A Game-Theoretic Approach for Minimizing Security Risks in the Internet-of-Things

George Rontidis*, Emmanouil Panaousis†, Aron Laszka‡, Tasos Dagiuklas*,
Pasquale Malacaria§, and Tansu Alpcan¶
* Hellenic Open University, Greece
† University of Brighton, UK
‡ Institute for Software Integrated Systems, Vanderbilt University, Nashville, USA
§ Queen Mary University of London, UK
¶ The University of Melbourne, Australia

***Abstract*—In the Internet-of-Things (IoT), users might share part of their data with different IoT *prosumers*, which offer applications or services. Within this open environment, the existence of an adversary introduces *security risks*. These can be related, for instance, to the theft of user data, and they vary depending on the security controls that each IoT prosumer has put in place. To minimize such risks, users might seek an "optimal" set of prosumers. However, assuming the adversary has the same information as the users about the existing security measures, he can then devise which prosumers will be preferable (e.g., with the highest security levels) and attack them more intensively. This paper proposes a decision-support approach that minimizes security risks in the above scenario. We propose a non-cooperative, two-player game entitled *Prosumers Selection Game* (PSG). The Nash Equilibria of PSG determine subsets of prosumers that optimize users' payoffs. We refer to any game solution as the *Nash Prosumers Selection* (NPS), which is a vector of probabilities over subsets of prosumers. We show that when using NPS, a user faces the least expected damages. Additionally, we show that according to NPS every prosumer, even the least secure one, is selected with some non-zero probability. We have also performed simulations to compare NPS against two different heuristic selection algorithms. The former is proven to be approximately 38% more effective in terms of security-risk mitigation.**

I. Introduction

Scientific research and technological achievements of the last few decades within the field of mobile and wireless communications have paved the way for a vast deployment of the Internet-of-Things (IoT). In addition to the advent of IoT, the growing use of smartphones enables the user to experience unprecedented services. For instance, having the vision of an IoT world, Apple developed iBeacon [1], a technology standard which permits mobile applications to receive beacon signals from the physical world and react accordingly. Beacons in the real world can be used in several applications enhancing user experience by providing futuristic services [2], [3].

However, this growth in terms of applications and services comes with the need users to share part of their data with different IoT prosumers [4]. A prosumer participates in IoT service development stages and therefore it offers services and applications. Although users benefit from IoT prosumers, *security* is a very important consideration in these "open" environments. Therefore, the set of prosumers that a user selects to share his/her data with determines the level of security risk that the user faces. For example an attacker can use the vulnerability CVE-2012-1823 to launch the `linux.darlloz` attack [5] that infects devices to mine crypto currency. The same attack vector can also redirect the user's browser to whatever the attacker desires or to make the user's device part of a botnet. According to Symantec [5], 38% on infections of this attack type are IoT devices, especially *routers*. To understand the scale of vulnerable IoT devices, the Tripwire Survey [6] reports that 80% of Amazon's top-25 best-selling SOHO wireless router models have security vulnerabilities.

A. Motivation

The motivation of our work lies within the field of decision-making for minimizing security risks. Suppose a user is within an IoT network infrastructure and requests different applications and services, which are likely to be offered by different prosumers. Following the architecture proposed in [7], an IoT Gateway updates the list of services that it manages on behalf of prosumers residing in the network, thus making these services consumable by both local (i.e., residing in the network) and remote (e.g., via Internet) users. The same gateway is aware of the security controls that each prosumer has put in place. This information can be used to elicit the *security levels* of all prosumers, and provide them to the user prior to his/her decision about sharing data with a set of prosumers. The security level [8] determines the *strength* (i.e., "inverse vulnerability") of a prosumer against different attacks. An application that supports this elicitation is the *Trust Feedback Toolkit* (TFT) [9] proposed in the *Usable Trust in the Internet of Things* (uTRUSTit) project [10], [11].

Apart from the user, any adversary can also be aware of the different prosumers' security controls akin to levels because he can appear as a normal user who requests such information from the IoT Gateway. This is a crucial assumption because the attacker can guess the set of prosumers that the user might choose; therefore, he has "good chances" of comprising user data successfully. More specifically, the attacker might assume that the users will take *a common-sense approach* choosing the prosumers with the highest security levels. However, in this paper, we prove that a game-theoretic approach outperforms the common-sense approach. Note that we have assumed that the adversary attacks only one prosumer in order (i) to minimize the likelihood of being detected, and (ii) to utilize his/her time in the most efficient way by focusing on one goal.

B. Environment

We investigate the case of an IoT infrastructure which hosts a set of prosumers as $\mathcal{P} := \{1, 2, \ldots, n\}$. Any user can share private data with any of these prosumers, including combinations of them, in return for some services. We suppose that an attacker lies within this IoT area aiming at stealing user data (e.g., credit card details) by compromising a prosumer that the user might select. To achieve this, the attacker must bypass the security measures that the targeted prosumer has implemented.

We model the *security level* of a prosumer i by a uniform random variable $S_i \in [0, 1)$, whose distribution is known to both the user and adversary by, for instance, using a mobile application as in [9]. Hence, we can state that $1 - S_i$ corresponds to the *vulnerability level* of prosumer i. We have assumed that $S_i \neq 1$, in any case, due to *zero-day vulnerabilities*. We also assume that the value of user data equals V. Note that our analysis does not change if we assume that V is the expectation of the User data value when this is a random variable.

To motivate the reader, we can think of a scenario where a shopping centre (playing the role of the user) seeks to recommend a set of IoT prosumers that can be used by the local shops to allow NFC payments for their clients/customers. To do that, the user performs an a priori analysis of the security of each of the available NFC payment systems and sets their security levels.

C. Contributions

The main contribution of this paper is a decision-support system for users to select a set of prosumers that minimizes security risks in presence of an adversary who threatens their "assets" (e.g., private data). We have formulated a complete information game, entitled Prosumers Selection Game (PSG) between two players: the *User* who chooses a set of prosumers and an *Attacker* who is attempting to penetrate a prosumer's system. We have investigated the IoT prosumer selection problem mathematically and we have provided constraints on the User's strategy at the equilibrium of PSG. We have devised optimal User strategies in *worst-case scenarios* where Attacker imposes the highest possible security risks, and we have proven that the game-theoretic solution, called Nash Prosumers Selection (NPS), performs in the best possible way. We have also undertaken simulations that demonstrate the efficiency of NPS as opposed to two other heuristic selection algorithms.

D. Outline

The remainder of this paper is organized as follows. Section II discusses related work, while in Section III we formulate the *Prosumers Selection Game* (PSG) by introducing the two players, their strategy sets, and the corresponding payoffs for both pure and mixed strategies. Section IV presents some theoretical results for the saddle points (i.e., equilibria) of PSG, while simulation results for different selection algorithms are presented in Section V. Finally, Section VI concludes this paper by summarizing its main contributions, limitations and providing our plans for future work.

II. Related Work

Security, privacy, and trust are ranked among the top research challenges for the IoT. Recent work has been undertaken by the *Usable Trust in the Internet of Things* (uTRUSTit) project [10]. An outcome of uTRUSTit is the development of the Trust Feedback Toolkit (TFT) [9], which informs users about the security of an IoT network. As a result, this feedback is available to literally every user, either benevolent or malicious.

Fritsch et al. [12] discuss trust issues related to different IoT devices and services, given that for every transaction committed, personal data are disclosed. According to the authors, whether a user should trust (and therefore share his/her data) or not a specific IoT infrastructure, greatly depends on the type of transaction. In their work, they present different trust strategies, varying from simple "always" or "never" trust to more complicated schemes involving central agents or analyzing mechanisms to evaluate trust. They conclude that there is not a single strategy in trusting IoT applications and they underline the significance of developing flexible trust management mechanisms.

Due to the pioneering nature of the IoT field, the number of game-theoretic approaches that are concerned with security and trust is very limited. In [13] Duan et al. study the problem of creating an effective algorithm in terms of energy consumption and bandwidth usage, capable of evaluating node's trust derivation process. They use game theory to support the node decision with regard to replying a trust request with respect to the incurred energy consumption.

A game based security model for medical applications is proposed, in [14], by Hamdi et al. The authors propose a decision support mechanism that assesses the remaining battery life, the channel bandwidth, the memory capacity, and the nearby compromised nodes, to determine whether or not the sender of a message should be authenticated.

Chen et al. propose a fusion-based defensive model to address intentional attacks in the IoT [8]. In their model the attacker is fully informed about network topology and capable of sabotaging all nodes simultaneously. In their zero-sum game between the adversary and defender, they introduce a nodal decision mechanism with minimum overhead, which is capable of guaranteeing robustness in large-scale IoT networks.

All the aforementioned papers use game theory to provide network nodes (i.e., things) with appropriate tools to mitigate certain attacks. In contrast, our work focuses on providing users with the suitable decision support mechanism, in order to assure at least a threshold above which the attacker cannot cause higher damage. To the best of our knowledge this is the first work done within the realm of IoT prosumers selection that aims at minimizing security risks. The foundation of our work is based on the game-theoretic model published by Fielder et al. in [15]. We see the cybersecurity targets and schedules considered in [15] as all available prosumers and the possible different subsets of them, correspondingly.

III. Game-Theoretic Formulation

In this section we formulate a two-player, deterministic, complete-information game, entitled Prosumers Selection Game (PSG), between the *User* and *Attacker*. In this game, players choose their strategies simultaneously. Thus the Attacker does not know which prosumers have been selected by the User, and the User is not aware of which prosumer is under attack. The User requires to communicate with k prosumers during a time period that defines a one-shot game. On the other hand, the Attacker wishes to successfully compromise a prosumer in order to reveal users' private data.

Fig. 1 is an abstract illustration of our model environment. This game model facilitates decisions related to which prosumers the User must trust (i.e., in this sense, trust and security are seen in a similar fashion) more when sharing his/her data or using their services. We assume that the Attacker attacks *only one prosumer* at a time, and that *he can attack any of them*. We consider the *worst-case scenario* for the User, where the Attacker knows all the available prosumers and their corresponding security levels modeling a *complete-information game*.

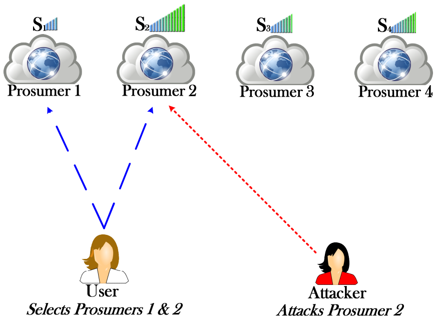

Fig. 1. Illustration of our model. The User chooses to communicate with 2 out of 4 prosumers, and the Attacker is attacking one of them.

A. Strategy Sets

The normal form of this game is described as follows. A pure strategy of the User is to choose k out of n prosumers to use some of their applications or services. Formally, the User chooses a size-k subset $\mathcal{P}' \subseteq \mathcal{P}$. A *pure strategy*, related to the selection of $\mathcal{P}'$, is represented by a tuple $\mathbf{s} = \langle s_i \rangle \in \{0,1\}^n$, where s_i equals 1 when prosumer i is chosen by the User (i.e., $i \in \mathcal{P}'$); or 0 otherwise. A *mixed strategy* $\mathbf{U} = \langle u_\mathbf{s} \rangle$ *of the User* is a probability distribution over the different tuples, where $u_\mathbf{s}$ is the probability of choosing subset $\mathbf{s}$. On the other hand, the Attacker's *pure strategy* space is the set of prosumers, seen as targets, while a *mixed strategy* is denoted by $\mathbf{A} = \langle a_i \rangle$, where a_i represents the probability of attacking prosumer i.

B. Payoffs

In this paper we formulate a zero-sum game according to which the loss of User equals the Attacker's benefit. Rationale of this choice is that a zero-sum game in the security risk management domain represents scenarios where the Attacker aims at causing the *maximum possible loss* to the User. Therefore, we aim at supporting the User's decision in worst-case scenarios. However, we provide game solutions beyond the zero-sum game by looking at cases where the Attacker's payoff is a negative affine transformation of the User's payoff.

Suppose the User chooses a subset $\mathcal{P}'$ of prosumers and prosumer i is attacked. Formally, if $i \in \mathcal{P}'$, the User loses V with probability $(1 - S_i)$ (i.e., we assume that a more secure prosumer is more difficult to be compromised, therefore yields V with lower probability), and the Attacker gains V with the same probability. Consequently, for any prosumer $i \notin \mathcal{P}'$, the User has *no security loss* and the Attacker has *no benefit*.

We define the *security risk* R_i of the user when sharing data with prosumer i, as the product of data value V and the probability $(1 - S_i)$ of the prosumer being compromised and therefore the User data being stolen. Formally, $R_i := (1 - S_i)\,V$. The expected payoff of the User, when the Attacker plays according to a mixed strategy $\mathbf{A}$ and the User selects $\mathbf{s}$, is given by

$$J_U(\mathbf{s}, \mathbf{A}) := -\sum_i s_i\, a_i\, R_i. \tag{1}$$

On the other hand, the expected payoff of the Attacker when attacking i and the User plays $\mathbf{U}$ is given by

$$J_A(\mathbf{U}, i) := \sum_\mathbf{s} s_i u_\mathbf{s}\, R_i. \tag{2}$$

From Eq. (1), we see that the User's strategic choice influences the payoffs only through the probability of selecting each prosumer. Since every prosumer may be present in more than one selected subsets, we must compute the probability of each individual prosumer to be selected. Hence the expected payoff of the User can be determined by the representation of User's mixed-strategy action spaces that are simpler than the canonical ones, defined as follows.

Definition 1: When the User requires to share data with k prosumers, we define the vector of prosumers induced by the strategy $\mathbf{U}$ as the marginal probabilities vector $\mathbf{p} = \langle p_i \rangle$, where the probability p_i of choosing prosumer i is given by $p_i := \sum_\mathbf{s} s_i u_\mathbf{s}$, where $0 \leq p_i \leq 1$, and $\sum_{i=1}^n p_i = k$.

It is easy to see that there is a mapping between $\mathbf{U}$ and $\mathbf{p}$, hence we refer to either of those as the mixed strategy of the User from now on.

IV. Theoretical Results

For a given mixed strategy $\mathbf{A}$ of the Attacker, User seeks to minimize the probability of his/her own data to be stolen by choosing the mixed strategy $\mathbf{U}$. Given the pair $\langle \mathbf{U}, \mathbf{A} \rangle$ of mixed strategies, the User's expected payoff is given by

$$\mathcal{J}_U(\mathbf{U}, \mathbf{A}) = -\sum_\mathbf{s} \sum_i u_\mathbf{s}\, a_i\, s_i\, R_i. \tag{3}$$

If we express the User's strategy by $\mathbf{p}$, then for the pair $\langle \mathbf{p}, \mathbf{A} \rangle$ of mixed strategies the User's payoff is given by

$$\mathcal{J}_U(\mathbf{p}, \mathbf{A}) = -\sum_i p_i \, a_i \, R_i. \tag{4}$$

Since we are investigating a two-person zero-sum game with finite number of actions for both players, according to Nash [16] it admits at least one mixed-strategy Nash Equilibrium (NE). Saddle-points correspond to Nash equilibria as discussed in [17].

From [18], we know that PSG admits a saddle point in mixed strategies, $(\mathbf{U}^*, \mathbf{A}^*)$, with the property $\mathbf{U}^* = \operatorname{argmax}_{\mathbf{U}} \min_{\mathbf{A}} \mathcal{J}_U(\mathbf{U}, \mathbf{A})$ and $\mathbf{A}^* = \operatorname{argmax}_{\mathbf{A}} \min_{\mathbf{U}} \mathcal{J}_A(\mathbf{U}, \mathbf{A})$. The pair of saddle point strategies $(\mathbf{U}^*, \mathbf{A}^*)$ are, at the same time, security strategies for the players, i.e., they ensure a minimum performance regardless of the opponent's actions. Furthermore, if the game admits multiple saddle points (and strategies), they have the ordered interchangeability property, i.e., the player achieves same performance level independent from the other player's choice of saddle-point strategy.

We refer to the strategy of User at the equilibrium as *Nash Prosumers Selection* (NPS). Our results can be extended to non-zero sum, bi-matrix games. In this case, the existence of a NE is also guaranteed, but the additional properties hold only in the case where Attacker's utility is a *negative affine transformation* of the defender's utility.

The minimax theorem [19] states that, for zero sum games NE, maxmin, and minimax solutions coincide. Therefore

$$\mathbf{U}^* = \operatorname*{argmin}_{\mathbf{U}} \max_{\mathbf{A}} \mathcal{J}_A(\mathbf{U}, \mathbf{A}). \tag{5}$$

This means that *regardless of the Attacker's strategy*, NPS guarantees a minimum performance, which is an upper limit of expected damage for the User.

On the other hand, the Attacker seeks his/her best response by attacking prosumers that maximize his/her payoff $J_A(\mathbf{p}, i) = J_A(p_i, i) := p_i \, R_i$ when the User plays $\mathbf{p}$. Therefore, the support of the Attacker's strategy has to be a subset of

$$\operatorname*{argmax}_i \big(p_i \, R_i\big). \tag{6}$$

We begin our analysis by providing a necessary condition on the NPS strategies.

Lemma 1: In PSG, for every prosumer i, $p_i = 1$ or $p_i \, R_i = \max_j p_j \, R_j$ must hold when the User plays the NPS strategy.

Proof: For the sake of contradiction, suppose that the claim of the lemma does not hold, that is, suppose that there exist a Nash equilibrium $(\mathbf{p}, \mathbf{A})$ and a prosumer i such that $p_i < 1$ and $p_i \, R_i < \max_j p_j \, R_j$. Given Eq. (6) and our assumption that $p_i \, R_i < \max_j p_j \, R_j$, we have that $a_i = 0$. Then, let k be an arbitrary prosumer such that $a_k > 0$. Since $\mathbf{A}$ is a best-response strategy, $p_k > 0$ must hold obviously. Now, consider the strategy $\mathbf{p}^*$ which is defined as follows:

$$\forall j \neq i, k \text{ let } p^*_j = p_j; \quad p^*_i = p_i + \Delta; p^*_k = p_k - \Delta, \tag{7}$$

where $\Delta = \min\{1 - p_i, p_k\}$. We can see that, from Eqs. (4) and (7), we have that

$$\begin{aligned}\mathcal{J}_U(\mathbf{p}^*, \mathbf{A}) - \mathcal{J}_U(\mathbf{p}, \mathbf{A}) &= -\sum_{j \neq i,k} p_j \, a_j \, R_j - (p_i + \Delta) \, a_i \, R_i \\ &- (p_k - \Delta) \, a_k \, R_k + \sum_{j \neq i,k} p_j \, a_j \, R_j + p_i \, a_i \, R_i + p_k \, a_k \, R_k \\ &\overset{a_i=0}{=} \Delta \, a_k \, R_k > 0, \text{ because } \Delta, a_k, R_k > 0. \end{aligned} \tag{8}$$

Therefore, we have that against $\mathbf{A}$, the strategy $\mathbf{p}^*$ achieves a higher payoff for the defender than strategy $\mathbf{p}$. However, this contradicts our initial assumption that $\mathbf{p}$ is a best response; consequently, the claim of lemma must hold. ■

Intuitively, the above lemma states that, in an equilibrium, the prosumers can be divided into two groups. Prosumers in the first group are always selected by the User; however, the Attacker's payoff for attacking these prosumers is less than or equal to the payoff for attacking prosumers in the second group. On the other hand, prosumers in the second group are selected by the User only with less-than-one probability.

The following corollary confirms the intuition that more secure prosumers should be selected with higher probability.

Corollary 1: For any NPS strategy and prosumers i, j, we have that $R_i \leq R_j$ implies $p_i \geq p_j$.

Proof: For the sake of contradiction, suppose there exist an NPS strategy $\mathbf{p}$ and prosumers i, j such that $R_i \leq R_j$ and $p_i < p_j$. Since $p_i < p_j \leq 1$, we have from Lemma 1 that $p_i \, R_i = \max_k p_k \, R_k$. However, this contradicts $p_i \, R_i \leq p_i \, R_j < p_j \, R_j$; hence, the corollary must hold. ■

The following theorem establishes the surprising result that, in an NPS strategy, every prosumer – even the least secure one – is selected with some non-zero probability.

Theorem 1: In PSG, if $k > 0$, the User selects every prosumer with some non-zero probability according to NPS.

Proof: Since $k > 0$, there exists at least one prosumer j such that $p_j > 0$; hence, $\max_j p_j \, R_j > 0$. From Lemma 1, we have that $p_i = 1$ or $p_i \, R_i = \max_j p_j \, R_j$ must hold for every prosumer i. Consequently, for every prosumer i, the probability p_i is equal either to $1 > 0$ or to $\frac{\max_j p_j \, R_j}{R_i} > 0$. ■

Finally, we show how to compute an NPS strategy efficiently, in $O(n^2)$ time.

Theorem 2: Without loss of generality, assume that $R_1 \leq R_2 \leq \ldots \leq R_n$ and $k < n$. Then, the following algorithm outputs an NPS strategy in $O(n^2)$ steps:

```
1) Let $S := k$.
2) Construct $\mathbf{p}(S) = \langle p_1(S), \ldots, p_n(S) \rangle$ such that:
    a) For every $i \leq S$, let $p_i(S) := 1$.
    b) For every $i > S$, let $p_i(S) := (k - S) \frac{\frac{1}{R_i}}{\sum_{j=S+1}^{n} \frac{1}{R_j}}$.
3) If $S = 0$ or $R_S \leq p_{S+1}(S) \, R_{S+1}$, then output $\mathbf{p}(S)$.
4) Otherwise, let $S := S - 1$ and continue from Step 2.
```

Proof: First, suppose that we are given a fixed S, and the User's strategic choice is restricted to strategies $\mathbf{p}$ where the number of prosumers i with $p_i = 1$ is S (i.e., the User selects exactly S prosumers with certainty, and $n - S$ prosumers with less-than-one probability). Then, from Corollary 1 and the assumption that prosumers are ordered by their R_i values, we readily have that $p_i = 1$ has to hold for every $i \leq S$ if $\mathbf{p}$ is an NPS strategy.

Next, it easy to see that $p_i = (k - S)\frac{\frac{1}{R_i}}{\sum_{j=S+1}^{n} \frac{1}{R_j}}$ must hold for every $i > S$ if $\mathbf{p}$ is an NPS strategy. Otherwise, either $\sum_i p_i = 1$ or the uniformity of $p_i\, R_i$ over $i > S$ (see Lemma 1) would be violated.

Consequently, if there exists an NPS strategy $\mathbf{p}$ for a given S, then it has to be the strategy $\mathbf{p}(S)$ defined in Steps 2.a and 2.b of the above algorithm. Hence, it remains to show that the algorithm outputs the strategy $\mathbf{p}(S)$ for a correct value of S. Firstly, if the condition $R_S \leq p_{S+1}(S)\, R_{S+1}$ is not satisfied for a strategy, then that strategy cannot be an NPS. To see this, consider the inequality $p_S(S)\, R_S = R_S > p_{S+1}(S)\, R_{S+1} \leq \max_k p_k(S)\, R_k$, which obviously contradicts Lemma 1.

Finally, we show that, of all the S values satisfying the condition $R_S \leq p_{S+1}(S)\, R_{S+1}$, the highest one is the optimal. Let $S_1 < S_2$ be two values satisfying the condition. From Lemma 1 and the definition of the attacker's payoff, it follows that attacking prosumer n is a best response for the attacker against $\mathbf{p}(S)$. Then, it is easy to see that

$$\begin{aligned} p_n(S_1) &= (k - S_1)\frac{\frac{1}{R_n}}{\sum_{j=S_1+1}^{n} \frac{1}{R_j}} \\ &> (k - S_2)\frac{\frac{1}{R_n}}{\sum_{j=S_2+1}^{n} \frac{1}{R_j}} = p_n(S_2). \end{aligned}$$

Consequently we have that the attacker's payoff and hence, the defender's loss is higher for S_1 than for S_2. Therefore, we have that the optimal value of S is the one that is used by the output of the algorithm, which concludes our proof. ■

V. Simulation Results

In this section, we present the results of numeric simulations undertaken by using a game-theoretic Python simulator enriched with the IoT security model proposed in this paper. We compare the efficiency of NPS against a Uniform and a Common Sense Strategy (CSS). According to the Uniform strategy, User selects a subset of prosumers by using a uniform probability distribution, while according to CSS, User selects the subset that includes the most secure prosumers.

We have simulated four different scenarios akin to *experiments*, where in each experiment we fix the number k of requested prosumers and vary the number n of prosumers. We have simulated an attacker who attacks prosumers in a proportional manner based on the security level of each prosumer. More specifically, the more controls a prosumer has implemented (i.e., higher security level) the more likely it is to be attacked by the adversary. This adversarial type assumes a *rational* attacker who believes that more users will select subsets that include prosumers with higher security levels. Thus, the weighted attack strategy determines that the probability of prosumer i to be attacked is given by $S_i / \sum_{i \in O} S_i$.

Each experiment consists of a number of cases. A case is determined by a pair (k, n). In each case we have simulated 500 selection decisions, representing 500 independent iterations of the PSG, in which the parameter values were varied. The latter represent 500 different users playing against the attacker. To evaluate the performance of NPS strategy as opposed to Uniform and CSS, we have aggregated the security risk inflicted by the attacker to 500 users for the 3 different strategies.

In Figs. 2-5 we present the simulation results for the aforesaid scenarios. All experiments corroborate the idea that for a given k, the security risk decreases when n grows. This was an expected outcome because when increasing the number of available prosumers the probability of a prosumer to be attacked decreases. It is also profound that when the user's choices are limited (i.e., when $k \to n$), greater security risk is anticipated. Every case studied proved that NPS always performs better than Uniform and CSS. The latter seems to perform, in overall, slightly better than Uniform, although their difference decreases as the number of requested services increases.

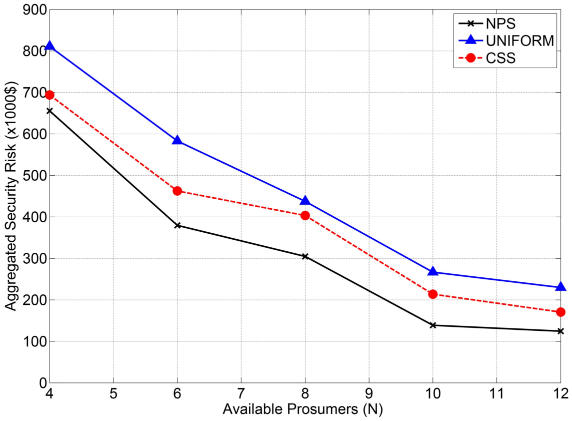

Fig. 2. Aggregated security risk when selecting 2 prosumers.

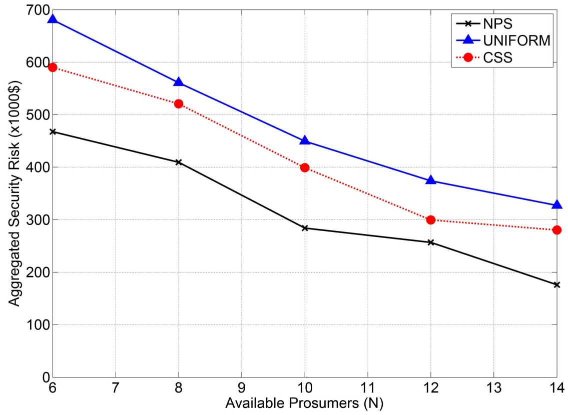

Fig. 3. Aggregated security risk when selecting 3 prosumers.

In the first experiment (Fig. 2), where the User selects 2 prosumers, NPS attributes an average of 25% lower security risk compared to Uniform and 16% to CSS. When the selected prosumers increase to 3 (Fig. 3), NPS decreases security risk by approximately 54% than Uniform and 34% than CSS. In these series of experiments, CSS was slightly better (15% - 22%) than Uniform.

The rest of experiments further show that NPS achieves on average one third lower security risk. More specifically, when the User selects 4 services (Fig. 4), NPS decreases security risk by an average of 54% and 43% as opposed to Uniform and CSS, respectively, while in the experiment with 5 services (Fig. 5), NPS achieves in average 35% less security risk than the other two strategies.

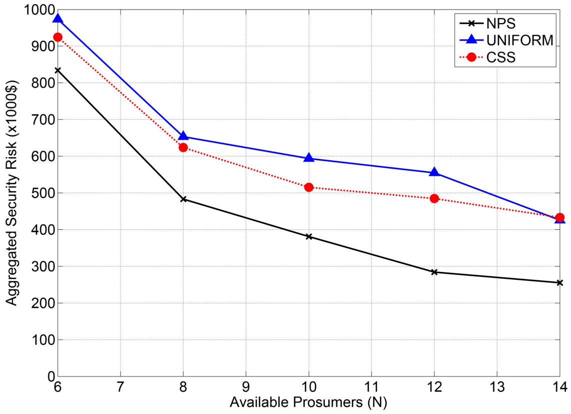

Fig. 4. Aggregated security risk when selecting 4 prosumers.

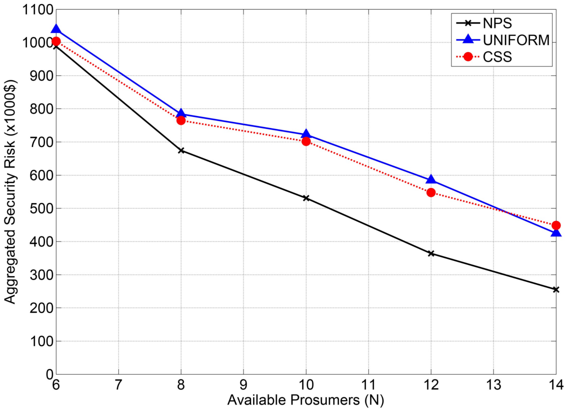

Fig. 5. Aggregated security risk when selecting 5 prosumers.

VI. Conclusion

In this paper, we provide a decision support methodology for users to select from a set of IoT prosumers in a way that minimizes their security risks. Such methodology can be implemented, for instance, by using software agents running on the users' devices. The game-theoretic solution discussed, called *Nash Prosumers Selection*, is a mixed-strategy Nash Equilibrium that can be translated to a vector of marginal probabilities over the set of IoT prosumers. By using a mixed strategy, the User, who abstracts any number of users, randomizes over the prosumer selection in an optimal manner. Such randomization aims at confusing the Attacker. It can also be interpreted as the percent of users in an IoT area who choose a particular subset of prosumers.

Future work will aim at increasing the realism of our model by modeling a Bayesian game (i.e., incomplete-information game). In this realm, the players initially have uncertainty about their opponents' preferences. For instance, the security levels of the prosumers might not be available to non-authorized users. Furthermore, we have plans to investigate a non-zero sum game by introducing some attacking cost and considering that the value of User data might be evaluated differently by the players. Another dimension of the same problem is when the Attacker is motivated by non-monetary profits, such as reputation acquired after successfully hacking a prosumer. We also plan to consider a game where the Attacker targets multiple prosumers, and the User takes into account network characteristics when deciding upon selection of a particular subset of prosumers. More importantly, we plan to consider different benefits, measured in terms of services provision, when the User chooses different prosumers.

Acknowledgments This work was supported in part by the National Science Foundation under Award CNS-1238959.

References

[1] iBeacon Website (accessed Jan. 2014) http://www.ibeacon.com

[2] Tulpen Park Website (accessed Jan. 2014) http://www.fluwelstulpenland.com

[3] San Francisco International Airport Application, (accessed Jan. 2014) http://indoo.rs/indoo-rs-and-san-francisco-international-airport-unveil-app-for-visually-impaired-passengers

[4] Martin, D., Alcarria, R., Robles, T., Morales, A.: A Systematic Approach for Service Prosumerization in IoT Scenarios. In Proc. of the 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp.494,499, 3-5 (July 2013)

[5] Symantec: "IoT Worm Used to Mine Cryptocurrency" http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency (accessed March 2014)

[6] Tripwire: 2014 Retail Security Survey Report (Feb 2014)

[7] Cirani S., Davoli L., Ferrari G., Léone R., Medagliani P., Picone M., Veltri L.: A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things. IEEE IoT Journal, 1(5) (2014)

[8] Chen P., Cheng S., Chen K.: Information Fusion to Defend Intentional Attack in Internet of Things. IEEE IoT Journal, Vol. 1, No.4 (Aug. 2014)

[9] Hochleitner C., Graf C., Unger D., Tscheligi M.: Making Devices Trustworthy: Security and Trust Feedback in the IoT. In Proc. of the 4th International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (June 2012)

[10] The uTRUSTit Project's Website: http://www.utrustit.eu (accessed Jan. 2014)

[11] Petro D., Vesztergombi G., Fritsch L.: uTRUSTit: D.3.2 Threat Analysis Search Lab (Apr. 2011)

[12] Fritsch L., Groven A.-K., Schulz T.: On the Internet of Things, Trust is Relative Constructing Ambient Intelligence, Ambient Intelligence (AmI) 2011 Workshops

[13] Duan J., Gao D., Yang D., Foh C., Chen H.: An Energy-Aware Trust Derivation Scheme With game-theoretic Approach in Wireless Sensor Networks for IoT Applications. IEEE IoT Journal, Vol. 1, No. 1, Feb. 2014

[14] Hamdi, M., Abie, H.: Game-Based Adaptive Security in the Internet of Things for eHealth. In Proc. of the IEEE International Conference on Communications (ICC) 2014

[15] Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F.: Game Theory Meets Information Security Management. In Proc. of the 29th IFIP International Information Security and Privacy Conference (2014)

[16] Nash, J.F.: Equilibrium points in n-person games. In Proc. of the National Academy of Sciences 36(1), pp. 48–49 (1950)

[17] Alpcan, T., Basar, T.: Network Security: A Decision and Game-Theoretic Approach. Cambridge University Press (2010)

[18] Basar, T., Olsder, G. J.: Dynamic noncooperative game theory. London Academic press, 2nd Edition (1995)

[19] Von Neumann, J., Morgenstern O.: Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition). Princeton university press (2007)