International Journal of Information Security (2020) 19:427–443
https://doi.org/10.1007/s10207-019-00460-z

REGULAR CONTRIBUTION

Security attacks on smart grid scheduling and their defences: a game-theoretic approach

M. Pilz[1] · F. Baghaei Naeini[1] · K. Grammont[2] · C. Smagghe[2] · M. Davis[1] · J.-C. Nebel[1] · L. Al-Fagih[1,3] · E. Pfluegel[1]

Published online: 9 August 2019

Abstract

The introduction of advanced communication infrastructure into the power grid raises a plethora of new opportunities to tackle climate change. This paper is concerned with the security of energy management systems which are expected to be implemented in the future smart grid. The existence of a novel class of false data injection attacks that are based on modifying forecasted demand data is demonstrated, and the impact of the attacks on a typical system's parameters is identified, using a simulated scenario. Monitoring strategies that the utility company may employ in order to detect the attacks are proposed, and a game-theoretic approach is used to support the utility company's decision-making process for the allocation of their defence resources. Informed by these findings, a generic security game is devised and solved, revealing the existence of several Nash equilibrium strategies. The practical outcomes of these results for the utility company are discussed in detail, and a proposal is made, suggesting how the generic model may be applied to other scenarios.

Keywords Cyber security · Game theory · Smart grid · False data injection · Defence strategies · Decision-making · Optimal resource allocation

1 Introduction

During the last decade, the rise of the smart grid has shown significant potential to address not only the traditional grid problems but also support the development of power generation from renewable sources. Indeed, since electricity suppliers must meet customers' demand during peak hours, they traditionally invest in power generation capacity able to sustain those high power consumption periods. This is an expensive solution as some of those resources are only exploited sporadically. On the other hand, with the increase in greenhouse gases that impact negatively on the Earth's ecosystem, better exploitation of renewable energy sources is seen as a way to reduce their emissions [29]. However, their inherent intermittency and unpredictability make their integration into the power grid particularly difficult. Therefore, management of consumption and production plays a crucial role to facilitate power distribution as well as reduction in cost for both suppliers and consumers [27].

Traditional Demand-Side Management has designed strategies to change consumers' consumption patterns so that they better match energy generation profiles: these include peak clipping, load shifting, and flattening consumers' loads [12]. Advancements in energy storage and renewable energy generation provide further opportunities to devise smarter and efficient power grids. For instance, storing energy during off-peak times eases supply during peak hours where there is high demand. Furthermore, local electricity generation reduces substantially power dissipation and transmission costs. Accordingly, the concept of 'microgrids' was introduced to facilitate distribution by dividing the power grid into several smaller local grids [45]. Efficient management of these microgrids requires a two-way communication system between suppliers and consumers, so that those smart grids can exploit distributed information for storage scheduling and pricing purposes [16].

✉ M. Pilz
Matthias.Pilz@kingston.ac.uk

[1] School of Computer Science and Mathematics, Kingston University, London KT12EE, UK

[2] ENSICAEN, UNICAEN, CNRS, Normandie Université, Caen, France

[3] Division of Engineering Management & Decision Sciences, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

Taking advantage of smart meters, energy storage, and trading strategies, a variety of energy consumption scheduling techniques aiming at optimally distributing daily power consumption have been put forward to reduce a smart grid's peak-to-average ratio (PAR) of the aggregated load. In particular, dynamic game-theoretic frameworks have been proposed to optimise energy cost using their Nash equilibrium [25,26]. Some consider advanced battery models [32] and integrate forecasting errors [31]. Alternatively, usage of a Stackelberg game minimising both the PAR and the system total cost has also proved promising [41]. More generally, comprehensive reviews reveal the significant contribution that game-theoretic solutions offer in terms of reducing consumer costs and PAR values [10,13,30,37,40].

Although those solutions are becoming more sophisticated, the smart grid can only be realised once appropriate security measures are in place. None of these papers [25,26, 31,32,41] are concerned with the security of the respective systems. Since smart grids rely on a communication network and smart meters, they may be vulnerable to cyber attacks [24]. As a result, appropriate defence strategies need to be put in place [14,20,36,42,46,50]. The main issue is the robustness and security of the communication channel between the smart meter and the utility company. Typically, the smart meter connects to the home Local Area Network (LAN) and from there to the Wide Area Network (WAN). Recently, there has been a move towards the systematic adoption of so-called Home Area Networks (HANs) for communication within the end-user's home.

HANs are based on wireless communication using Internet of Things (IoT) technologies and protocols, and over time, this will involve a more and more diverse and large number of devices, appliances, vendors, and protocols, lacking of compatibility and standards—in particular, in the area of security. As mentioned in [6], there are two particularly worrying trends in HANs: the increased usage of external cloud providers in order to cope with the growing number of data and the lack of security awareness and commitment on behalf of end-users who opt for convenience rather than precaution. We argue that all these phenomena lead to a rapidly growing attack surface of the smart meter system, making interception and modification of HAN traffic including forecasting data more realistic, easier, and probable. Thus, the most pressing security attacks on a smart home environment are typical examples of novel IoT security challenges that require specific and novel security mitigation techniques. In this paper, we propose the use of game theory in order to address these attacks.

False data injection (FDI) is one of the most common approaches to attack cyber-physical systems [21]. In general, FDI attacks target data integrity breaches to make profit or disturb a system. Since, in power grids, state estimators are the main data sources used for monitoring and controlling purposes, they are the target of data injection [19]. Such FDI attacks and possible defence strategies have been investigated in several scenarios: (i) the 'ideal' undetectable attack where the attack vector is built from complete knowledge of the state estimators' parameters [20]; (ii) a more realistic attack relying on a probability distribution function where only incomplete information about the system's parameters is available [35]; (iii) a stealth data injection in which an attacker has complete information about the system's topology [15]. Detection of cyber attacks and associated defence strategies is essential for a reliable grid. For instance, a fast detection algorithm has been proposed to deal with FDI and jamming attacks in smart grids [17].

Since game theory has been successful to design cyber security solutions [47], it has been applied in several scenarios dealing with grid security. When attackers target either a single or multiple state estimators, both Markovian and static strategies have been investigated to defend against load redistribution attacks by allocating optimal budgets to energy suppliers [48]. If attackers manipulate price information from the utility companies, the resulting impact can be mitigated exploiting a Stackelberg formulation [23]. Furthermore, it has been proposed to defend against coalitional attacks by multiple attackers using an iterated game-theoretic model [51], where a probability of attack detection is considered in each iteration: correlation between payoffs and penalty factors demonstrated the effectiveness of the defence system. A defence system against switching attacks based on a zero-determinant iterative game between controller and attacker showed that transient stabilisation could be achieved over time [11].

A different security game in [18] is proposed, which considers a variety of risk assessment measures integrated to a stochastic game to choose the best defence strategies. The simulated results illustrate that a conditional value-at-risk measure enables the defender to prioritise the most significant attacks. Moreover, a scenario with multiple adversaries and a single defender in smart grids is studied [38]. This framework considers two Stackelberg games to analyse the interaction between attackers and the defender. To solve the hybrid Nash equilibrium game, a search-based algorithm is introduced, showing that the defender can achieve the minimal loss by protecting a limited number of parameters. Also, the results indicate that multiple attackers can be destructive to each other leaving the smart grid unaffected. Another hybrid model in [52] proposes a hybrid zero-sum differential game and a stochastic zero-sum game for the physical layer and cyber layer, respectively. On the other hand, a multi-adversarial FDI attack is considered in [8] where the data are manipulated in the network transmission layer. In this scenario, the model is formulated by evolutionary game theory to maximise the adversaries' payoff in the grid. Although grid cyber security has been an active field of research, no defence scheme has yet been proposed to protect forecasting data in smart grids.

The contributions of this paper are as follows:

1. The design of a novel class of false data injection attacks, preserving average daily load in a smart energy scheduling system. The forecasted demand data are corrupted by a single attacker, targeting one or several households. Using extensive simulations, two families of attacks are investigated. The impact on both the PAR of the aggregated load and consumer bills as well as the resulting benefit for the attacker is analysed.
2. The design and analysis of an augmented security game for monitoring average-preserving false data injection attacks, based on a detailed model with strategies and payoff functions informed by the simulation findings. The conditions under which a pure Nash equilibrium exists are derived. This extends previous work by providing additional strategies and a more detailed payoff design, informed by the various cost and benefit functions of the utility company and the attacker.
3. To give practical guidelines to the utility company on how to protect itself against such attacks. The recommendations are based on combining a range of mitigation strategies and the results of the equilibrium analysis of the game, to aid the utility company with the decision-making process of investing in the security defence. The given advice is motivated by the simulation scenario, but can also be adapted to other situations. This is demonstrated using a concrete example.

This paper is organised as follows. The underlying smart grid management model is introduced in Sect. 2. Different types of attacks are developed, and their impacts are analysed in Sect. 3. A game-theoretic defence strategy for the utility company is proposed in Sect. 4. Finally, the paper is concluded in Sect. 5.

2 Smart grid management model

This section focuses on the description of the game-theoretic scheduling model used in a smart grid management model. After specifying the smart grid scenario including the battery model, cost function, and data specifications, the scheduling game is presented. Note that a more detailed description can be found in [31].

2.1 Scenario

The scenario of interest considers a residential neighbourhood comprised of M houses where each household is equipped with a smart meter. The set of households that participates in the demand-side management (DSM) programme is denoted by $\mathcal{N} \subset \mathcal{M}$, where $\mathcal{M}$ is the set of all households in the neighbourhood. The total number of participants is $N = |\mathcal{N}|$. It is assumed that all M households are served by the same utility company (UC).

Each day is split into T discrete intervals, where the set of all intervals is represented by $\mathcal{T}$. The DSM protocol runs as follows: the forecasted demand is sent to the UC where demand data are aggregated and sent to each DSM participant. Based on this input, the households play a dynamic non-cooperative game (cf. Sect. 2.2). Its outcome is a set of schedules, one for each household, that specify how they can make best use of their battery system. The households follow these schedules, even if their actual demand differs from the forecasted one. Instead of using a forecasting algorithm, random errors were added to actual demands in order to simulate a realistic average error of 8% in individual forecasted data as reported in [7]. More details about the process used to simulate realistic forecasts are given in Appendix 5.1.

Households that participate in the DSM scheme are equipped with a lithium-ion battery. The battery model includes charging, discharging, and self-discharging characteristics of the battery (cf. [31,32]). The decision of the player, i.e. how much they are charging or discharging the battery, is denoted by a.

The demand $d_m^t \geq 0$ of a household $m \in \mathcal{M}$ is defined as the amount of electricity that is needed to run all its appliances during the time interval $t \in \mathcal{T}$. Let l_m^t denote the load, i.e. the amount of energy drawn from the grid by household $m \in \mathcal{M}$ during the interval $t \in \mathcal{T}$. For the participants of the scheme, the load depends on the decision a_n^t taken at that specific interval. It combines the demand with the amount of energy that is charged or discharged by the battery $l_n^t = d_n^t + a_n^t$. Thus, the grid total load during interval t is given by $L^t = \sum_{m \in \mathcal{M}} l_m^t$.

In order to incentivise a reduction in load at peak times, the UC charges the DSM participants using a dynamic pricing tariff: the cost per energy unit is based on the aggregated load of all users and is calculated separately for each interval. As in [26,49], this is expressed by a quadratic cost function $g^t(y) = c_2 \cdot y^2 + c_1 \cdot y + c_0$, where y is the aggregated load at time t given by L^t and the coefficients are $c_2 > 0$, $c_1 \geq 0$, and $c_0 \geq 0$. The electricity bill B_n (cf. [26,32,41]) of each participant is given by:

$$B_n = -\Omega_n \sum_{t \in \mathcal{T}} g^t\left(L^t\right) \quad \forall n \in \mathcal{N}, \tag{1}$$

where $\Omega_n = \frac{\sum_t l_n^t}{\sum_t \sum_k l_k^t}$.

2.2 The scheduling game

Formally, the game used to schedule battery usage is a discrete time dynamic game, in which players, i.e. households, have to decide how to use their battery during each individual interval of the upcoming day. In this game, each household has the objective to minimise their own costs as defined by the electricity bill (1). As the electricity bill itself depends on the aggregated load, the selfish behaviour of each individual indirectly leads them to minimising the peak-to-average ratio of the aggregated load (cf. [41]). It is defined as

$$\mathrm{PAR} = T \cdot \frac{\max_{t \in \mathcal{T}} L^t}{\sum_{t \in \mathcal{T}} L^t} \, . \tag{2}$$

The theoretically optimal result is a perfectly flat curve with a PAR value equal to 1.0. Since the mathematical details of the game mechanics lie outside the scope of this manuscript, the interested reader should refer to [31] for a thorough description. In the following, the scheduling game is treated as a black box that takes forecasted demand data as an input and then outputs schedules (one for each household) of 'optimal' battery usage for the upcoming day as defined by its Nash equilibrium. A Nash equilibrium (NE) strategy has a local maximum property: any single player deviating from the NE strategy will suffer a reduced payoff. It is important to note that only unilateral strategy changes are considered in this concept. Hence, applying game theory for real-life scenarios is only a valid and useful tool if all participants agree to adopt it as a contract for strategic decision-making, in the modelled scenario.

Figure 1 shows an example of the scheduling impact of the game on the aggregated load for one day. Whereas the load profile without playing the game shows the usual peaks in the morning and evening, it is possible to obtain a relatively flat profile by means of the scheduling game. The first row of Fig. 9 (in Appendix 5.2) illustrates actual battery usage of each household using a battery. As the dashed curve in the last row of Fig. 9 shows, the higher the participation to the game, the flatter the aggregated load.

2.3 Experimental setup

Throughout the paper, all simulations are performed for a neighbourhood of $M = 25$ households over a period of 365 consecutive days to allow for statistical analysis of the outcomes. Each day is split into $T = 24$ intervals. The respective demand data are taken from [44]. Every participant of the DSM scheme is equipped with the same type of battery, i.e. the Tesla Powerwall 2 (cf. [43]). Battery characteristics such as efficiency, capacity, charging and discharging rates, and degeneration behaviour are read off its data sheet. This setup is deliberately chosen to be similar to the one investigated in [31,33] to allow for comparison of the outcomes.

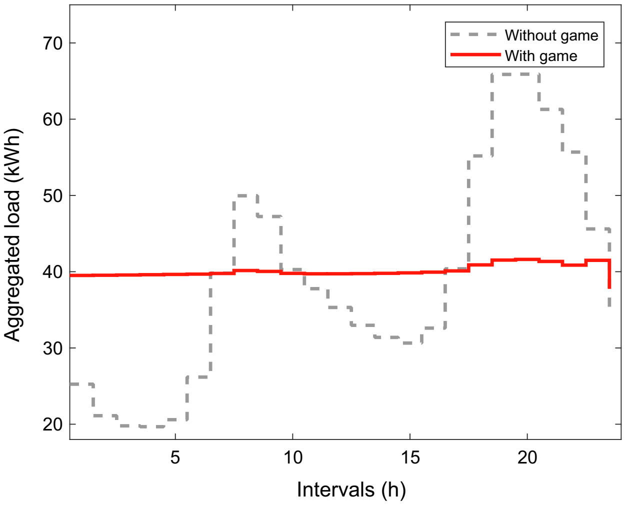

Fig. 1 Aggregated load comparison. The aggregated load of $M = 25$ households for a single day is shown for two scenarios: Without the game, and after playing the game. Every household is equipped with a battery. As players try to lower their electricity bill (1) (by means of their battery usage), they directly affect the load profile. In this example, the PAR value of the aggregated load (2) decreases from 1.69 to 1.04

3 False data injection on forecasts

As motivated in Sect. 1, the security of a smart energy system is of extreme importance and there is a lack of research on possible attacks on forecasted data. This section describes different types of potential attacks that may take advantage of the game-theoretic smart grid management model presented previously. Furthermore, outcomes of those attacks are analysed from the point of view of the attacker, the UC, and the other players. Various defence strategies to detect those attacks are proposed and analysed. Finally, attack mitigation is discussed.

3.1 Description of attacks

All attack scenarios investigated in this section rely on the following assumptions. First, the attacker (who is one of the players) exploits the vulnerability of the smart grid communication network: they have the ability not only to intercept forecasting data from all the other players, but also to replace them. Second, after the game has been played based on the tampered data, i.e. reached an equilibrium, the attacker adapts their storage schedule and takes advantage of the erroneous schedules that the other players follow. Finally, in order to limit the risk of having their attack detected, the attacker makes sure that the average daily aggregated load is not

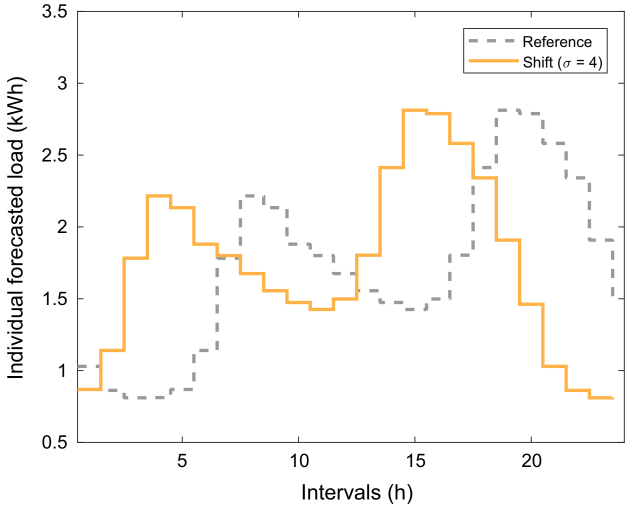

Fig. 2 Example of a shift attack. The reference curve shows the forecasted load of an individual household for the upcoming day. When the attacker applies the shift attack, they perform a circular shift of the interval data. The result of a shift with $\sigma = 4$ is shown as an example

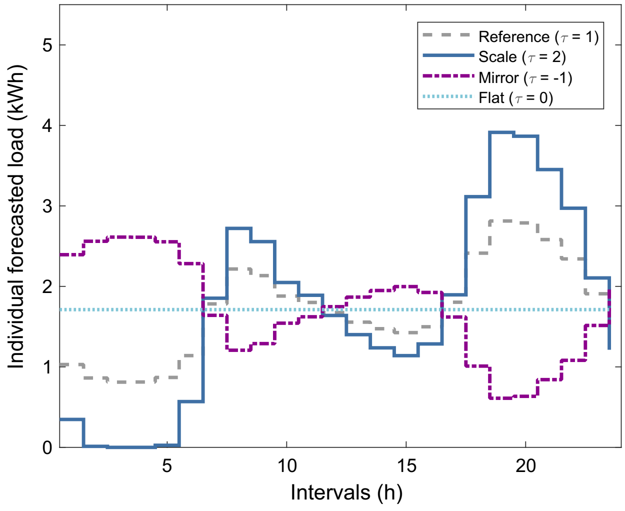

Fig. 3 Example of scale attacks. The reference curve shows the forecasted load of an individual household for the upcoming day. It is identical to the reference shown in Fig. 2. When the attacker applies the scale attack, they scale the interval data with respect to the daily average of the forecasted load. Scaling with a factor $\tau = 2$ leads to more severe troughs and peaks, while using $\tau = -1$ results in a mirrored forecast. $\tau = 0$ gives a perfectly flat load profile

affected by their actions. Although there are many strategies which can be applied to change forecasts while maintaining a constant aggregated value of the load, this study investigates two simple families of attacks: forecast shifting and scaling.

Shift Attack The shift attack replaces a given forecast with the original forecast after having undergone a circular shift of σ time intervals, where σ is an integer. Formally, we write the injected demand forecast $\tilde{d}_n^t$ as:

$$\tilde{d}_n^t = d_n^{t+\sigma} .$$

Since experimental results have shown that a shift attack of 4 hours, see Fig. 2, produces the most dramatic impact for the dataset of interest (cf. Sect. 2.3), that value is used for the rest of the study.

Scale Attack The scale attack substitutes a given forecast with a scaled version centred around its average value for the day. To ensure that the day average is not affected, the scaling parameter τ should be chosen such that no load becomes negative after scaling. Formally, we write the injected demand forecast $\tilde{d}_n^t$ as:

$$\tilde{d}_n^t = d_n^t + (\tau - 1) \cdot [d_n^t - \text{mean}] ,$$

where ‘mean’ is the average daily demand. Note that for the dataset of interest (cf. Sect. 2.3), a value of $\tau = 2$ remains acceptable: although a couple of values do become negative, they are set to 0; the day average is slightly increased, but it remains within a realistic forecast uncertainty (cf. Appendix 5.1). Figure 3 illustrates the effect of various scale attacks, i.e. $\tau = -1$, $\tau = 0$ and $\tau = 2$. While $\tau = 1$ returns the initial forecast, $\tau = 0$ and $\tau = -1$ produces a flat and mirrored forecast, respectively. In the rest of the paper, these two different attacks are called flat and mirror attack.

The outcome of an attack does not only depend on the type of attack and its associated parameter, but also on the number of forecasts which are replaced among all the players of a game: the higher the percentage ρ of attacked households, the more room for manoeuver the attacker has to profit from their attack.

3.2 Attack outcomes

3.2.1 Outcome for the attacker

Figure 4 illustrates the resulting load curves of attacker and victim in the case of a shift attack ($\sigma = 4$). The attacker benefits by having a high load during the periods when the victims have a low one and vice versa, so that the attacker’s higher consumption takes place when the aggregated load, and thus unit price, is low. This is exactly what the attacker tried to achieve by manipulating the forecasting data and thus the input to the scheduling game. More details about the cost function model are discussed in Sect. 2.1 and [30,34]. In this attack example, there is a high inverse correlation, i.e. ≈ -0.96, between the attacker’s load and the unit price.

An attacker’s financial benefit depends not only on the type of attack, but also the number of households using a battery, i.e. the participation rate N/M, as well as the proportion of

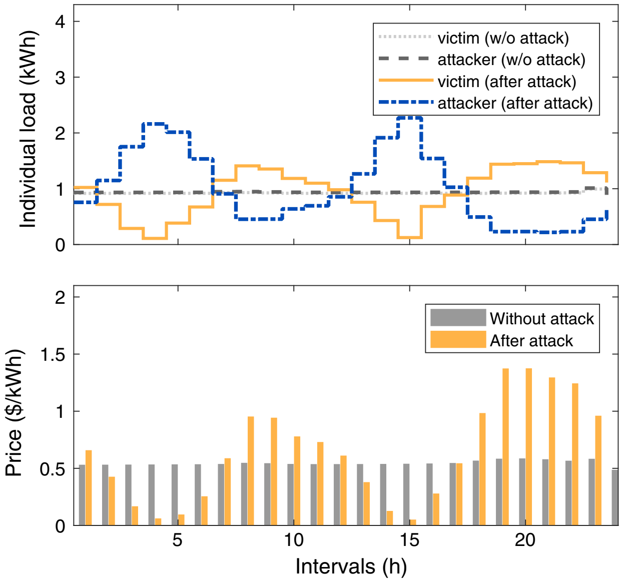

Fig. 4 Individual loads and unit price after scheduling. The top graph displays load profiles for one day of a randomly picked victim and the attacker for two different scenarios: with and without attack. While both references show an almost flat profile (cf. Fig. 1), the load curves after the attack differ considerably. This is a direct result of the attacker taking advantage of the falsely injected data. The bottom graph displays the change of price per unit during those two scenarios. As expected, the attacker's load has a high inverse correlation with the unit price (≈ -0.96)

targeted households ρ whose forecasts have been changed. In order to investigate this, attack simulations were conducted on a smart grid comprising $M = 25$ households for a duration of one year. Compared to the non-attack scenario, Fig. 5 displays the percentage change on the attacker's bill (yearly median of the daily changes) according to those parameters in the cases of shift ($\sigma = 4$), mirror ($\tau = -1$) and scale ($\tau = 2$) attacks. Simulations have revealed that a flat attack ($\tau = 0$) results in benefits similar to those of the shift attack ($\sigma = 4$) and is thus not shown.

Figure 5 reveals that for shift ($\sigma = 4$) and mirror ($\tau = -1$) attacks the attacker is never penalised by their action and their gains increase with both participation rate and percentage of targeted players. Bill reductions for the attacker reach up to 25.5% and 35.7%, respectively. However, in the case of the scale attack ($\tau = 2$), the graph displays a different picture: up to a relatively high participation rate ($N/M > 55\%$), the attacker is financially penalised by their attack. Indeed, while the other attacks lead players to charge their battery at a wrong time, this scale attack tends to make players charge their battery more than they need at a time when the attacker would also need to charge their battery. As Fig. 9 (cf. Appendix 5.2) reveals, when the participation rate is high, the aggregated load profile is inverted due to a large number of players charging their battery excessively at a time that was initially of low load and discharging their battery when a peak was expected. As a consequence, the aggregated load profile is now almost ideal for the attacker who can benefit from low prices at their time of high needs. Thus, they hardly need to use their battery and can gain up to 9.5% of bill reduction.

3.2.2 Outcome for the utility company and the other players

As mentioned in Sect. 2, for the utility company, the efficiency of a microgrid is assessed by its PAR value. Since attacks change the aggregated load, it is directly affected. The effect of the previously introduced attacks on PAR values is presented in Fig. 6. The different attack types are associated with a different graph, which presents several curves, each for a different percentage ρ of targeted players, showing the relationship between participation rates N/M and PAR values.

For the shift ($\sigma = 4$) and mirror ($\tau = -1$) attacks, an increase of ρ leads to a worsening of PAR values. Moreover, as in the non-attack scenario, PAR values tend to improve with an increase in participation rate. Note for the case of the mirror attack: if a high percentage of players are targeted, an increase in the participation rate contributes to the degradation of PAR values.

As analysed in the previous section, the outcomes of the scale attack ($\tau = 2$) are different from the others when the participation rate is below $N/M = 55\%$. In fact, Fig. 6 shows an improvement in the PAR values compared to the non-attack scenario when the percentage ρ of targeted players increases. Figure 9 clearly shows that at low participation rates the aggregated load is flatter than without an attack. The explanation is that this positive scaling incentivises participating households to work harder to flatten the load curve: As seen in Fig. 9, charging takes place at the same time but with a higher intensity. As a consequence, a 52% participation rate is sufficient to achieve a PAR that is similar to the one resulting from a 100% participation rate without any attack, i.e. PAR$=$1.11 and PAR$=$1.07, respectively. Participants work twice harder, which has the same effect as if everybody was working as they should. This extra work leads to higher bills for those households. An improved PAR value may suggest that the UC benefits from such attacks. In practice, this is not the case because in those scenarios the electricity bills of all players, including the attacker, increase substantially (data not shown), which will eventually lead to a loss of reputation and customers for the UC.

All attacks leading to the reduction in a single player's (the attacker) bill result in an increase in all the other players' bills by usually a comparable amount, see Tables 1 and 2. As a consequence, the aggregated bill for the whole neighbourhood is significantly increased. For example, a mirror ($\tau = -1$)

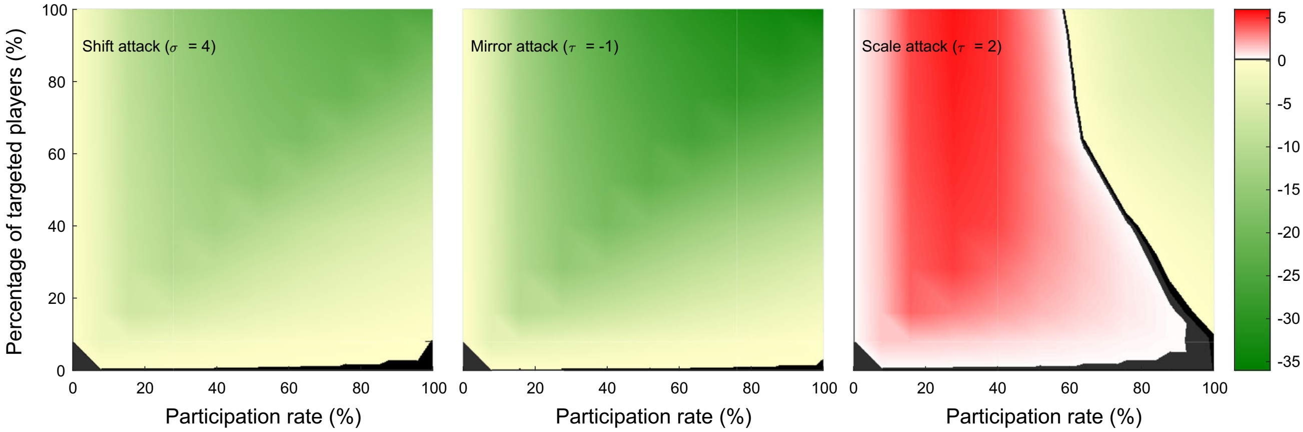

Fig. 5 Financial benefit for the attacker. The median change (compared to the non-attack scenario) over 365 days of the energy bill for the attacker is shown in per cent. The outcomes for three different attacks, i.e. shift attack with $\sigma = 4$, mirror attack, and scale attack with $\tau = 2$, are presented. The simulations were performed for $M = 25$ using various participation rates and percentages of targeted players. While the first two attacks display similar benefits, the third one indicates that for specific scenarios the attacker also has an increased electricity bill

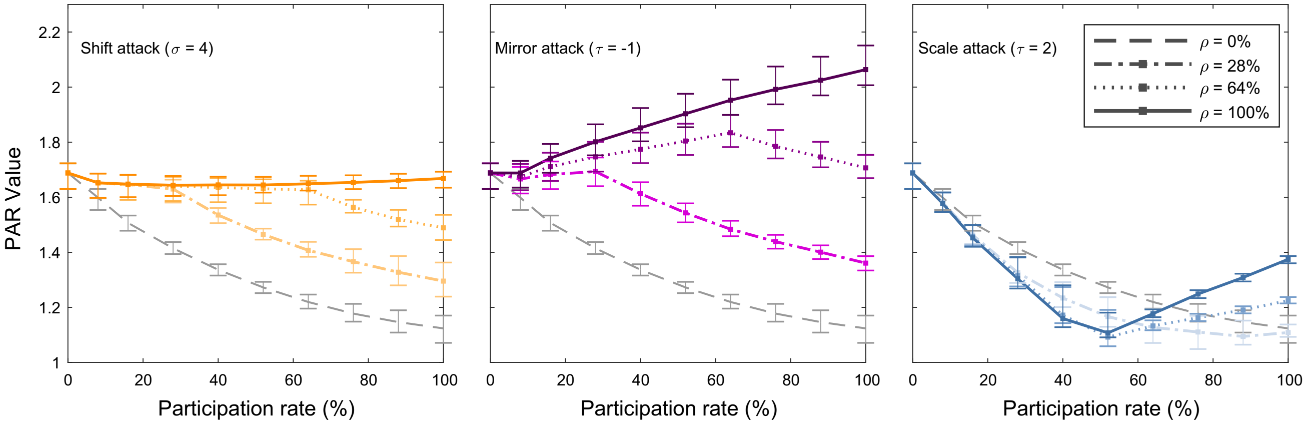

Fig. 6 Peak-to-average ratio (PAR) of the aggregated load for different attack scenarios. The median PAR value for a 365 day simulation is plotted together with the range between the first and third quartiles over the participation rate. The outcomes for three different attacks, i.e. shift attack with $\sigma = 4$, mirror attack, and scale attack with $\tau = 2$, are presented. For each attack, the individual graphs differ in their number of attacked players (denoted by ρ). This also includes the reference outcome of the scheduling game in which no player is attacked

attack targeting all players ($\rho = 100\%$) rewards the attacker with a 35.7% bill cut, while the other players must endure a 54.0% rise on average. Similarly, the attacker benefits from a scale attack ($\tau = -2$, $\rho = 28\%$) with a bill reduction of 1%, penalising the other households by a 2.3% increase.

3.3 Attack detection strategies

All investigated attacks affect the utility company negatively: when the participation rate is high, PAR values are systematically degraded compared to the non-attack scenario; otherwise, either PAR values become worse, or their improvement is at the cost of higher electricity bills for the average household. This is detrimental to the UC's credibility and competitiveness. Consequently, the UC needs to design defence strategies to prevent attacks that affect the storage scheduling process. In this study, the focus is on the detection of false data injection by monitoring the forecasting data that are transmitted every day on the smart grid communication system.

3.3.1 Attack detection through system monitoring

Forecast monitoring is considered at three different levels:

– Aggregated consumption forecast average, i.e. average amount monitoring

- Aggregated consumption forecast profile, i.e. deep aggregated monitoring
- Household consumption forecast profiles, i.e. deep individual monitoring

In each case, the UC would compare the received forecast data with its own estimate. While monitoring the aggregated consumption forecast total only requires the UC to forecast the daily total electricity consumption of the smart grid community as a whole, deep monitoring relies on producing hourly consumption estimates for either the entire community (deep aggregated monitoring) or each individual household (deep individual monitoring). The more precise the monitoring, the more resources are needed to implement it.

Since an individual average hourly forecast error for a 24-hour period is expected to be lower than 8% [7], the expectation is that the difference between two forecasts, i.e. the forecast provided by the received forecast data and the forecast estimated by the UC, to be lower than twice the 8% error of a single forecast. As a consequence, it is reasonable to assume that the UC could use a threshold of 20% to identify an attack when using deep individual monitoring. In the case of deep aggregated monitoring, the combination of forecasts tends to lead to error reduction. As a consequence, here a discrepancy of at least 10% is used to detect an attack. Finally, since in the proposed attack scenarios, the attacker always makes sure that their attack does not change the average daily aggregated forecast, a UC relying only on average amount monitoring would not be able to detect any attack. Eventually, the detection of a given attack depends not only on the chosen monitoring strategy, but also the type of attack, the participation rate N/M, and the percentage ρ of targeted players.

3.3.2 Attack impact analysis

Based on the three proposed monitoring strategies, the consequences of undetected attacks are studied. These are evaluated by estimating an attack's impact in terms of average bill change for the attacker and the other players, bill revenue change for the UC and PAR values. Assuming a participation rate of $N/M = 100\%$, this set of experiments considers, for each attack type of interest, i.e. shift ($\sigma = 4$), flat ($\tau = 0$), mirror ($\tau = -1$) and scale ($\tau = 2$ and $\tau = 1.29$), the most severe attack, in terms of the highest percentage ρ of targeted players, that has remained undetected according to the monitoring strategy.

As Tables 1 and 2 show, all of those attacks prove beneficial to the attacker in terms of reducing their bill, while other players suffer a bill increase. Regarding the UC, it benefits financially from the general bill rise, but sees its PAR value degraded. Note that the impact of a scale ($\tau = 1.29$) attack is evaluated because it is the most powerful scale attack which can target all players ($\rho = 100\%$) without being detected by any of the proposed monitoring strategies.

Table 1 reports the impact of undetected attacks despite average amount monitoring. As such monitoring is ineffective against the considered attacks, the attacker is able to carry out their attack with maximum strength, i.e. ($\rho = 100\%$), without being detected. The mirror ($\tau = -1$) attack is particularly efficient: the attacker's bill is reduced by 35.7% at the cost of the other players' bills, i.e. 54.0%, and a large increase in the PAR value to 2.06 from a non-attack value of 1.12.

Once deep aggregated monitoring is in place, the strength of the attacks that remain undetectable is reduced significantly. As Table 2 shows, the attacker's bill is lowered by 1.9% at most. However, although, in this case, the other players are hardly affected—their bills only increase by 0.3%, the UC suffers from a significant degradation of the PAR to 1.23. One should note that although the scale ($\tau = 2$) attack with ($\rho = 28\%$) produces a slightly better PAR value, i.e. 1.11 instead of 1.12 from the non-attack scenario, this is achieved by increasing the average electricity costs by 2.2%.

Finally, although the most stringent monitoring strategy, i.e. deep individual monitoring, would detect most attacks whatever ρ, i.e. shift ($\sigma = 4$), flat ($\tau = 0$), mirror ($\tau = -1$) and scale ($\tau = 2$), some limited scale attacks such as ($\tau = 1.29, \ \rho = 100\%$) still cannot be discovered (cf. last line of Table 2). Although none of the proposed monitoring strategies can detect all attacks, they are able to recognise the most severe ones. Moreover, they can detect false data injection for a wide range of attacks.

3.4 Attack mitigation

Once an attack has been detected, some response needs to be provided. For the most serious attacks, households may be instructed not to follow the calculated battery schedule, but use an alternative one. Several options are possible such as keeping the same schedule as the previous day or recalculating their schedule only taking into account their own data. In the latter case, scheduling is executed without using the game-theoretic framework, but by performing a simple optimisation of battery usage for their own consumption forecast.

Those options were evaluated in a previous study [33]. It showed that, although both approaches lead to a PAR reduction, local scheduling should be the defence of choice since it systematically outperforms previous day scheduling. Still, this mitigating strategy has its own cost: at medium participation rates N/M, the PAR reduction can be up to $\approx 25\%$ lower

Table 1 Impact of undetected attacks despite average amount monitoring

Attack type	ρ (%)	Attacker bill change (%)	Other players' bill change (%)	Utility company	
				Revenues change (%)	PAR value
Shift ($\sigma = 4$)	100	– 25.5 (5.8)	28.3 (13.1)	26.3 (12.3)	1.67 (0.06)
Flat ($\tau = 0$)	100	– 21.0 (6.6)	16.7 (4.3)	15.1 (4.0)	1.66 (0.09)
Mirror ($\tau = -1$)	100	– 35.7 (12.5)	54.0 (11.1)	50.3 (10.5)	2.06 (0.14)
Scale ($\tau = 2$)	100	– 9.5 (2.8)	21.4 (4.4)	20.1 (4.2)	1.37 (0.03)
Scale ($\tau = 1.29$)	100	– 1.5 (0.8)	3.1 (0.8)	2.9 (0.7)	1.13 (0.03)

Results show median values over 365-day simulations together with their respective interquartile range. The participation rate is $N/M = 100\%$

Table 2 Impact of undetected attacks despite deep aggregated monitoring

Attack type	ρ (%)	Attacker bill change (%)	Other players' bill change (%)	Utility company	
				Revenues change (%)	PAR value
Shift ($\sigma = 4$)	16	– 0.8 (0.7)	1.1 (0.5)	1.0 (0.5)	1.22 (0.11)
Flat ($\tau = 0$)	28	– 1.9 (1.1)	0.3 (0.5)	0.2 (0.5)	1.23 (0.05)
Mirror ($\tau = -1$)	16	– 1.7 (1.1)	0.9 (0.7)	0.8 (0.7)	1.25 (0.06)
Scale ($\tau = 2$)	28	– 1.0 (0.7)	2.3 (0.7)	2.2 (0.7)	1.11 (0.04)
*Scale ($\tau = 1.29$)	100	– 1.5 (0.8)	3.1 (0.8)	2.9 (0.7)	1.13 (0.03)

Results show median values over 365-day simulations together with their respective interquartile range. The participation rate is $N/M = 100\%$
*Attack that remains undetected even when applying deep individual monitoring

than when the game is played. As Tables 1 and 2 show, only the most powerful attacks have an impact on the PAR which is higher than reverting to the local scheduling strategy. This suggests that the best reaction to a low- impact attack would be to let it happen. In terms of monitoring, only deep aggregated monitoring would prove useful, since it is able to detect all attacks for which the proposed mitigation strategy is beneficial. Therefore, a two-level detection system may be the most suitable strategy for the UC: it should conduct either no monitoring at all, or deep aggregated monitoring.

Before deciding on a complete defence strategy, which includes detection and mitigation, all costs and benefits must be taken into account by the UC, i.e. cost of monitoring, cost of mitigating action, cost of reputation loss, and benefit of increased consumption. The main challenge for the utility company is to control the spending on their security measures, as organisations typically have a restricted budget. For example, if the expected probability of an attack is low, a low investment in security could be justified. On the other hand, if an attacker is aware of such a strategy, they would be more likely to attack as they would expect less resistance. Finding a solution to this decision-making problem cannot be achieved by optimisation alone, but instead non-cooperative game theory helps in devising suitable models and advising on the expected likelihood of attacks.

4 Game-theoretic defence strategy

When planning to defend against the false data injection attacks described in the previous section, the need for the utility company to allocate resources for the defence in the most efficient way has been highlighted. This section proposes to use game theory in order to support this decision-making process. The game is motivated and introduced based on detailing the payoff functions of the two players describing the game normal form. This is followed by solving the game using various assumptions. Finally, the solution is discussed with respect to their implications for the simulated scenario and potential alternatives.

4.1 Game theory for security

Game theory is increasingly being employed for modelling attacker–defender scenarios in cyber security, for a broad range of scenarios such as intrusion detection in network security [1], managing the security of information in an organisation [28], and predicting the likelihood of cyber attacks [5].

Non-cooperative game theory is based on the assumption that players are rational, i.e. they choose between actions such that they maximise their payoffs. The associated strategies can be identified using the fundamental concept of the Nash equilibrium (cf. Sect. 2.2). Although not all games have Nash equilibrium, Nash's theorem states that nonzero-sum games always admit a mixed strategy equilibrium. However, for practical applications it may not be easy to interpret [2].

In this paper, x and y denote a pure or mixed strategy of the first and second player in a two-player game, and x^* and y^* are used for equilibrium strategies of these players. A *strategy profile* $s = (x, y)$ groups strategies of each player together. If the grouped strategies are in equilibrium, this strategy profile is written as s^*. A two-player nonzero-sum game can be represented in normal form, based on the players' payoff matrices A and B [39].

An *Nash equilibrium strategy profile* is a strategy profile $s^* = (x^*, y^*)$ satisfying

$$x^*Ay^* \geq xAy^* \ \ \forall x, \quad x^*By^* \geq x^*By \ \ \forall y \ . \tag{3}$$

Here, the strategies may be pure or mixed, and the corresponding NE is referred to as pure or mixed. Furthermore, if all of the inequalities in the above definition are strict, one has a *strict* NE. Otherwise, the NE is *non-strict*.

4.2 Proposed security game

The proposed security game is a two-player nonzero-sum *complete information* game [39] between the utility company $\mathcal{U}$ and the attacker $\mathcal{A}$. The game is inspired by the nonzero-sum Intrusion Detection System (IDS) game of [1] which has been thoroughly analysed in the literature and is well understood. Table 3 illustrates the game where the two strategies available to the defender are to monitor or not, denoted by the strategy space $S_{\mathcal{D}} = \{s^{\mathcal{D}}_{\text{mon}}, s^{\mathcal{D}}_{-\text{mon}}\}$, and the attacker chooses between attacking and not attacking: $S_{\mathcal{A}} = \{s^{\mathcal{A}}_{\text{att}}, s^{\mathcal{A}}_{-\text{att}}\}$. The positive parameters α_c, α_f, α_m, β_c and β_s are used to denote the payoffs corresponding to the various strategies. The main characteristic of this game is the design of the payoff functions in such a way that the monitoring defender only has an incentive to defend in the presence of an attack. The attacker is discouraged from attacking if there is defence in place. This design leads to a circular path when considering payoff-incrementing unilateral changes of strategy, hence prohibiting the existence of a pure Nash equilibrium.

Table 3 IDS game of [1] in normal form

$\mathcal{D}\downarrow\ \ \mathcal{A}\rightarrow$	$s^{\mathcal{A}}_{att}$		$s^{\mathcal{A}}_{-att}$	
$s^{\mathcal{D}}_{mon}$	$\alpha_c,$	$-\beta_c$	$-\alpha_f,$	0
$s^{\mathcal{D}}_{-mon}$	$-\alpha_m,$	β_s	$0,$	0

4.2.1 Description of the game

Here, an augmented security game is introduced, extending the IDS game described previously by an additional action. The rationale behind this extended game model is twofold: Sect. 3.3.1 demonstrates the existence of low-impact attacks which cannot be detected by standard monitoring techniques, and it would be desirable to capture these in a more sophisticated game model. Second, an extended game might better match real-world scenarios and might lead to simpler solutions, i.e. pure equilibria rather than mixed ones.

Game Strategies Section 3 presents three possible monitoring strategies for $\mathcal{U}$: to monitor the daily average of forecasting data, to inspect the daily profile of the aggregated forecast, and to inspect the individual forecast data with the same level of detail. In this work, the assumption is made that the first and second monitoring strategies are most useful in a realistic setting, as they have an observable impact on the strength and outcome of successful attacks while the third monitoring strategy merely eliminates attacks that are possible for weaker monitoring levels. Furthermore, as the data of aggregated forecasts are readily available to the UC, the first monitoring strategy is not costly and is identified with the strategy $s^{\mathcal{U}}_{-\text{mon}}$. The second monitoring strategy is denoted as $s^{\mathcal{U}}_{\text{mon}}$ so that the strategy space for the defender $\mathcal{U}$ is as in the previous game $S_{\mathcal{U}} = \{s^{\mathcal{U}}_{\text{mon}}, s^{\mathcal{U}}_{-\text{mon}}\}$. The attacker $\mathcal{A}$ has three different strategies: to attack strongly with high impact, to perform a weaker attack with low impact, or not to attack at all. This is denoted by the strategy space $S_{\mathcal{A}} = \{s^{\mathcal{A}}_{\text{att}^\circ}, s^{\mathcal{A}}_{\text{att}}, s^{\mathcal{A}}_{-\text{att}}\}$.

The additional weak attack strategy $s^{\mathcal{A}}_{\text{att}^\circ}$ offers an alternative incentive of not monitoring to the UC, preferring to save monitoring cost when facing a weak attack. No assumption is made on the relationship between the attacker's overall payoff when choosing the two different attack types, and a discussion of conditions clarifying this relationship is the main subject of the game analysis in the next section.

Game Payoff Functions The following notations for the payoffs for $\mathcal{U}$ are introduced: $c^{\mathcal{U}}_{\text{mon}}$ is the cost for monitoring the daily profile of the aggregated forecast (second monitoring strategy), and $c^{\mathcal{U}}_{\text{def}}$ is an additional cost for investing in defence mechanisms such as actions discussed in Section 3.4. Losses from weak and strong attacks are denoted by $l^{\mathcal{U}}_{\text{att}^\circ}$ and $l^{\mathcal{U}}_{\text{att}}$, respectively. The payoff functions corresponding to $\mathcal{A}$ are the benefits and costs associated with weak and strong attacks, denoted by $b^{\mathcal{A}}_{\text{att}^\circ}$, $c^{\mathcal{A}}_{\text{att}^\circ}$, and $b^{\mathcal{A}}_{\text{att}}$ and $c^{\mathcal{A}}_{\text{att}}$, respectively.

The monitoring activity always leads to monitoring costs for $\mathcal{U}$. If there is no monitoring, $\mathcal{U}$ incurs losses $l^{\mathcal{U}}_{\text{att}^\circ}$ and $l^{\mathcal{U}}_{\text{att}}$ due to weak and strong attacks. Otherwise, despite monitoring, weak attacks cannot be detected; hence, there is a resulting loss $l^{\mathcal{U}}_{\text{att}^\circ}$. Strong attacks, however, are detected and

Table 4 Security game in normal form

$\mathcal{U}\downarrow\ \mathcal{A}\rightarrow$	$s^{\mathcal{A}}_{att^\circ}$	$s^{\mathcal{A}}_{att}$	$s^{\mathcal{A}}_{-att}$
$s^{\mathcal{U}}_{mon}$	$-c^{\mathcal{U}}_{mon} - l^{\mathcal{U}}_{att^\circ}, \quad l^{\mathcal{U}}_{att^\circ} - c^{\mathcal{A}}_{att^\circ}$	$-c^{\mathcal{U}}_{mon} - c^{\mathcal{U}}_{def}, \quad -c^{\mathcal{A}}_{att}$	$-c^{\mathcal{U}}_{mon}, \quad 0$
$s^{\mathcal{U}}_{-mon}$	$-l^{\mathcal{U}}_{att^\circ}, \quad l^{\mathcal{U}}_{att^\circ} - c^{\mathcal{A}}_{att^\circ}$	$-l^{\mathcal{U}}_{att}, \quad l^{\mathcal{U}}_{att} - c^{\mathcal{A}}_{att}$	$0, \quad 0$

mitigated against through some countermeasures, preventing any losses but leading to a defence cost $c^{\mathcal{U}}_{\text{def}}$. Finally, if there is no attack, then the only arising nonzero payoff function involved is the monitoring cost for $\mathcal{U}$. The attacker $\mathcal{A}$ obtains a benefit $b^{\mathcal{A}}_{\text{att}^\circ}$ from a weak attack, but has to invest in attack costs $c^{\mathcal{A}}_{\text{att}^\circ}$. Similarly, the cost $c^{\mathcal{A}}_{\text{att}}$ arises from a strong attack; however, the model assumes the lack of a benefit for $\mathcal{A}$ due to the UC's defence mechanism. Using these notations, the proposed security game $\mathcal{G}$ can be represented in normal form as shown in Table 4.

4.2.2 Game assumptions

In this section, assumptions on the relationship of the various cost and benefit functions, which are part of the game payoff matrices, are listed and justified.

Assumptions from the IDS Game The cost for missing an attack $\alpha_m = l^{\mathcal{U}}_{\text{att}} > 0$ is interpreted as losses from an attack that is not mitigated against, the false alarm cost $\alpha_f = c^{\mathcal{U}}_{\text{mon}} > 0$ as an ongoing monitoring cost, and the detection penalty $\beta_c = c^{\mathcal{A}}_{\text{att}} > 0$ as the cost for the attacker to conduct a strong attack. The gain from detection $\alpha_c = -c^{\mathcal{U}}_{\text{mon}} - c^{\mathcal{U}}_{\text{def}} > 0$ is reformulated as necessary cost to monitor and to defend in order to prevent damage. In order to preserve the mixed equilibrium property of the security game given by $-\alpha_m < \alpha_c$, it is then assumed that this attack prevention cost is less than the actual incurring attack damage, i.e. $c^{\mathcal{U}}_{\text{mon}} + c^{\mathcal{U}}_{\text{def}} < l^{\mathcal{U}}_{\text{att}}$. This assumption is natural: in a typical security game, the defender does not spend more on attack prevention than what they potentially loose from an attack. Finally, $\beta_s = l^{\mathcal{U}}_{\text{att}} - c^{\mathcal{A}}_{\text{att}} > 0$ is the difference between the benefit from an undetected attack and the attack effort. This expresses a similar principle as above, but this time applied to the attacker $\mathcal{A}$ who does not spend more on an attack than the expected gain from it. These assumptions can be referred to as the Security Game Assumptions.

Augmented Security Game The assumptions required for the augmented security game are in parts inspired by those of the IDS game and also motivated by the experimental results presented in Sect. 3 which suggest that strong attacks require targeting more victims, i.e. a bigger effort.

For a weak attack, the attacker receives a greater payoff than the cost of the attack, implying

$$c^{\mathcal{A}}_{\text{att}^\circ} < l^{\mathcal{U}}_{\text{att}^\circ} \ . \tag{4}$$

It can also be assumed that the cost for launching a strong attack is higher than that for a weak attack since a higher number of households have to be attacked

$$c^{\mathcal{A}}_{\text{att}} > c^{\mathcal{A}}_{\text{att}^\circ} \ . \tag{5}$$

Finally, a strong attack leads to higher losses for the utility (cf. Sect. 3.2.1)

$$l^{\mathcal{U}}_{\text{att}} > l^{\mathcal{U}}_{\text{att}^\circ} \ . \tag{6}$$

Note that in order to aid the game analysis, an assumption made in this game is that the benefit of the attacker is equal to the loss of the defender, $b^{\mathcal{A}}_{\text{att}} = l^{\mathcal{U}}_{\text{att}}$ and $b^{\mathcal{A}}_{\text{att}^\circ} = l^{\mathcal{U}}_{\text{att}^\circ}$.

4.3 Game analysis

In this section, analysis of the security game $\mathcal{G}$ reveals existence of several NE strategies. Following the study of practical examples, the relevance of these strategies is discussed so that they can be used to inform UC's security investments.

4.3.1 Nash equilibrium strategies

To solve the augmented security game, three distinct cases are considered. This is based on discussing the second-order difference that is defined here as:

$$\Delta = q_{\text{att}^\circ} - q_{\text{att}} \ , \tag{7}$$

where $q_{\text{att}^\circ} = l^{\mathcal{U}}_{\text{att}^\circ} - c^{\mathcal{A}}_{\text{att}^\circ}$ and $q_{\text{att}} = l^{\mathcal{U}}_{\text{att}} - c^{\mathcal{A}}_{\text{att}}$ describe the net benefit for the attacker in the case of a weak and strong attack, respectively.

Case 1 ($\Delta > 0$) In this case, the existence of a unique pure NE for the game $\mathcal{G}$ can be asserted. The corresponding NE strategy is for the UC to not monitor and for the attacker to carry out a weak attack.

Proposition 1 *If $l^{\mathcal{U}}_{\text{att}^\circ} - c^{\mathcal{A}}_{\text{att}^\circ} > l^{\mathcal{U}}_{\text{att}} - c^{\mathcal{A}}_{\text{att}}$, the game $\mathcal{G}$ admits a unique pure Nash equilibrium strategy profile of the form $s^* = (s^{\mathcal{U}}_{-\text{mon}}, s^{\mathcal{A}}_{\text{att}^\circ})$ and the corresponding payoffs are $s^*_{\mathcal{U}} = -l^{\mathcal{U}}_{\text{att}^\circ}$ and $s^*_{\mathcal{A}} = l^{\mathcal{U}}_{\text{att}^\circ} - c^{\mathcal{A}}_{\text{att}^\circ}$.*

Proof First, it needs to be verified that when choosing the pure strategy profile $(s^{\mathcal{U}}_{-\text{mon}}, s^{\mathcal{A}}_{\text{att}^\circ})$, none of the two players benefits from a unilateral change of pure strategy.

Focusing on the UC, the change of strategy $s^{\mathcal{U}}_{-\mathrm{mon}} \rightarrow s^{\mathcal{U}}_{\mathrm{mon}}$ diminishes its payoff since $-l^{\mathcal{U}}_{\mathrm{att}^\circ} > -c^{\mathcal{U}}_{\mathrm{mon}} - l^{\mathcal{U}}_{\mathrm{att}^\circ}$ due to the assumption of a positive monitoring cost. Considering the attacker, the change $s^{\mathcal{A}}_{\mathrm{att}^\circ} \rightarrow s^{\mathcal{A}}_{\mathrm{att}}$ is not beneficial because of the main assumption $\Delta > 0$ of this case. Finally, the change of strategy $s^{\mathcal{A}}_{\mathrm{att}^\circ} \rightarrow s^{\mathcal{A}}_{-\mathrm{att}}$ reduces the payoff due to Assumption (4). Second, a careful inspection of the payoff functions of the remaining strategies of the game, together with the fact that the assumption of Case 1 implies $l^{\mathcal{U}}_{\mathrm{att}^\circ} - c^{\mathcal{A}}_{\mathrm{att}^\circ} > -c^{\mathcal{A}}_{\mathrm{att}}$, shows that there is no other pure NE. □

Case 2 ($\Delta < 0$) Similar to the IDS game, the augmented security game has the same property of circular paths when performing unilateral changes strategy with increasing payoffs, hence prohibiting the existence of any pure NE.

Proposition 2 *If $l^{\mathcal{U}}_{\mathrm{att}^\circ} - c^{\mathcal{A}}_{\mathrm{att}^\circ} < l^{\mathcal{U}}_{\mathrm{att}} - c^{\mathcal{A}}_{\mathrm{att}}$, the game $\mathcal{G}$ admits no pure NE.*

Proof The proof of this proposition is done similar to that of Proposition 1 by comparing the changes in payoff, following a unilateral change of strategy. It is clear that there is no pure NE in the game restricted to the attacker strategies $s^{\mathcal{A}}_{\mathrm{att}}$ and $s^{\mathcal{A}}_{-\mathrm{att}}$, as the resulting subgame is identical to the IDS game. When augmented by the weak attack strategy $s^{\mathcal{A}}_{\mathrm{att}^\circ}$, two cases may arise, depending on which of the strategy changes $s^{\mathcal{A}}_{\mathrm{att}} \rightarrow s^{\mathcal{A}}_{\mathrm{att}^\circ}$ or $s^{\mathcal{A}}_{\mathrm{att}^\circ} \rightarrow s^{\mathcal{A}}_{\mathrm{att}}$, starting from the initial strategy profile $(s^{\mathcal{U}}_{\mathrm{mon}}, s^{\mathcal{A}}_{\mathrm{att}})$, lead to an increased payoff for the attacker.

In the first case, one observes the additional sequence of strategy changes $s^{\mathcal{U}}_{\mathrm{mon}} \rightarrow s^{\mathcal{U}}_{-\mathrm{mon}}$, $s^{\mathcal{A}}_{\mathrm{att}^\circ} \rightarrow s^{\mathcal{A}}_{\mathrm{att}}$ and $s^{\mathcal{U}}_{-\mathrm{mon}} \rightarrow s^{\mathcal{U}}_{\mathrm{mon}}$ leading back to the original strategy profile. These changes entail increased payoffs due to the assumption of positive monitoring cost, the condition $\Delta < 0$, and the Security Game Assumptions. In the second case, the unilateral payoff change joins the circular path of the IDS game, from which the proof follows as shown earlier. □

Case 3 ($\Delta = 0$) In this last case, one derives the inequality $l^{\mathcal{U}}_{\mathrm{att}^\circ} - c^{\mathcal{A}}_{\mathrm{att}^\circ} = l^{\mathcal{U}}_{\mathrm{att}} - c^{\mathcal{A}}_{\mathrm{att}} > -c^{\mathcal{A}}_{\mathrm{att}}$ as in Case 1 and obtains a similar but weaker result, as the pure NE is not strict. A formal proof of the following proposition is omitted as it can be done similarly as that of Proposition 1 since the same payoff deviations are involved.

Proposition 3 *If $l^{\mathcal{U}}_{\mathrm{att}^\circ} - c^{\mathcal{A}}_{\mathrm{att}^\circ} = l^{\mathcal{U}}_{\mathrm{att}} - c^{\mathcal{A}}_{\mathrm{att}}$, the game $\mathcal{G}$ admits a unique pure non-strict Nash equilibrium strategy profile of the form $s^* = (s^{\mathcal{U}}_{-\mathrm{mon}}, s^{\mathcal{A}}_{\mathrm{att}^\circ})$ and the corresponding payoffs are $s^*_{\mathcal{U}} = -l^{\mathcal{U}}_{\mathrm{att}^\circ}$ and $s^*_{\mathcal{A}} = l^{\mathcal{U}}_{\mathrm{att}^\circ} - c^{\mathcal{A}}_{\mathrm{att}^\circ}$.*

4.3.2 Quantitative examples

Attacks discussed in Sect. 3 are further analysed using the proposed augmented security game. In order to establish which case they correspond to, estimations of the sign of Δ (7) are performed using previous simulation calculations. More specifically, $b^{\mathcal{A}}_{\mathrm{att}}$ and $b^{\mathcal{A}}_{\mathrm{att}^\circ}$ are represented by the values of the Àttacker bill change’ (γ and $\gamma_\circ$), reported in Tables 1 and 2, respectively, multiplied by the actual amount of the bill λ, e.g. $b^{\mathcal{A}}_{\mathrm{att}} = l^{\mathcal{U}}_{\mathrm{att}} = \gamma \cdot \lambda$. Moreover, assuming a linear relationship between the number of attacked players and the cost of an attack, $c^{\mathcal{A}}_{\mathrm{att}}$ and $c^{\mathcal{A}}_{\mathrm{att}^\circ}$ can be expressed using the values of percentage of targeted players (ρ and $\rho_\circ$) shown in Tables 1 and 2, respectively, e.g. $c^{\mathcal{A}}_{\mathrm{att}} = \rho \cdot \kappa$. As a consequence, an attack type corresponds to Case 2, i.e. ($\Delta < 0$), iff the following inequality is satisfied:

$$\frac{\gamma_\circ - \gamma}{\rho_\circ - \rho} > \frac{\kappa}{\lambda} \tag{8}$$

with Assumption (4) stating $\gamma_\circ/\rho_\circ > \kappa/\lambda$.

Evaluations of attacks reported in Tables 1 and 2 show that Case 2 applies to the shift ($\sigma = 4$), flat ($\tau = 0$), mirror ($\tau = -1$), and scale ($\tau = 2$) attacks. Hence, for none of those attacks a pure NE exits and only mixed strategies can be offered. Using the mirror attack as an example, Eq. (8) requires $0.41 > \kappa/\lambda$ and Assumption (4) imposes $0.11 > \kappa/\lambda$.

Since the scale ($\tau = 1.29$) attack was especially designed to be undetectable by the proposed monitoring solution, it cannot be analysed by the game which assumes that a successful monitoring strategy is available. On the other hand, the best strategy for such attack is self-evident: since all attacks result in gains for the attacker, they should attack, while the UC should not waste any resources in ineffective defence.

In order to investigate the mixed strategies associated with those attacks, numeral values were selected so that mixed strategies could be computed using an NE solver [4]: $\lambda = 100$, $\kappa = 10$, $c^{\mathcal{U}}_{\mathrm{mon}} = 10$, and $c^{\mathcal{U}}_{\mathrm{def}} = 20$. Table 5 shows representative mixed strategy probabilities associated with the investigated Case 2 attacks, here the mirror attack. The attacker either performs a strong (63.7% probability) or weak (36.3% probability) attack, while the UC chooses to use monitoring with a 71.7% probability.

Table 5 Representative mixed strategy probabilities for Case 2 attacks based on simulations (cf. Sect. 3.3.2)

	$p_{\mathrm{att}^\circ} = 36.3\%$	$p_{\mathrm{att}} = 63.7\%$	$p_{-\mathrm{att}} = 0\%$
$p_{\mathrm{mon}} = 71.7\%$	26.0%	45.7%	0%
$p_{-\mathrm{mon}} = 28.3\%$	10.3%	18.0%	0%

Note that the choice of numerical values is not critical. As long as all the game assumptions are fulfilled, the probability for the monitoring action of the UC is at least 70%.

4.3.3 Discussion

Theoretical analysis of the proposed extended game model has shown that according to the sign of Δ (7), three different cases should be considered. While both Case 1 ($\Delta > 0$) and Case 3 ($\Delta = 0$) are associated with a pure NE, only Case 1's is strict. However, in both cases, the NE strategy for the UC is the same: not to monitor. On the other hand, Case 2 ($\Delta < 0$) only leads to mixed strategies. Practical analysis, investigating the attack examples described in Sect. 3 based on a 100% participation rate, revealed that only Case 2 was practically relevant. This is consistent with expectations that the net benefits, i.e. benefits minus costs, of strong attacks are supposed to be higher than those of weak attacks. Note that for the scale ($\tau = 2$) attack, different cases could arise at lower participation rates due to its specific behaviour as shown in Figs. 5 and 9.

Regarding Case 2, for a UC, the practical application of equilibrium strategies, as illustrated in Table 5, is not straightforward. Actually many suggestions have been made regarding possible interpretations of mixed strategies [2,3,9]. In the specific context of this work, that proposed by [9] is of particular interest: indeed, assuming that the UC supplies a set of microgrids, where security strategy is decided at the microgrid level, they, seen as a population, would choose defence strategies following the mixed probabilities. Alternatively, as suggested in [22,39], the probability associated with defence could be interpreted as an index of security criticality which would inform the UC's decisions regarding its defence investments. Interestingly, experiments (not shown) indicate that when the cost of attacking a single player, i.e. κ, decreases, the mixed strategy probability for monitoring grows, increasing defence needs.

Finally, the undetectable scale ($\tau = 1.29$) attack is a reminder that no practical monitoring strategy is perfect and the best defence strategy may be not to defend if the losses associated with an attack can be considered as acceptable.

5 Conclusion

Protecting smart grids from cyber attacks is essential for them to deliver their promises. Investigating different classes of false data injection attacks against the forecasts required for smart energy scheduling, extensive simulations showed the extent of damages that a single attacker can cause to both the utility company (growth of PAR value by up to 84%) and its consumers (bill increase by up to 54%). The need for mitigation having been established, monitoring and defence strategies were proposed. In order to assess their value and advise utility companies on their attack prevention strategy, a novel and generic security game that considers low and high-impact attacks was designed. Its analysis highlighted, in particular, conditions under which a Nash equilibrium exists. Interestingly, in those cases, the best strategy is for the utility company not to invest in any monitoring and the attacker to conduct low-impact attacks. Numerical evaluations considering the previously studied classes of attacks revealed that there is a type of attack where, indeed, no monitoring is the best strategy. However, in all the other cases, only mixed strategies can be offered. Their practical interpretation by UCs was discussed. In conclusion, the proposed security game offers utility companies the ability to investigate the most appropriate monitoring and defence strategies so that false data injection attacks have only limited, if any, impact on smart energy scheduling.

Acknowledgements This work was supported by the Doctoral Training Alliance (DTA) Energy, the Erasmus+ Programme of the European Union, and the Kingston University First Grants Scheme.

Compliance with ethical standards

Conflicts of interest All authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Appendix

5.1 Simulating forecasting errors

Since forecasting electricity consumption is out of the scope of this study, forecasts were simulated instead of produced by a forecasting algorithm. However, in order to consider forecasts as realistic, they must show some deviation from the actual consumption. As it has been reported that the average error in individual forecasted data is around 8% [7], some random error is added to the actual consumption values to produce sufficiently inaccurate forecasts. Although

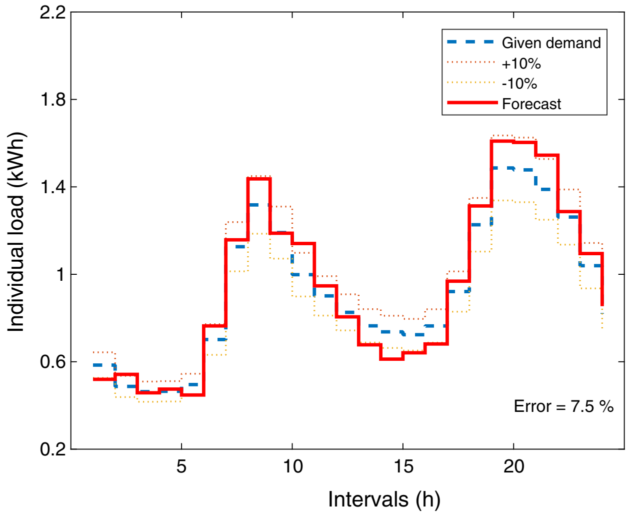

Fig. 7 Individual forecast created by adding random errors. While the dashed curve is the actual demand of an household, addition and subtraction of 10% are represented by the two dotted curves. The bold curve is one example of simulated forecast produced using the described method. Here, whereas the average error is 7.5%, there are some values outside the 10% error area

errors could be added following a Gaussian law, the obtained forecasted profile would prove unrealistic since it would display random jumps. As a consequence, some smoothing effect is added by linking successive values. More specifically, for each value i, a random error is initially calculated e_i, and then, the actual error added to the value i is the average of the corresponding e_i and its neighbours, i.e. $E_i = \frac{e_{i-1}+e_i+e_{i+1}}{3}$.

As seen in Fig. 7, with this approach, simulated forecast is smoother and, as a consequence, more realistic. Due to the relatively large number of players, despite the added errors, the aggregated forecast remains quite similar to the aggregated demand (an average error of around 2% was estimated experimentally). As a consequence, game solutions based on forecast with and without errors are close: drawing the histogram of the error per day during a whole year (not shown) reveals an average error of 8% [31].

5.2 Supplementary material

Figure 8 shows a flow diagram of the augmented security game which helps to understand the analysis in Sect. 4. Figure 9 provides details to the discussion in Sect. 3.2.1 about individual household schedules and the influence of the scale attack with $\tau = 2$.

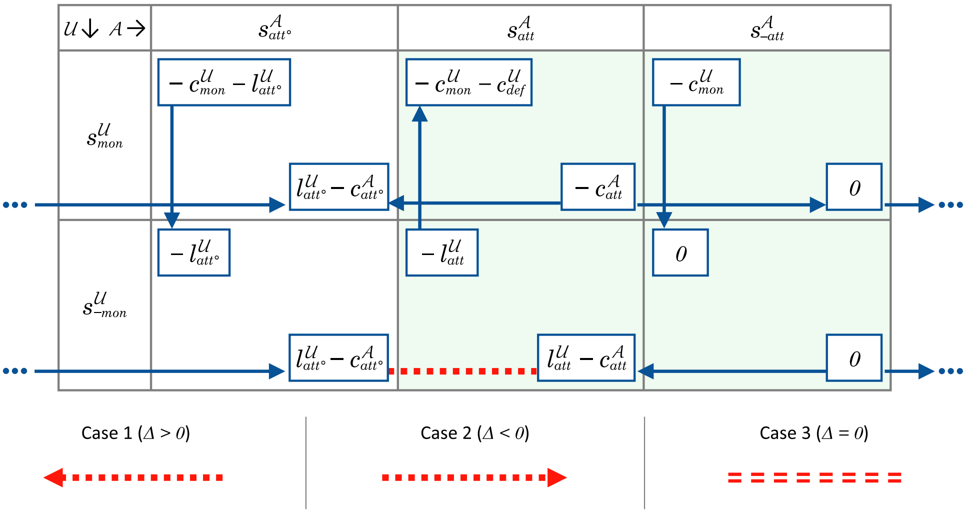
$\mathcal{U}\downarrow \ \mathcal{A}\rightarrow$
$s^{\mathcal{A}}_{att^\circ}$
$s^{\mathcal{A}}_{att}$
$s^{\mathcal{A}}_{\neg att}$
$s^{\mathcal{U}}_{mon}$
$s^{\mathcal{U}}_{\neg mon}$
$-c^{\mathcal{U}}_{mon} - l^{\mathcal{U}}_{att^\circ}$
$-c^{\mathcal{U}}_{mon} - c^{\mathcal{U}}_{def}$
$-c^{\mathcal{U}}_{mon}$
$l^{\mathcal{U}}_{att^\circ} - c^{\mathcal{A}}_{att^\circ}$
$-c^{\mathcal{A}}_{att}$
0
$-l^{\mathcal{U}}_{att^\circ}$
$-l^{\mathcal{U}}_{att}$
0
$l^{\mathcal{U}}_{att^\circ} - c^{\mathcal{A}}_{att^\circ}$
$l^{\mathcal{U}}_{att} - c^{\mathcal{A}}_{att}$
0
Case 1 ($\Delta > 0$)
Case 2 ($\Delta < 0$)
Case 3 ($\Delta = 0$)

Fig. 8 Advanced security game flow diagram. This figure is a more extensive representation of the game shown in Table 4, including the relations between the respective quantities. The arrows indicate which strategy would be more preferable in terms of the individual players' utility function. As discussed in Sect. 4.3, the connection between the IDS game (in green) and the proposed augmented security game is defined by the second-order difference Δ (7) which is highlighted here by the red dotted lines. Depending on the sign of Δ (7), the direction of the arrows varies as illustrated in the three cases. Note that the double line represents equality (color figure online)

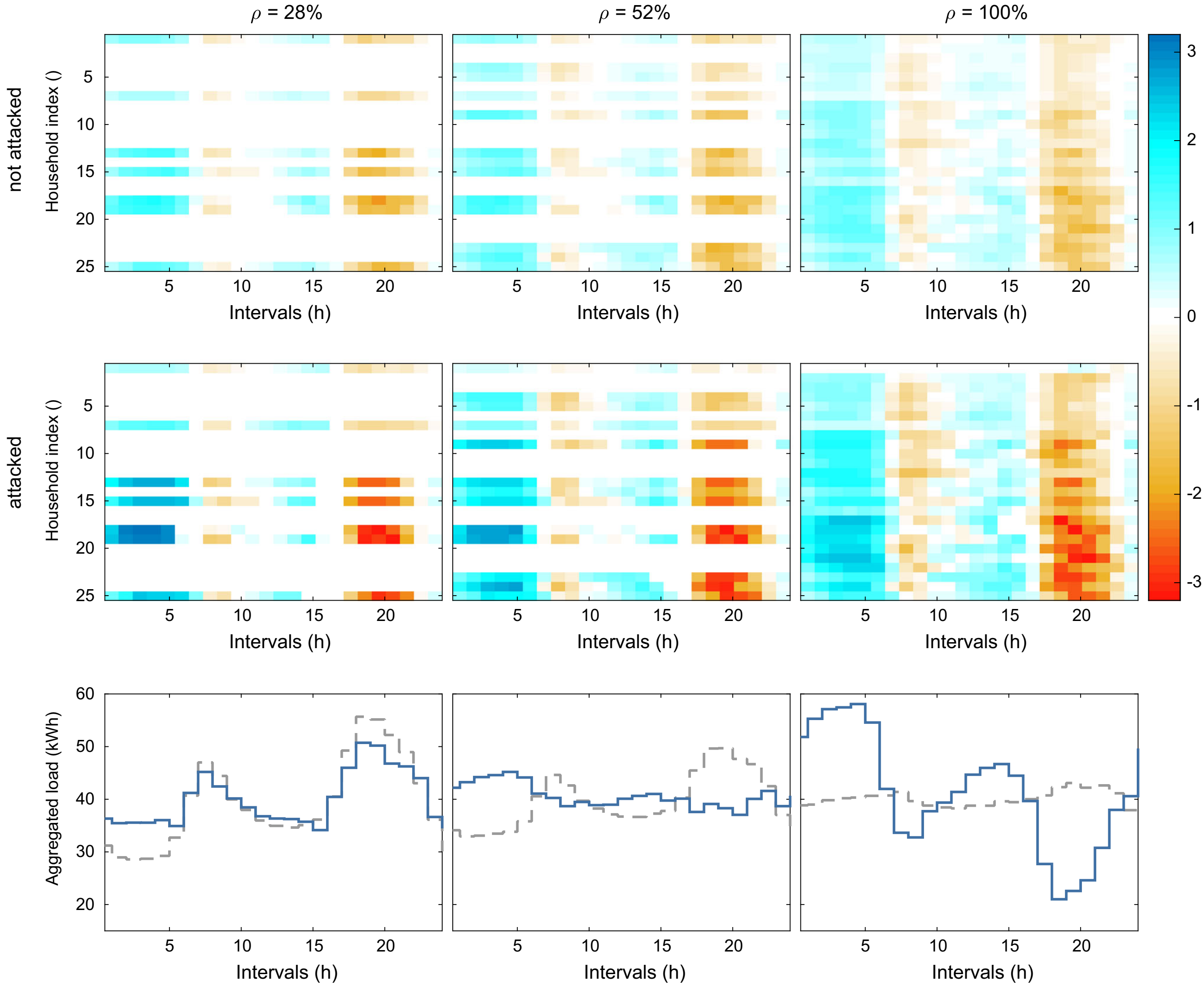

Fig. 9 Aggregated load and battery schedule without and under a scale ($\tau = 2$) attack targeting all players for different household participation rates (ρ). Each column corresponds to a different participation rate, i.e. from left to right $\rho = 28\%$, $\rho = 52\%$, and $\rho = 100\%$. The first row shows battery schedules of each individual household; the second row shows battery schedules of each individual household under attack—note that the first household is the attacker; the third row compares aggregated loads without—dashed curves—and with—bold curves—attacks. Without attack, participation of all households, i.e. $\rho = 100\%$, is required to flatten the aggregated load (PAR $= 1.07$). However, excessive battery usage by attacked households (the second row shows stronger charges and discharges) leads to a relatively flat (PAR $= 1.11$) aggregated load at $\rho = 52\%$. However, at $\rho = 100\%$ the aggregated load profile is almost inverted; in this case, the attacker hardly needs to use their battery (color figure online)

References

1. Alpcan, T., Basar, T.: Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, Cambridge (2010)
2. Auman, R.J.: What is game theory trying to accomplish. In: Arrow, K., Honkapohja, S. (eds.) Frontiers of Economics, pp. 5–46. Basil Blackwell, Oxford (1985)
3. Aumann, R.: Epistemic conditions for Nash equilibrium. Econometrica **65**(5), 1161–1180 (1995)
4. Avis, D., Rosenberg, G., Savani, R., von Stengel, B.: Enumeration of Nash equilibria for two-player games. Econ. Theory **42**, 9–37 (2010)
5. Bao, T., Shoshitaishvili, Y., Wang, R., Kruegel, C., Vigna, G., Brumley, D.: How shall we play a game?: a game-theoretical model for cyber-warfare Games. In: Proceedings—IEEE Computer Security Foundations Symposium (2017). https://doi.org/10.1109/CSF.2017.34
6. Batalla, J.M., Vasilakos, A., Gajewski, M.: Secure smart homes: opportunities and challenges. ACM Comput. Surv. **50**(5), 75:1–75:32 (2017). https://doi.org/10.1145/3122816
7. Bichpuriya, Y.K., Soman, S.A., Subramanyam, A.: Combining forecasts in short term load forecasting: empirical analysis and identification of robust forecaster. Sadhana **41**(10), 1123–1133 (2016). https://doi.org/10.1007/s12046-016-0542-3

8. Boudko, S., Abie, H.: An evolutionary game for integrity attacks and defences for advanced metering infrastructure (September) (2018). https://doi.org/10.1145/3241403.3241463
9. Chen, H., Ngan, H., Zhang, Y.: Power System Optimisation: Large-Scale Complex Systems Approaches. Wiley, Hoboken (2017)
10. Fadlullah, Z.M., Nozaki, Y., Takeuchi, A., Kate, N.: A survey of game theoretic approaches in smart grid. In: International Conference on Wireless Communications and Signal Processing, WCSP (2011). https://doi.org/10.1109/WCSP.2011.6096962
11. Farraj, A., Hammad, E., Daoud, A.A., Kundur, D.: A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. IEEE Trans. Smart Grid **7**(4), 1846–1855 (2016). https://doi.org/10.1109/TSG.2015.2440095
12. Gellings, C.W.: The concept of demand-side management for electric utilities. Proc. IEEE **73**(10), 1468–1470 (1985). https://doi.org/10.1109/PROC.1985.13318
13. Gupta, A., Yadav, A.: Challenges in demand side management in smart power grid: a review. Int. J. Eng. Sci. Math. **6**(8), 120–125 (2017)
14. He, H., Yan, J.: Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys. Syst. Theory Appl. **1**(1), 13–27 (2016). https://doi.org/10.1049/iet-cps.2016.0019
15. Huang, Y., Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z., Li, H., Song, L.: Bad data injection in smart grid: attack and defense mechanisms. IEEE Commun. Mag. **51**(1), 27–33 (2013). https://doi.org/10.1109/MCOM.2013.6400435
16. Ipakchi, A., Albuyeh, F.: Grid of the future. IEEE Power Energy Mag. **7**(2), 52–62 (2009). https://doi.org/10.1109/MPE.2008.931384
17. Kurt, M.N., Yilmaz, Y., Wang, X.: Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Trans. Inf. Forensics Secur. **14**(2), 498–513 (2018). https://doi.org/10.1109/TIFS.2018.2854745
18. Law, Y.W., Alpcan, T., Member, S., Palaniswami, M.: Security games for risk minimization in automatic generation control. IEEE Tran. Power Syst. **30**(1), 223–232 (2015). https://doi.org/10.1109/TPWRS.2014.2326403
19. Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y.: A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid **8**(4), 1630–1638 (2017). https://doi.org/10.1109/TSG.2015.2495133
20. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 21–32 (2009). https://doi.org/10.1145/1952982.1952995
21. Lun, Y.Z., D'Innocenzo, A., Malavolta, I., Di Benedetto, M.D.: Cyber-physical systems security: a systematic mapping study, pp. 1–32 (2016)
22. Maghrabi, L., Pfluegel, E., Al-Fagih, L., Graf, R., Settanni, G., Skopik, F.: Improved software vulnerability patching techniques using CVSS and game theory. In: International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) (2017)
23. Maharjan, S., Zhu, Q., Zhang, Y., Gjessing, S., Basar, T.: Dependable demand response management in the smart grid: a Stackelberg game approach. IEEE Trans. Smart Grid **4**(1), 120–132 (2013). https://doi.org/10.1109/TSG.2012.2223766
24. Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., Sinopoli, B.: Cyber-physical security of a smart grid infrastructure. Proc. IEEE **100**(1), 195–209 (2012). https://doi.org/10.1109/JPROC.2011.2161428
25. Mohsenian-Rad, A.H., Wong, V.W.S., Jatskevich, J., Schober, R.: Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid. In: Innovative Smart Grid Technologies Conference, ISGT, pp. 1–6 (2010). https://doi.org/10.1109/ISGT.2010.5434752
26. Mohsenian-Rad, A.H., Wong, V.W.S., Jatskevich, J., Schober, R., Leon-Garcia, A.: Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. IEEE Trans. Smart Grid **1**(3), 320–331 (2010). https://doi.org/10.1109/TSG.2010.2089069
27. Palensky, P., Dietrich, D.: Demand side management: demand response, intelligent energy systems, and smart loads. IEEE Trans. Ind. Inform. **7**(3), 381–388 (2011). https://doi.org/10.1109/TII.2011.2158841
28. Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., Smeraldi, F.: Cybersecurity games and investments: a decision Support approach, pp. 266–286 (2014). https://doi.org/10.1007/978-3-319-12601-2_15
29. Panwar, N.L., Kaushik, S.C., Kothari, S.: Role of renewable energy sources in environmental protection: a review. Renew. Sustain. Energy Rev. **15**(3), 1513–1524 (2011). https://doi.org/10.1016/j.rser.2010.11.037
30. Pilz, M., Al-Fagih, L.: Recent advances in local energy trading in the smart grid based on game-theoretic approaches. IEEE Trans. Smart Grid (2017). https://doi.org/10.1109/TSG.2017.2764275
31. Pilz, M., Al-Fagih, L.: A dynamic game approach for demand-side management: scheduling energy storage with forecasting errors. Dyn. Games. Appl. (2019). https://doi.org/10.1007/s13235-019-00309-z
32. Pilz, M., Al-Fagih, L., Pfluegel, E.: Energy storage scheduling with an advanced battery model: a game-theoretic approach. Inventions **2**(4), 30 (2017). https://doi.org/10.3390/inventions2040030
33. Pilz, M., Nebel, J.C., Al-Fagih, L.: A practical approach to energy scheduling: a game worth playing? In: IEEE PES Innovative Smart Grid Technologies Conference Europe (2018)
34. Rahbar, K., Xu, J., Zhang, R.: Real-time energy storage management for renewable integration in microgrid: an off-line optimization approach. IEEE Trans. Smart Grid **6**(1), 124–134 (2015). https://doi.org/10.1109/TSG.2014.2359004
35. Rahman, M.A., Mohsenian-Rad, H.: False data injection attacks with incomplete information against smart power grids. In: IEEE Global Telecommunications Conference, pp. 3153–3158 (2012). https://doi.org/10.1109/GLOCOM.2012.6503599
36. Rawat, D.B., Bajracharya, C.: Cyber security for smart grid systems: status, challenges and perspectives. SoutheastCon **2015**, 1–6 (2015). https://doi.org/10.1109/SECON.2015.7132891
37. Saad, W., Han, Z., Poor, H.V., Başar, T.: Game-theoretic methods for the smart grid: an overview of microgrid systems, demand-side management, and smart grid communications. IEEE Signal Process. Mag. **29**(5), 86–105 (2012). https://doi.org/10.1109/MSP.2012.2186410
38. Sanjab, A., Saad, W.: Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. IEEE Trans. Smart Grid **7**(4), 2038–2049 (2016). https://doi.org/10.1109/TSG.2016.2550218
39. Shoham, Y., Leyton-Brown, K.: Multiagent Systems, 1st edn. Cambridge University Press, Cambridge (2009)
40. Sioshansi, F.P.: Smart grid. In: International Conference on Wireless Communications and Signal Processing, WCSP (2012). https://doi.org/10.1016/C2010-0-68348-9
41. Soliman, H.M., Leon-Garcia, A.: Game-theoretic demand-side management with storage devices for the future smart grid. IEEE Trans. Smart Grid **5**(3), 1475–1485 (2014). https://doi.org/10.1109/TSG.2014.2302245
42. Tan, S., De, D., Song, W.Z., Yang, J., Das, S.K.: Survey of security advances in smart grid: a data driven approach. IEEE Commun. Surv. Tutor. **19**(1), 397–422 (2017). https://doi.org/10.1109/COMST.2016.2616442
43. Tesla: Tesla powerwall 2 (2017). https://www.tesla.com/en_GB/powerwall

44. U.S. Dept. of Energy: Commercial and residential hourly load profiles for all TMY3 locations in the United States (2013). https://openei.org/doe-opendata/dataset
45. U.S. Dept. of Energy: Microgrid definition (2016). https://building-microgrid.lbl.gov/microgrid-definitions
46. Wang, W., Lu, Z.: Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**(5), 1344–1371 (2013). https://doi.org/10.1016/j.comnet.2012.12.017
47. Wu, H., Wang, W.: A game theory based detection method for internet of things systems. IEEE Trans. Inf. **13**(6), 1432–1445 (2018)
48. Xiang, Y., Wang, L.: A game-theoretic study of load redistribution attack and defense in power systems. Electr. Power Syst. Res. **151**, 12–25 (2017). https://doi.org/10.1016/j.epsr.2017.05.020
49. Yaagoubi, N., Mouftah, H.T.: User-aware game theoretic approach for demand management. IEEE Trans. Smart Grid **6**(2), 716–725 (2015). https://doi.org/10.1109/TSG.2014.2363098
50. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on cyber security for smart grid communications. IEEE Commun. Surv. Tutor. **14**(4), 998–1010 (2012). https://doi.org/10.1109/SURV.2012.010912.00035
51. Yang, X., He, X., Lin, J., Yu, W., Yang, Q.: A game-theoretic model on coalitional attacks in smart grid. In: Proceedings—15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 435–442 (2016). https://doi.org/10.1109/TrustCom.2016.0094
52. Zhu, Q., Bas, T.: Robust and resilient control design for cyber-physical systems with an application to power systems, pp. 4066–4071 (2011). https://doi.org/10.1109/CDC.2011.6161031

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.