`FlipIn`: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things

Rui Zhang, *Student Member*, and Quanyan Zhu, *Member, IEEE*

***Abstract*— Internet of Things (IoT) is highly vulnerable to emerging Advanced Persistent Threats (APTs) that are often operated by well-resourced adversaries. Achieving perfect security for IoT networks is often cost-prohibitive if not impossible. Cyber insurance is a valuable mechanism to mitigate cyber risks for IoT systems. In this work, we propose a bi-level game-theoretic framework called `FlipIn` to design incentive-compatible and welfare-maximizing cyber insurance contracts. The framework captures the strategic interactions among APT attackers, IoT defenders, and cyber insurance insurers, and incorporates influence networks to assess the systemic cyber risks of interconnected IoT devices. The `FlipIn` framework formulates a game over networks within a principal-agent problem of moral-hazard type to design a cyber risk-aware insurance contract. We completely characterize the equilibrium solutions of the bi-level games for a network of distributed defenders and a semi-homogeneous centralized defender and show that the optimal insurance contracts cover half of the defenders' losses. Our framework predicts the risk compensation of defenders and the Peltzman effect of insurance. We study a centralized security management scenario and its decentralized counterpart, and leverage numerical experiments to show that network connectivity plays an important role in the security of the IoT devices and the insurability of both distributed and centralized defenders.**

***Index Terms*— Cyber insurance, Internet of Things, game-theoretic design, `FlipIt` game, influence network, principal-agent problem, moral hazard, information asymmetry, risk compensation, peltzman effect, network effects.**

I. Introduction

The Internet of Things (IoT) has witnessed applications in many areas such as smart cities, healthcare, and transportations [1], [2]. However, IoT networks and devices can be highly vulnerable to adversaries who can inflict huge financial and non-financial losses on government, companies, and nonprofit organization [3]–[7]. For example, Mirai botnet in 2016 has compromised numerous IoT devices and knocked out popular sites, such as Netflix, Spotify, Twitter, and GitHub, with massive distributed denial-of-service (DDoS) attacks [8], [9].

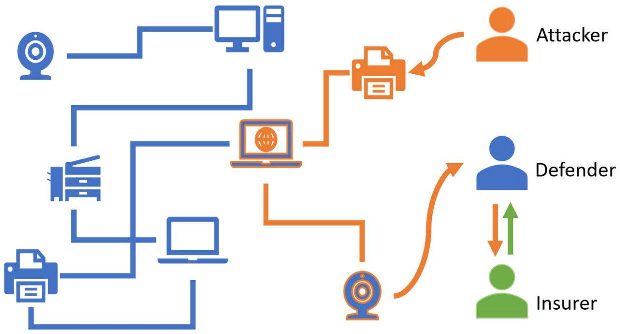


Fig. 1. Cyber insurance for IoT against APTs.

One important class of sophisticated cyber-attacks called advanced persistent threats (APTs) has posed severe threats to IoT devices [10]–[14]. Different from traditional cyber-attacks, APTs are executed by resourceful attackers, and they usually involve multiple steps and persist for a long period of time. For example, Stuxnet attack on Iran's nuclear program has compromised the target system's logic controllers, and then took control of the centrifuges, bringing them to failure [15], [16].

The vulnerabilities of IoT devices to APTs arise from several aspects [5], [17], [18]. First of all, security is not the primal concern during their design and the manufacturing. Users of the devices tend to adopt default or weak passwords. In addition, users do not maintain and patch their devices unless they stop working properly. Therefore, malicious activities of APTs are often unnoticed on IoT devices before they launch attacks and inflict significant losses. It is challenging to design effective defense methods and protect IoTs against APTs due to the coexistence of multiple types of devices and the lack of industrial standards. Moreover, the complexity of the IoT networks makes it difficult to investigate past cyber incidents. The defense solutions are also constrained by limited computational resources on IoT devices.

Cyber insurance becomes a new way to mitigate the risks from APTs to complement technological solutions and plays an important role when the technologies are imperfect [19]–[21]. An illustration of cyber insurance for IoT is provided in Fig. 1. A defender first pays a premium to an insurer on his IoT devices, and when the devices are compromised by APTs, the insurer provides a financial coverage on various types of losses, such as data breaches, physical damages, and service shutdown. The coverage and

Manuscript received April 23, 2019; revised September 23, 2019 and November 21, 2019; accepted November 21, 2019. Date of publication November 26, 2019; date of current version January 30, 2020. This work was supported in part by the U.S. Department of Homeland Security under Award 2015-ST-061-CIRC01, in part by the National Science of Foundation (NSF) under Award ECCS-1847056, Award CNS-1544782, and Award SES-1541164, and in part by the Army Research Office (ARO) under Grant W911NF-19-1-0041. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Rui Zhang.)*

The authors are with the Department of Electrical and Computer Engineering, New York University, Brooklyn, NY 11201 USA (e-mail: rz885@nyu.edu; qz494@nyu.edu).

Digital Object Identifier 10.1109/TIFS.2019.2955891

the financial protection against losses may prevent defenders from business discontinuities and provide them un-deprived resources to take actions to recover and defend themselves.

Traditional insurance frameworks are not completely sufficient to address challenges of cyber insurance as the risks from APTs are caused by malicious attackers rather than accidents [10], [11]. The design of effective cyber insurance contracts should take into account the attacker's behaviors and their impacts on the IoT systems. Moreover, the impact of APTs can propagate over IoT devices through network connections, and thus the insurers may bear extra risks if they fail to take into account the risk that arises from the interdependencies among IoT devices [12]–[14].

In this paper, we propose a bi-level game-theoretic framework called FlipIn to study the interactions among APT attackers, IoT defenders, and cyber insurance insurers over a network of IoT devices. In this framework, attackers and defenders compete over the ownership of IoT devices. The attackers aim to control longer periods so that they can conduct various malicious activities which inflict huge losses on the defenders. The defenders aim to reduce their losses by either controlling longer periods or purchasing cyber-insurance from insurers. With an objective of maximizing the revenue, the insurers charge premiums to the defenders and provide financial coverage to them when they face cyberattack-induced losses.

As the impact of the attackers can propagate to other devices through network connections, there is a need to quantify the systemic risk of the whole network. To this end, we adopt linear influence models to capture the impact of one node on the others [22]–[24]. We further consider two scenarios of cyber insurance. The first one is a distributed scenario where each defender owns an IoT device in a network while the second one is its centralized counterpart where a centralized agent owns the network of nodes and plans the network defense. In both scenarios, there exists an attacker at each IoT device to compete with the defender over its ownership.

FlipIt game has been broadly used to model the interactions between one APT attacker and one defender [25]–[28]. We capture the adversarial interactions over networks by constructing local FlipIt games at each node in the distributed scenario and developing a global FlipIt game over a network in the centralized scenario. In the distributed scenario, the local FlipIt games are composed into a network FlipIt game among multiple defenders and multiple attackers, which can be viewed as a bottom-up approach. In the centralized scenario, the proposed global FlipIt game can be decomposed into local FlipIt games at each node, which can be viewed as a top-down approach.

Our FlipIn framework captures several unique features of IoT networks. Our framework does not require the networks to be homogeneous or fully connected. It captures IoT networks that are featured by various types of software, protocol, and hardware. Attackers or defenders may have different costs to attack or defend different IoT devices with unique physical components, respectively. In our framework, we capture those differences by the cost functions or parameters for the players to claim or reclaim the ownership of the IoT devices. Moreover, the failures of the IoT devices with sensitive information or crucial missions inflict huge losses to defenders while the failures of other devices may inflict less significant losses. Thus, defenders could encounter different losses on different devices, which is captured by the different loss parameters of defenders in our framework. Furthermore, IoT devices are often managed by different entities, and such decentralized ownership of IoT devices is investigated in the distributed scenario.

Each defender interacts with an insurer, which is modeled by a class of moral-hazard type of principal-agent problems with incomplete information. The insurer acts as a principal and announces the insurance contract to the defender, while the defender acts as an agent and makes rational decisions. The incomplete information comes from the fact that the insurer cannot directly observe the interactions among defenders and attackers but can indirectly measure the defenders' losses as a consequence of their actions as well as the attackers' actions.

The principal-agent problem and the network-based FlipIt games constitute a bi-level game among three parties, and the equilibrium solution to this composed game enables us to design effective cyber insurance contracts and mitigate financial impacts on the IoT networks and their operations. We fully analyze the insurability of defenders by taking into account the individual rationalities for both defenders and insurers. We completely solve the insurance contract design problems in the distributed scenario and the semi-homogeneous centralized scenario. The optimal insurance contracts in both cases cover half of the defenders' losses when they are insurable. With numerical experiments, we show that network effects can damage the security of IoT networks and decrease the insurability of defenders. Our numerical experiments further indicate that nodes with more neighbors and networks with lower connectivities are less insurable.

Our framework offers several insights on the best practices for IoT defenders on cyber risk management. Firstly, when the network influences are weak, defenders can successfully mitigate their risks through cyber insurance; when the network influences become stronger, defenders need to focus on deploying local protections instead of adopting cyber insurance. Secondly, the defenders who manage highly connected devices or sparsely connected networks do not benefit from cyber insurance. Thirdly, for weakly connected networks, decentralized management outperforms its centralized counterpart and each node is recommended to defend on its own while for strongly connected networks, centralized management outperforms its decentralized counterpart and a global defender is preferred to be in charge of all devices.

A. Organization of the Paper

The rest of this paper is organized as follows. In Section II, we discuss the related works. Section III formulates the problems and outlines the bi-level games for both distributed

Summary of Notations	
d, a	Defender, Attacker
D, C	Distributed Scenario, Centralized Scenario
$\mathscr{N}$, n	Set of Nodes, Node $n \in \mathscr{N}$
$p_{d,n}$, $p_{a,n}$	Defending Strategy/Frequency, Attacking Strategy/Frequency
α_n	Expected Proportion of the Attacker's Controlling Time
R_n, X_n, β_n	Defender's Risk, Direct Loss, Effective Loss
w_{mn}, w^*_{mn}	Network Influence
η	Discount Ratio of the Network Influence
$\gamma_{a,n}$, $c_{a,n}$	Attacker's Utility Parameter, Cost Parameter
$\gamma_{d,n}$, $c_{d,n}$	Defender's Loss Parameter, Cost Parameter
s_n, s	Insurance Coverage level
T_n, T	Insurance Premium

and centralized scenarios. Section IV provides an overview of finding the equilibrium. Section V and Section VI analyze the insurance contract design problems for two scenarios. Section VII presents numerical experiments and Section VIII provides concluding remarks. A summary of notations has been provided in the following table.

II. Related Works

Cyber insurance has been devised to mitigate cyber-risks by covering some of the losses caused by cyber-attacks [19]–[21]. Various frameworks have been proposed to study cyber-insurance from different perspectives. For example, Pal et al., have proposed a supply-demand model and showed that cyber insurance with client contract discrimination can improve network security [29]; Khalili et al., have investigated the interdependent nature of cyber security and proposed a pre-screening method which is able to create profit opportunities for insurers [30]–[32]; Böhme et al., have proposed several market models to study the information asymmetries between defenders and insurers as well as the interdependent security and correlated risks among defenders [20]; Vakilinia et al., have proposed a coalitional insurance framework where organizations insure a common platform instead of themselves under the consideration of their security interdependency [33]. However, most of the current frameworks have not considered that the risks of cyber-attacks come from stealthy attackers with specific objectives and malicious activities, which is different from traditional insurance of mitigating risks from accidents.

Game theory has been applied extensively to capture various types of cyber-attacks [34]–[36]. For example, zero-sum games have been used to capture Jamming attacks and DoS/DDoS cyber-attacks [37], [38]; Stackelberg games have been applied to study moving target defense, honeypots, and correlated attacks [39]–[41]; Signaling games have been used to investigate deception and data integrity attacks [42], [43]; other applicable games have also been introduced to model different cyber-attack scenarios [44], [45]. Game theory provides a theoretical analysis of cyber-attacks and offers valuable insights for cyber security administrators and managers to design detection and defense methods against them.

APTs are severe threats to cyber security with the stealthiness and persistence nature [10]–[14]. Various papers have proposed different game-theoretic frameworks to investigate APTs and their impacts in different applications. In [46], Huang et al., have used a multi-stage Bayesian game to capture ATPs on cyber-physical systems; in [47], Hu et al., have characterized the interplay among defenders, APT attackers, and insiders with a two-layer differential game; in [48], Xiao et al., have applied prospect theory to investigate APTs on cloud storage systems; in [49], Min et al. have captured the interactions between an APT attacker and a defender in a cloud storage system by a Colonel Blotto game; in [50], Rass et al., have proposed a sequential game-theoretic framework to design defense strategies against APTs.

The security aspect of IoT devices and their vulnerabilities to cyber-attacks have been reviewed and summarized by a lot of recent studies [3]–[7]. Several game-theoretic frameworks have been proposed to investigate cyber-attacks towards IoT systems [51]–[53]. For example, Hamdi et al., have devised a game-theoretic model to study the adaptive security of eHealth IoT systems [54]; Pouryazdan et al., have proposed a game-theoretic framework for trustworthy cloud-centric IoT applications [55]; Namvar et al., have modeled the interaction between an IoT access point and a jammer with a Colonel Blotto game and proposed a centralized mechanism to address the jamming problem in the IoT systems composed of resource-constrained devices [56].

IoT systems could be extremely vulnerable to APTs because of complex types of devices and network connections, lack of detection and defense methods, and restricted computational resources [5], [12], [13], [17], [18]. Game theory becomes a valuable tool to study APTs in IoT systems and design defense mechanisms against them. For example, in [14], Hu et al., have proposed an expert system based APT detection game and showed its effectiveness to increase the security level of IoT systems; in [57], Lee et al., have proposed a game-theoretic vulnerability quantification method for social IoT systems against cyber-attacks including APTs.

In this paper, we adopt `FlipIt` games to model APTs on IoT systems [25]. The `FlipIt` games have been used extensively to study APTs and investigate their impacts in various applications. In [26], Bowers et al., have demonstrated the application of `FlipIt` games to password reset policies, key rotation, VM refresh, and cloud auditing; in [27], Pawlick et al., have used `FlipIt` game to model the competition between a defender and an attacker over the ownership of a cloud server; in [58], Spyridopoulos et al., have proposed a variant of `FlipIt` game to study malware proliferation. These works have focused on the competition between one attacker and one defender over one resource.

`FlipThem` games have been proposed to extend the `FlipIt` games and study the interactions between one defender and on attacker over multiple resources [59]–[62]. In [59], Laszka et al., have proposed an AND control model where an attacker takes control of all resources to compromise the system and an OR model where an attacker only needs to take control of one resource to achieve that; in [60], Zhang et al., have considered a situation where a defender and an attacker have strict constraints on their actions across all the resources; in [61] and [62], Leslie et al., have investigated a scenario where an attacker compromises a defender's resources with a threshold. However, they have not considered situations where multiple defenders and attackers interact in the same network of resources. Moreover, they have not captured the risk-dependencies between neighboring resources.

Influence networks have been used to capture the interdependencies among neighboring nodes in cyber risk management [24]. For example, in [22], Miura-Ko et al., have adopted influence networks to model interdependent security investments; in [23], Nguyen et al., have presented an influence network model to study the vulnerability correlations of security assets. In this paper, we combine `FlipIt` games and influence networks and devise two scenarios of networked `FlipIt` games to capture the interactions between IoT defenders and APT attackers.

We further capture the interactions between defenders and cyber insurance insurers by a moral-hazard type of principal-agent problem with incomplete information. Moral hazard has been discussed extensively in traditional insurance paradigm [63], [64], and it has also been considered

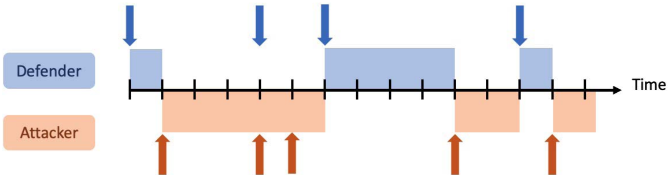


Fig. 2. The FlipIt game on Node n between a defender and an attacker.

in cyber insurance [65], [66]. Principal-agent problems have also been applied to analyze cyber insurance [67], [68]. The principal-agent problem and the nested FlipIt games constitute a bi-level game [69], [70]. The game-of-games structure in bi-level games has been presented in various recent studies on cyber security [45], [71].

Compared with the bi-level game-theoretic cyber insurance framework proposed in [72], our framework captures the interactions between defenders and attackers with FlipIt games instead of zero-sum games to model APTs on IoT systems. One of our main contributions is that we extend the FlipIt game between one defender and one attacker to a network of FlipIt games by incorporating influence networks. We further consider both distributed and centralized scenarios of IoT defenders and analyze their interactions with both APT attackers and insurers. Our numerical experiments investigate the impacts of homogeneous/heterogeneous networks, homogeneous/heterogeneous players, and network connectivities to the security management of IoT defenders and the insurance contract designation of insurers, which have not been addressed in [72]. The analysis offers several insights on the best practices for IoT defenders on cyber risk management and cyber insurance. Our framework further indicates that the optimal insurance coverage level is $1/2$ in the distributed scenario and the semi-homogeneous scenario and we show that an insurer can make a nonzero profit by providing cyber insurance.

III. Problem Formulation

APTs are different from traditional cyber-attacks with the stealthiness and persistence nature. APT attackers have very specific objectives and compromise a system stealthily and slowly to maintain a small footprint and reduce detection risks. APTs, in general, could persist for long periods of time in a system. Moreover, APT attackers may prefer to stay anonymously and steal sensitive data or information instead of completely destroying services or physical components, which could inflict different types of financial and nonfinancial losses on defenders.

We use FlipIt game to capture the competition between a defender and an APT attacker over the ownership of an IoT device [25]. In this game, a player takes control of the IoT device by moving with a cost and he only finds out about the state of the IoT device when he moves. This stealthy aspect of the game makes it suitable to capture APTs. The attacker has a specific objective to maximize his expected controlling time over the device. The attacker's malicious activities during the time that he controls the device could inflict various types of losses on the defender. The objective of the defender is to minimize his total expected losses caused the attacker.

An illustration of the FlipIt game is provided in Fig. 2: the game starts at time 0 and the defender owns the device; at time 1, the attacker attacks the device and then claims the ownership of it; at time 6, the defender defends the device and reclaims the ownership of it; the game continues and the ownership of the device switches between the defender and the attacker. Note that when the defender defends and the attacker attacks at the same time, e.g., time 4, we follow the tie-breaking rule from [25] that their actions are "canceled" and the ownership of the device does not change. Such a tie-breaking rule considers that the current owner of the device has the advantage to win the competition against the other player with prior knowledge or both players prefer not to move at the same time to avoid revealing themselves. This tie-breaking rule makes the game fully symmetric and allows us to handle ties smoothly.

Consider an IoT network modeled by a directed graph $\mathscr{G}(\mathscr{N}, \mathscr{E})$ with $\mathscr{N} := \{1, \ldots, N\}$ and $\mathscr{E}$ denoting the set of nodes and the set of edges, respectively. Each node $n \in \mathscr{N}$ represents an IoT device which is controlled in turn by a defender and an APT attacker. Let us denote the sequence of the defender's defending time or the attacker's attacking time at node n as an infinite non-decreasing sequence which can be specified as follows:

$$\text{Defender: } t_{d,n,1}, t_{d,n,2}, \ldots, t_{d,n,k-1}, t_{d,n,k}, t_{d,n,k+1}, \ldots \quad (1)$$

$$\text{Attacker: } t_{a,n,1}, t_{a,n,2}, \ldots, t_{a,n,k-1}, t_{a,n,k}, t_{a,n,k+1}, \ldots \quad (2)$$

Let $\phi_{d,n}(t_{d,n,k})$ or $\phi_{a,n}(t_{a,n,k})$ denote the feedback that the defender or the attacker at node n receives when he defends or attacks at $t_{d,n,k}$ or $t_{a,n,k}$, where $\phi_{d,n} \in \Phi_{d,n}$ or $\phi_{a,n} \in \Phi_{a,n}$ with $\Phi_{d,n}$ or $\Phi_{a,n}$ denoting the set of all the possible forms of the feedback of the defender or the attacker, respectively. Some of the possible forms are listed here as examples [25].

- (Non-adaptive) a player obtains no information, i.e., $\phi_{d,n}(t_{d,n,k}) = 0$ or $\phi_{a,n}(t_{a,n,k}) = 0$;
- (Last move) a player obtains the opponent's last move time, i.e., $\phi_{d,n}(t_{d,n,k}) = \max\{t_{a,n,k'} | t_{a,n,k'} \leq t_{d,n,k}\}$ or $\phi_{a,n}(t_{a,n,k}) = \max\{t_{d,n,k'} | t_{d,n,k'} \leq t_{a,n,k}\}$;
- (Full history) a player obtains the full history of both players' moves, i.e., $\phi_{d,n}(t_{d,n,k}) = \big((t_{d,n,1}, \ldots, t_{d,n,k}), (t_{a,n,1}, \ldots, t_{a,n,k'})\big)$ or $\phi_{a,n}(t_{a,n,k}) = \big((t_{d,n,1}, \ldots, t_{d,n,k'}), (t_{a,n,1}, \ldots, t_{a,n,k})\big)$ where $t_{a,n,k'} = \max\{t_{a,n,k'} | t_{a,n,k'} \leq t_{d,n,k}\}$ or $t_{d,n,k'} = \max\{t_{d,n,k'} | t_{d,n,k'} \leq t_{a,n,k}\}$.

A player decides the time of his next move following a strategy based on his current time of move and the received feedback. Let $p_{d,n} : \mathbb{R}_{\geq 0} \times \Phi_{d,n} \to \mathbb{R}_{\geq 0}$ and $p_{a,n} : \mathbb{R}_{\geq 0} \times \Phi_{a,n} \to \mathbb{R}_{\geq 0}$ denote the defending strategy and the attacking strategy for the defender and the attacker at node n, respectively, we have

- when the defender defends at time $t_{d,n,k}$ and receives feedback $\phi_{d,n}(t_{d,n,k})$, his next defend will be at $t_{d,n,k+1} = p_{d,n}(t_{d,n,k}, \phi_{d,n}(t_{d,n,k}))$;
- when the attacker attacks at time $t_{a,n,k}$ and receives feedback $\phi_{a,n}(t_{a,n,k})$, his next attack will be at $t_{a,n,k+1} = p_{a,n}(t_{a,n,k}, \phi_{a,n}(t_{a,n,k}))$.

Let $\alpha_n \in [0, 1]$ denote the expected proportion of the time that the attacker controls node n when the defender adopts a strategy of $p_{d,n}$ and the attacker adopts a strategy of $p_{a,n}$. While controlling the IoT devices, the attackers can benefit from conducting malicious activities, such as monitoring sensitive operations, stealing private information, and injecting ransomware. The objective of the attacker is to maximize the expected proportion of the time that he controls the

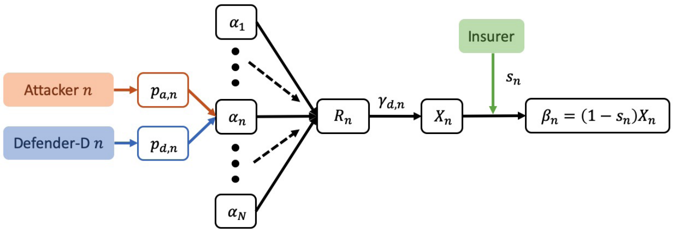


Fig. 3. Interactions among players at node n in Defender-D.

device, which can be captured by the following optimization problem:

$$\max_{p_{a,n} \in \mathscr{S}_{a,n}} \quad \gamma_{a,n}\alpha_n - c_{a,n}(p_{a,n}), \tag{3}$$

where $\gamma_{a,n} \in \mathbb{R}_{\geq 0}$ denotes the utility parameter of the attacker and $\mathscr{S}_{a,n} = \{p_{a,n}\}$ denotes the set of all possible strategies by the attacker. Function $c_{a,n} : \mathscr{S}_{a,n} \to \mathbb{R}_{\geq 0}$ captures the cost of the attacker when he adopts a strategy of $p_{a,n}$. Different $\gamma_{a,n}$ and $c_{a,n}$ capture the trade-offs between a larger proportion of controlling time and a smaller cost of the attacker.

The attackers' activities can inflict huge financial and nonfinancial losses on defenders. A defender at one node may also face losses caused by the attackers at neighboring nodes, for example, the attackers can denial the services, send misleading information, or spread computer viruses to this node. Moreover, the impacts of attackers could propagate through network connections, such as computer worms and viruses, and thus, the defender may even face losses caused by undirectly connected nodes.

To measure the losses of defenders with respect to the attackers' controlling times, we first define the defender's risk level at node n as

$$R_n = g_n(\alpha_1, \alpha_2, \ldots, \alpha_N), \tag{4}$$

where $g_n : ([0, 1])^N \to \mathbb{R}_{\geq 0}$ is a function of all the expected proportions of attackers' controlling times in this network. We further assume that the defender's loss X_n follows an exponential distribution of $\frac{1}{\gamma_{d,n} R_n}$ with its density function expressed as

$$f(x_n|\gamma_{d,n} R_n) = \frac{1}{\gamma_{d,n} R_n} \exp\left(-\frac{1}{\gamma_{d,n} R_n} x\right), \quad \forall x_n \in \mathbb{R}_{\geq 0}. \tag{5}$$

The parameter $\gamma_{d,n} \in \mathbb{R}_{>0}$ controls the level of the defender's losses, and a crucial IoT devices may have a larger $\gamma_{d,n}$. For example, an IoT device which monitors or controls nuclear reactors has a larger $\gamma_{d,n}$ than an IoT device which records the room temperature in a supermarket. The exponential distribution has been widely applied to risk and insurance analysis [73]–[75]. We can see from the exponential distribution that the defender has a larger probability of facing a larger loss when he has a higher risk level. Furthermore, the expected loss satisfies that $\mathbb{E}(X_n) = \gamma_{d,n} R_n$, and the defender has a larger expected loss with the increase of his risk level. An illustration of the relations between $p_{a,n}$, $p_{d,n}$, α_n, R_n, and X_n can be found in Fig. 3.

Remark 1: When node n has no network connections to any other nodes or there is only one node n in this network, we could assume that $R_n = g(\alpha_1, \alpha_2, \ldots, \alpha_N) = \alpha_n$, which indicates that the defender at node n has a higher risk level or faces a larger expected loss if the attacker at node n has a larger expected proportion of controlling time.

The defenders can also purchase cyber-insurance to cover their losses. After paying a premium to the insurer, a defender receives a coverage from the insurer when he faces losses caused by attackers. In this paper, we consider two different scenarios of defenders, which are discussed separately in the following subsections. In summary, Defender-D represents a "distributed" case where each defender at each node only considers his own losses, while Defender-C indicates a "centralized" case where a global defender considers the overall loss of this IoT network. We present two examples to illustrate applications of Defender-D and Defender-C.

Example 1 (Centralized Scenario): Consider a smart home which contains IoT devices, such as laptops, wireless routers, smart speakers, cameras, and sweeping robots. An APT attacker could compromise a smart speaker and record private conversions over days or months. The smart home owner could hardly notice the existence of the attacker as the smart speaker functions normally. The attacker could further leak the recorded conversions to the public or blackmail the owner. Similarly, APT attackers could record private videos from cameras or steal sensitive documents from laptops. The smart home owner could choose to insure his IoT devices with cyber insurance and the insurer would provide financial coverage to his losses from the leakage of private information by APT attackers. It is natural for the smart home owner to insure all the devices together, which indicates a centralized scenario.

Example 2 (Distributed Scenario): In vehicular applications and inter-networking technologies (VANET), a vehicle dynamically adjusts its route to destinations by communicating with different IoT devices, such as other vehicles, smart traffic lights, and phones owned by pedestrians. An APT attacker could compromise the vehicle and hijack the data sent and received by it. Different from traditional cyber-attacks, APTs aim not to immediately damage the vehicle as it can be detected by the security systems. With small modifications on the data over a long period of time, the vehicle may arrive at the desired destination by the attacker [76]–[78]. Moreover, an APT attacker could even affect the route of a target vehicle by sending misleading data from other vehicles and traffic lights. Cyber insurance could provide financial coverage to the passengers for their losses from arriving at a wrong destination. In this case, the security status of the vehicle is also affected by other IoT devices in this network.

A. Defender-D

In this case, there exist N defenders in this IoT network and each IoT device is occupied by a defender. An illustration of the interactions between an attacker, a defender, and an insurer in one node is provided in Fig. 3. Note that each attacker has no information about the players in other nodes and his objective is to maximize his expected proportion of controlling time α_n as in (3). Each defender has no information about the actions of the players in other nodes, however, he may face losses caused by the attackers from other nodes.

After paying a premium to the insurer, the defender at node n is entitled to receive a coverage $s_n X_n$ from the insurer when he faces a loss of X_n, where $s_n \in (0, 1]$ denotes the coverage level of the insurance. The defender now has an effective loss of $\beta_n = X_n - s_n X_n = (1 - s_n)X_n$. Note that $s_n = 0$ indicates that there is no insurance and the defender's effective loss β_n

equals to his direct loss X_n. As a result, the expected effective loss of the defender can be described as

$$\mathbb{E}[\beta_n] = \mathbb{E}[(1-s_n)X_n] = (1-s_n)\gamma_{d,n}R_n. \tag{6}$$

The objective of each defender is to minimize his expected effective loss, which can be captured by the following optimization problem after plugging (4) into (6):

$$\min_{p_{d,n}\in\mathscr{S}_{d,n}} \; (1-s_n)\gamma_{d,n}g_n(\alpha_1,\dots,\alpha_N)+c_{d,n}(p_{d,n}), \tag{7}$$

where $\mathscr{S}_{d,n} = \{p_{d,n}\}$ denotes the set of all possible strategies by the defender. Function $c_{d,n} : \mathscr{S}_{d,n} \to \mathbb{R}_{\geq 0}$ captures the cost of the defender under the strategy $p_{d,n}$. The parameter $\gamma_{d,n}$ and function $c_{d,n}$ capture the trade-offs between a smaller expected effective loss and a higher cost.

By comparing (3) and (7), we can see that the attacker aims to maximize the expected proportion of his controlling time while the defender aims to minimize it. The conflicting interest between the defender and the attacker constitutes a FlipIt-D game in each IoT device, and its Nash equilibrium is defined as follows.

Definition 1: Let $\mathscr{S}_{a,n}$ and $\mathscr{S}_{d,n}$ denote the strategy sets for the attacker and the defender at node n, respectively; let $J_{a,n}(p_{a,n}, p_{d,n})$ and $J_{d,n}(p_{d,n}, p_{a,n}; s_n, \{\alpha_m\}_{m\neq n})$ denote the objective functions from (3) and (7), respectively. A strategy profile $\{p_{a,n}^*, p_{d,n}^*\}$ is a Nash equilibrium of the FlipIt-D game at node n defined by $\langle\{$Attacker, Defender-D$\}, \{\mathscr{S}_{a,n}, \mathscr{S}_{d,n}\}, \{J_{a,n}, J_{d,n}\}\rangle$ if

$$J_{a,n}(p_{a,n}^*, p_{d,n}^*) \geq J_{a,n}(p_{a,n}, p_{d,n}^*), \quad \forall p_{a,n}\in\mathscr{S}_{a,n};$$
$$J_{d,n}(p_{d,n}^*, p_{a,n}^*; s_n, \{\alpha_m\}_{m\neq n}) \leq J_{d,n}(p_{d,n}, p_{a,n}^*; s_n, \{\alpha_m\}_{m\neq n}), \quad \forall p_{d,n}\in\mathscr{S}_{d,n}.$$

Furthermore, a strategy profile $\{\{p_{a,n}^*\}, \{p_{d,n}^*\}\}$ is a global Nash equilibrium of the G-FlipIt-D game defined by $\langle\{$Attackers, Defender-Ds$\}, \{\{\mathscr{S}_{a,n}\}, \{\mathscr{S}_{d,n}\}\},\{\{J_{a,n}\}, \{J_{d,n}\}\}\rangle$ if

$$J_{a,n}(p_{a,n}^*, p_{d,n}^*) \geq J_{a,n}(p_{a,n}, p_{d,n}^*), \quad \forall p_{a,n}\in\mathscr{S}_{a,n}, n\in\mathscr{N};$$
$$J_{d,n}(p_{d,n}^*, p_{a,n}^*; s_n, \{\alpha_m^*\}_{m\neq n}) \leq J_{d,n}(p_{d,n}, p_{a,n}^*; s_n, \{\alpha_m^*\}_{m\neq n}), \quad \forall p_{d,n}\in\mathscr{S}_{d,n}, n\in\mathscr{N},$$

where α_m^* denotes the expected proportion of the time that the attacker controls node m when the defender adopts a strategy of $p_{d,m}^*$ and the attacker adopts a strategy of $p_{a,m}^*$.

An illustration of the FlipIt-D game and the G-FlipIt-D game is provided in Fig. 4. The Nash equilibrium of the FlipIt-D game is affected by the strategies of other players in the network, and it also affects the results of other FlipIt-D games. The complex interactions among all attackers and defenders constitute a G-FlipIt-D game, whose Nash equilibrium is achieved when all the FlipIt-D games in each node reach their Nash equilibriums. Note that the Nash equilibrium of the FlipIt-D game is affected by the coverage level s_n through $J_{d,n}$, and the Nash equilibrium of the G-FlipIt-D game is affected by the coverage levels $\{s_n\}$ of all nodes.

The defender at node n has to pay a premium $T_n \in \mathbb{R}_{\geq 0}$ to receive a coverage of his losses. A rational defender purchases cyber insurance only when his total loss including the premium under the insurance is lower than his total loss without the insurance, which can be expressed as the following individual rationality constraint for the defender:

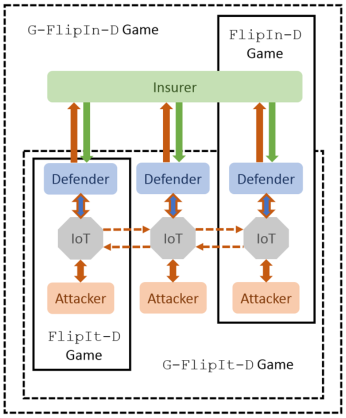


Fig. 4. The structure of the games in Defender-D. There are N defenders in this case. The FlipIt-D game is played between a defender and an attacker on one IoT device while the G-FlipIt-D game captures the interactions among all defenders and all attackers over the IoT network. The FlipIn-D game captures the interactions between a defender, an attacker and the insurer while the G-FlipIn-D game describes the interactions between all defenders, all attackers, and the insurer.

$$(1-s_n)\gamma_{d,n}g_n\left(\alpha_1,\dots,\alpha_n^*(s_n),\dots,\alpha_N\right)+c_{d,n}\left(p_{d,n}^*(s_n)\right)+T_n \leq \gamma_{d,n}g_n\left(\alpha_1',\dots,\alpha_n^*(0),\dots,\alpha_N'\right)+c_{d,n}\left(p_{d,n}^*(0)\right). \tag{8}$$

Note that we have abused the notation with the purpose of simplifying illustration: $\alpha_n^*(s_n)$ and $\alpha_n^*(0)$ denote the equilibrium expected proportions of the attacker's controlling time at node n with the insurance of coverage level s_n and without the insurance, respectively; $p_{d,n}^*(s_n)$ and $p_{d,n}^*(0)$ denote the equilibrium defending strategies of the defender at node n with the insurance of coverage level s_n and without the insurance, respectively. Specially, α_m and α_m' represent the expected proportions at node $m \neq n$ given the coverage level s_n and $s_n = 0$ at node n, respectively.

The insurer receives a premium T_n from the defender and provides coverage $s_n\gamma_{d,n}g_n\left(\alpha_1,\dots,\alpha_n^*(s_n),\dots,\alpha_N\right)$ to him. Thus, the insurer has a profit of $T_n - s_n\gamma_{d,n}g_n(\alpha_1,\dots,\alpha_n^*(s_n),\dots,\alpha_N)$. The insurer insures the defender only when he can make a profit, which can be expressed as the following individual rationality constraint for the insurer:

$$T_n - s_n\gamma_{d,n}g_n\left(\alpha_1,\dots,\alpha_n^*(s_n),\dots,\alpha_N\right) \geq 0. \tag{9}$$

The objective of the insurer is to make a larger profit from providing the insurance, which can be captured as the following optimization problem:

$$\max_{\{s_n,T_n\}} \; T_n - s_n\gamma_{d,n}g_n\left(\alpha_1,\dots,\alpha_n^*(s_n),\dots,\alpha_N\right) \quad \text{s.t. (8), (9).} \tag{10}$$

We can see that the solution of (10) depends on both the outcome of the FlipIt-D game at node n and the expected proportions of the attackers' controlling times at other nodes. An effective insurance contract must satisfy both (8) and (9). The interactions between the defender and the insurer constitute a moral-hazard type of principal-agent problem where the insurer as a principal announces the insurance contract and the defender as an agent makes rational decisions on purchasing the insurance. Note that the insurer has incomplete information about the defender as he decides the insurance contract based on the outcome of the FlipIt-D game.

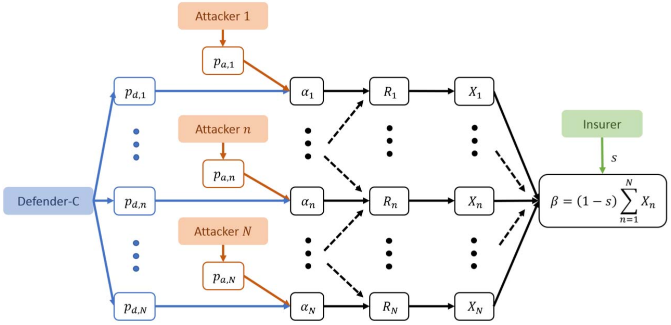


Fig. 5. Interactions among players in the IoT network in Defender-C.

The complex interactions between an attacker, a defender, and an insurer constitute a bi-level FlipIn-D game whose Nash equilibrium is defined as follows.

Definition 2: *Let* $\mathscr{S}_{i,n} = \{\{s_n, T_n\} | s_n \in (0,1], T_n \in \mathbb{R}_{\geq 0}, (8), (9)\}$ *denote the action set for the insurer; let* $J_{i,n}(s_n, T_n)$ *denote the objective function from (10). Recall* $\mathscr{S}_{d,n}$, $\mathscr{S}_{a,n}$, $J_{d,n}$, $J_{a,n}$ *from Definition 1, a strategy profile* $\{p^*_{a,n}, p^*_{d,n}, \{s^*_n, T^*_n\}\}$ *is a Nash equilibrium of the bi-level* FlipIn-D *game defined by* $\langle\{\text{Attacker, Defender-D, Insurer}\}, \{\mathscr{S}_{a,n}, \mathscr{S}_{d,n}, \mathscr{S}_{i,n}\}, \{J_{a,n}, J_{d,n}, J_{i,n}\}\rangle$ *if* $\{s^*_n, T^*_n\}$ *solves (10) and* $\{p^*_{a,n}, p^*_{d,n}\}$ *is a Nash equilibrium of the* FlipIt-D *game defined in Definition 1 under* $\{s^*_n, T^*_n\}$.

Furthermore, a strategy profile $\{\{p^*_{a,n}\}, \{p^*_{d,n}\}, \{\{s^*_n\}, \{T^*_n\}\}\}$ *is a global Nash equilibrium of the bi-level* G-FlipIn-D *game defined by* $\langle\{\text{Attackers, Defender-Ds, Insurer}\}\ \{\{\mathscr{S}_{a,n}\}, \{\mathscr{S}_{d,n}\}, \{\mathscr{S}_{i,n}\}\}, \{\{J_{a,n}\}, \{J_{d,n}\}, \{J_{i,n}\}\}\rangle$ *if* $\{s^*_n, T^*_n\}$ *solves (10) for all* $n \in \mathscr{N}$ *and* $\{\{p^*_{a,n}\}, \{p^*_{d,n}\}\}$ *is a Nash equilibrium of the* G-FlipIt-D *game defined in Definition 1 under* $\{\{s^*_n\}, \{T^*_n\}\}$.

An illustration of the FlipIn-D game and the G-FlipIn-D game has been provided in Fig. 4. The Nash equilibrium of the FlipIn-D game is affected by the other FlipIn-D games through α_m in (10). The complex interactions among all players constitute a G-FlipIn-D game, whose Nash equilibrium is achieved when all the FlipIn-D games reach their Nash equilibriums.

B. Defender-C

In this case, there exists only one global defender in this IoT network. The interactions between the defender, attackers, and an insurer are illustrated in Fig. 5. Similar to the case of Defender-D, each attacker has no information about the players in other nodes. The insurer offers one insurance contract $\{s, T\}$ to the defender which covers the losses of all the IoT devices. The defender's expected effective loss β in this case can be expressed as

$$\mathbb{E}(\beta) = \mathbb{E}\left((1-s)\sum_{n=1}^{N} X_n\right) = (1-s)\sum_{n=1}^{N} \gamma_{d,n} g_n(\alpha_1, \ldots, \alpha_N). \tag{11}$$

The defender aims to minimize his overall expected effective losses, which can be captured by the following optimization problem:

$$\min_{\{p_{d,n}\}} (1-s)\sum_{n=1}^{N} \gamma_{d,n} g_n(\alpha_1, \ldots, \alpha_N) + \sum_{n=1}^{N} c_{d,n}(p_{d,n}). \tag{12}$$

The interactions between the defender and N attackers in this IoT network constitute a global FlipIt-C game, which is defined as follows.

Definition 3: *Let* $\mathscr{S}_{a,n}$ *and* $\mathscr{S}_d$ *denote the strategy sets for the attacker and the defender, respectively; let* $J_{a,n}(p_{a,n}, p_{d,n})$ *and* $J_d(\{p_{d,n}\}, \{p_{a,n}\}; s)$ *denote the objective functions from (3) and (12), respectively. A strategy pair* $\{\{p^*_{a,n}\}, \{p^*_{d,n}\}\}$ *is a Nash equilibrium of the* FlipIt-C *game defined by* $\langle\{\text{Attackers, Defender-C}\}, \{\{\mathscr{S}_{a,n}\}, \mathscr{S}_d\}, \{\{J_{a,n}\}, J_d\}\rangle$ *if*

$$J_{a,n}(p^*_{a,n}, p^*_{d,n}) \geq J_{a,n}(p_{a,n}, p^*_{d,n}),\ \forall p_{a,n} \in \mathscr{S}_{a,n},\ n \in \mathscr{N};$$
$$J_d(\{p^*_{d,n}\}, \{p^*_{a,n}\}; s) \leq J_d(\{p_{d,n}\}, \{p^*_{a,n}\}; s), \quad \forall \{p_{d,n}\} \in \mathscr{S}_d.$$

Note that the Nash equilibrium of the FlipIt-C game is affected by the coverage level s through J_d. In the previous subsection, we have shown that N FlipIt-D games constitute a global G-FlipIt-D game, while in this subsection, we show that the FlipIt-C game may be decentralized into N local L-FlipIt-C games under certain conditions.

Remark 2 (Decentralization): *If* $g_n(\alpha_1, \ldots, \alpha_N)$ *is additively separable for all* $1 \leq n \leq N$, *i.e.,* $g_n(\alpha_1, \ldots, \alpha_N) = \sum_{m=1}^{N} g_{n,m}(\alpha_m)$, *we have* $\sum_{n=1}^{N} \gamma_{d,n} g_n(\alpha_1, \ldots, \alpha_N) = \sum_{n=1}^{N}\sum_{m=1}^{N} \gamma_{d,n} g_{n,m}(\alpha_m) = \sum_{n=1}^{N}\sum_{m=1}^{N} \gamma_{d,m} g_{m,n}(\alpha_n)$. *Thus, solving the global problem (12) is equivalent to solving the following* N *sub-problems at each node*:

$$\min_{p_{d,n}} (1-s)\sum_{m=1}^{N} \gamma_{d,m} g_{m,n}(\alpha_n) + c_{d,n}(p_{d,n}). \tag{13}$$

With Remark 2, the interactions between the attacker and the defender at node n constitute a L-FlipIt-C game, which is defined as follows.

Definition 4: *Let* $\mathscr{S}_{a,n}$ *and* $\mathscr{S}_{d,n}$ *denote the strategy sets for the attacker and the defender at node n, respectively; let* $J_{a,n}(p_{a,n}, p_{d,n})$ *and* $J_{d,n}(p_{d,n}, p_{a,n}; s)$ *denote the objective functions from (3) and (13), respectively. A strategy profile* $\{p^*_{a,n}, p^*_{d,n}\}$ *is a Nash equilibrium of the* L-FlipIt-C *game at node* n *defined by* $\langle\{\text{Attacker, Defender-C}\}, \{\mathscr{S}_{a,n}, \mathscr{S}_{d,n}\}, \{J_{a,n}, J_{d,n}\}\rangle$ *if*

$$J_{a,n}(p^*_{a,n}, p^*_{d,n}) \geq J_{a,n}(p_{a,n}, p^*_{d,n}), \quad \forall p_{a,n} \in \mathscr{S}_{a,n};$$
$$J_{d,n}(p^*_{d,n}, p^*_{a,n}; s) \leq J_{d,n}(p_{d,n}, p^*_{a,n}; s), \quad \forall p_{d,n} \in \mathscr{S}_{d,n}.$$

An illustration of the FlipIt-C game and the L-FlipIt-C games is provided in Fig. 6. We can see that all the L-FlipIt-C games are independent of each other as (3) and (13) do not depend on the outcomes of other L-FlipIt-C games. However, the L-FlipIt-C game at node n takes the parameters $\{\gamma_m\}$ from other nodes into consideration. Note that when $g_n(\alpha_1, \ldots, \alpha_N)$ is not additively separable, we cannot decentralize the FlipIt-C game and obtain the L-FlipIt-C games.

The defender pays a premium $T \in \mathbb{R}_{\geq 0}$ to insure the IoT network and receive a coverage when he faces losses from any devices. Following similar steps in Section III.A., the defender's individual rationality constraint in this case can be written as

$$(1-s)\sum_{n=1}^{N} \gamma_{d,n} g_n(\alpha^*_1(s), \ldots, \alpha^*_N(s)) + \sum_{n=1}^{N} c_{d,n}(p^*_{d,n}(s)) + T$$
$$\leq \sum_{n=1}^{N} \gamma_{d,n} g_n(\alpha^*_1(0), \ldots, \alpha^*_N(0)) + \sum_{n=1}^{N} c_{d,n}(p^*_{d,n}(0)). \tag{14}$$

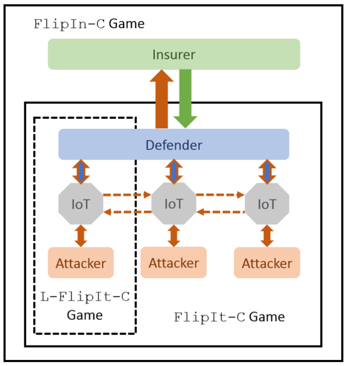


Fig. 6. The structure of the games in Defender-C. There is only one defender in this case. The FlipIt-C game captures the interactions between a defender and all attackers in the IoT network while the L-FlipIt-C game captures the interactions between the defender and an attacker on one IoT device. The FlipIn-C captures the interactions between the defender, all attackers, and the insurer.

The insurer's individual rationality constraint can be written as

$$T - s\sum_{n=1}^{N} g_n\left(\alpha_1^*(s), \dots, \alpha_N^*(s)\right) \geq 0. \tag{15}$$

The insurer aims to maximize the profit as follows:

$$\max_{\{s,T\}}\ T - s\sum_{n=1}^{N} \gamma_{d,n} g_n\left(\alpha_1^*(s), \dots, \alpha_N^*(s)\right)$$
$$\text{s.t. } (14), (15). \tag{16}$$

Similar to the case in the previous subsection, the interactions between the defender and the insurer constitute a principal-agent problem with incomplete information; the complex interactions between the defender, the attackers, and the insurer constitute a bi-level FlipIn-C game whose Nash equilibrium is defined as follows.

Definition 5 (Equilibrium Concept for FlipIn-C): Let $\mathscr{S}_i = \{\{s, T\}|s \in (0, 1], T \in \mathbb{R}_{\geq 0}, (14), (15)\}$ denote the action set for the insurer; let $J_i(s, T)$ denote the objective function from (16). Recall $\mathscr{S}_d$, $\mathscr{S}_{a,n}$, J_d, $J_{a,n}$ from Definition 3, a strategy profile $\{\{p^*_{a,n}\}, \{p^*_{d,n}\}, \{s^*, T^*\}\}$ is a global Nash equilibrium of the bi-level FlipIn-C game defined by $\langle\{\text{Attackers}, \text{Defender-C}, \text{Insurer}\}, \{\{\mathscr{S}_{a,n}\}, \mathscr{S}_d, \mathscr{S}_i\}, \{\{J_{a,n}\}, J_d, J_i\}\rangle$ if $\{s^*, T^*\}$ solves (16) and $\{p^*_{a,n}, p^*_{d,n}\}$ is a Nash equilibrium of the FlipIt-C game defined in Definition 3 under $\{s^*, T^*\}$.

An illustration of the FlipIn-C game has been provided in Fig. 6. Compared with the G-FlipIn-D game, the FlipIn-C game contains only one principal-agent problem and there is only one defender who competes with each attacker on the ownership of each IoT device. Moreover, the G-FlipIn-D game can be considered as a bottom-up approach on a distributed scenario as the distributed games constitute a centralized game, while the FlipIn-C game can be considered as a top-down approach on a centralized scenario as the centralized FlipIt-C game can be decentralized into distributed L-FlipIt-C games.

IV. Overview of Finding the Equilibrium

It is challenging to directly compute the equilibrium of the bi-level FlipIn games in both the distributed case and the centralized case due to the complex relations among three networked parties of players and the various strategy choices of defenders and attackers. In this paper, we consider that both defenders and attackers adopt non-adaptive periodic strategies. The periodic strategy could be viewed as a routine security examination of the defender or programmed attacks of the attacker. Moreover, we incorporate linear influence models to capture the risk dependencies between neighboring nodes, which have been used extensively to study risk propagation over networks [22]–[24]. The periodic strategy and linear influence model enable us to solve the lower-level security games and further analyze the higher-level insurance problems. The obtained results yield critical insights on network topology and insurance contract designation, and they provide valuable baselines for future analysis on both FlipIt games and cyber insurance.

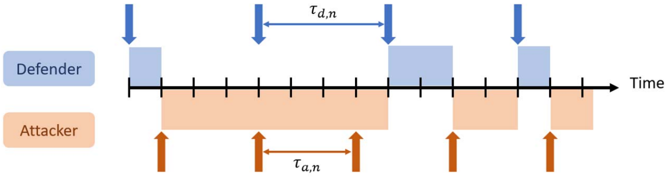


Fig. 7. The FlipIt game on Node n between a defender and an attacker with both players adopting non-adaptive periodic strategies.

Both the defender and the attacker adopt non-adaptive periodic strategies, i.e., both players have fixed intervals $\tau_{d,n} \in \mathbb{R}_{>0}$ and $\tau_{a,n} \in \mathbb{R}_{>0}$ between two consecutive moves as shown in Fig. 7, respectively. In the following sections, we abuse the notations of strategies $p_{d,n} = \frac{1}{\tau_{d,n}}$ and $p_{a,n} = \frac{1}{\tau_{a,n}}$ to denote the defending frequency and the attacking frequency, respectively. We can compute α_n, i.e., the expected proportion of the time that the attacker controls node n by following the arguments in Section 4.1 in [25]. When $p_{d,n} \geq p_{a,n}$, i.e., $\tau_{d,n} \leq \tau_{a,n}$, the probability that the attacker moves in a given defender's move interval $\tau'_{d,n}$ is $p_{a,n}/p_{d,n}$; moreover, he moves exactly once within $\tau'_{d,n}$ since $\tau_{d,n} \leq \tau_{a,n}$ and his move is uniformly distributed at random within $\tau'_{d,n}$. Thus, we obtain $\alpha_n = \frac{p_{a,n}}{2p_{d,n}}$. Similarly, when $p_{d,n} < p_{a,n}$, we obtain $\alpha_n = 1 - \frac{p_{d,n}}{2p_{a,n}}$. As a result, we have

$$\alpha_n = \begin{cases} 0, & p_{a,n} = 0; \\ \dfrac{p_{a,n}}{2p_{d,n}}, & p_{d,n} \geq p_{a,n} > 0; \\ 1 - \dfrac{p_{d,n}}{2p_{a,n}}, & p_{a,n} > p_{d,n} \geq 0. \end{cases} \tag{17}$$

Note that when $p_{a,n} = 0$, i.e., there is no attacker or the attacker chooses not to attack, we have $\alpha_n = 0$ for $p_{d,n} \geq 0$ which indicates that the IoT device is always controlled by the defender. We can see from (17) that the attacker has a larger α_n with the increase of his frequency $p_{u,n}$ and the decrease of the defender's frequency $p_{d,n}$. We could also see that α_n is continuous in both $p_{a,n}$ and $p_{d,n}$ as $\frac{p_{a,n}}{2p_{d,n}} = 1 - \frac{p_{d,n}}{2p_{a,n}} = \frac{1}{2}$ when $p_{a,n} = p_{d,n}$.

We capture the risk dependencies between neighboring nodes with linear influence models. We use the following remark to illustrate linear influence models.

Remark 3 (Linear Influence Models): The defender's risk level at node n can be expressed as

$$R_n = \alpha_n + \eta\sum_{m=1}^{N} w_{mn} R_m. \tag{18}$$

The first term is the expected proportion of the attacker's controlling time at node n, and a higher proportion indicates a higher risk level of the defender at this node. The second term captures the risks caused by neighboring nodes. The parameter $\eta \in [0, 1]$ denotes the discount ratio of the network influence, and a larger η denotes a stronger influence from neighboring nodes and indicates that the network is strongly connected; the parameters $w_{mn} \in [0, 1]$ denote the probability that node n is attacked by the attacker at its neighboring node m and they satisfy

$$w_{nn} = 0, \ \sum_{n=1}^{N} w_{mn} = 1. \tag{19}$$

Note that we have $w_{nn} = 0$ as the influence of the attacker at node n has been captured by α_n.

With linear influence models, we could achieve the following remark from Proposition 6 in [72].

Remark 4: Let $\mathbf{W}$ denote the network matrix with the m-th row and n-th column being w_{mn} and let $\mathbf{I}_N$ denote an identity matrix of size N, we have

$$R_n = g_n(\alpha_1, \alpha_2, \ldots, \alpha_N) = \sum_{m=1}^{N} w^*_{nm}\alpha_m, \tag{20}$$

where w^*_{nm} is the element at the n-th row and m-th column of matrix $\mathbf{W}^* = (\mathbf{I}_N - \eta\mathbf{W}^T)^{-1}$ with scalar $\eta \in [0, 1]$ being the discount ratio of the network influence. The matrix $\mathbf{W}^*$ is valid as the inverse of $\mathbf{I}_N - \eta\mathbf{W}^T$ exists. Furthermore, w^*_{nm} satisfies

(i) $w^*_{nn} > 1$ *and* $w^*_{nm} \geq 0$ *for all* $n, m \in \mathcal{N}$*;*

(ii) $\sum_{m=1}^{N} w^*_{mn} = \frac{1}{1-\eta}$ *for all* $n \in \mathcal{N}$.

Remark 4 indicates that the defender's risk level at one node is also affected by α_m in other nodes. The defender's risk level is higher when any attacker in this network has a larger expected proportion of controlling time, which captures a negative impact of the network influence on cyber security.

Remark 5: From (17) and Remark 4, the defender at node n has a higher risk level or faces a larger expected loss if

- *the attacker at node n has a larger expected proportion of controlling time, i.e., α_n is larger;*
- *the attacker at node n attacks more frequently, i.e., the attacker has a larger $p_{a,n}$;*
- *the defender at node n defends less frequently, i.e, the defender has a smaller $p_{d,n}$;*
- *the attackers at other nodes have larger expected proportions of controlling time, i.e., α_m is larger for $m \neq n$.*

The players' problems in both Defender-D and Defender-C under periodic strategies and linear influence models could be obtained by plugging (17) and (20) into the corresponding problems. Since solving the insurer's problem relies on the results of the FlipIt games, we first solve the lower-level FlipIt games and obtain the reactions of both defenders and attackers to the insurance contracts. Then, we solve the insurer's problem and obtain optimal insurance contracts. Note that we consider linear costs of defenders and attackers in the following sections, and we abuse the notations of $c_{d,n}$ and $c_{a,n}$ to denote the corresponding cost parameters. The attacker's problem (3) can now be written as

$$\max_{p_{a,n}} \ \gamma_{a,n}\alpha_n - c_{a,n}p_{a,n}. \tag{21}$$

Different $\gamma_{a,n}$ and $c_{a,n} \in \mathbb{R}_{\geq 0}$ capture the trade-offs between a larger proportion of time and a smaller attacking frequency of the attacker.

We could obtain the following problem after plugging (20) into the defender's problem (7) in Defender-D.

$$\min_{p_{d,n}} \ (1 - s_n)\gamma_{d,n} \sum_{m=1}^{N} w^*_{nm}\alpha_m + c_{d,n}p_{d,n}. \tag{22}$$

The parameters $\gamma_{a,n}$ and $c_{d,n} \in \mathbb{R}_{\geq 0}$ capture the trade-offs between a smaller expected effective loss and a larger defending frequency of the defender.

Remark 6 (Distributed Computations): Since α_m is a constant with respect to $p_{d,n}$ if $m \neq n$, problem (22) can be simplified further into the following problem

$$\min_{p_{d,n}} \ (1 - s_n)\gamma_{d,n}w^*_{nn}\alpha_n + c_{d,n}p_{d,n}. \tag{23}$$

Problem (23) indicates that the defender's decision on $p_{d,n}$ in one FlipIt-D *game is not affected by results of other* FlipIt-D *games given the coverage level s_n. However, the expected loss of the defender $\mathbb{E}[X_n]$ is still affected by the outcomes of other* FlipIt-D *games.*

We could obtain the following problem after plugging (20) into the defender's problem (12) in Defender-C.

$$\min_{\{p_{d,n}\}} \ (1 - s)\sum_{n=1}^{N}\sum_{m=1}^{N} \gamma_{d,n}w^*_{nm}\alpha_m + \sum_{n=1}^{N} c_{d,n}p_{d,n}. \tag{24}$$

Note that $g_n(\alpha_1, \ldots, \alpha_N)$ in (20) is additively separable for all $1 \leq n \leq N$, thus, the L-FlipIt-C games exist under periodic strategy and linear influence model and problem (24) is equivalent to the following N sub-problems from Remark 2.

$$\min_{p_{d,n}} \ (1 - s)\sum_{m=1}^{N} \gamma_{d,m}w^*_{mn}\alpha_n + c_{d,n}p_{d,n}. \tag{25}$$

Note that the FlipIt-D games and the L-FlipIt-C games share similar structures: the attackers in both cases solve the same optimization problems (21); the defenders' problems (23) and (25) can be written into one unified optimization problem as

$$\min_{p_{d,n}} \ (1 - \tilde{s}_n)\tilde{\gamma}_{d,n}\alpha_n + c_{d,n}p_{d,n}, \tag{26}$$

where

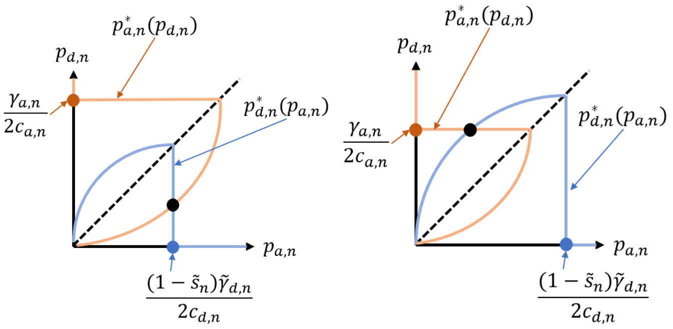
$$\tilde{s}_n = \begin{cases} s_n, & \text{Defender-D;} \\ s, & \text{Defender-C,} \end{cases} \tag{27}$$

$$\tilde{\gamma}_{d,n} = \begin{cases} \gamma_{d,n}w^*_{nn}, & \text{Defender-D;} \\ \sum_{m=1}^{N} \gamma_{d,m}w^*_{mn}, & \text{Defender-C.} \end{cases} \tag{28}$$

Remark 7: Problem (26) can be interpreted that the defender aims to minimize the expected proportion of the attacker's controlling time. Thus, given the same coverage level on an IoT device, the defender in Defender-C cares more about reducing the impacts from the attackers compared with the defenders in Defender-D as $\sum_{m=1}^{N} \gamma_{d,m}w^*_{mn} \geq \gamma_{d,n}w^*_{nn}$.

We can further define an unified local FlipIt game as follows.

Definition 6: Let $\mathcal{S}_{a,n} = \{p_{a,n} | p_{a,n} \in \mathbb{R}_{\geq 0}\}$ and $\mathcal{S}_{d,n} = \{p_{d,n} | p_{d,n} \in \mathbb{R}_{\geq 0}\}$ denote the action sets for the attacker



(a) $\frac{\gamma_{a,n}}{2c_{a,n}} \geq \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$ (b) $\frac{\gamma_{a,n}}{2c_{a,n}} < \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$

Fig. 8. Equilibrium of the local FlipIt game at node n. $p^*_{a,n}(p_{d,n})$ denotes the best response of the attacker given the defender's defending frequency $p_{d,n}$ while $p^*_{d,n}(p_{a,n})$ denotes the best response of the defender given the attacker's attacking frequency $p_{a,n}$.

and the defender at node n, respectively; let $J_{a,n}(p_{a,n}, p_{d,n})$ and $J_{d,n}(p_{d,n}, p_{a,n}; \tilde{s}_n)$ denote the objective functions from (3) and (26), respectively. A strategy profile $\{p^*_{a,n}, p^*_{d,n}\}$ is a Nash equilibrium of the local FlipIt *game at node n defined by $\langle\{$Attacker, Defender$\}, \{\mathscr{S}_{a,n}, \mathscr{S}_{d,n}\}, \{J_{a,n}, J_{d,n}\}\rangle$ if*

$$J_{a,n}(p^*_{a,n}, p^*_{d,n}) \geq J_{a,n}(p_{a,n}, p^*_{d,n}), \quad \forall p_{a,n} \in \mathscr{S}_{a,n};$$
$$J_{d,n}(p^*_{d,n}, p^*_{a,n}; \tilde{s}_n) \leq J_{d,n}(p_{d,n}, p^*_{a,n}; \tilde{s}_n), \quad \forall p_{d,n} \in \mathscr{S}_{d,n}.$$

We can obtain the solutions of the FlipIt-D games and the L-FlipIt-C games by plugging (27) and (28) into the solution of the local FlipIt game defined in Definition 6. The solutions of the G-FlipIt-D game and the FlipIt-C game can be further obtained by their Definitions 1 and 3, respectively. Thus, we can solve all FlipIt games in both Defender-D and Defender-C by solving the local FlipIt game.

The local FlipIt game defined in Definition 6 is different from the original FlipIt game presented in [25] as the defender here aims to minimize the losses caused by the attacker while the defender in the original FlipIt game aims to maximize the proportion of his controlling time. Following similar steps as in [25], we can obtain the equilibrium of the local FlipIt game defined in Definition 6 by finding the intersection of the players' best responses as shown in Fig. 8.

Proposition 1: The Nash equilibrium of the local FlipIt *game defined in Definition 6 can be summarized into two different cases as shown in Fig. 8.*

- *If $\frac{\gamma_{a,n}}{2c_{a,n}} \geq \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$, the equilibrium (**FlipIt-E1**) is achieved at*
$$p^*_{d,n} = \frac{(1-\tilde{s}_n)^2\tilde{\gamma}^2_{d,n}c_{a,n}}{2\gamma_{a,n}c^2_{d,n}}, \quad p^*_{a,n} = \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}; \quad (29)$$
- *If $\frac{\gamma_{a,n}}{2c_{a,n}} < \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$, the equilibrium (**FlipIt-E2**) is achieved at*
$$p^*_{d,n} = \frac{\gamma_{a,n}}{2c_{a,n}}, \quad p^*_{a,n} = \frac{\gamma^2_{a,n}c_{d,n}}{2(1-\tilde{s}_n)\tilde{\gamma}_{d,n}c^2_{a,n}}. \quad (30)$$

Proof: The equilibrium can be obtained by finding the intersection between the best responses as shown in Fig. 8. □

Note that $p^*_{d,n} = 0$ and $p^*_{a,n} = 0$ are also the intersection of the best responses. However, we exclude them in this paper as there are no defender and attacker when $p^*_{d,n} = 0$ and $p^*_{a,n} = 0$. We can see from Proposition 1 that the equilibrium is affected by the coverage level $\tilde{s}_n$, and we have the following remarks regarding the relations between them.

Remark 8 (Equilibrium Shift): If $\gamma_{a,n}c_{d,n} \geq \tilde{\gamma}_{d,n}c_{a,n}$, we have $\frac{\gamma_{a,n}}{2c_{a,n}} \geq \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$ for $0 < \tilde{s}_n \leq 1$, and thus the equilibrium is FlipIt-E1 for $0 < \tilde{s}_n \leq 1$.

If $\gamma_{a,n}c_{d,n} < \tilde{\gamma}_{d,n}c_{a,n}$, we note that $\frac{\gamma_{a,n}}{2c_{a,n}} < \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$ when $0 < \tilde{s}_n < 1 - \frac{\gamma_{a,n}c_{d,n}}{\tilde{\gamma}_{d,n}c_{a,n}}$, and thus the equilibrium is FlipIt-E2. However, we have $\frac{\gamma_{a,n}}{2c_{a,n}} \geq \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}}{2c_{d,n}}$ when $1 - \frac{\gamma_{a,n}c_{d,n}}{\tilde{\gamma}_{d,n}c_{a,n}} \leq \tilde{s}_n \leq 1$, and thus the equilibrium is FlipIt-E1. As a result, the equilibrium shifts from FlipIt-E2 to FlipIt-E1 as the coverage level increases.

Remark 9 (Risk Compensation and Peltzman Effect): At FlipIt-E1, both the defender and the attacker reduce their frequencies as the coverage level increases. The defender's reckless behavior under the insurance in this case is referred as risk compensation [79]. The proportion of the attacker's controlling time $\alpha^*_n = 1 - \frac{(1-\tilde{s}_n)\tilde{\gamma}_{d,n}c_{a,n}}{2\gamma_{a,n}c_{d,n}}$ increases with the coverage level, as a result, the defender faces a higher risk, and such phenomena under the insurance is referred as Peltzman effect [80].

However, at FlipIt-E2, the defender does not change his frequency while the attacker increases his frequency as the coverage level increases. The proportion of the attacker's controlling time $\alpha^*_n = \frac{\gamma_{a,n}c_{d,n}}{2(1-\tilde{s}_n)\tilde{\gamma}_{d,n}c_{a,n}}$ increases with the coverage level. Thus, at FlipIt-E2, there is no risk compensation, but we can observe Peltzman effect.

With the results of the local FlipIt game, we can solve the insurer's problems and obtain the optimal insurance contracts. In the following sections, we discuss cyber insurance separately for Defender-D and Defender-C.

V. Cyber Insurance: Defender-D

In this section, we aim to solve the insurer's problem (10) in Defender-D. We can obtain the results of the FlipIt-D game by plugging $\tilde{s}_n = s_n$ and $\tilde{\gamma}_{d,n} = \gamma_{d,n}w^*_{nn}$ into Proposition 1. Let us abuse the notations $p^*_{d,n}(s_n)$, $p^*_{a,n}(s_n)$, and $\alpha^*_n(s_n)$ to denote the equilibrium results under the coverage level s_n; let $K^*_{d,n}(s_n) = J_{d,n}(p^*_{d,n}, p^*_{a,n}; s_n)$ from Definition 6. Note that $s_n = 0$ indicates the results under no insurance.

Remark 10: The defender's decision on $p_{d,n}$ is not affected by the players' decisions at other nodes from Remark 6 while the attacker's decision on $p_{a,n}$ is also not affected by the players' decisions at other nodes from (3). Thus, we have $\alpha'_m = \alpha_m, \forall m \neq n$ in (8). As a result, (8) can be rewritten as

$$T_n \leq K^*_{d,n}(0) - K^*_{d,n}(s_n) + s_n\gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m. \quad (31)$$

Since the insurer aims to maximize his profit, he sets highest possible premium at

$$T_{n,\max} = K^*_{d,n}(0) - K^*_{d,n}(s_n) + s_n\gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m. \quad (32)$$

As a result, solving the insurer's problem (10) is equivalent to solving the following problem after plugging (32) into (10):

$$s^*_n = \arg\max_{0<s_n\leq 1} K^*_{d,n}(0) - K^*_{d,n}(s_n) - s_n\gamma_{d,n}w^*_{nn}\alpha^*_n(s_n)$$
$$\text{s.t. } K^*_{d,n}(0) - K^*_{d,n}(s_n) - s_n\gamma_{d,n}w^*_{nn}\alpha^*_n(s_n) \geq 0, \quad (33)$$

and the premium T^*_n can be achieved by plugging s^*_n into (32). Since we have achieved the equilibrium results of the `FlipIt-D` game in the previous section, we can directly solve (33).

A. High-Risk Regime: $\gamma_{a,n}c_{d,n} \geq \gamma_{d,n}w^*_{nn}c_{a,n}$

In this case, the `FlipIt-D` game between the defender and the attacker achieves *FlipIt-E1* as in Remark 8. After plugging the results of *FlipIt-E1*, problem (33) can be expressed as

$$\begin{aligned} s^*_n = \ & \arg \max_{0<s_n\leq 1} \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}(1-s_n)s_n \\ & \text{s.t. } \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}(1-s_n)s_n \geq 0. \end{aligned} \tag{34}$$

Note that $\frac{\gamma^2_{d,n}\ w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}$ is constant for s_n and the constraint is satisfied for $0 < s_n \leq 1$. Thus, we only need to find s^*_n that minimizes the objective function to obtain the optimal insurance contract.

Lemma 1: If $\gamma_{a,n}c_{d,n} \geq \gamma_{d,n}w^*_{nn}c_{a,n}$, the optimal insurance contract is

$$s^*_n = \frac{1}{2}, \quad T^*_n = \frac{\gamma_{d,n}w^*_{nn} + \gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m}{2}. \tag{35}$$

The insurer's profit under this contract is $\frac{\gamma^2_{d,n}\ w^{*2}_{nn}c_{a,n}}{8\gamma_{a,n}c_{d,n}}$.

Proof: We can achieve that $s^*_n = \frac{1}{2}$. T^*_n can be achieved by plugging s^*_n into (32). □

B. Low-Risk Regime: $\gamma_{a,n}c_{d,n} < \gamma_{d,n}w^*_{nn}c_{a,n}$

In this case, the equilibrium of the `FlipIt-D` game shifts from *FlipIt-E2* to *FlipIt-E1* as the coverage level increases from Remark 8. When $0 < s_n < 1 - \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}}$, the `FlipIt-D` game achieves *FlipIt-E2* and we have $T_{n,\max} = K^*_{d,n}(0) - K^*_{d,n}(s_n) - s_n\gamma_{d,n}w^*_{nn}\alpha^*_n(s_n) = -s_n\gamma_{d,n}w^*_{nn}\alpha^*_n(s_n) < 0$. Thus, the insurer does not provide any insurance contracts with $0 < s_n < 1 - \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}}$.

When $1 - \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} \leq s_n \leq 1$, the `FlipIt` game achieves *FlipIt-E1* under the insurance and *FlipIt-E2* without the insurance, and after plugging the results of *FlipIt-E1* and *FlipIt-E2* into (33), we have

$$\begin{aligned} s^*_n \in \ & \arg\max_{s_n} \frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \gamma_{d,n}w^*_{nn} + \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}(1-s_n)s_n \\ & \text{s.t. } \frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \gamma_{d,n}w^*_{nn} + \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}(1-s_n)s_n \geq 0. \end{aligned} \tag{36}$$

We first obtain the following proposition regarding the insurability of the defender.

Proposition 2 (Insurability): The defender is not insurable, i.e., there exists no effective insurance contract and the equilibrium of the `FlipIn-D` game does not exist, if

$$0 < \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} < \frac{1}{2} + \frac{\sqrt{2}}{4}. \tag{37}$$

Proof: See Appendix. □

Proposition 2 comes from the individual rationality constraints of both insurer and defender, and it reflects situations that the insurer has no incentive to provide insurance to the defender as he cannot make a profit from it or the defender has no incentive to accept any insurance as he has larger costs with it. We can further achieve the following remark regarding the condition (37).

Remark 11: The defender is not insurable if:

(i) *$\gamma_{d,n}$ is high, i.e., the attacker inflicts large losses on the defender;*

(ii) *$c_{d,n}$ is low, i.e., the defender has a low cost to control the device frequently;*

(iii) *$\gamma_{a,n}$ is low, i.e., the attacker has a low benefit of controlling the device;*

(iv) *$c_{a,n}$ is high, i.e., the attacker has a high cost to control the device frequently;*

(v) *w^*_{nn} is high, i.e., the network effect is high.*

We have that the following proposition regarding the optimal insurance contracts when the defender is insurable.

Lemma 2: If $\frac{1}{2} + \frac{\sqrt{2}}{4} \leq \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} < 1$, the optimal insurance contract is

$$s^*_n = \frac{1}{2}, \quad T^*_n = \frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \frac{\gamma_{d,n}w^*_{nn}}{2} + \frac{\gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m}{2}. \tag{38}$$

The insurer's profit under this contract is $\frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \gamma_{d,n}w^*_{nn} + \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{8\gamma_{a,n}c_{d,n}}$.

Proof: We can achieve that $s^*_n = \frac{1}{2}$ from (36), and it satisfies the constraint $1 - \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} \leq s_n \leq 1$. T^*_n can be obtained by plugging s^*_n into (32). □

With Lemma 1, Proposition 2, and Lemma 2, we have the following proposition regarding the equilibrium of the `FlipIn-D` game defined in Definition 2.

Proposition 3: The Nash equilibrium of the `FlipIn-D` game defined in Definition 2 can be summarized into the following three cases:

- *if $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} \geq 1$, the equilibrium is achieved at*

$$s^*_n = \frac{1}{2}, \quad T^*_n = \frac{\gamma_{d,n}w^*_{nn}}{2} + \frac{\gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m(s_m)}{2},$$
$$p^*_{d,n} = \frac{\gamma^2_{d,n}\ w^{*2}_{nn}c_{a,n}}{8\gamma_{a,n}c^2_{d,n}}, \ p^*_{a,n} = \frac{\gamma_{d,n}w^*_{nn}}{4c_{d,n}};$$

- *if $\frac{1}{2} + \frac{\sqrt{2}}{4} \leq \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} < 1$, the equilibrium is achieved at*

$$s^*_n = \frac{1}{2},$$
$$T^*_n = \frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \frac{\gamma_{d,n}w^*_{nn}}{2} + \frac{\gamma_{d,n}\sum_{m\neq n} w^*_{nm}\alpha_m(s_m)}{2},$$
$$p^*_{d,n} = \frac{\gamma^2_{d,n}\ w^{*2}_{nn}c_{a,n}}{8\gamma_{a,n}c^2_{d,n}}, \ p^*_{a,n} = \frac{\gamma_{d,n}w^*_{nn}}{4c_{d,n}};$$

- *if $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} < \frac{1}{2} + \frac{\sqrt{2}}{4}$, the equilibrium does not exist. The defender and the attacker have*

$$p^*_{d,n} = \frac{\gamma_{a,n}}{2c_{a,n}}, \quad p^*_{a,n} = \frac{\gamma^2_{a,n}c_{d,n}}{2\gamma_{d,n}w^*_{nn}c^2_{a,n}}.$$

Proof: This proposition follows from combining Proposition 1, Lemma 1, Proposition 2, and Lemma 2. □

We can see that when the defender is insurable, the optimal insurance contract provides a coverage level of $\frac{1}{2}$.

Remark 12: The Nash equilibrium of the `G-FlipIn-D` game defined in Definition 2 could be obtained with Proposition 3 by combing the results of all the `FlipIn-D` games.

We could also obtain the Nash equilibrium of the `FlipIn-D` game when there are no network connectivities by following the similar steps in this section. In this case, all the IoT devices are not connected with each other or there is only one IoT device in this network.

Corollary 1: When the network is not connected, the Nash equilibrium of the `FlipIn-D` *game can be summarized into the following three cases*:

- *if* $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}c_{a,n}} \geq 1$, *the equilibrium is achieved at* $s_n^* = \frac{1}{2}$, $T_n^* = \frac{\gamma_{d,n}}{2}$, $p_{d,n}^* = \frac{\gamma_{d,n}^2 \, c_{a,n}}{8\gamma_{a,n}c_{d,n}^2}$, $p_{a,n}^* = \frac{\gamma_{d,n}}{4c_{d,n}}$;
- *if* $\frac{1}{2} + \frac{\sqrt{2}}{4} \leq \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}c_{a,n}} < 1$, *the equilibrium is achieved at* $s_n^* = \frac{1}{2}, T_n^* = \frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \frac{\gamma_{d,n}}{2}$, $p_{d,n}^* = \frac{\gamma_{d,n}^2 \, c_{a,n}}{8\gamma_{a,n}c_{d,n}^2}$, $p_{a,n}^* = \frac{\gamma_{d,n}}{4c_{d,n}}$;
- *if* $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}c_{a,n}} < \frac{1}{2} + \frac{\sqrt{2}}{4}$, *the equilibrium does not exist. The defender and the attacker have* $p_{d,n}^* = \frac{\gamma_{a,n}}{2c_{a,n}}$, $p_{a,n}^* = \frac{\gamma_{a,n}^2 c_{d,n}}{2\gamma_{d,n}c_{a,n}^2}$.

Recall $w_{nn}^* > 1$ and $w_{nm}^* \geq 0$ from Remark 4. By comparing Proposition 3 and Corollary 1, we can see that the network effect decreases the insurability as the insurable defender could be uninsurable because of network effects when $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w_{nn}^* c_{a,n}} < \frac{1}{2} + \frac{\sqrt{2}}{4} \leq \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}c_{a,n}}$. Moreover, the premium of the optimal insurance contract is also higher with network connectivity when $\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w_{nn}^* c_{a,n}} \geq 1$.

VI. Cyber Insurance: Defender-C

In this section, we analyze the insurer's problem (16) for the `FlipIn-C` game. Following similar steps in the previous section, let $K_{d,n}^*(s) = J_{d,n}(p_{d,n}^*, p_{a,n}^*; s)$ from Definition 6. The defender's individual rationality constraint (14) indicates that:

$$T \leq \sum_{n=1}^{N} \left(K_{d,n}^*(0) - K_{d,n}^*(s)\right). \tag{39}$$

Thus, the highest premium that the insurer can charge is

$$T_{\max} = \sum_{n=1}^{N} \left(K_{d,n}^*(0) - K_{d,n}^*(s)\right). \tag{40}$$

As a result, solving the insurer's problem (16) is equivalent to solving the following problem after plugging (40) into (16):

$$\begin{aligned} s^* = \ & \arg\max_{0<s\leq 1} \sum_{n=1}^{N} \left(K_{d,n}^*(0) - K_{d,n}^*(s) - s \sum_{m=1}^{N} \gamma_{d,m} w_{mn}^* \alpha_n^*(s) \right) \\ & \text{s.t.} \sum_{n=1}^{N} \left(K_{d,n}^*(0) - K_{d,n}^*(s) - s \sum_{m=1}^{N} \gamma_{d,m} w_{mn}^* \alpha_n^*(s) \right) \geq 0. \end{aligned} \tag{41}$$

Problem (41) is a nonlinear programming problem and it is challenging to find the analytical solution. We can leverage numerical methods to compute s^* and obtain T^* with (40). We can then find $p_{d,n}^*$ and $p_{a,n}^*$ by plugging s^* into Proposition 1, and further obtain the solution of the `FlipIn-C` game defined in Definition 5.

A. Semi-Homogeneous Case

Problem (41) can be directly solved in a semi-homogeneous case following similar steps in the previous section. In this semi-homogeneous case, we consider that all players in one party are homogeneous with the same parameters, i.e., $c_{d,n} = c_d$, $\gamma_{d,n} = \gamma_d$, $c_{a,n} = c_a$, and $\gamma_{a,n} = \gamma_a$ for $n \in \mathscr{N}$. Note that the network can be heterogeneous, i.e., each node may have a different number of neighbors with different w_{mn}.

Recall (28), we have $\tilde{\gamma}_{d,n} = \sum_{m=1}^{N} \gamma_{d,m} w_{mn}^* = \gamma_d \sum_{m=1}^{N} w_{mn}^* = \frac{\gamma_d}{1-\eta}$ for $n \in \mathscr{N}$ from Remark 4. Since the equilibrium of the `L-FlipIt-C` game only depends on $c_{d,n}$, $\tilde{\gamma}_{d,n}$, $c_{a,n}$, $\gamma_{a,n}$, and $\tilde{s}_n$, which are same for each node, all nodes have the same results at the equilibrium, i.e., $p_{d,n}^* = p_d^*$, $p_{a,n}^* = p_a^*$, $\alpha_n^* = \alpha^*$, and $J_{d,n}(p_{d,n}^*, p_{a,n}^*; s) = J_d(p_d^*, p_a^*; s)$. Thus, let $K_d^*(s) = J_d(p_d^*, p_a^*; s)$, the insurer's problem can be simplified into the following problem

$$\begin{aligned} s^* = \ & \arg\max_{0<s\leq 1} \ K_d^*(0) - K_d^*(s) - s\frac{\gamma_d}{1-\eta}\alpha^*(s) \\ & \text{s.t. } K_d^*(0) - K_d^*(s) - s\frac{\gamma_d}{1-\eta}\alpha^*(s) \geq 0. \end{aligned} \tag{42}$$

Note that the premium $T^* = N(K_d^*(0) - K_d^*(s^*))$, where N is the number of nodes. We note that the structure of the games in this subsection is similar to the structure of the games in Defender-D, and we can obtain the equilibrium of the `FlipIn-C` game in this semi-homogeneous case using the results from Section V.

Corollary 2: The Nash equilibrium of the `FlipIn-C` *game defined in Definition 2 of a semi-homogeneous case can be summarized into the following three cases*:

- *if* $\frac{(1-\eta)\gamma_a c_d}{\gamma_d c_a} \geq 1$, *the equilibrium is achieved at* $s^* = \frac{1}{2}$, $T^* = \frac{N\gamma_d}{2(1-\eta)}$, $p_d^* = \frac{\gamma_d^2 \, c_a}{8(1-\eta)^2\gamma_a c_d^2}$, $p_a^* = \frac{\gamma_d}{4(1-\eta)c_d}$;
- *if* $\frac{1}{2} + \frac{\sqrt{2}}{4} \leq \frac{(1-\eta)\gamma_a c_d}{\gamma_d c_a} < 1$, *the equilibrium is achieved at* $s^* = \frac{1}{2}, T^* = \frac{Nc_d\gamma_a}{c_a} - \frac{N\gamma_d}{2(1-\eta)}$, $p_d^* = \frac{\gamma_d^2 \, c_a}{8(1-\eta)^2\gamma_a c_d^2}$, $p_a^* = \frac{\gamma_d}{4(1-\eta)c_d}$;
- *if* $\frac{(1-\eta)\gamma_a c_d}{\gamma_d c_a} < \frac{1}{2} + \frac{\sqrt{2}}{4}$, *the equilibrium does not exist. The defender and the attacker have* $p_d^* = \frac{\gamma_a}{2c_a}$, $p_a^* = \frac{(1-\eta)\gamma_a^2 c_d}{2\gamma_d c_a^2}$.

We can see that the equilibrium results of the semi-homogeneous `FlipIn-C` game do not depend on the network topology. We could also obtain the equilibrium results of the `FlipIn-D` games of Defender-D in this semi-homogeneous case by Proposition 3. Note that $\frac{(1-\eta)\gamma_a c_d}{\gamma_d c_a} < \frac{\gamma_a c_d}{\gamma_d w_{nn}^* c_a}$ as $w_{nn}^* < \frac{1}{1-\eta}$ from Remark 4, thus, the defender in Defender-C is less insurable than the defenders in Defender-D. Moreover, both the defender and the attacker act more frequently in Defender-C than in Defender-D when the defenders in both Defender-D and Defender-C are insurable. The defender defends at the same rate in Defender-D and in Defender-C while the attacker attacks more frequently in Defender-D than in Defender-C when the defenders in both Defender-D and Defender-C are not insurable.

VII. Numerical Analysis

In this section, we present three numerical experiments and compare the results in Defender-D and the results in Defender-C. In the first and second experiments, we consider homogeneous players and investigate the impacts of network

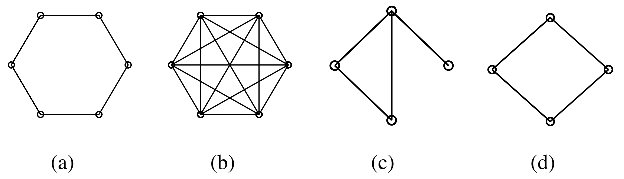


Fig. 9. Networks.

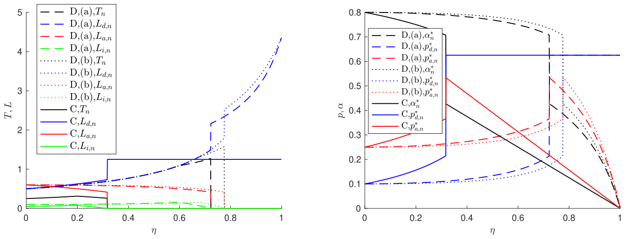
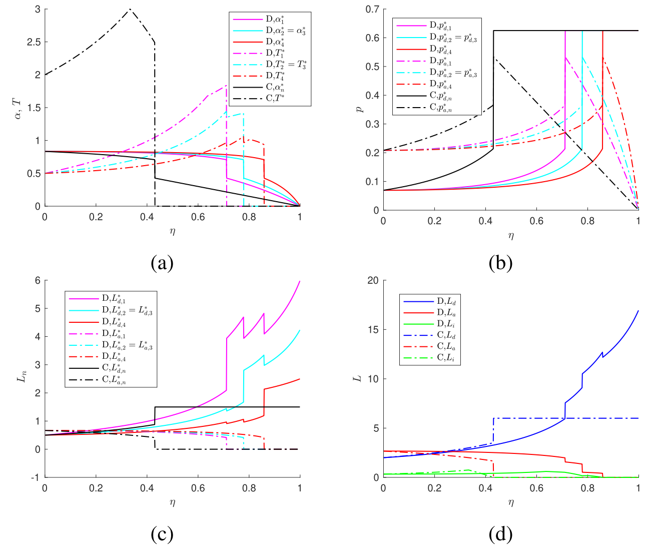


Fig. 10. Numerical results of homogeneous networks with homogeneous players in Fig. 9(ab). The x-axis is the network discount ratio η. “D” and “C” represent Defender-D and Defender-C, respectively. “(a)” and “(b)” represent networks (a) and (b) in Fig. 9, respectively. Note that each node in (a) and (b) has 2 and 5 neighbors, respectively. All nodes in both graphs satisfy $\gamma_{d,n} = 1.0$, $\gamma_{a,n} = 1.0$, $c_{d,n} = 1.0$, and $c_{a,n} = 0.8$. Each link in (a) and (b) satisfies $w_{nm} = 0.5$ and 0.2, respectively. Different line styles indicate results in different networks while different line colors indicate different variables. Note that there are only one insurer and one defender for the case Defender-C, and we plot $T_n = T/N$ and $L_{d,n} = L_d/N$ instead of T and L_d to compare with the results in Defender-D.



(a) (b)

(c) (d)

Fig. 11. Numerical results of a heterogeneous network with homogeneous IoT devices in Fig. 9(c). The x-axis is the network discount ratio η. “D” and “C” represent Defender-D and Defender-C, respectively. Note that nodes 1, 2, 3, and 4 have 3, 2, 2, and 1 neighbors, respectively, thus, $w_{12} = w_{13} = w_{14} = 0.3333$, $w_{21} = w_{23} = w_{31} = w_{32} = 0.5$, and $w_{41} = 1$. All nodes satisfy $\gamma_{d,n} = 1.0$, $\gamma_{a,n} = 1.0$, $c_{d,n} = 1.2$, and $c_{a,n} = 0.8$. Different line colors indicate results of different nodes while different line styles indicate different variables. Note that we plot the global results of Defender-D in Fig. 11(d) to compare with the results of Defender-C.

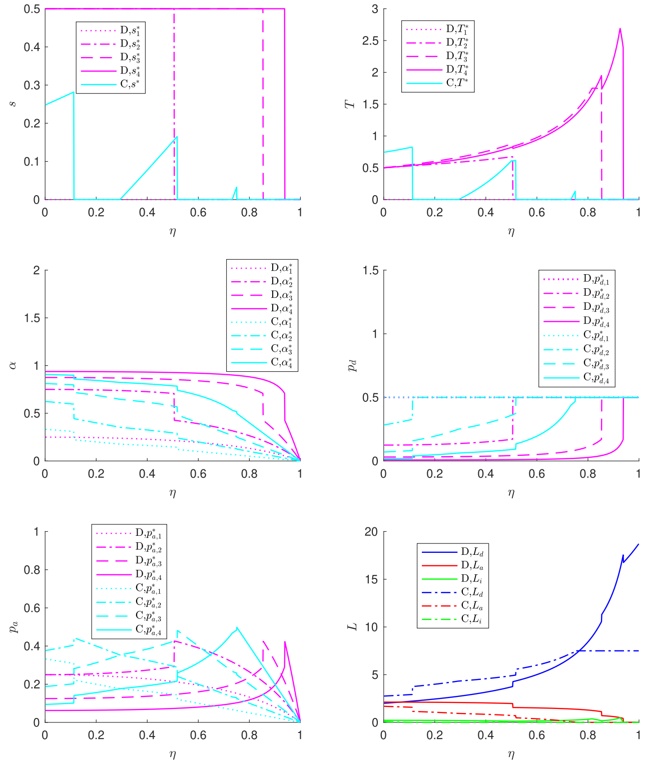


Fig. 12. Numerical results of a homogeneous network with heterogeneous IoT devices in Fig. 9(d). “D” and “C” represent Defender-D and Defender-C, respectively. All nodes satisfy $\gamma_{d,n} = 1.0$, $\gamma_{a,n} = 1.0$, and $c_{a,n} = 1.0$; all links satisfy $w_{nm} = 0.5$. Note that $c_{d,1} = 0.5$, $c_{d,2} = 1$, $c_{d,3} = 2$, and $c_{d,4} = 4$. Note that we plot the global results of Defender-D in the last subfigure of Fig. 12 to compare with the results of Defender-C.

topology. The first experiment compares the results of homogeneous networks with different levels of connectivity, while the second experiment compares the results of nodes with different numbers of neighbors in a heterogeneous network. In the last experiment, we consider heterogeneous players in a homogeneous network and compare the results of defenders with different cost parameters.

These three experiments are inspired by real-world IoT applications. The first and second experiments consider homogeneous IoT devices, such as thermal controllers, surveillance cameras, and unmanned aerial vehicles (UAVs). It is important for both defenders and insurers to know how network topology affects the security of IoT networks. The third experiment considers heterogeneous IoT devices in a network. One example is that a smart home may contain laptops, wireless routers, smart speakers, cameras, and sweeping robots. Different devices may have distinct vulnerabilities and require different protection methods. Moreover, some devices, such as laptops and cameras, contain sensitive information of the household, and they may inflict higher losses on the defenders once they are compromised. Thus, it is also crucial to study cyber insurance on different devices in a network.

All the results in three experiments have been plotted with respect to the network discount ratio η as shown in Figs. 10, 11, and 12. A larger η indicates that the network is strongly connected and an attacker can inflict larger losses on the neighboring IoT devices. We plot the losses of defenders as $L_{d,n}$ or L_d, utilities of attackers as $L_{a,n}$ or L_a, and profits of insurers as $L_{i,n}$ or L_i. Note that $L_{d,n}$ in Defender-D is computed through (7) instead of (23) as there are also losses caused by the attackers in neighboring nodes. In all figures, $T = 0$ or $T_n = 0$ indicate that the defender is not insurable and there exists no effective insurance contract. In the first and second experiments, the coverage level of the optimal insurance contract is $\frac{1}{2}$ in both Defender-C and Defender-D when the defenders are insurable.

We have two important observations from all experiments. We can see that the premiums in both Defender-D and Defender-C have an upward trend with the increase of η, which indicates that defenders are required to pay higher premiums on strongly connected networks. However, when η is too large, the premiums drop to 0, i.e., the defenders are not insurable. As a result, we can conclude that the network effect decreases the insurability of defenders. The insurers should either charge higher premiums or provide no insurance to defenders while the defenders should improve local protections instead of purchasing insurance on strongly connected networks.

We can also see from all experiments that when η is small and defenders are insurable, the defender's total loss in Defender-C is higher than the defenders' global loss in Defender-D, however, when the η is large and defenders are not insurable, the defender's total loss in Defender-C is lower than the defenders' global loss in Defender-D. This phenomenon provides guidance for IoT defenders to decide between centralized management or decentralized management: for weakly connected networks, decentralized management is better than centralized management and each defender should monitor his or her own device; for strongly connected networks, centralized management outperforms decentralized management and a global defender should in charge of all devices.

The results of the first experiment are presented in Fig. 10. Since all players are homogeneous and all networks are homogeneous, we only plot the results of one node for either network. Since all players are homogeneous, we can achieve the same results for both networks in Defender-C as discussed in Section VI.A.; thus, we only plot the results of one network in Defender-C. Comparing the results of network (a) and network (b) in Defender-D, we can see that nodes in network (a) become uninsurable at a smaller η, which indicates that networks with lower connectivities are less insurable. Moreover, the global defender in Defender-C becomes uninsurable at a smaller η than the defenders in Defender-D for both networks, which indicates that a defender who controls the whole network is less insurable than a defender who controls a single device.

The results of the second experiment are presented in Fig. 11. Note that all nodes reach the same L-FlipIt-C equilibrium in Defender-C as discussed in Section VI.A., and thus we only need to plot the results of one node for Defender-C. We also plot $L_d = \sum_{n\in\mathcal{N}} L_{d,n}$, $L_a = \sum_{n\in\mathcal{N}} L_{a,n}$, and $L_i = \sum_{n\in\mathcal{N}} L_{i,n}$ for Defender-D in Fig.11(d). Comparing the results of different nodes in Defender-D, we note that node 1 has a higher premium than nodes 2-4 and node 1 becomes uninsurable at a smaller η from Fig. 11(a). Thus, nodes with more neighbors are less insurable and they should be charged with higher premiums. Moreover, the defender at node 1 has a higher loss than the defenders at nodes 2-4, which indicates that nodes with more neighbors are more vulnerable.

The results of the third experiment are presented in Fig. 12. Note that the defenders have different cost parameters in different nodes, thus, we need to solve problem (41) with numerical methods to find the optimal insurance contracts in Defender-C. Comparing the results of different nodes in Defender-D, we can see that node 1 is always not insurable and node 2 becomes uninsurable at a smaller η than nodes 3-4, which indicates that a defender who has a lower cost to protect his or her device is less insurable. Different from the first and second experiments, the defender switches between insurable statuses and uninsurable statuses with the increase of η in Defender-C, and the coverage level is not $\frac{1}{2}$. We can see that both the coverage level and the premium increase with the increase of η when the defender is at one insurable status.

VIII. Conclusion

In this article, we have established the framework of FlipIn by composing FlipIt games and principal-agent problems to describe the complex interactions among defenders, attackers, and insurers over IoT networks. The framework has provided a theoretical underpinning for the quantitative assessment of cyber risks, the development of cross-layer defense mechanisms, and the design of cyber insurance policies. Through the analysis of the composed games, we have investigated the Peltzman effect of IoT owners and studied the fundamental concept of insurability. We have completely characterized the optimal insurance contracts for the case with a network of distributed defenders and the case with a centralized defender over a semi-homogeneous network. It has been shown that the optimal incentive-compatible insurance contract is to cover half of the defender's losses. Observations from numerical experiments have provided design guidelines and insights for designing policies for security management. There exists a nonlinear relationship between the level of connectivity and insurability. Nodes with low insurability need to invest in local cyber defense instead of counting on cyber insurance. One of the future directions would be the investigation of the dynamic FlipIn framework with partial observations that explores the optimal contract design under the time-varying cyber risks with imperfect measurements.

Appendix
Proof of Proposition 2

From the constraint in (36), we have

$$\frac{\gamma_{a,n}c_{d,n}}{c_{a,n}} - \gamma_{d,n}w^*_{nn} + \frac{\gamma^2_{d,n}w^{*2}_{nn}c_{a,n}}{2\gamma_{a,n}c_{d,n}}(1-s_n)s_n \geq 0$$
$$\Leftrightarrow \left(s_n - \frac{1}{2}\right)^2 \leq 2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4},$$

where $\delta_n = \frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}}$ has been introduced to simplify the representations in this proof. Note that $\gamma_{a,n}c_{d,n} < \gamma_{d,n}w^*_{nn}c_{a,n}$ indicates $\delta_n < 1$ and $1-\frac{\gamma_{a,n}c_{d,n}}{\gamma_{d,n}w^*_{nn}c_{a,n}} \leq s_n \leq 1$ indicates $1-\delta_n \leq s_n \leq 1$.

There exists s_n only when $2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4} \geq 0$. As a result, s_n is not feasible if $\frac{1}{2} - \frac{\sqrt{2}}{4} < \delta_n < \frac{1}{2} + \frac{\sqrt{2}}{4}$.

We can further obtain that s_n should satisfy

$$\frac{1}{2} - \sqrt{2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4}} \leq s_n \leq \frac{1}{2} + \sqrt{2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4}}.$$

Note that s_n should also satisfy $1 - \delta_n \leq s_n \leq 1$. Thus, s_n is feasible only when

$$\frac{1}{2} - \delta_n \leq \sqrt{2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4}}.$$

If $0 < \delta_n \le \frac{1}{2} - \frac{\sqrt{2}}{4}$, we have that $\left(\frac{1}{2} - \delta_n\right)^2 \le 2\left(\frac{1}{2} - \delta_n\right)^2 - \frac{1}{4}$. Thus, δ_n should satisfy $\delta_n \ge 1$ or $\delta_n \le 0$, which contradicts to $0 < \delta_n \le \frac{1}{2} - \frac{\sqrt{2}}{4}$. As a result, s_n is not feasible if $0 < \delta_n \le \frac{1}{2} - \frac{\sqrt{2}}{4}$.

If $\frac{1}{2} + \frac{\sqrt{2}}{4} \le \delta_n < 1$, we have that $\frac{1}{2} - \delta_n < 0 \le \sqrt{2\left(\delta_n - \frac{1}{2}\right)^2 - \frac{1}{4}}$. As a result, s_n is feasible if $\frac{1}{2} + \frac{\sqrt{2}}{4} \le \delta_n < 1$.

After summarizing everything, we can obtain that s_n is not feasible if $0 < \delta_n < \frac{1}{2} + \frac{\sqrt{2}}{4}$, thus, Proposition 2 holds.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. IEEE Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 3, Mar. 2012, pp. 648–651.

[5] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2013, pp. 663–667.

[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[8] M. Antonakakis *et al.*, "Understanding the mirai botnet," in *Proc. USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[9] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[10] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Netw. Secur.*, vol. 2011, no. 8, pp. 16–19, 2011.

[11] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Oxford, U.K.: Newnes, 2012.

[12] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur.*, vol. 4, no. 1, pp. 65–88, 2015.

[13] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 795–800.

[14] Q. Hu, S. Lv, Z. Shi, L. Sun, and L. Xiao, "Defense against advanced persistent threats with expert system for Internet of Things," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2017, pp. 326–337.

[15] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[16] D. Kushner, "The real story of stuxnet," *IEEE Spectr.*, vol. 50, no. 3, pp. 48–53, Mar. 2013.

[17] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[18] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[19] R. P. Majuca, W. Yurcik, and J. P. Kesan, "The evolution of cyberinsurance," 2006, *arXiv:cs/0601020*. [Online]. Available: https://arxiv.org/abs/cs/0601020

[20] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Proc. WEIS*, 2010, pp. 1–36.

[21] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Comput. Sci. Rev.*, vol. 24, pp. 35–61, May 2017.

[22] R. A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell, "Security investment games of interdependent organizations," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 252–260.

[23] K. C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," in *Proc. Int. Conf. Game Theory Netw. (GameNets)*, May 2009, pp. 697–703.

[24] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[25] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FLIPIT: The game of 'stealthy takeover,'" *J. Cryptol.*, vol. 26, no. 4, pp. 655–713, 2013.

[26] K. D. Bowers *et al.*, "Defending against the unknown enemy: Applying FLIPIT to system security," in *Proc. Int. Conf. Decis. Game Theory Secur.* Berlin, Germany: Springer, 2012, pp. 248–263.

[27] J. Pawlick, S. Farhang, and Q. Zhu, "Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2015, pp. 289–308.

[28] J. Chen and Q. Zhu, "Security as a service for cloud-enabled Internet of controlled things under advanced persistent threats: A contract design approach," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2736–2750, Nov. 2017.

[29] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in *Proc. IEEE INFOCOM*, Apr./May 2014, pp. 235–243.

[30] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security pre-screening," in *Proc. Int. Conf. Game Theory Netw.* Cham, Switzerland: Springer, 2017, pp. 63–73.

[31] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies in the presence of security interdependence," in *Proc. 12th Workshop Econ. Netw., Syst. Comput.*, 2017, Art. no. 7.

[32] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: The role of pre-screening and security interdependence," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2226–2239, Sep. 2018.

[33] I. Vakilinia and S. Sengupta, "A coalitional cyber-insurance framework for a common platform," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1526–1538, Jun. 2019.

[34] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2010, pp. 1–10.

[35] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A colonel blotto game for interdependence-aware cyber-physical systems security in smart cities," in *Proc. 2nd Int. Workshop Sci. Smart City Oper. Platforms Eng.*, 2017, pp. 7–12.

[36] Z. Han, D. Niyato, W. Saad, and T. Başar, *Game Theory for Next Generation Wireless and Communication Networks: Modeling, Analysis, and Design*. Cambridge, U.K.: Cambridge Univ. Press, 2019.

[37] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[38] T. Spyridopoulos, G. Oikonomou, T. Tryfonas, and M. Ge, "Game theoretic approach for cost-benefit analysis of malware proliferation prevention," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2013, pp. 28–41.

[39] S. G. Vadlamudi *et al.*, "Moving target defense for Web applications using Bayesian Stackelberg games," in *Proc. Int. Conf. Auton. Agents Multiagent Syst.*, 2016, pp. 1377–1378.

[40] C. Kiekintveld, V. Lisý, and R. Píbil, "Game-theoretic foundations for the strategic use of honeypots in network security," in *Cyber Warfare*. Cham, Switzerland: Springer, 2015, pp. 81–101.

[41] M. Zhu and S. Martínez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *Proc. Amer. Control Conf. (ACC)*, Jun./Jul. 2011, pp. 4063–4068.

[42] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Secur. Commun. Netw.*, vol. 4, no. 10, pp. 1162–1172, 2011.

[43] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2014, pp. 4372–4378.

[44] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, Mar. 2014.

[45] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 46–65, Feb. 2015.

[46] L. Huang and Q. Zhu, "Analysis and computation of adaptive defense strategies against advanced persistent threats for cyber-physical systems," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2018, pp. 205–226.

[47] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 747–755.

[48] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud storage defense against advanced persistent threats: A prospect theoretic study," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 534–544, Mar. 2017.

[49] M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, and N. B. Mandayam, "Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4250–4261, Dec. 2018.

[50] S. Rass and Q. Zhu, "GADAPT: A sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2016, pp. 314–326.

[51] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, 2013.

[52] N. Abuzainab and W. Saad, "Dynamic connectivity game for adversarial Internet of battlefield things systems," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 378–390, Feb. 2018.

[53] Y. Hu, A. Sanjab, and W. Saad, "Dynamic psychological game theory for secure Internet of battlefield things (IoBT) systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3712–3726, Apr. 2019.

[54] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for ehealth," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 920–925.

[55] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, and P. Bouvry, "Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric Internet-of-Things (IoT) applications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM) Workshops, 5th Int. Workshop Cloud Comput. Syst., Netw., Appl. (CCSNA)*, Dec. 2016, pp. 1–6.

[56] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the Internet of Things: A game-theoretic perspective," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[57] S. Lee, S. Kim, K. Choi, and T. Shon, "Game theory-based security vulnerability quantification for social Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 752–760, May 2018.

[58] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, "A game theoretic defence framework against DoS/DDoS cyber attacks," *Comput. Secur.*, vol. 38, pp. 39–50, Oct. 2013.

[59] A. Laszka, G. Horvath, M. Felegyhazi, and L. Buttyán, "FlipThem: Modeling targeted attacks with FLIPIT for multiple resources," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2014, pp. 175–194.

[60] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2015, pp. 93–112.

[61] D. Leslie, C. Sherfield, and N. P. Smart, "Threshold FlipThem: When the winner does not need to take all," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2015, pp. 74–92.

[62] D. Leslie, C. Sherfield, and N. P. Smart, "Multi-rate threshold FlipThem," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2017, pp. 174–190.

[63] M. V. Pauly, "The economics of moral hazard: Comment," *Amer. Econ. Rev.*, vol. 58, no. 3, pp. 531–537, 1968.

[64] S. Shavell, "On moral hazard and insurance," in *Foundations of Insurance Economics*. Dordrecht, The Netherlands: Springer, 1979, pp. 280–301.

[65] L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Commun. ACM*, vol. 46, no. 3, pp. 81–85, 2003.

[66] L. M. D. Bailey, "Mitigating moral hazard in cyber-risk insurance," *JL Cyber Warfare*, vol. 3, p. 1, 2014.

[67] R. Pal, *Improving Network Security Through Cyber-Insurance*. Princeton, NJ, USA: Citeseer, 2014.

[68] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 2, pp. 358–372, Mar./Apr. 2019.

[69] E. Ghotbi and A. K. Dhingra, "A bilevel game theoretic approach to optimum design of flywheels," *Eng. Optim.*, vol. 44, no. 11, pp. 1337–1350, 2012.

[70] M. Jenabi, S. M. T. F. Ghomi, and Y. Smeers, "Bi-level game approaches for coordination of generation and transmission expansion planning within a market environment," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2639–2650, Aug. 2013.

[71] R. Zhang and Q. Zhu, "A game-theoretic approach to design secure and resilient distributed support vector machines," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 11, pp. 5512–5527, Nov. 2018.

[72] R. Zhang, Q. Zhu, and Y. Hayel, "A bi-level game approach to attack-aware cyber insurance of computer networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 779–794, Mar. 2017.

[73] A. Dassios and P. Embrechts, "Martingales and insurance risk," *Commun. Statist. Stochastic Models*, vol. 5, no. 2, pp. 181–217, 1989.

[74] P. Čížek, W. K. Härdle, and R. Weron, *Statistical Tools for Finance and Insurance*. Springer, 2005.

[75] K. Balakrishnan, *Exponential Distribution: Theory, Methods and Applications*. Evanston, IL, USA: Routledge, 2018.

[76] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[77] D. Gantsou, "On the use of security analytics for attack detection in vehicular ad hoc networks," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–6.

[78] T. Zhang and Q. Zhu, "Strategic defense against deceptive civilian GPS spoofing of unmanned aerial vehicles," in *Proc. Int. Conf. Decis. Game Theory Secur.* Cham, Switzerland: Springer, 2017, pp. 213–233.

[79] F. Ewold, "Insurance and risk," in *The Foucault Effect: Studies in Governmentality*. 1991, pp. 197–210.

[80] S. Peltzman, "The effects of automobile safety regulation," *J. Political Economy*, vol. 83, no. 4, pp. 677–725, 1975.

Rui Zhang received the B.S. degree in optical information science and technology from Wuhan University, China, in 2014, and the M.S. degree in electrical engineering from New York University, USA, in 2016, where he is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. His research interests include cybersecurity, adversarial machine learning, cyber insurance, and optimal transport. He was a recipient of the Runner Up Best Student Award at the International Conference on Information Fusion 2015.

Quanyan Zhu received the B.Eng. degree (Hons.) in electrical engineering from McGill University in 2006, the M.A.Sc. degree from the University of Toronto in 2008, and the Ph.D. degree from the University of Illinois at Urbana–Champaign (UIUC) in 2013. After stints at Princeton University, he is currently an Assistant Professor with the Department of Electrical and Computer Engineering, New York University. His current research interests include resilient and secure interdependent critical infrastructures, the Internet of Things, cyber-physical systems, game theory, machine learning, network optimization, and control. He was a recipient of many awards, including the NSF CAREER Award, the NYU Goddard Junior Faculty Fellowship, the NSERC Postdoctoral Fellowship (PDF), the NSERC Canada Graduate Scholarship (CGS), and the Mavis Future Faculty Fellowships. He spearheaded and chaired the INFOCOM Workshop on Communications and Control on Smart Energy Systems (CCSES) and the Midwest Workshop on Control and Game Theory (WCGT). He has served as the General Chair for the 7th Conference on Decision and Game Theory for Security (GameSec) in 2016, the 9th International Conference on NETwork Games, COntrol and OPtimisation (NETGCOOP) in 2018, and the 5th International Conference on Artificial Intelligence and Security (ICAIS 2019) in 2019.