existing in the coalition. The organizations receiving profits from the shared information should pay to the information possessor.

As an example, consider we have $O = \{o_1, o_2, o_3\}$. o_1 detects a vulnerability v_k and shares its feature set F_{v_k} to o_2 and o_3. Then, $\mathcal{S}$ computes the patching benefit of this vulnerability over o_2 and o_3 as $\pi_{2,k} = 5, \pi_{3,k} = 12$. In this case, for $|S| = 1$ or $o_1 \notin S$, no information is getting shared and as a result the value of coalition is zero. For, $S = \{o_1, o_2\}$, $S = \{o_1, o_3\}$, and $S = \{o_1, o_2, o_3\}$, the coalition values are $v(S) = 5$, $v(S) = 12$, and $v(S) = 17$ respectively.

In this setting, it is trivial that, there is no incentive for any subset of the members to separate and form a smaller cooperation. In other words this game is *Superadditive*. In following, we investigate the Shapley value and Nucleolus allocations for the cybersecurity information sharing game.

Theorem 1. The *Shapley Value* allocation for the cybersecurity information sharing coalitional game is located in the *Core*.

Proof. The Shapley Value solution of a convex game is in the core [21]. Thus we investigate the convexity of the game. As in this game $\mathrm{v}(S \cup T) = \mathrm{v}(S) + \mathrm{v}(T)$ and the value of $\mathrm{v}(S \cap T) \geq 0$, thus the game is convex and the Shapley Value solution is in the core. □

Theorem 2. The Shapley Value of the o_i(information possessor) is half of the total patching benefits of other organizations accessing the information, and the Shapley value for $o_{j \neq i}$ is half of its patching benefit from accessing the information in cybersecurity information sharing game.

Proof. First we start from the Shapley Value of the o_i. Let $(S \subseteq N \setminus \{i\}, |S| = p)$, we calculate $\mathcal{V}_p$ as

$$\mathcal{V}_p = \frac{p!(n-p-1)!}{n!} \tag{6}$$

Combining equations (3) and (6), we can write

$$\phi_i(\mathrm{v}) = \sum_{p=1}^{n-1} \mathcal{V}_p . \sum_{S \subseteq N \setminus \{i\}} [\mathrm{v}(S \cup \{i\}) - \mathrm{v}(S)]$$

Note that, when $p = n$, then the coalition contains o_i, thus we do not count this subset. Based on equation (5), $\mathrm{v}(S) = 0$ and the value of $\mathrm{v}(S \cup \{i\})$ is a coefficient of $\sum_j \pi_{j,k}$, in other words $\mathrm{v}(S \cup \{i\}) = \alpha_p \cdot \sum_j \pi_{j,k}$. Hence, we can rewrite $\phi_i(\mathrm{v})$ as

$$\phi_i(\mathrm{v}) = \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \alpha_p \cdot \sum_j \pi_{j,k}$$

As the number of subsets $(S \subseteq N \setminus \{i\}, |S| = p)$ is $\binom{n-1}{|S|}$ and for each subset S, we have $\frac{p}{n-1}$ benefit values, thus we can calculate α_p as

$$\alpha_p = \binom{n-1}{p} \cdot \frac{p}{n-1}$$

Thus $\phi_i(v)$ is

$$\begin{aligned}
\phi_i(\mathrm{v}) &= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \binom{n-1}{p} \cdot \frac{p}{n-1} \cdot \sum_j \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!(n-1)! \cdot p}{n!p!(n-p-1)! \cdot (n-1)} \cdot \sum_j \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{2} \cdot \sum_j \pi_{j,k}
\end{aligned}$$

Now we compute o_j's Shapley Value. For o_j, we need to count the subsets S containing o_i, since the coalition values for other subsets are zero. In this case, we have $[\mathrm{v}(S \cup \{j\}) - \mathrm{v}(S)] = \pi_{j,k}$. Thus, we have $\sum_{S \subseteq N \setminus \{i\}} [\mathrm{v}(S \cup \{j\}) - \mathrm{v}(S)] = \beta_p \cdot \pi_{j,k}$, where β_p is the number of subsets $\{S \subseteq N \setminus \{j\}, \{i\} \in S, |S| = p\}$ which is

$$\beta_p = \binom{n-2}{p-1}$$

Thus we have

$$\begin{aligned}
\phi_j(\mathrm{v}) &= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \binom{n-2}{p-1} \cdot \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!(n-2)!}{n!(p-1)!(n-p-1)!} \cdot \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \pi_{j,k} \\
&= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \pi_{j,k} \\
&= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \pi_{j,k} \\
&= \frac{1}{2} \cdot \pi_{j,k}
\end{aligned}$$

□

Theorem 3. The Shapley Value and Nucleolus solution concepts, coincide in the cybersecurity information sharing game.

Proof. In order to proof this theorem, we calculate the excess value in equation (4) with the Shapley Value allocation. Let o_i indicate the information possessor and $o_{j \neq i}$ represent other organizations. For subsets $|S| = 1$ and $i \notin S$, the coalition value is zero $\mathrm{v}(S) = 0$ and we have $\sum_{j \in S} x_j = 0$, thus we have $e(x, S) = 0$. For the remain subsets, according to theorem (2) o_i's allocation is $\frac{1}{2} \sum_{j \in S} \pi_{j,k}$ and o_j' allocation is $\frac{1}{2} \pi_{j,k}$. By replacing the coalition value according to equation (5) characteristic function, we have

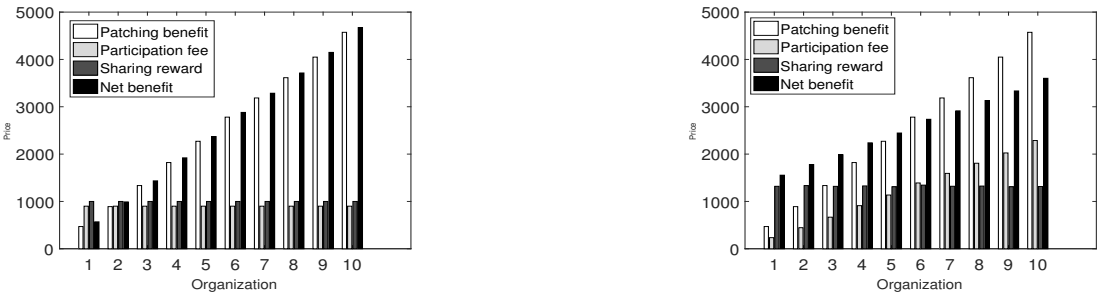
$$\begin{aligned}
e(x, S) &= \mathrm{v}(S) - (x_i + \sum_{j \in S} x_j) \\
&= \sum_{j \in S} \pi_{j,k} - (\frac{1}{2} \sum_{j \in S} \pi_{j,k} + \sum_{j \in S} \frac{1}{2} \pi_{j,k}) = 0
\end{aligned}$$

As the excess value for all of the subsets are equal to zero and since Nucleolus present a unique solution, then we conclude that the solution concepts of the Shapley Value and Nucleolus coincide in the cybersecurity information sharing game.

□

V. Simulation Result

In this section, we evaluate the simulation result. We set $n = 10, m = 100$ and assume each vulnerability randomly detected by an organization and the rest of organizations are vulnerable with probability 0.5. Organizations are sorted in the list based on their size in terms of their patching benefit $\pi_{j,k}$ (e.g. o_{10} is the largest organization and o_1 is the smallest organization). We assume the patching benefit is proportional to the organization's size and we calculate it as $\pi_{j,k} \sim \mathcal{N}(j \times 10, 5)$. We compare our proposed game-theoretic mechanism discussed in section IV with the static allocation where participation-fee and reward are constant values for all



(a) Non-game-theoretic approach

(b) Game-theoretic approach

Fig. 3: Comparing the game-theoretic and non-game-theoretic approaches

of the organizations and every vulnerability information sharing. In the static model, we consider $r_{i,k} = 100, x_{j,k} = 20$. Figure 3b shows the improvement achieved by game-theoretic formation as compared to the non-game-theoretic approach as depicted in Figure 3a. We calculate *net benefit* value as the summation of patching benefit and sharing reward deducted by the participation-fee. As it can be seen, using the game-theoretic approach results in better distribution of the payoff among organizations while in the non-game-theoretic model the larger organizations benefit more from the system. It is due to the fact that in the non-game-theoretic setting, participation-fee is same for all of the organizations without consideration of their benefit from the system, while in the game-theoretic approach, the participation-fee is dynamically calculated based on the patching benefit. Besides that, as the reward value in the game-theoretic is dynamically calculated based on the patching benefit, organizations are stimulated to share more useful information to the system. In our simulation, the game-theoretic approach results in higher rewards comparing to the non-game-theoretic approach.

VI. Conclusion

Despite the benefits of sharing the cybersecurity information, stimulating organizations to share their cybersecurity information is a big challenge. As such sharing is costly, organizations tend to free-ride in the system and as a result, useful information is not getting shared. To motivate sharing behavior, we have proposed a reward/participation-fee allocation mechanism based on coalitional game theory. We have also investigated the Shapley Value and Nucleolus solution concepts of cybersecurity information sharing as a coalitional game to reach a fair, dynamic, and stable profit sharing method. The simulation results depict the efficiency of the profit sharing compare to static reward/participation-fee allocation mechanism.

References

[1] S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 43–49, ACM, 2015.

[2] E. Fischer, E. Liu, J. Rollins, and C. Theohary, "The 2013 cybersecurity executive order: Overview and considerations for congress," 2013.

[3] https://www.congress.gov/bill/114th-congress/senate-bill/754.

[4] "Cyber-security information sharing partnership (cisp)." https://www.ncsc.gov.uk/cisp.

[5] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7341–7346, IEEE, 2015.

[6] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[7] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[8] M. Khouzani, V. Pham, and C. Cid, "Strategic discovery and sharing of vulnerabilities in competitive environments," in *International Conference on Decision and Game Theory for Security*, pp. 59–78, Springer, 2014.

[9] A. Rapoport and A. M. Chammah, *Prisoner's dilemma: A study in conflict and cooperation*, vol. 165. University of Michigan press, 1965.

[10] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, *et al.*, "Cybex: The cybersecurity information exchange framework (x. 1500)," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 5, pp. 59–64, 2010.

[11] S. Laube and R. Böhme, "The economics of mandatory security breach reporting to authorities," *Journal of Cybersecurity*, p. tyw002, 2016.

[12] J. Steinberger, A. Sperotto, M. Golling, and H. Baier, "How to exchange security events? overview and evaluation of formats and protocols," in *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pp. 261–269, IEEE, 2015.

[13] P. Kampanakis, "Security automation and threat information-sharing options," *Security & Privacy, IEEE*, vol. 12, no. 5, pp. 42–51, 2014.

[14] D. Liu, Y. Ji, and V. Mookerjee, "Knowledge sharing and investment decisions in information security," *Decision Support Systems*, vol. 52, no. 1, pp. 95–107, 2011.

[15] L. S. Shapley, "A value for n-person games," *Contributions to the Theory of Games*, vol. 2, no. 28, pp. 307–317, 1953.

[16] D. Schmeidler, "The nucleolus of a characteristic function game," *SIAM Journal on applied mathematics*, vol. 17, no. 6, pp. 1163–1170, 1969.

[17] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp. 77–97, 2009.

[18] C. Singh, S. Sarkar, A. Aram, and A. Kumar, "Cooperative profit sharing in coalition-based resource allocation in wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 1, pp. 69–83, 2012.

[19] J. Cai and U. Pooch, "Allocate fair payoff for cooperation in wireless ad hoc networks using shapley value," in *Parallel and distributed processing symposium, 2004. Proceedings. 18th International*, p. 219, IEEE, 2004.

[20] S. Muto, M. NAKAYAMA, J. POTTERS, and S. TIJS, "On big boss games," *The Economic Studies Quarterly*, vol. 39, no. 4, pp. 303–321, 1988.

[21] L. S. Shapley, "Cores of convex games," *International journal of game theory*, vol. 1, no. 1, pp. 11–26, 1971.