Attack Strategies Among Prosumers in Smart Grids: A Game-Theoretic Approach

Mattia Borgo, Bruno Principe, Lorenzo Spina, Laura Crosara, and Leonardo Badia
Department of Information Engineering, University of Padova, Italy
{ mattia.borgo@studenti., bruno.principe@studenti., lorenzo.spina@studenti., laura.crosara.1@phd., leonardo.badia@} unipd.it

Elvina Gindullina
R&I, Athonet Srl
Vicenza, Italy
elvina.gindullina@athonet.com

***Abstract*—Smart grids provide the 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 propose a novel game-theoretic model for 2 prosumers of a smart grid, acting as players that can both attack and defend themselves, 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 equilibria solutions. The obtained results may serve as guidelines to understand the performance of smart grid systems and handle reliability issues.**

***Index Terms*—Cyberattacks; Game theory; Energy harvesting; Energy trading; Smart grids.**

I. Introduction

Smart grids enable two-way communication and data exchange between power generators, consumers, and grid operators so as to improve the efficiency, reliability, and sustainability of electricity generation, distribution, and consumption [1], [2]. They are a special instance of a network system, where nodes are the energy consumers, requiring energy and being supported by a high-developed communication and control system, and some special nodes, called *prosumers*, are entities capable to utilize but also generate energy, e.g., through solar cells or other forms of energy harvesting [3]–[5].

Due to their high reliance on cybercomponents, smart grids are also vulnerable to cyberattacks from both external actors and internal participants. A particularly malicious type of attack as an example is false data injection (FDI), during which adversaries sabotage the communication through data alteration, resulting in bad choices of the network possibly leading to a global collapse [6]. FDIs are often assumed to be committed by an outside attacker [7]–[10], but inner nodes of the grid may use them to damage neighboring competitors and take their place [11]. In this paper, we focus on the latter case.

This problem was studied via several methodologies, such as bi-level (attackers and defenders) models that allow sequential and security-constrained economic dispatch [12]. These models work under the strong assumption of complete knowledge for players, which is not generally valid in real-life scenarios [13]–[15]. Moreover, they consider the problem only from the attacker's perspective.

Another set of investigations handles the case of incomplete information, such as Q-learning that has been used to identify the optimal strategy of attack [16], or attack region identification for unknown topologies by adding lines with arbitrary reactance values [15], and an adaptation of matrix theory to case of incomplete information [17]. Such algorithms mainly provide approximate solutions via heuristics.

Some more studies took the perspective of the defender, and they examined its protection; however, identifying secure measurements is often NP-hard [18]. Detection schemes have adopted for example a joint transformation combined with Kullback–Leibler distance [19] and short-term state forecasting considering temporal correlation [20]. Artificial intelligence approaches are also used, such as those based on deep supervised learning [21], as well as reinforcement learning through the SARSA algorithm [22]. These latter models are evaluated assuming that decisions made by one of the two parties (attackers, defenders) do not condition future decisions of the other, which is reasonable only provided that security is seen no longer be seen as a binary property, but rather as a probabilistic measurement on the resilience and mitigation of the system, which unfolds into a complex analysis [23]. Another proposed detection approach is a novel forecasting-aided anomaly detection system that uses an CNN-LSTM based sequence-to-sequence autoencoder to combat against FDI attacks via a two-stage approach: forecasting and detection of anomalies within the forecasting [24].

A deep learning architecture was also used in [25] to discover the exact locations of data intrusions in real-time. A detection method was developed for FDI attacks based on reinforcement learning with attention. This makes it easier for the model to focus on the state parameters that show whether an attack was launched.

These approaches only take into account one side of the decision process (either attackers or defenders) and did not look at the totality of players in the environment. To study both sides of cybersecurity attacks, we can think of implementing a game theory rationale [26], [27]. In this spirit, multiple re-interpretations of this same scenario can be framed as static games, such as zero-sum games to identify defense and attack measurements in electricity markets [7] or to optimize the deployment of PMUs [28]. Also, it is possible to adopt Stackelberg games [29] to decide which sensors to attack, in the cases of 1 [30] up to n [31] different adversaries, or games of incomplete information [32]. Finally, an interpretation of

the problem as a bi-level multi-stage Bayesian game where players use the game history to update the beliefs was adopted to identify the total losses caused by all FDI attacks that target a specific measurement [6].

The contribution of this paper is to analyze a model where prosumers compete to provide service to a consumer. Each of the prosumers is interested in selling its over-production of energy to the consumer, and they may attack each other with cyber-threats to gain this spot. The consumer will choose the prosumer that can generates the most of energy and is unscathed by the cyberattack. The prosumers decide whether to *attack* each other and whether or not they are willing to *defend* themselves. This is formalized as a strategic interaction, i.e., a game, for which we derive equilibria and infer practical conclusions, also through numerical practical evaluations.

The rest of this paper is organized as follows. Section II deals with the game-theoretic model of our solution, and we derive the pure Nash equilibria in II-A, its general strict dominance relations in II-B and the mixed Nash equilibria in II-C. The model is analyzed numerically in Section III, which leads to the conclusions and future research directions in Sections IV.

II. Game theoretical model

We consider a pair of prosumers denoted as 1 and 2. Their action set is defined as $A_i = \mathbb{N} \times \{0,1\} \ni (X_i, d_i)$, where X_i is the number of attacks launched by i and d_i is a binary flag denoting the self-defense choice of i. In the general case of $n > 2$, multiple entries of X are associated with various targets of the attack. Further, we define the utilities associated with each strategy. We assume that each player acts 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

$$c_i\left(X_i, d_i\right) = a_i X_i + b_i d_i\,. \tag{1}$$

We denote the generation of prosumer i as E_i^{out}, whereas the consumer asks for an amount of power equal to 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 power parameters are common knowledge, therefore, without loss of generality, we assume that the prosumers are ordered w.r.t. E_i^{out}, that is, $E_1^{\text{out}} \leq E_2^{\text{out}}$. Each attack may succeed and defense may fail with probabilities $p > 0$ and $q < 1$, respectively: when an attack is successful we say it to be *effective*. If an effective attack is performed against an ineffectively-defended prosumer, this prosumer will not be able to provide enough power to the consumer, therefore it will not be selected. A prosumer is ineffectively-defended if they do not choose to defend themselves.

By considering expected utilities, we can write

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

One can see that player 2 has no incentive to attack player 1, as its utility only decreases — any strategy with $X_2 \neq 0$ is strongly dominated by the equivalent with $X_2 = 0$; a similar argument can be made regarding d_1, where $d_1 = 0$ strongly dominates $d_1 = 1$. We can further simplify (2) to

$$u_1'\left(X_1, d_2\right) = \left(1 - \left(1 - pq^{d_2}\right)^{X_1}\right) E^{\text{ask}} - a_1 X_1 \tag{3}$$

$$u_2'\left(X_1, d_2\right) = \left(1 - pq^{d_2}\right)^{X_1} E^{\text{ask}} - b_2 d_2 \tag{4}$$

A. Pure Nash equilibria

If $E^{\text{ask}} = 0$ then both utilities are reduced to pure costs, and the only pure Nash equilibrium 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 made before becoming counterproductive. The pure Nash equilibria are strategies X_1^*, d_2^* satisfying both

$$X_1^* = \arg\max_{X_1} u_1'\left(X_1, d_2^*\right) \tag{5}$$

$$d_2^* = \arg\max_{d_2} u_2'\left(X_1^*, d_2\right) \tag{6}$$

Substituting (4) in (6) we have that

$$\begin{aligned} (1-pq)^{X_1^*} - (1-p)^{X_1^*} \leq \tilde{b} &\implies d_2^* = 0 \\ (1-pq)^{X_1^*} - (1-p)^{X_1^*} \geq \tilde{b} &\implies d_2^* = 1 \end{aligned} \tag{7}$$

whereas for (5), we exploit (3) and solve the maximization by relaxing the constraint $X_1 \in \mathbb{N}$, obtaining

$$X_1^* = \arg\max_x \left(1 - \left(1 - pq^{d_2^*}\right)^x - \tilde{a}x\right) \tag{8}$$

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

$$\begin{aligned} &\Delta\left(1 - \left(1 - pq^{d_2^*}\right)^x - \tilde{a}x\right) \\ &= \left(1-pq^{d_2^*}\right)^x - \left(1-pq^{d_2^*}\right)^{x+1} - \tilde{a} = \left(1-pq^{d_2^*}\right)^x pq^{d_2^*} - \tilde{a} \end{aligned} \tag{9}$$

with Δ denoting the *forward difference operator*, that is, $(\Delta T)(x) = T(x+1) - T(x)$.

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 (9) is equal to $-\tilde{a}$ and therefore the optimal x is $x = 0$; 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*, in which prosumer 1's attacks will always be effective. Then, (9) 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

$$x = \frac{\ln\left(\tilde{a}^{-1} pq^{d_2^*}\right)}{\ln\left(1 - pq^{d_2^*}\right)^{-1}} \tag{10}$$

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

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

d_2^*	X_1^*	x from (9)	u_1' (relative 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 $x \in \mathbb{N}$

In (7), $p > 0$ and $pq > 0$, $(1-p)^x$ and $(1-pq)^x$ are both decreasing functions of x; as a result, substituting X_1^* we get

$$\begin{aligned}&(1-pq)^{\max\{\lceil x \rceil, 0\}} - (1-p)^{\max\{\lceil x \rceil, 0\}} \\ &= \max\left\{(1-pq)^{\lceil x \rceil} - (1-p)^{\lceil x \rceil}, 0\right\}.\end{aligned} \tag{11}$$

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

$$\begin{aligned}\max\{a, b\} \leq c &\iff a \leq c \wedge b \leq c \\ \max\{a, b\} \geq c &\iff a \geq c \vee b \leq c\end{aligned} \tag{12}$$

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

B. 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 it is split as for the pure Nash equilibria.

If $E^{\text{ask}} = 0$, (3) becomes $-a_1 X_1$, (4) 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 Nash equilibria.

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 $p < 1$, (3) becomes

$$\left(1 - \left(1 - p[d_2 = 0]\right)^{X_1}\right) - \tilde{a} X_1 \tag{13}$$

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

$$(1 - p[d_2 = 0])^x < (1 - p[d_2 = 0])^{x+1} + \tilde{a} \tag{14}$$

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

$$x > \frac{\ln\left(\tilde{a}^{-1} p\right)}{\ln(1-p)^{-1}} \tag{15}$$

and therefore the remaining choices for X_1 are finite.

If $E^{\text{ask}} > 0$ and $q > 0$ but $p = 1$, (3) becomes

$$\left(1 - (1 - q^{d_2})^{X_1}\right) - \tilde{a} X_1 \tag{16}$$

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

$$\left(1 - q^{d_2}\right)^x < \left(1 - q^{d_2}\right)^{x+1} + \tilde{a} \tag{17}$$

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

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

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

$$x > \frac{\ln\left(\tilde{a}^{-1} p q^{d_2}\right)}{\ln\left(1 - p q^{d_2}\right)^{-1}} \tag{19}$$

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

C. Mixed Nash equilibria

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

$$\tilde{b} < \inf_x \left((1-pq)^x - (1-p)^x\right) \tag{20}$$

that requires $\tilde{b} < 0$ for the case $x = 0$. Yet, $d_2 = 0$ can strictly dominate $d_2 = 1$ as in the 4 following cases from

$$\tilde{b} > \sup_x \left((1-pq)^x - (1-p)^x\right). \tag{21}$$

1) The case $p = 1$ and $q = 0$: For the dominance condition, (21) is in this case equivalent to $\tilde{b} > 1$; this corresponds to one or both of the first two pure Nash equilibria in Table I. When $\tilde{b} \leq 1$, two cases follow. (i) $\tilde{a} = 1$: in this case, $X_1 = 0$ is equivalent to $X_1 = 1$ as far as payoffs are concerned; therefore strategies of the form $\beta \langle X_1 = 0 \rangle + (1-\beta) \langle X_1 = 1 \rangle$ are a Nash equilibrium when joined by $d_2^* = 0$ with the condition that $\beta \geq 1 - \tilde{b}$. Or (ii) $\tilde{a} < 1$: there are two strategies for each player none of which are dominated. Therefore, we can compute a mixed Nash equilibrium 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 satisfied for $\alpha=\tilde{a}$ and $\beta=1-\tilde{b}$. Therefore, we have a mixed Nash equilibrium with

$$\begin{aligned}(1-\tilde{b})\langle X_1^*=0\rangle+\tilde{b}\langle X_1^*=1\rangle\\ \tilde{a}\langle d_2^*=0\rangle+(1-\tilde{a})\langle d_2^*=1\rangle\end{aligned}\tag{22}$$

and there are no other mixed Nash equilibria.

2) The case $p<1$ and $q=0$ (perfect defense): Firstly, (21) 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 Nash equilibrium, namely the third one in Table I. 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 Nash equilibrium 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

$$\frac{(1-p)^{j-i}\left(1-(1-p)^{k-j}\right)}{1-(1-p)^{j-i}}=\frac{k-j}{j-i}.\tag{23}$$

The left-hand side 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, the equality never holds, and there cannot be more than two values in the support of any mixed Nash equilibria. We are left with 4 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' solved for α as given above, whereas for β we get

$$(1-\beta)(1-p)^j+\beta(1-p)^i=1-\tilde{b}\tag{24}$$

$$\text{whose solution is}\quad \beta=\frac{1-(1-p)^j-\tilde{b}}{(1-p)^i-(1-p)^j}.\tag{25}$$

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

$$\forall k\neq i.\ \frac{1-(1-p)^{j-i}}{j-i}\geq\frac{1-(1-p)^{k-i}}{k-i}.\tag{26}$$

As the function $\frac{1-(1-p)^x}{x}$ is decreasing in x, an interesting observation can readily be made: if $i\neq 0$, setting $k=0$ is a valid choice in the function above; but then, as $i<j$, the left-hand side with parameter $0<j-i$ will always be lower than the right-hand side. On the other hand, when $i=0$ then the lowest k can go is $k=1$, which therefore forces $j=i+k=1$. Ultimately, we have a mixed Nash equilibrium with

$$\begin{aligned}\left(1-\frac{\tilde{b}}{p}\right)\langle X_1^*=0\rangle+\frac{\tilde{b}}{p}\langle X_1^*=1\rangle\\ \frac{\tilde{a}}{p}\langle d_2^*=0\rangle+\left(1-\frac{\tilde{a}}{p}\right)\langle d_2^*=1\rangle\end{aligned}$$

which only exists for $\tilde{a},\tilde{b}<p$. For $\tilde{a}=p$ a similar mixed Nash equilibrium 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 (22) 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 Nash equilibrium. The argument distinguishes 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 argument 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 $\alpha=1-\frac{\tilde{a}j-1}{(1-q)^j}$. It is however known from (18) 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 then left with the only remaining case, namely $i>0$. 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 $i>0$ unfortunately implies that $\alpha=1$, which is also impossible (it would require $i=j$). Ultimately, there are no mixed Nash equilibria for this case. We note that in handling it, we did not refer to (21), which is true when $\tilde{b}>1-q$, and indeed does not need to be exploited. For a more rigorous analysis one can note that said condition would hold for β to be valid in the first place.

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

$$\alpha=\frac{\tilde{a}(j-i)-((1-pq)^i-(1-pq)^j)}{((1-p)^i-(1-p)^j)-((1-pq)^i-(1-pq)^j)}.\tag{27}$$

This value is in the correct range only if

$$(1-pq)^i-(1-pq)^j<\tilde{a}(j-i)<(1-p)^i-(1-p)^j\tag{28}$$

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

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

By contrast, equilibrium inequalities are complex and do not easily admit analysis. A detailed study is left for future research.

III. Numerical analysis

For a better understanding of the results, we consider some practical numerical evaluations.

Fig. 1 shows the values of X_1^* for the third Nash equilibrium in Table I 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. Its formula is readily obtained from the definition of x, and namely it is $x^*=\frac{1-p}{p}$. As a function of $\tilde{a}$, it decreases exponentially since $\tilde{a}$ becomes very small (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 each attack always prevails, and overwhelms the diminishing

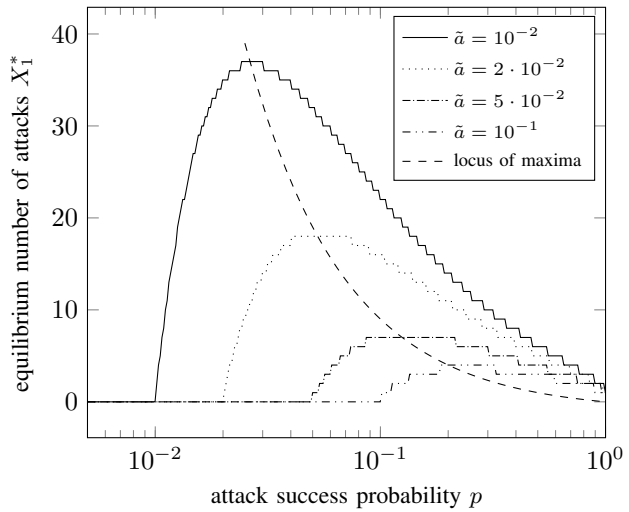

Fig. 1. Number of attacks at equilibrium X_1^* as a function of attack success probability p for various relative attack costs $\tilde{a}$.

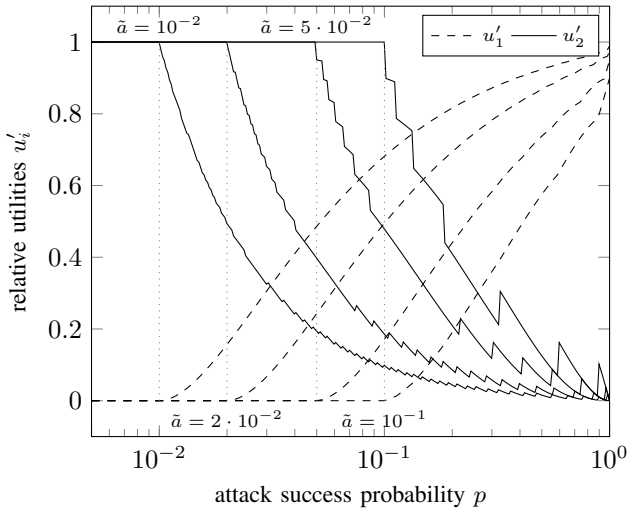

Fig. 2. Relative utilities of attacker (u_1') and defender (u_2') vs. attack success probability p for various relative attack costs $\tilde{a}$.

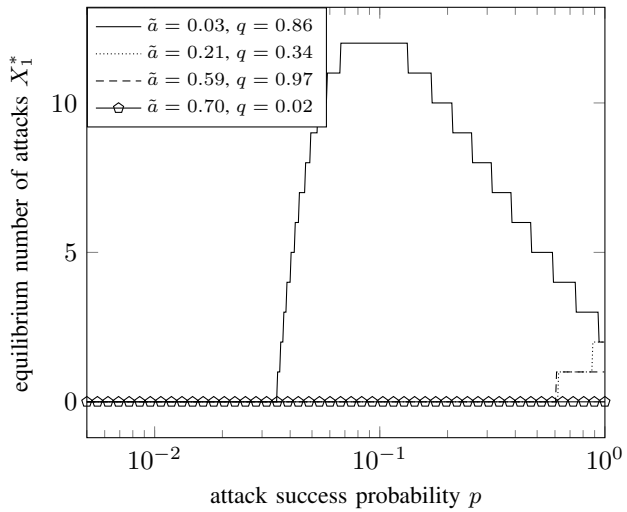

Fig. 3. Number of attacks at equilibrium X_1^* vs. attack success probability p for various values of defense failure probability q and relative attack cost $\tilde{a}$.

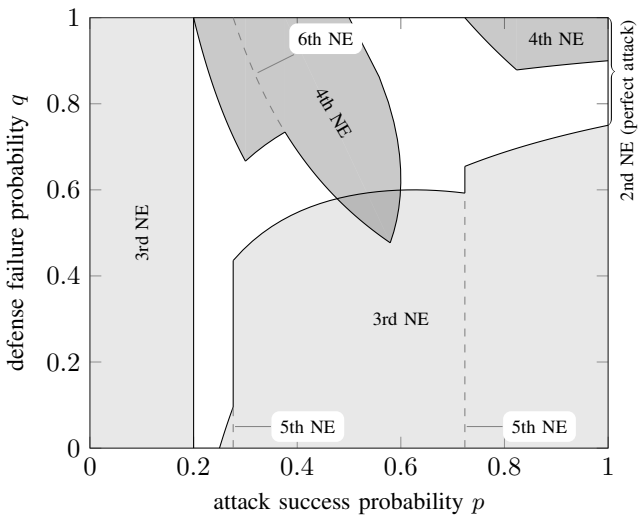

Fig. 4. Pure Nash equilibria as a function of attack success probability p and defense failure probability probability q with relative attack cost $\tilde{a} = \frac{1}{5}$ and relative defense cost $\tilde{b} = \frac{1}{4}$. Nash equilibria numbered as per Table I.

gain that is expected from it. This occurs up until $p = \tilde{a}$, at which point there is no more incentive to attack.

Relative 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. It is interesting that, in the case of no defense, u_2' is not monotonically decreasing; this is especially evident in the jagged case $\tilde{a} = 10^{-1}$. A 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 repeats the same analysis, but considering an increasing value of $\tilde{a}$ and a decreasing value of q as a function of p to see how many attacks a prosumer can handle. It is expected that the number of attacks increases as the attack cost decreases and the probability of defense holding up increases. On the other hand, the higher the probability of a successful attack, the lower the number of attacks, to contain the costs.

Finally, Fig. 4 shows a phase diagram of the game, i.e., the areas for p and q in which the major pure Nash equilibria exist. The light-grey area is associated the third Nash equilibrium in Table I, 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 dark-grey shaded areas and dashed hyperbolic segments. It can be seen that in many ranges of p and q there is no pure Nash equilibrium, and that the two main ones coexist only for a small sliver of the domain. Nevertheless, such empty areas must include a mixed Nash equilibrium.

IV. Conclusions

We considered a smart grid scenario where prosumers contending for the role of energy supplier of a consumer can attack each other or enact some defense mechanism, which is

modeled a static game of complete information. Focusing on 2 prosumers, we studied the Nash equilibria and we analyzed the resulting model. A complex correlation between network parameter values and number, type, and associated utilities of Nash equilibria was discovered. For example, we found out that increasing the cost of an attack does not always correspond to a lower optimal number of attacks.

The model discussed in this paper can be generalized in various directions, such as introducing more than one consumer, each with its own E_i^{ask} or assuming partial knowledge over power parameters and probabilities p and q [33]. The topology of the grid can also vary in time, either due to natural dynamics or because of malicious interventions of some nodes [11], [34], 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 [29] or a dynamic-parallel interaction Bayesian game by introducing multiple player types [35]. All of these are interesting developments to be explored in future research.

REFERENCES

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

[2] Á. F. Gambin, E. Gindullina, L. Badia, and M. Rossi, "Energy cooperation for sustainable IoT services within smart cities," in *Proc. IEEE WCNC*, 2018.

[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] E. Gindullina, L. Badia, and X. Vilajosana, "Energy modeling and adaptive sampling algorithms for energy-harvesting powered nodes with sampling rate limitations," *Trans. Emerg. Telecommun. Techn.*, vol. 31, no. 3, p. e3754, 2020.

[6] 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.

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

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

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

[10] 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.

[11] 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.

[12] 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.

[13] V. Vadori, M. Scalabrin, A. V. Guglielmi, and L. Badia, "Jamming in underwater sensor networks as a Bayesian zero-sum game with position uncertainty," in *Proc. IEEE Globecom*, 2015.

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

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

[16] 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.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] G. Cavraro and L. Badia, "A game theory framework for active power injection management with voltage boundary in smart grids," in *Proc. IEEE ECC*, 2013, pp. 2032–2037.

[27] A. Blinovas, K. Urazaki, Jr, L. Badia, and E. Gindullina, "A game theoretic approach for cost-effective management of energy harvesting smart grids," in *Proc. IWCMC*, 2022, pp. 18–23.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, 2016.

[35] E. Gindullina and L. Badia, "Asymmetry in energy-harvesting wireless sensor network operation modeled via Bayesian games," in *Proc. IEEE WoWMoM*, 2017.