Attack Strategies Among Prosumers in Smart Grids: A Game Theoretic Analysis

Leonardo Badia, *Senior Member, IEEE,* Mattia Borgo, Bruno Principe, Lorenzo Spina, Laura Crosara, *Graduate Student Member, IEEE,* and Elvina Gindullina

***Abstract*—Smart grids provide energy distribution with empowered capabilities thanks to the technological resources of information systems. However, this also poses security threats related to cyberattacks that are difficult to characterize. In this paper, we present a game theoretic model of the interplay between 2 prosumers of a smart grid, interacting as attacker and defender in a strategic setup, and one consumer which is assumed to be passive. We analyze this problem by framing it as a static game of complete information and providing theoretical and numerical discussions of the Nash equilibrium solutions. Finally, we obtain results that can serve as guidelines to characterize the performance of smart grid systems and handle their reliability.**

***Index Terms*—Energy management; Game theory; Smart grids; Power system security; Cyberattacks.**

I. Introduction

Smart grids enable two-way communication and data exchange between power generators, consumers, and grid operators to enhance the efficiency, reliability, and sustainability of electricity generation, distribution, and consumption [1], [2]. They are a special kind of networks, where nodes are the consumers, all of which require energy and are supported by advanced communication and control systems, but some of them, called *prosumers*, are also able to generate energy, e.g., through solar cells or other forms of energy harvesting, in addition to utilize it [3], [4]. Some SG implementations, such as community smart microgrids, foresee the option for peer-to-peer energy exchange that can happen on multiple timescales, even real-time. This is crucial to balance energy fluctuations when the production is based on harvesting from the environment, e.g., from solar or wind sources, which can vary rapidly [5], [6], and is one of the key scenarios envisioned by next generation communication networks [7], [8].

Manuscript received 7 June 2024; revised 13 August 2024; accepted 16 September 2024. Date of publication xxx XXXXX xxxx; date of current version xxx XXXXX xxxx. Paper 2024-PSEC-0743.R1, presented at the 2023 IEEE icSmartGrid Conference, Paris, France, June 3–4 [1], and approved for publication in the IEEE Transactions on Industry Applications by XXXXX XXXXX XXXXXX [DOI: XXXXXXXXXXXXX]. This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE0000001 - program "RESTART"). *(Corresponding author: Leonardo Badia)*

L. Badia, M. Borgo, B. Principe, L. Spina, and L. Crosara are with the Dept. of Information Engineering, University of Padova, Italy.
Email: leonardo.badia@unipd.it, {mattia.borgo, bruno.principe, lorenzo.spina, laura.crosara.1}@studenti.unipd.it .

E. Gindullina is with the R&I Dept. of Hewlett Packard Enterprise Italia.
Email: elvina.gindullina@hpe.com.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIA.XXXXXXXX.

Digital Object Identifier 10.1109/TIA.XXXXXX.

However, due to their high reliance on cybercomponents, smart grids are vulnerable to cyberattacks from both external agents and internal participants. A particular threat is represented by false data injection (FDI), involving adversaries that sabotage the communication through data alteration, resulting in wrong choices of the network management [9]. FDI is often assumed to be committed by an outside attacker [10]–[13], but in a community SG environment, the prosumers themselves can perform it, to damage neighboring competitors for their own advantage, such as obtaining better profit from the energy production towards the consumers [14].

In this contribution, we investigate the latter case, i.e., strategic interaction in a community microgrid between prosumers. We focus on the attack-defense interplay between 2 prosumers with the aim to sell energy to a consumer, where the outcome entirely follows from the communication signaling exchanges and is therefore vulnerable to FDI [15]. Through a game theoretic framework, we discuss the resulting Nash equilibria (NEs) as possible operating points, which allows to gain insight on the interaction but also hint at possible guidelines for improving security in community SGs [16]. We remark that, while our analysis focuses on the simultaneous interaction of 2 prosumers with complete information, ours are to be seen as foundational results that allow the extension in future work to more complex scenarios, including more than 2 prosumers, different timescales, and possibly incomplete information complemented with Bayesian reinforcement learning [17]–[21].

A. Related literature

Driven by the need to decrease carbon emissions and improve energy efficiency, energy management systems for smart homes are gaining momentum [8]. In particular, peer-to-peer sharing mechanisms enables prosumers within a community microgrid to trade energy resources such as small-scale wind turbines, solar photovoltaic panels, electric vehicle batteries among each other, based on decentralized markets [22].

However, the integration with the communication network also brings vulnerability to cyber-threats [11]. For example, the exchange of false information may lead to wrong operations and service disruptions [9]. In a less conspicuous way, this is also a loophole that can be exploited by network prosumers to their own profit [14]. This problem was investigated via several methodologies, such as bi-level (attackers and defenders) models that allow sequential and security-constrained economic dispatch [23]. Most studies consider the problem

from the attacker's standpoint, or identify the problem in a scenario of complete information, without exploring the strategic consequences [24], [25]. Other papers handle the case of incomplete information, tackled by techniques such as Q-learning, used to identify the optimal strategy of attack [26], or attack region identification for unknown topologies by adding lines with arbitrary reactance values [27], and an adaptation of matrix theory to the case of incomplete information [28]. These studies often provide approximate solutions via heuristics.

Some more investigations took the perspective of the defender, and examined its protection; however, these studies are mostly just concerned on identifying how generic security mechanisms can be introduced in the measurements, and it ought to be noted that this often involves complex, possibly NP-hard, techniques [29]. Detection schemes have adopted, e.g., a joint transformation combined with Kullback-Leibler distance [30] and short-term forecasting leveraging temporal correlation [31]. Automated reasoning is exploited also in these cases, based on deep supervised [32] or reinforcement learning [20], [33]. These latter models are evaluated assuming that decisions made by either attackers or defenders do not condition future decisions of the other agents. This is reasonable only under the assumption that security is a probabilistic measurement on the resilience and mitigation of the system, which unfolds into a complex analysis [34]. Another proposed detection approach is a forecasting-aided anomaly detection system exploiting a sequence-to-sequence autoencoder to combat FDI via a two-stage approach: (i) forecasting and (ii) detection of anomalies within the forecasting [35]. A deep learning architecture was used in [36], to discover data intrusions, which allows the model to focus on the parameters that show whether an attack was launched.

These approaches only take into account one side of the decision process (either attackers or defenders). To study both sides of cybersecurity attacks, a game theory rationale is required [21]. Multiple re-interpretations of this same scenario can be framed as static games, such as zero-sum interactions to identify defense and attack in electricity markets [10] or to optimize the deployment of PMUs [15]. Stackelberg games [37] can be employed to decide which sensors to attack, in the cases of 1 [18] up to n [17] adversaries, or games of incomplete information [19]. Finally, a formulation as a bi-level multi-stage Bayesian game where players exploit game history to update their beliefs can be used to identify the losses caused by FDI attacks that target a specific measurement [38].

B. Contribution of the paper

We present a game theoretic analysis of cyberattack and defense among prosumers in a smart microgrid community [2]. This is a scenario where multiple prosumers can sell their overproduction of energy to a consumer, with a transaction system that can take place over a very fast timescale, with little supervision or regulation [14], [27]. The consumer, which is not taken here as a strategic agent, would just choose to buy energy from the prosumer reporting the highest production level. However, another prosumer with lower production may employ FDI to falsely alterate the reports and gain the spot to sell energy to the consumer. In turn, the prosumer with the legitimate highest level of production can adopt (or not) some countermeasures to nullify this intervention [35].

In the end, our analysis considers the interaction between these prosumers, seen as an attacker and a defender; however, this can be expanded to multiple prosumers with different levels of productions and the option to attack each other or defend themselves by focusing on their pair-wise interplay. The focus here is to analyze the strategic interaction between these two prosumers, i.e., a game, for which we derive NEs and infer practical conclusions through quantitative evaluations [15].

On a broader level, our analysis enables the derivation of criteria for enhancing security of community SG systems, such as giving analytical guidelines for how to prevent FDI attacks. This can be based on increasing surveillance so as to make them more costly, or assessing the level of self-defense success rate for which the attack can be thwarted - actually, if the attacker is aware of these parameters being unfavorable to a malicious activity, it will not even attempt it [9].

C. Paper outline

The rest of this paper is organized as follows. Section II introduces the game theoretic model. We then derive the pure Nash equilibria in Section III, general strict dominance relations in Section III, and the mixed Nash equilibria in Section IV. Numerical evaluations are shown in Section V, which leads to the conclusions and future research directions in Section VI.

II. Game Theory analysis

We consider a smart grid community with multiple prosumers and one consumer. Each prosumer has a different energy production level and is interested in selling it to the consumer. The latter chooses the prosumer providing the highest energy level, to ensure efficiency and reliability [6]. As will be clear in the following, we can restrict the analysis to the case of two prosumers only, denoted as 1 and 2, without loss of generality. This is because we assume that prosumer 2 is the one with the highest energy level, yet prosumer 1 is able to launch attacks to gain the opportunity to serve the customer. The case with more than 2 prosumers, all able to attack each other, can generalize this atomic interaction through pairwise attack-defense relationships in a broader network [17].

In the absence of malicious activity by prosumer 1, prosumer 2 will be selected by the consumer as the energy provider, as it reports a higher energy level. However, prosumer 1 can launch an FDI attack [9], [25] to manipulate the selection process and cause a denial of service to prosumer 2. For example, prosumer 1 can falsely report a higher energy level, or a lower energy level on behalf of prosumer 2. This misrepresentation causes the consumer to believe that 2 has less available energy than 1, resulting in the latter being selected as the energy provider.

This kind of attack implies that the malicious provider must be able to conduct reconnaissance to gather information about the communication protocols, data formats, and security measures used for reporting energy levels in the smart grid [16]. Therefore, this relies on known vulnerabilities in the data reporting system, such as weak authentication mechanisms or lack of encryption. However, it is not easy to prevent this kind of attack as the malicious provider, having access to the communication channels for its own legitimate data, can also exploit them to inject false information, possibly by intercepting and altering data packets in transit or directly submitting fabricated data into the reporting system.

As a result of receiving the falsified lower energy report for prosumer 2, the consumer incorrectly selects prosumer 1 as the energy provider. This acts like a denial of service attack for prosumer 2 as it effectively prevents it from supplying energy, disrupting the efficiency and reliability of the smart grid.

Prosumer 2 can actually defend against this kind of attack by implementing more robust data authentication mechanisms, encrypt communication channels to prevent tampering, deploy anomaly detection systems to identify unusual data patterns, and use redundancy and cross-validation to verify the accuracy of reported energy levels. In the end, all of these countermeasures are energy-consuming and can possibly lower the actual energy that prosumer 2 is able to supply to the consumer. For this reason, we model any kind of defense action by prosumer 2 as an energy-consuming activity d, which ought to enacted only if prosumer 1 is deemed to be maliciously active.

This reasoning underlines the strategic interaction between the prosumers as game-theoretic players. Prosumer 1 can exploit vulnerabilities to mislead the consumer into selecting it over prosumer 2 through a FDI; however, prosumer 2 can enact some form of defense against this attack and it may well be that this successfully counteract the FDI. Both of these actions (attacks and defense) are not guaranteed to be successful and come at a cost, assuming that part of the energy available for transfer to the consumer is spent for attacking or defending, which stacks up, each action having its own cost [35]. Moreover, the eventual outcome of this interaction depends on the joint strategic choices of both prosumers. The prosumer that is eventually selected by the customer gets a positive return, but this is decreased by the related energy expenditure if it needed to spend energy to attack or self-defend. A prosumer that is not selected has no return whatsoever [14].

The action set of the players $i \in \mathcal{P} = \{1, 2\}$ is defined as $A_i = \mathbb{N} \times \{0, 1\} \ni (X_i, d_i)$, where X_i denotes the number of attacks launched towards the other prosumer [38]. For the sake of generality, we allow player 2 to attack player 1, and conversely player 1 to defend, even though, as will be shown next, these are dominated strategies and therefore it is correct to see players 1 and 2 as an attacker and a defender, respectively.

We define set $\mathcal{S} \subseteq \mathcal{P}$ to be such that

$$\mathbb{P}[i \in \mathcal{S}] = \left(1 - pq^{d_i}\right)^{\sum_{j \in \mathcal{P}} X_j}. \tag{1}$$

TABLE I
NOTATION ADOPTED IN THE PAPER

symbol	meaning
X_i	number of attacks performed by prosumer i
d_i	self-defense binary indicator of prosumer i
$C_i(X_i, d_i)$	cost encountered by prosumer i
c_i	$= \mathbb{E}[C_i(X_i, d_i)]$, i.e., expected cost by prosumer i
E^{ask}	energy requirement of the consumer
E_i^{out}	energy provision level of prosumer i
p	probability of successful attack
q	probability of self-defense failure
a_i	attack cost of prosumer i
b_i	defense cost of prosumer i
$\tilde{a}$	$= a_1/E^{\text{ask}}$, relative attack cost of prosumer 1
$\tilde{b}$	$= b_2/E^{\text{ask}}$, relative defense cost of prosumer 2
u_i	utility value of prosumer i

Further, we define the utilities associated with each strategy. We assume that each player wants to maximize its own (monetary) gain, for which we define a fixed price per unit of power. Each of the players incurs (separate) expenditures for enacting attacks or self-defense mechanisms. We assume that for player i, attack and defense have respective costs $a_i > 0$ and $b_i > 0$. Thus, the cost of the action chosen is

$$C_i\left(X_i, d_i\right) = a_i X_i + b_i d_i. \tag{2}$$

We denote the generation of prosumer i as E_i^{out}, whereas the consumer asks for power E^{ask} so that $E_i^{\text{out}} \geq E^{\text{ask}}$. If this condition is not satisfied, then the prosumer cannot be selected by the consumer. All these parameters are common knowledge. Since the prosumer indices are ordered w.r.t. E_i^{out}, we have $E_1^{\text{out}} \leq E_2^{\text{out}}$. We can then define the utility for player i to be the quantification in monetary terms of its profit, being equal to the difference between the revenue and the paid cost, as

$$\begin{aligned} &u_i\left((X_i, d_i)_{1 \leq i \leq 2}\right) \\ &= \left[i \in \mathcal{S} \wedge \bigwedge_{i < j \leq 2} j \notin \mathcal{S}\right] E^{\text{ask}} - C_i\left(X_i, d_i\right). \end{aligned} \tag{3}$$

What computed in (3) is actually a random variable, yet we can apply *expected utility theory*, positing that a rational player i will strive to maximize the expected value of u_i [39]. Thus, if we set $c_i = \mathbb{E}\big[C_i(X_i, d_i)\big]$, we obtain

$$\begin{aligned} &\mathbb{E}\left[u_i\Big((X_i, d_i)_{1 \leq i \leq 2}\Big)\right] \\ &= \mathbb{E}\left[\left[i \in \mathcal{S} \wedge \bigwedge_{i < j \leq 2} j \notin \mathcal{S}\right]\right] E^{\text{ask}} - c_i \\ &= \mathbb{P}[i \in \mathcal{S}]\Bigg(\prod_{i < j \leq 2} \mathbb{P}[j \notin \mathcal{S}]\Bigg) E^{\text{ask}} - c_i. \end{aligned} \tag{4}$$

We remark that some models of agents in the smart grid electricity markets may follow different definitions of the objective of the players. For example, the profit of the prosumer may not be linear in the production level, due to increasing marginal costs. However, since in our analysis we give an ordinal meaning to utilities, our conclusion is still unaffected

as long as we can claim that higher profits are desirable for prosumers [40].

Each attack may succeed and defense may fail with probabilities p and q, respectively, with $p, q \in [0, 1]$. When an attack/defense action is successful, we say it to be *effective*. If an effective attack is performed against an ineffectively-defended prosumer, the latter will not be able to provide enough power to the consumer, therefore it will not be selected. A prosumer that does not choose self defense, is always ineffectively defended if attacked. By considering expected utilities, we can write

$$\begin{aligned} u_1\left((X_1, d_1), (X_2, d_2)\right) &= \mathbb{P}[1 \in S]\mathbb{P}[2 \notin S]E^{\text{ask}} - c_1 \\ u_2\left((X_1, d_1), (X_2, d_2)\right) &= \mathbb{P}[2 \in S]E^{\text{ask}} - c_2 \end{aligned} \tag{5}$$

Lemma II.1. *Player 2 has no incentive to attack player 1, that is, any strategy with $X_2 \neq 0$ is strongly dominated by its equivalent with $X_2 = 0$.*

Proof. See Appendix A. □

Lemma II.2. *Player 1 has no incentive to defend, that is, $d_1 = 0$ strongly dominates $d_1 = 1$.*

Proof. See Appendix B. □

We can then further simplify (5) to

$$u_1(X_1, d_2) = \left(1 - \left(1 - pq^{d_2}\right)^{X_1}\right) E^{\text{ask}} - a_1 X_1 \tag{6}$$

$$u_2(X_1, d_2) = \left(1 - pq^{d_2}\right)^{X_1} E^{\text{ask}} - b_2 d_2 \tag{7}$$

III. Pure Nash equilibria

If $E^{\text{ask}} = 0$ then both utilities are reduced to pure costs, and the only pure strategy NE is $X_1^* = 0 \wedge d_2^* = 0$; hence in the following $E^{\text{ask}} \neq 0$, and we write $\tilde{a} = \frac{a_1}{E^{\text{ask}}}$ and $\tilde{b} = \frac{b_2}{E^{\text{ask}}}$. Note that $\tilde{a}$ can be interpreted as the maximum number of attacks that can be performed before becoming counterproductive. Pure strategy NEs correspond to X_1^*, d_2^* satisfying both

$$X_1^* = \arg\max_{X_1} u_1(X_1, d_2^*) \tag{8}$$

$$d_2^* = \arg\max_{d_2} u_2(X_1^*, d_2) \tag{9}$$

Substituting (7) in (9) we have that

$$\begin{aligned} (1-pq)^{X_1^*} - (1-p)^{X_1^*} \leq \tilde{b} &\implies d_2^* = 0 \\ (1-pq)^{X_1^*} - (1-p)^{X_1^*} \geq \tilde{b} &\implies d_2^* = 1 \end{aligned} \tag{10}$$

whereas for (8), we exploit (6) and solve the maximization by relaxing the constraint $X_1 \in \mathbb{N}$, obtaining

$$X_1^* = \arg\max_x \left(1 - \left(1 - pq^{d_2^*}\right)^x - \tilde{a}x\right) \tag{11}$$

for $x \in \mathbb{R}$. We then need to study the sign of

$$\begin{aligned} &\Delta\left(1 - (1 - pq^{d_2^*})^x - \tilde{a}x\right) \\ &= (1 - pq^{d_2^*})^x - (1 - pq^{d_2^*})^{x+1} - \tilde{a} \\ &= (1 - pq^{d_2^*})^x pq^{d_2^*} - \tilde{a} \end{aligned} \tag{12}$$

with Δ denoting the *forward difference operator*, that is, $(\Delta T)(x) = T(x+1) - T(x)$, as a function of x. There are two extreme cases to consider: (i) $q = 0$ and $d_2^* = 1$, giving *perfect defense*, i.e., prosumer 1 cannot make an effective attack. In this case, the right-hand side of (12) is equal to $-\tilde{a}$ and therefore the optimal x is 0; but $\tilde{b} > 0 = (1-pq)^0 - (1-p)^0$ and therefore $d_2^* = 1$ cannot be an equilibrium; and (ii) $p = 1$ and $d_2^* = 0$, that is the case of *perfect attack*, where prosumer 1's attacks are always effective. Then, (12) is equal to $[x = 0] - \tilde{a}$ and has $x = 0$ if $\tilde{a} \geq 1$ and $x = 1$ if $\tilde{a} \leq 1$ as optimal values; the former is always an equilibrium, whereas the latter is one only if $\tilde{b} \geq 1 - q$. We can now assume $0 < pq^{d_2^*} < 1$. There is an inflection point around

$$x = \frac{\ln\left(\tilde{a}^{-1} pq^{d_2^*}\right)}{\ln\left(1 - pq^{d_2^*}\right)^{-1}} \tag{13}$$

and thus, for $x \neq \mathbb{Z}$, $X_1^* = \max\{\lceil x \rceil, 0\}$. For $x < 0$, the only solution is 0, whereas for $x \in \mathbb{N}$ both x and $x + 1$ are solutions.

In (10), $p > 0$ and $pq > 0$, $(1-p)^x$ and $(1-pq)^x$ are both decreasing functions of x; as a result, substituting X_1^* we get

$$\begin{aligned} &(1-pq)^{\max\{\lceil x \rceil, 0\}} - (1-p)^{\max\{\lceil x \rceil, 0\}} \\ &\quad = \begin{cases} 0 & x \leq 0 \\ (1-pq)^{\lceil x \rceil} - (1-p)^{\lceil x \rceil} & x > 0 \end{cases} \\ &\quad = \max\left\{(1-pq)^{\lceil x \rceil} - (1-p)^{\lceil x \rceil}, 0\right\}. \end{aligned} \tag{14}$$

The following equivalences allow us to remove $\tilde{b} \geq 0$ and $\tilde{b} \leq 0$, which are always true and false conditions, respectively:

$$\begin{aligned} \max\{a, b\} \leq c &\iff a \leq c \wedge b \leq c \\ \max\{a, b\} \geq c &\iff a \geq c \vee b \leq c \end{aligned} \tag{15}$$

The result of these simplifications is shown in Table II, along with better representations of u_1 and u_2 whenever available.

Now that all pure strategy NEs have been identified, some properties can be proven about them.

Theorem III.1. *If $E^{\text{ask}} \neq 0$ and $p \leq \tilde{a}$ then there is a pure strategy NE such that $X_1^* = 0$ and $d_2^* = 0$ for any $q < 1$.*

Proof. See Appendix C. □

Moreover, the following Theorem also holds.

Theorem III.2. *If $E^{\text{ask}} \neq 0$ and $p < \tilde{a}$ then the equilibrium defined by Theorem III.1 is the* only *pure strategy NE.*

Proof. See Appendix D. □

These two theorems justify the notion that, for low values of attack success p, it becomes unfeasible for the attacker to attack at all, as the risk of not incapacitating the defender is higher than the benefit gained from an effective attack.

TABLE II

PURE NASH EQUILIBRIA. RELATIVE COST OF ATTACK $\tilde{a}$, CONSUMER REQUIREMENT E^{ask}, PROBABILITIES (p, q) OF (ATTACK SUCCESS, DEFENSE FAILURE).

d_2^*	X_1^*	x from (12)	u_1 (utilities for players 1 and 2)	u_2	Condition on $\tilde{b}$ (relative cost of defense)	Other conditions
0	0		0	0		$E^{\text{ask}} = 0$ or $p = 1$ and $\tilde{a} \geq 1$
0	1		$1 - \tilde{a}$	0	$\tilde{b} \geq 1 - q$	$E^{\text{ask}} \neq 0$, $p = 1$ and $\tilde{a} \leq 1$
0	$\max\{\lceil x \rceil, 0\}$	$\frac{\ln \frac{\tilde{a}}{p}}{\ln(1-p)}$			$\tilde{b} \geq (1-pq)^{\lceil x \rceil} - (1-p)^{\lceil x \rceil}$	$E^{\text{ask}} \neq 0$ and $p < 1$
1	$\max\{\lceil x \rceil, 0\}$	$\frac{\ln \frac{\tilde{a}}{pq}}{\ln(1-pq)}$			$\tilde{b} \leq (1-pq)^{\lceil x \rceil} - (1-p)^{\lceil x \rceil}$	$E^{\text{ask}} \neq 0$ and $q > 0$
0	$x + 1$	$\frac{\ln \frac{\tilde{a}}{p}}{\ln(1-p)}$	$1 - \tilde{a}\left(x + \frac{1}{p}\right)$	$\frac{1-p}{p}\tilde{a}$	$\tilde{b} \geq (1-pq)^x - (1-p)^x$	$E^{\text{ask}} \neq 0$, $p < 1$ and $x \in \mathbb{N}$
1	$x + 1$	$\frac{\ln \frac{\tilde{a}}{pq}}{\ln(1-pq)}$	$1 - \tilde{a}\left(x + \frac{1}{pq}\right)$	$\frac{1-pq}{pq}\tilde{a} - \tilde{b}$	$\tilde{b} \leq (1-pq)^x - (1-p)^x$	$E^{\text{ask}} \neq 0$, $q > 0$ and $x \in \mathbb{N}$

IV. STRICT DOMINANCE

Despite a countable infinity of actions being available to prosumer 1, those not strongly dominated are finite in number. The analysis to prove this is split, as for the pure strategy NEs. If $E^{\text{ask}} = 0$, (6) becomes $-a_1 X_1$, (7) becomes $-b_2 d_2$, then $X_1 = 0$ and $d_2 = 0$ is a strictly dominant strategy. There are, in other words, no strictly mixed strategy NEs. If $E^{\text{ask}} > 0$ but $q = 0$ and $p = 1$, we have that $X_1 = 1$ strictly dominates all $X_1 = x > 1$ as the conditions for strict dominance ultimately reduce to $\tilde{a}(x-1) > 0$. Furthermore, if $\tilde{a} > 1$, then $X_1 = 0$ strictly dominates $X_1 = 1$, whereas the converse is impossible as it requires $\tilde{a} < 0$. If $E^{\text{ask}} > 0$ and $q = 0$ but $p < 1$, (6) becomes

$$\left(1 - (1 - p[d_2 = 0])^{X_1}\right) - \tilde{a} X_1 \tag{16}$$

and $X_1 = x$ strictly dominates $X_1 = x + 1$ whenever

$$(1 - p[d_2 = 0])^x < (1 - p[d_2 = 0])^{x+1} + \tilde{a} \tag{17}$$

which is always true for $d_2 = 1$ whereas for $d_2 = 0$ we get

$$x > \frac{\ln\left(\tilde{a}^{-1} p\right)}{\ln(1-p)^{-1}} \tag{18}$$

and therefore the remaining choices for X_1 are finite. If $E^{\text{ask}} > 0$ and $q > 0$ but $p = 1$. Thus, (6) becomes

$$\left(1 - \left(1 - q^{d_2}\right)^{X_1}\right) - \tilde{a} X_1 \tag{19}$$

so that $X_1 = x$ strictly dominates $X_1 = x + 1$ whenever

$$\left(1 - q^{d_2}\right)^x < \left(1 - q^{d_2}\right)^{x+1} + \tilde{a} \tag{20}$$

which is equal to $x > 1 \vee \tilde{a} > 1$ for $d_2 = 0$ whereas for $d_2 = 1$ we get

$$x > \frac{\ln\left(\tilde{a}^{-1} q\right)}{\ln(1-q)^{-1}}. \tag{21}$$

If $E^{\text{ask}} > 0$ and $p < 1, q > 0$. We get that $X_1 = x$ strictly dominates $X_1 = x + 1$ whenever

$$x > \frac{\ln\left(\tilde{a}^{-1} p q^{d_2}\right)}{\ln\left(1 - p q^{d_2}\right)^{-1}} \tag{22}$$

with a computation similar to the one above. This analysis justifies the intuition that it is not sensible to attack indefinitely, since the cost will eventually exceed the (expected) gain. Also, if $\tilde{a} > 1$, then $X_1 = 0$ strictly dominates all other choices for X_1, which forces $d_2 = 0$, leaving this as the only joint strategy.

From the analysis above we derive the following properties.

Theorem IV.1. *If $E^{\text{ask}} > 0$, then a strategy with $X_1^* \neq 0$ is not strictly dominated only if $d_2 = 1$ and $\tilde{a} < q \leq p$ or $\tilde{a} < p \leq q$ or only if $d_2 = 0$ and $q < \tilde{a} < p$.*

Proof. See Appendix E. □

Corollary IV.1.1. *With the same assumption of Theorem IV.1: if $p > \tilde{a}$, $q > \tilde{a}$ with $\tilde{a} \approx 0$, $q > p$ or $p > q$ and $d_2 = 1$, then there is a strategy $X_1^* \neq 0$ that is strictly dominant.*

Proof. See Appendix F. □

V. MIXED NASH EQUILIBRIA

To find the mixed strategy NEs, $E^{\text{ask}} > 0$ and $\tilde{a} \leq 1$ are assumed. We have that $d_2 = 1$ never strictly dominates $d_2 = 0$ since the condition for dominance is

$$\tilde{b} < \inf_x \left((1-pq)^x - (1-p)^x\right) \tag{23}$$

that requires $\tilde{b} < 0$ for the case $x = 0$. Yet, $d_2 = 0$ can strictly dominate $d_2 = 1$ as in the following cases from

$$\tilde{b} > \sup_x \left((1-pq)^x - (1-p)^x\right). \tag{24}$$

1) The case $p = 1$ and $q = 0$: For the dominance condition, (24) is in this case equivalent to $\tilde{b} > 1$; this corresponds to one or both of the first two pure strategy NEs in Table II. When $\tilde{b} \leq 1$, two cases follow. (i) $\tilde{a} = 1$: n this case, $X_1 = 0$ is equivalent to $X_1 = 1$ as far as payoffs are concerned; therefore, strategies of the form $\beta \langle X_1 = 0 \rangle + (1-\beta) \langle X_1 = 1 \rangle$ constitute a NE when combined with $d_2^* = 0$, with the condition that $\beta \geq 1 - \tilde{b}$. Or (ii), if $\tilde{a} < 1$: the players choose strategies, neither of which are dominated. Therefore, we can compute a mixed strategy NE by setting the strategy of prosumer 1 to be $\alpha \langle d_2 = 0 \rangle + (1-\alpha) \langle d_2 = 1 \rangle$ and for

prosumer 2, $\beta \langle X_1 = 0 \rangle + (1-\beta) \langle X_1 = 1 \rangle$. The equations for the mixed equilibrium are

$$\begin{aligned} (1-\beta)(\alpha - \tilde{a}) &= 0 \\ (1-\beta)(\alpha - \tilde{a}) &= \alpha(1-\tilde{a}) - (1-\alpha)\tilde{a} \\ \alpha\beta + (1-\alpha)(1-\tilde{b}) &= \beta \\ \alpha\beta + (1-\alpha)(1-\tilde{b}) &= 1-\tilde{b} \end{aligned} \tag{25}$$

that are satisfied for $\alpha = \tilde{a}$ and $\beta = 1-\tilde{b}$. Therefore, we have a mixed strategy NE with

$$\begin{aligned} (1-\tilde{b}) \langle X_1^* = 0 \rangle + \tilde{b} \langle X_1^* = 1 \rangle \\ \tilde{a} \langle d_2^* = 0 \rangle + (1-\tilde{a}) \langle d_2^* = 1 \rangle \end{aligned} \tag{26}$$

and there are no other mixed strategy NEs.

2) The case $p < 1$ and $q = 0$ (perfect defense): Firstly, (24) is valid if and only if $\tilde{b} \geq 1$. When $1-(1-p)^{\lceil x \rceil} \leq \tilde{b} < 1$ there exists a pure strategy NE, namely the third one in Table II. Now let m_1 be a mixed strategy whose support contains three distinct values $i < j < k$ for X_1. Among the conditions for it to be a mixed strategy NE, we get that $\alpha = \frac{j-i}{(1-p)^i-(1-p)^j}\tilde{a}$ and the same replacing j for i and k for j. The two must be equal, which implies

$$\frac{(1-p)^{j-i}\left(1-(1-p)^{k-j}\right)}{1-(1-p)^{j-i}} = \frac{k-j}{j-i}. \tag{27}$$

The LHS is strictly decreasing in p for $0 < p < 1$ and its limit value for $p \to 0$ is $\frac{k-j}{j-i}$. In other words, equality never holds, and there cannot be more than two values in the support of any mixed strategy NE. We are left with four equations, namely the conditions for $\beta \langle X_1 = i \rangle + (1-\beta) \langle X_1 = j \rangle$, with $i < j$, and $\alpha \langle d_2 = 0 \rangle + (1-\alpha) \langle d_2 = 1 \rangle$ to be an equilibrium; the first two conditions on u_1 solve for α as given above, whereas for β we have that

$$(1-\beta)(1-p)^j + \beta(1-p)^i = 1-\tilde{b} \tag{28}$$

whose solution is

$$\beta = \frac{1-(1-p)^j-\tilde{b}}{(1-p)^i-(1-p)^j}. \tag{29}$$

The other two equations are trivial. The equilibrium inequalities for X_1 have the form

$$\forall k \neq i.\ \frac{1-(1-p)^{j-i}}{j-i} \geq \frac{1-(1-p)^{k-i}}{k-i}. \tag{30}$$

As the function $\frac{1-(1-p)^x}{x}$ is decreasing in x, an interesting remark can be made: if $i \neq 0$, then $k = 0$ is a valid choice in the function above; but also, as $i < j$, the LHS with parameter $0 < j-i$ will always be lower than the RHS. On the other hand, when $i = 0$ then the lowest value that k can go is $k = 1$, which therefore forces $j = i + k = 1$. Ultimately, we have a mixed strategy NE with

$$\left(1-\frac{\tilde{b}}{p}\right) \langle X_1^* = 0 \rangle + \frac{\tilde{b}}{p} \langle X_1^* = 1 \rangle \tag{31}$$

$$\frac{\tilde{a}}{p} \langle d_2^* = 0 \rangle + \left(1-\frac{\tilde{a}}{p}\right) \langle d_2^* = 1 \rangle\ , \tag{32}$$

which only exists for $\tilde{a}, \tilde{b} < p$. For $\tilde{a} = p$ a similar mixed strategy NE exists for $d_2^* = 0$ and arbitrary $\beta \geq 1 - \frac{\tilde{b}}{p}$. One can see that these equilibria are nothing but a generalization of (26) with $p < 1$.

3) The case $p = 1$ and $q > 0$ (perfect attack): We consider as in the previous case a mixed strategy m_1 with support containing at least three distinct values $i < j < k$, and again we obtain that such a strategy can never be a NE. We can see it by distinguishing two cases: if $i > 0$ then the formula for α is opposite to the one found above, namely $\alpha = 1 - \frac{j-i}{(1-q)^i-(1-q)^j}\tilde{a}$, and the conclusion follows from the previous analysis; for $i = 0$, on the other hand, we get the same formula for j and k, whereas for i and j it has the form $\alpha = 1 - \frac{\tilde{a}j-1}{(1-q)^j}$. However, we know from (21) that all values of X_1 greater than a bound, which is easily seen to be always below $\tilde{a}^{-1}$, are strictly dominated; an equilibrium, mixed or otherwise, containing a value $j > \tilde{a}^{-1}$ is therefore impossible: but that implies $\alpha > 1$, which is impossible. We are left with the only case of $i > 0$. The value for β is seen to be $\beta = \frac{\tilde{b}-(1-q)^j}{(1-q)^i-(1-q)^j}$; but the additional condition for u_2 in $i > 0$ implies that $\alpha = 1$, which is impossible (it would require $i = j$). Ultimately, there are no mixed strategy NEs for this case. Note that we did not refer to (24), which holds when $\tilde{b} > 1-q$, and does not need to be exploited. One can also see that said condition would hold for β to be valid in the first place.

4) The case $p < 1$ and $q > 0$: Similar to above, we prove that for a generic mixed strategy m_1 we cannot have three different values $i < j < k$ in its support; repeating the analysis for i and j as before, we obtain

$$\alpha = \frac{\tilde{a}(j-i) - \left((1-pq)^i - (1-pq)^j\right)}{\left((1-p)^i-(1-p)^j\right) - \left((1-pq)^i-(1-pq)^j\right)}. \tag{33}$$

This value is in the correct range only if

$$(1-pq)^i - (1-pq)^j < \tilde{a}(j-i) < (1-p)^i - (1-p)^j \tag{34}$$

and this double inequality allows us to prove that it is impossible that there be two values of α satisfying a similar equivalence as those above. We find a formula for β, namely

$$\beta = \frac{(1-pq)^j - (1-p)^j - \tilde{b}}{\left((1-p)^i-(1-p)^j\right) - \left((1-pq)^i-(1-pq)^j\right)} \tag{35}$$

Conversely, equilibrium inequalities are complex and do not easily admit closed-form analysis. A detailed study is left for future research.

VI. Numerical Results

For a better understanding of the results, we consider some quantitative evaluations. These are all assessments of the performance at the NEs found in the analysis. For this reason, they are not affected by issues of numerical convergence or computational complexity, as they just correspond to substituting different parameters into the formulas.

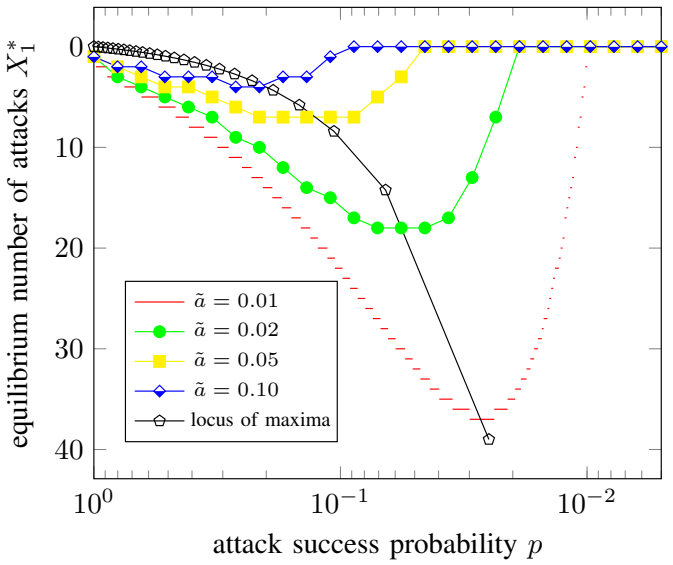


Fig. 1. Number of attacks at equilibrium X_1^* as a function of attack success probability p for various relative attack costs $\tilde{a}$.

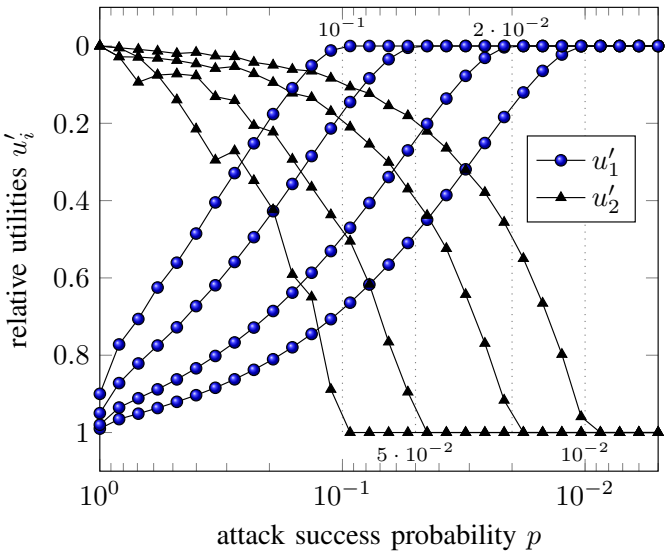


Fig. 2. Utilities of attacker (u_1) and defender (u_2) vs. attack success probability p for various relative attack costs $\tilde{a}$.

These are not to be interpreted in a comparison sense among different techniques, but rather as theoretical performance assessments. Contrarily to studies where alternative approaches are confronted, we enable an evaluation of the resulting performance that the prosumers can get [13], [38]. An immediate application would be in the identification of guidelines and trends for enhancing security of community SGs, e.g., showing the ranges of parameters causing the attacker to be inactive.

A first set of results displays the performance in terms of number of attacks carried by player 1 at the Nash equilibrium, i.e., X_1^*, or the resulting utilities of the players, as a function of the attack success probability p. The latter is reported in logarithmic scale to allow for a wider range of values.

Fig. 1 shows X_1^* for the third NE in Table II as a function of p. The curves are ordered from flattest to sharpest, for various values of $\tilde{a}$. The locus of maxima for X_1^* is displayed as the dashed line, obtained from the definition of x as $x^* = \frac{1-p}{p}$. Seen as a function of $\tilde{a}$, it decreases exponentially, since when $\tilde{a}$ diminishes i.e., the relative attack cost goes down, the amount of failures that can be tolerated increases as attacks are cheap and can be massively launched. Eventually, the linearly additive cost of attacks prevails over the diminishing gain expected from it. This occurs until $p = \tilde{a}$, at which point there is no incentive to attack.

Utilities u_1 and u_2 are shown in Fig. 2 as functions of p in the case of the third pure equilibrium; the values for $\tilde{a}$ are the same as before. Interestingly, in the case of no defense, u_2 is not monotonically decreasing; this is especially evident in the jagged case $a = 10^{-1}$. The defender may yet prefer slightly *higher* successful attack probabilities, as they will trick the attacker into launching fewer attacks, for which they are not prepared (as $d_2^* = 0$).

Fig. 3 shows the same analysis, but considers an increasing

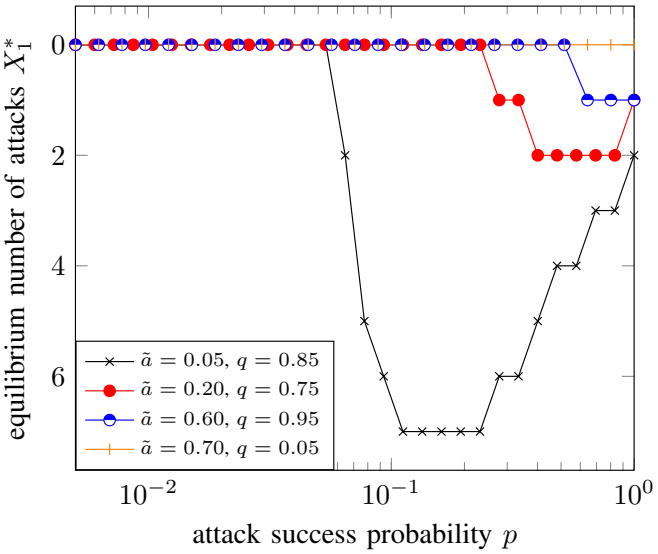


Fig. 3. Number of attacks at equilibrium X_1^* vs. attack success probability p for various defense failure probabilities q and relative attack costs $\tilde{a}$.

value of $\tilde{a}$ and a decreasing value of q, to quantify the attacks that prosumer 1 is expected to launch. The number of attacks generally increases as their cost decreases and the probability of successful defense increases. However, the curves also show a decrease as the probability of a successful attack becomes very high, since in this case it is convenient for prosumer 1 to avoid unnecessary extra attacks, as a lower number would still be enough, to contain the costs. This general trend is present in all the following plots, albeit to a different extent depending on the parameters.

Fig. 4 represents the extreme case; for values of q lower than $\tilde{a}$, the attacker has no incentive to attack at all, and therefore X_1^* reduces to a flat zero. This is consistent with

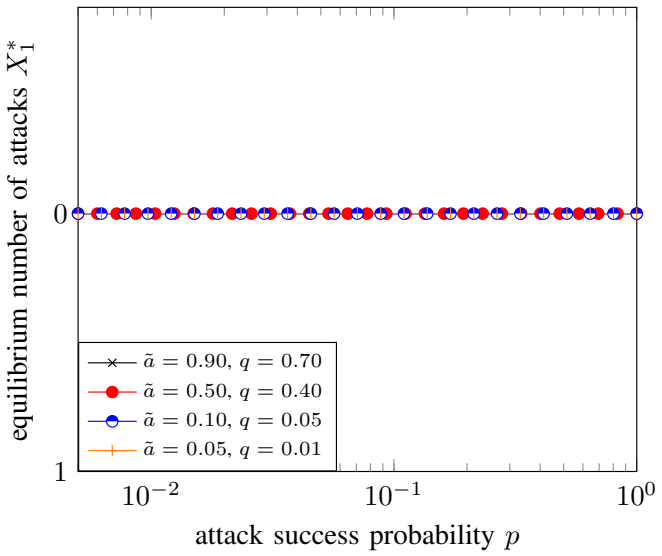


Fig. 4. Number of attacks at equilibrium X_1^* vs. attack success probability p for various defense failure probabilities $q < \tilde{a}$ and relative attack costs $\tilde{a}$.

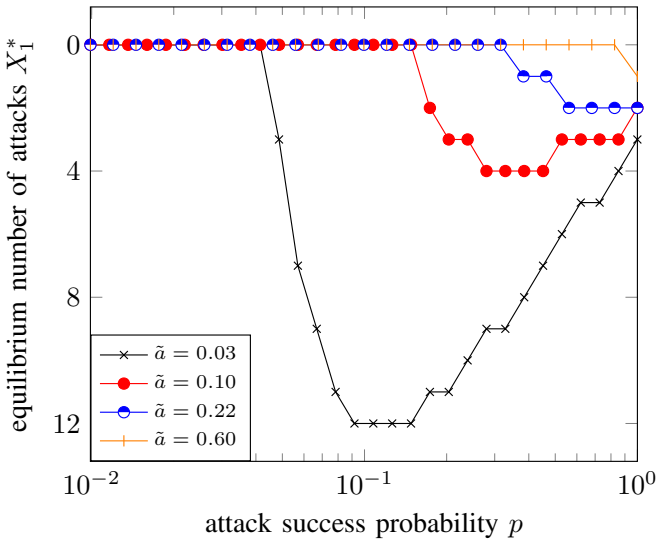


Fig. 5. Number of attacks at equilibrium X_1^* vs. attack success probability p for defense failure probabilities $q = \frac{2}{3}$ and relative attack costs $\tilde{a}$.

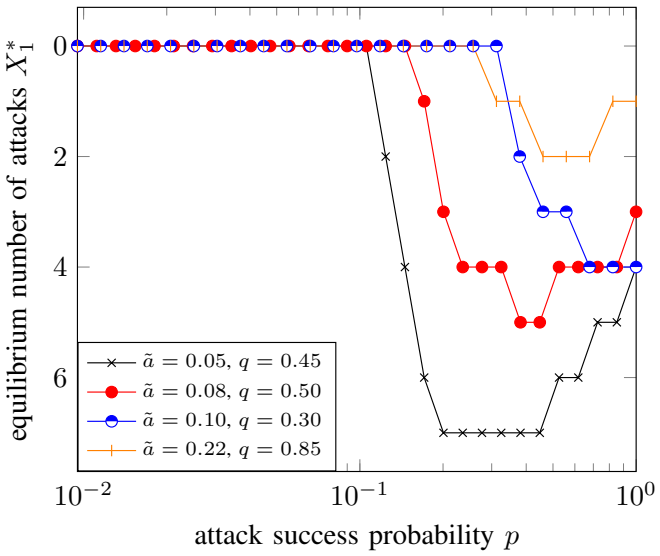


Fig. 6. Number of attacks at equilibrium X_1^* vs. attack success probability p for various defense failure probabilities $q > \tilde{a}$ and relative attack costs $\tilde{a}$.

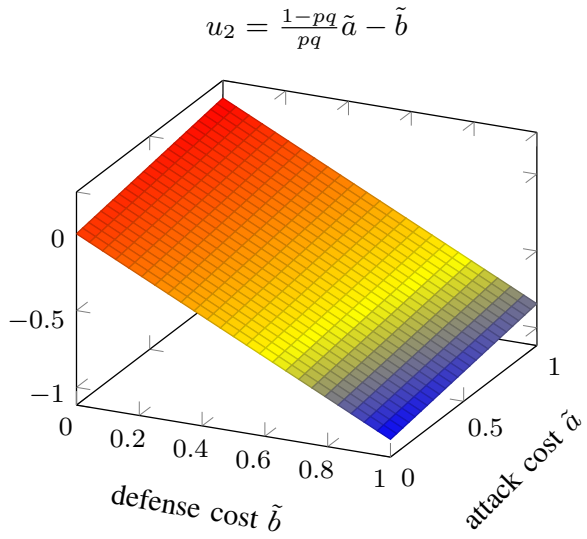


Fig. 7. Utility of the defender at the 6th pure strategy NE as a function of attack success probability $p = 0.6$, the defense failure probability $q = 0.1$, the relative attack cost $\tilde{a}$ and the relative defense cost $\tilde{b}$.

the results in Theorems III.1 and III.2, and is a general game theoretic principle that an attacker, realizing that intervention is too expensive or easily counteracted, will abstain from malicious activity [9]. This may also serve a useful guideline to identify practical countermeasures to inhibit attacks, from the perspective of either a security agency or a network manager; this would correspond to increase the costs of an attack (even in expectation), e.g., by establishing external penalties.

Similarly, Fig. 5 considers a setting where the defender has a very high defense failure probability q. It is shown how there is no need to significantly increase the number of attacks launched, as even few attempts will be successful. The number of attacks increases only if their cost is extremely low.

On the other hand, Fig. 6 considers an array of scenarios where the relative attack cost $\tilde{a}$ is lower than the probability of defense failure q. The figure shows that the number of attacks X_1^* increases in their success probability p, but only if the latter is relatively high. In other words, even cheap attacks with low probability of contrast by the defender are performed only if they have a high probability to break the system.

To sum up, all these plots show that NE corresponds to an active adversary that launches multiple attacks only if their success is sufficiently likely and their cost is sufficiently low – notably, lower than the probability of successful defense, i.e., $\tilde{a} < q$. All of this may hint at possible criteria for securing the system from the perspective of the defender, aligning with

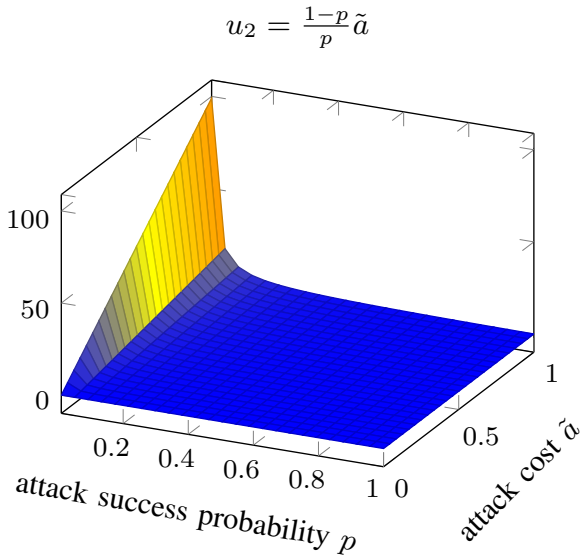


Fig. 8. Utility of the defender at the 5th pure strategy NE as a function of attack success probability p and the relative attack cost $\tilde{a}$.

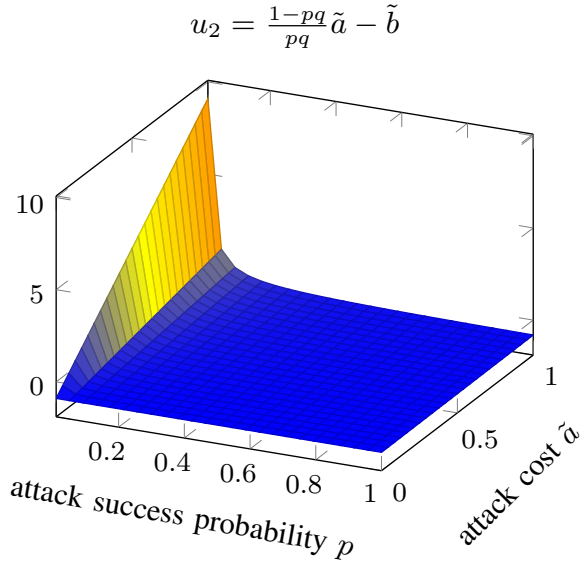


Fig. 9. Utility of the defender at the 6th pure strategy NE as a function of attack success probability p, the defense failure probability $q = 0.1$, the relative attack cost $\tilde{a}$ and the relative defense cost $\tilde{b} = 0.9$.

two major research directions. The former would correspond to empower cyber-defense or detection techniques so as to thwart the attack [26], but at the same time our results show that an adversary driven by selfish utility is repelled by high costs, which may intervene as an alternative countermeasure.

Next, we focus on comparing the 5th and 6th pure strategy NEs, which differ in the defense strategy of player 2, i.e., $d_2^* = 0$ and $d_2^* = 1$, respectively. Since no self-defense is chosen in the 5th NE, the defense cost $\tilde{b}$ and the probability of self-defense failure q do not influence the resulting utility. Conversely, we can see in Fig. 7 that the utility value u_2

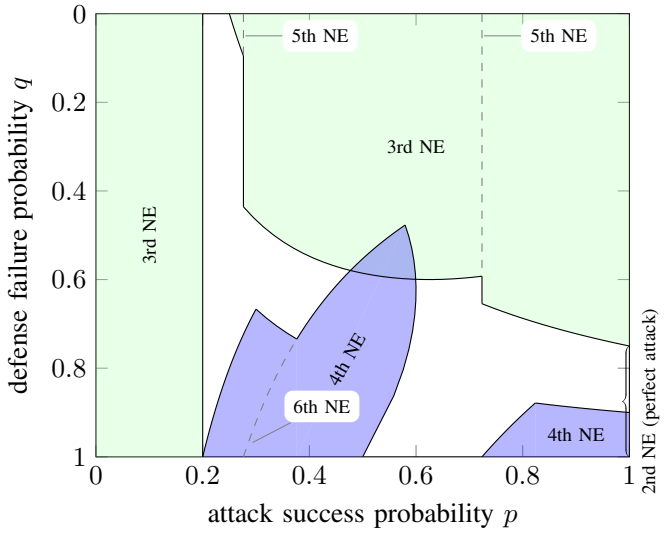


Fig. 10. Pure Nash equilibria as a function of attack success probability p and defense failure probability q with relative attack cost $\tilde{a} = \frac{1}{5}$ and relative defense cost $\tilde{b} = \frac{1}{4}$.

linearly depends on both $\tilde{a}$ and $\tilde{b}$ (the trend is increasing in $\tilde{a}$ and decreasing in $\tilde{b}$), and the coefficient of $\tilde{a}$ depends on p and q so that, ultimately, the utility of prosumer 2 can be positive or negative depending on all these parameters.

As a result, the utility of prosumer 2 in the 5th NE, shown in Fig. 8, turns out to be non-zero only if the cost of an attack $\tilde{a}$ is very high, and its success is unlikely, in which case prosumer 1 will not attack. A visually similar trend is visibile for the 6th NE in Fig. 9, which considers $\tilde{b} = 0.9$ and $q = 0.1$, albeit different values obtain similar trends. In this case, prosumer 2 chooses to defend, but it is an expensive action, and in turn this gives a positive utility only if, once again, the attacks from prosumer 1 are inconvenient (both expensive and not likely to succeed). Also, while the trend is the same, the utility of player 2 is lower than in the 5th NE since defense is expensive.

Finally, Fig. 10 shows a phase diagram of the game, i.e., the areas for p and q in which the pure NEs exist. The green area is associated with the third Nash equilibrium in Table II, and both the third and the fifth are present when p lies on one of the dashed vertical lines. The same can be said for the fourth and sixth equilibria, which lie in the blue-shaded areas and dashed segments. It can be seen that in many ranges of p and q there is no pure strategy NE and that the two main ones coexist only for a small sliver of the domain. Nevertheless, such empty areas must include a mixed strategy NE.

VII. Conclusions

Community SG scenarios are important applications combining information and communication technologies with energy provision in a shared fashion [22]. While pilot projects of P2P energy sharing communities are developed around the world, it is important to explore whether the combination of energy and information exchanges is vulnerable to malicious behavior by some participants [7].

To this end, we studied a case where prosumers contending for the role of energy supplier of a consumer can attack each other or enact defense mechanisms [16]. This is modeled as a static game of complete information, for which we studied the NEs and analyzed the implications, e.g., in terms of correlation between network parameters and number, type, and associated utilities of NEs. For example, we found that increasing the cost of an attack does not always correspond to a lower optimal number of attacks. Another important consequence is the establishment of structural protections against inside attacks, which are obtained whenever the cost parameters do not support an advantageous attack strategy. This can be seen as a preliminary effort to enact for a secure interaction in the SG community [9].

The model can be generalized in various directions, such as introducing more than one consumer, each with its own energy requirement E_i^{ask}, or assuming partial knowledge over power parameters and probabilities p and q [41]. The topology of the grid can also vary in time, either due to natural dynamics or because of malicious interventions of some nodes [14], [27], and the model may be developed considering various rounds as well as player types by extending it to a multi-stage Stackelberg game with strategic interactions [37], or a Bayesian game with multiple player types [21]. All of these are interesting developments to explore in future research.

Appendix A
Proof of Lemma II.1

From the definition of expected utility for player 2 in (5) and of cost in (2) we have

$$\begin{aligned} u_2((X_1,d_1),(X_2,d_2)) &= \mathbb{P}[2\in S]E^{\text{ask}} - a_2X_2 - b_2d_2 \\ &< \mathbb{P}[2\in S]E^{\text{ask}} - b_2d_2 = u_2((X_1,d_1),(0,d_2)). \end{aligned} \tag{36}$$

Appendix B
Proof of Lemma II.2

From Lemma II.1, we may assume $X_2 = 0$. From player 1's expected utility in (5) and cost in (2) we have

$$\begin{aligned} u_1((X_1,d_1),(0,d_2)) &= \mathbb{P}[1\in S]\mathbb{P}[2\notin S]E^{\text{ask}} - a_1X_1 - b_1d_1 \\ &= \mathbb{P}[2\notin S]E^{\text{ask}} - a_1X_1 - b_1d_1 \\ &< \mathbb{P}[2\notin S]E^{\text{ask}} - a_1X_1 = u_1((X_1,0),(0,d_2)). \end{aligned} \tag{37}$$

□

Appendix C
Proof of Theorem III.1

The proof is split into two parts, considering different cases. First, suppose $p < 1$. The other conditions for the third equilibrium in Table II are satisfied, and we know that $\ln\frac{\tilde{a}}{p} > 0$ and therefore the value of x is negative. Thus the condition on $\tilde{b}$ reduces to $\tilde{b} \geq (1-pq)^0 - (1-p)^0 = 0$, which is always satisfied; the third equilibrium exists and has $X_1^* = 0$, since $\lceil x \rceil \leq 0$. Alternatively, let $p = 1$. Then the hypothesis becomes $1 \leq \tilde{a}$; in other words, all conditions for the first equilibrium in Table II are satisfied. In both cases, we also have that $d_2^* = 0$, which completes the proof. □

Appendix D
Proof of Theorem III.2

As for Theorem III.1, the proof is split into two cases. Suppose $p < 1$. We know that the first and second equilibria in Table II do not exist; it is enough to prove that neither all the others but the third do. To that end, note that $pq < p < \tilde{a}$ and therefore $\ln\frac{\tilde{a}}{pq} > 0$ as well; thus, if either the fourth or the sixth equilibrium were to exist, they would have $X_1^* = 0$. But then that would imply that $\tilde{b} \leq (1-pq)^0 - (1-p)^0$, which is impossible; neither equilibrium can then exist. Finally, the condition $x \in \mathbb{N}$ for the fifth equilibrium cannot hold, for $\ln\frac{\tilde{a}}{p} > 0$ and thus $x < 0$. In the remaining case, let $p = 1$. Then the hypothesis becomes $1 \leq \tilde{a}$: the second equilibrium cannot exist. It is now sufficient to prove that neither can the fourth or the sixth. To that end, suppose that there exists an equilibrium for which the condition on $\tilde{b}$ is true, namely $\tilde{b} \leq (1-q)^{\lceil x \rceil} - [\lceil x \rceil = 0]$. If $\lceil x \rceil = 0$ then this condition cannot be satisfied as it reduces to $\tilde{b} \leq 0$. But on the other hand, if $\lceil x \rceil > 0$ then it must be that $\ln\frac{\tilde{a}}{p} < 0$ and therefore $p > \tilde{a}$, which is false by hypothesis. □

Appendix E
Proof of Theorem IV.1

The case $p < \tilde{a}$ is already proven by Lemma III.2, from now on we are considering that $\tilde{a} < 1$ as assumption; let therefore $q < \tilde{a} < p$, taking into account that (13) for the case $d_2 = 1$ simplifies out into $x = -\frac{\ln(pq/\tilde{a})}{\ln(1-pq)}$ and so analyzing its sign we can affirm that $\ln(1-pq) < 0$ and the numerator is greater than 0, now considering the negative sign of the equation $x < 0$. By definition of the number of attacks $X_1^* = \max\{\lceil x \rceil, 0\}$, and so in this specific case $X_1^* = 0$, meaning that $X_1^* \neq 0$ is strictly dominated. If $q < \tilde{a}$ and $\tilde{a} = p$ for $d_2 = 0$ the denominator of the inflection point x is 0, $\ln(\frac{p}{\tilde{a}}) = \ln(\frac{p}{p}) = \ln(1) = 0$, and so $x = 0$ concluding that also in this case strategy $X_1^* = 0$ is strictly dominant over $X_1^* \neq 0$. In case $d_2 = 1$, the equation becomes $x = -\frac{\ln(q)}{\ln(1-pq)}$, the denominator is always less than 0 and, recalling that $0 < q < 1$, we have $\ln(q) < 0$, hence $x < 0$ reaching the same conclusion of the previous case, that is, $X_1^* = 0$ is strictly dominant. The case $q < \tilde{a} < p$ leads to the same outcomes in cases as $\tilde{a} < q < p$ and $\tilde{a} \leq q$ with $q = p$ under condition of $d_2 = 0$, in fact $x = -\frac{\ln(p/\tilde{a})}{ln(1-p)}$ in which $-\ln(\frac{p}{\tilde{a}}) < 0$, therefore concluding with $x > 0$ that $X_1^* \neq 0$ is a non strictly dominated strategy. The last two cases confirming the strict dominance of $X_1^* \neq 0$ over the other strategies are $\tilde{a} < q < p$ and $\tilde{a} < q$ with $q = p$, considering $d_2 = 1$ this time. For the first case, the denominator of x becomes $-\ln\frac{qp}{\tilde{a}} < 0$, thus obtaining $x > 0$. The latter case $\tilde{a} < q$ with $q = p$ works under the prior assumption that $p^2 > \tilde{a}$, thus for the denominator of the inflection point x, we have $-\ln\frac{p^2}{\tilde{a}} < 0$, which results in $x > 0$ as stated before. □

APPENDIX F
PROOF OF COROLLARY IV.1.1

From (13), we know that $x = \frac{\ln\left(\tilde{a}^{-1}pq^{d_2^*}\right)}{\ln\left(1-pq^{d_2^*}\right)^{-1}}$, which in turn implies $x = \frac{\ln\left(\tilde{a}^{-1}pq\right)}{\ln(1-pq)^{-1}}$. Following either $\tilde{a} < p < q$ or $\tilde{a} < q < p$, we end up into one of the cases listed in the previous theorem, which implies that the border value $X_1 = 0$ cannot be the best choice, which is instead in a local maximum $X_1^* \neq 0$ that represents a strictly dominant strategy. □

REFERENCES

[1] M. Borgo, B. Principe, L. Spina, L. Crosara, E. Gindullina, and L. Badia, "Attack strategies among prosumers in smart grids: A game-theoretic approach," in *Proc. IEEE icSmartGrid*, 2023, pp. 01–06.

[2] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication technologies for smart grid: A comprehensive survey," *Sensors*, vol. 21, no. 23, p. 8087, 2021.

[3] D. Brown, S. Hall, and M. E. Davis, "Prosumers in the post subsidy era: an exploration of new prosumer business models in the UK," *En. Policy*, vol. 135, p. 110984, 2019.

[4] N. Patrizi, S. K. LaTouf, E. E. Tsiropoulou, and S. Papavassiliou, "Prosumer-centric self-sustained smart grid systems," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6042–6053, 2022.

[5] D. Roana, S. Boscolo, L. Crosara, L. Badia, and E. Gindullina, "Strategic energy trading among prosumers in a smart grid," in *Proc. IEEE icSmartGrid*, 2023, pp. 01–06.

[6] A. Boumaiza, "Towards a blockchain-enabled transactive renewable energy trading market," in *Proc. IEEE icSmartGrid*, 2024, pp. 42–47.

[7] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, "The internet of energy: a web-enabled smart grid system," *IEEE Network*, vol. 26, no. 4, pp. 39–45, 2012.

[8] R. Bonetto, I. Sychev, and F. H. Fitzek, "Power to the future: Use cases and challenges for mobile, self configuring, and distributed power grids," in *Proc. IEEE SmartGridComm*, 2018, pp. 1–6.

[9] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "A game of age of incorrect information against an adversary injecting false data," in *Proc. IEEE Int. Conf. Cyber Security Resilience (CSR)*, 2023, pp. 347–352.

[10] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," vol. 4, no. 1, pp. 160–169, 2013.

[11] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comp. Netw.*, vol. 169, p. 107094, 2020.

[12] G. Cisotto and L. Badia, "Cyber security of smart grids modeled through epidemic models in cellular automata," in *Proc. IEEE WoWMoM*, 2016, pp. 1–6.

[13] X. G. Shan and J. Zhuang, "A game-theoretic approach to modeling attacks and defenses of smart grids at three levels," *Reliability Eng. Syst. Safety*, vol. 195, p. 106683, 2020.

[14] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.

[15] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *Int. J. Elec. Power En. Syst.*, vol. 104, pp. 169–177, 2019.

[16] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[17] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, 2016.

[18] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A stackelberg game analysis," *IEEE Trans. Autom. Control*, vol. 63, no. 10, pp. 3503–3509, 2018.

[19] Y. Xiang and L. Wang, "An improved defender–attacker–defender model for transmission line defense considering offensive resource uncertainties," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2534–2546, 2019.

[20] V. Vivek, R. B. Diddigi, and S. Bhatnagar, "Dynamic energy management in competing microgrids using reinforcement learning," in *Proc. IEEE ISGT*, 2024, pp. 1–5.

[21] A. Tolio, D. Boem, T. Marchioro, and L. Badia, "A Bayesian game framework for a semi-supervised allocation of the spreading factors in LoRa networks," in *Proc. IEEE Ann. Ubiq. Comp. Elec. Mob. Commun. Conf. (UEMCON)*, 2020, pp. 0434–0439.

[22] F. Alfaverh, M. Denai, and Y. Sun, "A dynamic peer-to-peer electricity market model for a community microgrid with price-based demand response," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 3976–3991, 2023.

[23] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Plasma Sci.*, vol. 34, no. 2, pp. 1513–1523, 2019.

[24] Y. Shang, "False positive and false negative effects on network attacks," *J. Stat. Phys.*, vol. 170, no. 1, pp. 141–164, 2018.

[25] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Sec. (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[26] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2019.

[27] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, 2017.

[28] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, 2019.

[29] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2016.

[30] S. K. Singh, K. Khanna, R. Bose, B. K. Panigrahi, and A. Joshi, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 1, pp. 89–97, 2018.

[31] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, 2017.

[32] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[33] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, 2019.

[34] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Scalable solutions of markov games for smart-grid infrastructure protection," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 47–55, 2013.

[35] A. Mahi-al rashid, F. Hossain, A. Anwar, and S. Azam, "False data injection attack detection in smart grid using energy consumption forecasting," *Energies*, vol. 15, no. 13, 2022.

[36] R. Huang, Y. Li, and X. Wang, "Attention-aware deep reinforcement learning for detecting false data injection attacks in smart grids," *Int. J. Elec. Power En. Syst.*, vol. 147, p. 108815, 2023.

[37] L. Canzian, L. Badia, and M. Zorzi, "Promoting cooperation in wireless relay networks through Stackelberg dynamic scheduling," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 700–711, 2013.

[38] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: A dynamic Bayesian game-theoretic approach," *ISA Trans.*, vol. 115, pp. 108–123, 2021.

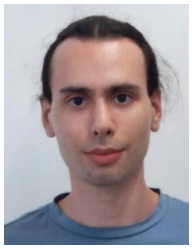
[39] C. Cappello, D. Zonta, and B. Glišić, "Expected utility theory for monitoring-based decision-making," *Proc. IEEE*, vol. 104, no. 8, pp. 1647–1661, 2016.

[40] K. Jhala, B. Natarajan, and A. Pahwa, "Prospect theory-based active consumer behavior under variable electricity pricing," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2809–2819, 2018.

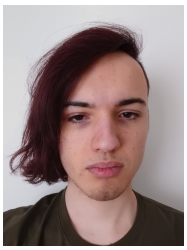
[41] N. Michelusi, K. Stamatiou, L. Badia, and M. Zorzi, "Operation policies for energy harvesting devices with imperfect state-of-charge knowledge," in *Proc. IEEE ICC*, 2012, pp. 5782–5787.

Leonardo Badia (Senior Member, IEEE) received the Laurea degree (Hons.) in electrical engineering and the Ph.D. degree in information engineering from the University of Ferrara, Italy, in 2000 and 2004, respectively. From 2002 to 2003, he was visiting scholar at the Radio System Technology Labs (currently, Wireless@KTH), Royal Institute of Technology, Stockholm, Sweden. After having been with the Engineering Department, University of Ferrara, he joined in 2006 the IMT Institute for Advanced Studies, Lucca, Italy. In 2011, he moved to the University of Padua, Italy, where he is currently Associate Professor. He published more than 250 research papers. His scientific interests include protocol design for multihop networks, cross-layer optimization of wireless communication, transmission protocol modeling, and applications of game theory to radio resource management. He is an active referee of research articles, having served on the editorial boards and still being a reviewer for many scientific periodicals, as well as technical program committee chair for conferences in the broad areas of communications and networking.

Mattia Borgo received the B.Sc. degree in Computer Engineering from the University of Padova, Italy, in 2021. He is currently pursuing his M.Sc. degree, also in Computer Engineering at the University of Padova. During his education, he has developed a strong foundation in data-driven methodologies and computational approaches. His research interests span from algorithmic game theory to machine learning.

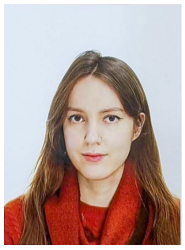


Bruno Principe received the B.Sc. degree in Computer Engineering from the University of Salerno, Italy, in 2021. He is pursuing his M.Sc. degree in Computer Engineering from the University of Padova, Italy. His current research interests include graph representation learning, machine learning, and data mining, including extensions to game theoretic methodologies, and algorithmic approaches.



Lorenzo Spina received the B.Sc. degree and M.Sc. degree, both in Computer Engineering, from the University of Padova, Italy, in 2021 and 2024, respectively. During his academic activity, he investigated web scraping and the application of autoencoders to enhance metagenomic binning. His research interests lie in the areas of machine learning and artificial intelligence, where he seeks to contribute innovative solutions.

Laura Crosara (Graduate Student Member, IEEE) received the B.Sc. degree in information engineering and the M.Sc. degree in ICT for Internet and multimedia engineering (both with honors) from the University of Padova, Italy, in 2019 and 2021 respectively. She is pursuing the Ph.D. degree in information engineering with the Department of Information Engineering at the University of Padova. Her current research interests include authentication techniques for global navigation satellite systems, physical layer security, and wireless communications.



Elvina Gindullina is R&I engineer in Hewlett Packard Enterprise Italia. She received the Ed.S. degree in Economics and Management at Enterprises (with honors) from Ufa State Petroleum Technological University, Russia, in 2013 and the M.S. degree (with honors) in applied mathematics and computer science from Ufa State Aviation Technical University, Russia, in 2015. In 2016, she joined the Horizon 2020 project SCAVENGE at the University of Padova, Italy, as an early-stage researcher, under the Marie Skłodowska-Curie Actions program, working on battery management and energy cooperation for energy harvesting IoT networks, which ultimately led to her PhD in 2020. During 2018, she conducted an internship in Worldsensing (Barcelona, Spain) as a research engineer. From 2020 to 2023 she was Research Assistant at the University of Padova, Italy, where she lectured on game theory and contributed to an interdisciplinary bio-engineering project focused on developing and analyzing models and methods for estimating effective connectivity in whole-brain networks.