Game of Trade-off in Differential Privacy

Md Tamjid Hossain, Shamik Sengupta
University of Nevada, Reno, NV, USA
Email: mdtamjidh@nevada.unr.edu, ssengupta@unr.edu

***Abstract*—**

***Index Terms*—Data Privacy, Data Security, Data Utility, Cyber-Physical Systems (CPS), Differential Privacy (DP), Game theory**

I. Introduction

Differential privacy (DP) is an emerging privacy-preserving technique which has caught a lot of attention lately [1]. Modern Cyber-physical Systems (CPSs) (e.g., smart grid, smart health care, etc.) as well as various leading technology companies all around the world (e.g., Apple [2], Google [3], Uber [4]) are integrating DP for data privacy-preservation and training various Machine Learning (ML) models in order to carry out advanced analytics for business improvement with predictive and statistical analysis. However, the privacy guarantee of the DP mechanism comes with the cost of data utility. Over the years, several research have been conducted to address the optimization problem between data privacy and data utility [need ref]. Some of them have also utilized game theoretic approach to model and subsequently solve the trade off problem.

Nevertheless, the trade-off scenario between data privacy and data utility in DP-mechanism can largely vary with the application requirements. For example, state estimation of a smart grid requires highly accurate data since various real-time operations (e.g, synchronization of generators, islanding, load balancing, etc.) depend on the computed state estimation. Therefore, in these type of mission-critical settings, privacy requirements can be lower than the utility requirements. Contrarily, energy consumption, used for the applications such as consumer's demand prediction for day ahead, carry the confidential information of customers and thus require high data privacy. So, the game theoretic DP-models and solutions can also vary based on application requirements which is why more research need to be conduct to address this requirements and variations while modelling the trade-off game in DP-based applications.

Moreover, a new backdoor attack avenue has been identified exploiting DP lately [5], [6]. The attack leverages the noise of the DP mechanism to create stealthy False Data Injection (FDI) attacks. In particular, the integrity of the data can be reduced exploiting large noise induced by DP mechanism. So, the confidentiality of the data through DP-mechanism comes with not only the cost of less data utility but also the risk of more integrity attacks (or, security). With this new development on backdoor attacks exploiting DP, it has now become an alarming issue to use DP without properly analyzing the application-specific data privacy, security and utility requirement. At the same time, as DP has been proposed to apply in edge computing to protect the privacy of the resource-constraints edge devices, it is crucial to analyze the impact of the resources during trade-off scenario analysis. Generally, edge devices possess limited resources and computational ability which is why various defensive measures (e.g., firewalls, IDSs-Intrusion Detection Systems, honeypots, bad data filtration, etc.) cannot be applied directly to them. Rather, such defensive measures may be applied for only the mission-critical applications on a need basis. Therefore, it has become an issue of paramount importance to analyze the trade-off scenario among data privacy, utility, and security considering the resource constraints of the end devices.

This trade-off scenario can be modeled as a game between a defender and an attacker (or adversary) where being a rational player, each one of them will try to maximize their own profits (i.e., defender's profit is maximum data privacy, utility and security while the attacker's profit is maximum damage and minimum disclosure). As the trade-off scenario has all the elements of a game, it can be portrayed as traditional non-cooperative game which can be analyzed and successively solved for optimal solution using game theory. Therefore, it is non-trivial to devise more and more game theoretic models for solving the trade-off game among data privacy, utility and security in DP-based applications considering adversarial presence.

A. *Motivations*

Our main motivation behind this research comes from the fact that the data integrity can be compromised exploiting the data privacy-preserving procedure used in DP-mechanism. In particular, the more privacy we apply over the data through DP-technique, the more the attacker gets opportunity to compromise data integrity through traditional data poisoning attacks (e.g., FDI attacks). So, in some cases, it requires to sacrifice some data privacy over data utility and data integrity while in other settings, the requirement follows opposite.

On the other hand, game theory is a very popular framework for understanding the choices in situations among competing players [7]–[10]. It helps the players to reach optimal decision-making when confronted by independent and competing actors in a strategic setting. Therefore, in DP-based applications, where both the defender and the attacker are playing against each other to maximize their payoffs, it is crucial to understand the trade-offs among choices and their impacts over the overall data privacy, utility, and security offered by the DP-technique. In this regard, the game theory can be very beneficial to model the choices of the players as a game based on their strategies and successively solve the game to achieve the optimal solution for both the players.

Previous research have mostly focused on the game-theoretic approach for solving the trade-off problem between data privacy and data utility in DP-mechanism [11]–[13]. However, to the best of our knowledge, very little research have been conducted (if none) to consider game-theoretic approach to solve the trade-off problem not only between the data privacy and utility but also in the inter-section of data security considering adversarial presence.

B. Contributions

In this research, we aim to formulate the trade-off problem among the data privacy, utility, and security in DP-based CPS application as a attack-defender non-zero sum game. For this, we consider a smart grid domain where smart meters are acting as the edge nodes and the SCADA (Supervisory Control and Data Acquisition) control station as the master node. Moreover, we take the resource limitation of the edge devices and adversarial presence into account while formulating the game. Finally, we find the optimal solution of the game with necessary conditions. Our contributions in this research can be summarized as –

- We have modeled the trade-off among data privacy, utility, and security in differential privacy through a game theoretic approach under a resource-constraint environment whereas most of the previous studies have considered only the trade-off between data privacy and utility; not the data security.
- We have formulated a sample game (non-cooperative, non-zero-sum, sequential and complete but imperfect information game) among the edge nodes (smart meter), master node (SCADA control station), customers, and attacker.
- We have developed the necessary conditions to obtain the solution of the game by computing the subgame perfect Nash equilibrium (SPNE).

The rest of the paper is organized as follows. Related works along this research direction have been discussed in section II. Section III describes the research problem, adversarial model, attacker's and defender's goal. In section IV, the game has been formulated by describing the necessary components (e.g., players, strategies, utilities, etc.) while section V discuss our proposed game-theoretic approach to solve the trade-off problem among data privacy, security, and utility in DP-mechanism by computing subgame perfect Nash equilibrium (SPNE). Finally, we conclude the paper by mentioning some future research directions along this path in section VI.

II. Related Works

DP has been widely used as a privacy-preserving tool, specially from a last couple of years in various applications [1], [14]–[16]. However, a well known drawback of DP is the data utility reduction with respect to the data privacy increment [17]–[20]. Over the years, many research have been conducted to tackle this problem and find out the optimal solution of the trade-off problem between the data privacy and utility [21]–[23]. However, to the best of our knowledge, no research has been conducted on the trade-off problem of data privacy, utility, and security through game-theoretic approach.

Another related line of works focuses on the impacts and the defenses of data integrity attacks (e.g., FDI attack) on state estimation, future consumption prediction, billing, and pricing, etc. in the smart grid domain [24], [25]. Several techniques have been proposed over the years to prevent data integrity attacks using methods such as bad data filtration, blockchain, cryptographic encryption, etc. [26]. In particular, the integration of blockchain to achieve security and integrity has been found effective in the smart grid sector [27]–[29]. Although these works have considered the active attacks in their proposed schemes, they have not formulated these attacks in a system that uses DP-mechanism as a privacy-preserving tool.

Though some works have considered modelling the solutions of FDI attacks in a DP-based smart grid domain [30], they have not considered modelling the solutions for the type of FDI attacks which leverage the DP-noise in a smart grid domain. [..... will continue] Game theory in DP: [11]–[13]

Game theory on FDI attacks: [31]–[34]

Research on the trade-off of data privacy, utility, and security in DP-mechanism: [5], [6] [..... will continue]

III. Problem Statement

In this section, we first discuss about the key problems in this research direction and then talk about the adversarial model. Then, we investigate the capability of the adversary as well as his objectives. We also outlines the defender's objectives as well as our research objectives. The major symbols used in this paper are given in Table I.

A. Exploitation of DP-noise

Let's consider an intuitive overview depicting how the attacker can exploit DP to avoid the detection. Suppose, a smart meter is sending energy consumption data of the users to a master station, following a sequence of positive values,

TABLE I
List of major symbols and their description

Symbols	Description	Symbols	Description
A	Attacker	D	Defender
A_i	Attack impact	D_c	Attack disclosure
S_A	Attacker's Strategy	S_D^x	Defender's strategy
η	Laplace noise	x	Measurement value
ε	Privacy loss	Δf	Data sensitivity
P	Data privacy	U	Data utility
S	Data security	R	Resources
I_A	Attacker's income	I_D	Defender's income
E_A	Attacker's expenses	E_D	Defender's expenses
G_A	Attacker's utility	G_D	Defender's utility
I_P	Privacy incentive	I_{cu}	Utility incentive
I_{cs}	Security incentive	V_{pen}	Attack disclosure penalty
V_p	Penalty for privacy leakage	V_q	Penalty for utility degradation
V_s	Penalty for security breach	F_B	Fixed cost for bad data filters
F_I	Fixed cost for IDSs	F_S	Fixed cost for attack setup
G	Entire game	G'	Subgame

$x(0), x(1), x(2), ...$ If we consider a regular scenario where $\mid x(i-1) - x(i) \mid < k$ for some constant k, then violating the condition will raise alarm or detect anomalous behaviour of the data at the master station.

An attacker can manipulate a portion of the data (e.g., $x(0), x(1), x(2), ...x(m)$) and make them larger to misguide the master station. However, if the attacker wants to conduct stealthy attack, he can only modify each value by maximum k relative to the previous value and in the process can only get $x(m) \leq x(0) + k.m.$

Till this end, no privacy preserving mechanism have been considered. But, if we consider DP-mechanism to protect the smart meter values, the values will be changed accordingly the DP-mechanism. In particular, DP-mechanism will add random noise from any distribution that satisfies the DP-condition (e.g., Laplace, Gaussian, Exponential, etc.). Let's say, noise $\eta(i)$ is drawn from a Laplace distribution (i.e. $\eta(i) = Lap(\frac{\Delta f}{\varepsilon})$ where Δf is the data sensitivity and ε is the privacy loss) and added to each measurement values to get $x'(i)$ (i.e., $x'(i) = x(i) + \eta(i)$). Then, the condition for checking anomalous behavior of the data will be changed as $\mid x'(i-1) - x(i) \mid < 1.1k$ considering 99% probability. The adversary can exploit this changed scenario and manipulate the data by a larger value while remain undetected.

To tackle this problem of exploiting DP as a tool to conduct conventional data poisoning attacks (or FDI attacks) in a man-in-the-middle manner, first, it is essential to understand the data privacy, utility and security requirement of the considered application and then, need to select the magnitude of the noise by tuning the privacy loss (ε) to the desired level.

B. Resource Limitation

Resource limitation is another key problem in smart grid domain. As we discussed earlier in section I, generally, edge devices are limited with fewer computational power, memory, storage, etc. Therefore, they can only perform simpler task than the SCADA controller or other higher level nodes. This resource restriction prevents the edge devices to host various defensive measures such as honeypots, IPSs (Intrusion Prevention Systems), IDSs (Intrusion Detection Systems), firewall, encryption mechanisms, bad data filtration etc. Consequently, the edge devices normally cannot detect or prevent malicious presence. At the same time, hosting above defensive measures in the master node (i.e., SCADA control station) also incurs monetary cost and computational overhead. So, during the trade-off analysis among data privacy, utility, and security in DP-mechanism, cost of installing additional resources to detect the malicious actor and filter the anomalous data for producing sanitized data must be considered. Otherwise, the game will not be a realistic game and the solution of the game will not come to any help.

C. Trade-off Problem among Resource Limitation, Data Privacy, Utility, and Security

The DP-based application aims to maximize the data security, privacy, and utility while keeping resource utilization at a minimum level. This too depends on the privacy loss parameter of DP-mechanism (ε). A small ε (alternatively, large noise) may provide high data privacy but reduces the data utility significantly in the process. Similarly, minimizing resource utilization (i.e., less computation, minimum bandwidth utilization, less memory consumption, etc.) conflicts with the defender's objective of maximizing the minimum disclosure probability. On the other hand, deploying more defensive measures (e.g., IDSs, firewalls, BDD etc.) maximizes the probability of identifying malicious activity but at the same time, also maximizes the resource utilization. Therefore, a game of trade-off is essential to solve the conflicting cases and maximize the optimal payoff of both the defender and the attacker. We elaborate this trade-off problem in a game theoretic approach and successively reach to the optimal solutions based on different circumstances in Section IV.

D. Adversarial Model

The adversary provides false query values to the customers who are expecting differentially private result that contains the Laplacian noise. In particular, we consider several entities namely, edge nodes, master node, customers, and malicious node in our setting. However, though the edge nodes and the customers are influencing the decisions of the master node and the malicious node by providing granular data and incentives respectively, the main players of our proposed game are the master node (acting as defender) and the malicious node (attacker). A malicious actor, playing as a man-in-the-middle, can compromise some of the edge nodes (smart meters) physically and inject false data in the data packets going out from edge nodes [35]. Additionally, the adversary can intercept the communication path and forge data packets while transferring to the master nodes (e.g., SCADA control station) from the edge nodes (e.g., smart meters) of the grid network [36]–[40]. Alternatively, the attacker can also modify the master node database [41]. For our proposed model, we also consider that the attack (FDI attack) will happen eventually and formulate the game based on this assumption. Moreover, as the DP is applied to protect the privacy of the edge nodes, we consider applying DP while transferring the edge data to the control station (i.e., local DP).

E. Attacker's objective

The main objective of the adversary is to create devastating attacks. The more damaging the attacks are, the more incentives the adversary obtains. Nonetheless, another objective of the adversary is to conduct stealthy attacks. More specifically, the adversary wishes to hide his attacks from the IDSs as well as wants to remain undetected as long as possible. In short, the objectives of the adversary (A) can be describe as –

$$\max_{A} \; A_i \;\; To\; maximize\; the\; attack\; impact$$
$$\min_{A} \; D_c \;\; To\; minimize\; the\; disclosure$$

To achieve the first objective, the adversary tries to manipulate the original value as large as possible. In particular, the adversary injects a large magnitude of false measurement into the original measurement and hides behind the DP-noise. For instance, in a power outage prediction ML model that uses differentially private energy consumption data as the training data, the adversary may want to misclassify an actual power outage incident (or blackout event) of an area as uninterrupted power delivering case through targeted data (or model) poisoning attacks. Therefore, the metrics of measuring the first objective (i.e., the maximum attack impact, $\max_{A} \; A_i$) indicates the maximum deviation of the manipulated value from original value.

The second objective of the adversary (i.e., minimum disclosure, $\min_{A} \; D_c$) requires the attack to be as stealthy as possible. This can be achieved by evading the anomaly detectors or bad data detection (BDD) mechanism in the master node. However, the defensive approach based on BDD mostly works in the post-attack phase and does not guarantee enough protection during the on-going attack scenario. The adversary can leverage this information and try to fulfil his first objective for a short period. Nevertheless, to remain undetected and thus be able to carry out the attack for a longer period, the adversarial output should be as close as the original value. This can be achieved by – (1) injecting a small amount of false measurement or (2) only manipulating the targeted value while keeping the overall data utility stable and satisfactory.

Therefore, these two objectives of the adversary are conflicting in a sense that achieving maximum attack impact requires injecting high amount of false measurement whereas achieving stealthiness requires injecting low amount of false measurement. To optimize these two objectives, the adversary will follow the multi-criteria optimization procedure as described by our proposed game model in Section IV.

F. Defender's Objective

In an attack-defense or defense-attack setting, the defender's sole objective is to minimize the maximum utility of the adversary. More specifically, the defender's objective is restrict the ability of the adversary from conducting devastating attack (i.e., closing the gap of the original outcomes and manipulated outcomes) as well as detect the attack as soon as possible. In short, the objective of the defender (D) can be described as –

$$\min_{D} \max_{A} \; A_i \;\; and \;\; \max_{D} \; D_c$$

The first objective of the defender (i.e. minimize the maximum attack impact, $\min_{D} \max_{A} \; A_i$) can be achieved by carefully selecting the privacy loss parameter (ε) of DP-mechanism for each node. This is because, selection of small ε yields to larger noise, which in turn, assists the adversary to achieve his first objective. The second objective of the defender is related to the resource utilization. The more he uses the resources to increase the performance of the anomaly detector in differentiating small manipulation from original value, the more the probability of maximizing the attack disclosure.

G. Research Objective

In this research, we focus on finding the optimal decisions for both the attacker and defender in a resource-constraint environment for the DP-based smart grid applications. The optimal decisions for both the players are based on the target of achieving maximum data privacy, utility, and security (defender) as well as achieving maximum damage and minimum disclosure (attacker). More specifically, the key objectives of our research are to–

- Analyze the criterion affecting the data privacy, utility, and security in a DP-based setting under adversarial configuration
- To model the trade-off problem among data privacy, utility, and security based on the attacker's target to achieve maximum damage and minimum disclosure in a game-theoretic approach under a resource-constraint environment
- To derive the necessary conditions for obtaining the solution of the game by computing SPNE.

IV. Proposed Model

In this section, we first classify the game based on players, strategies, and their utilities. Then, we describe the PSU of the game (i.e., P: Players, S: Strategies, U: Utilities). Next, we demonstrate the rule of the game to be played, finally, we outlines the optimal way to find the equilibrium strategies of the players based on various circumstances. An overview of our proposed game model is illustrated in Fig. 1.

A. Game Taxonomy

The game between the attacker and defender in our proposed setting can be illustrated as either a defense-attack game or a defense-attack-defense game. In the defense-attack scenario, the defender first design the DP-based grid network (i.e., selects privacy loss, ε for each and every node based on application requirements) and the defense mechanism (i.e., IDSs operational principle, number of IDSs, placement of IDSs throughout nodes, etc.) considering adversarial presence. And then, the adversary selects his strategy for meeting his objectives and perform the attack. On the other hand, in the defense-attack-defense scenario, the defender first design the DP-based grid network as a part of defense strategy and then the adversary attacks the grid network according to his optimal strategy. Finally, the defender deploys the defensive measures (i.e., the resources such as IDSs, IPSs, firewalls, BDD, etc.) to detect the attack and sanitize the output. From this perspective, both

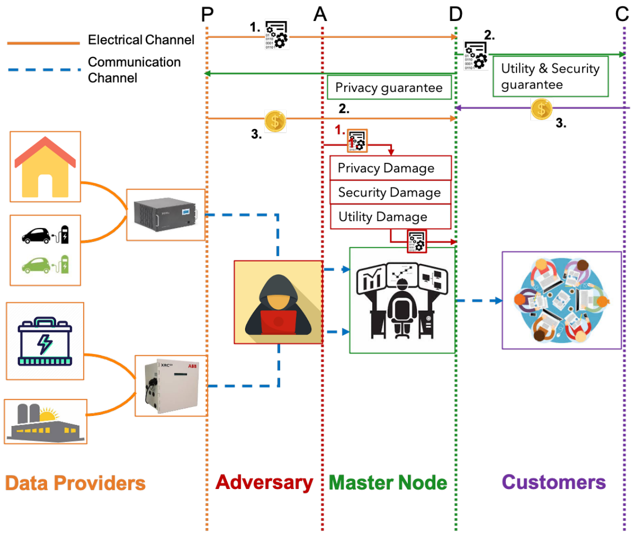

Fig. 1. Proposed model

the settings classify the game as a dynamic game. In our proposed model, for the simplicity we are only considering the later approach which is defense-attack-defense model. The taxonomy of our proposed game model (i.e., defense-attack-defense) is shown and described in Table II.

B. Players

In our proposed game model, there are two players; attacker and defender. So, it is essentially a two-person game. However, this game can also be modeled as N-person game where there can be multiple defenders and multiple attackers. Though the game is a two-person game, there can be multiple other parties involved (e.g., data providers, customers, etc.). For instance, a number of earlier research suggest to incorporate other privacy-preserving mechanisms (e.g., randomized perturbation [42], homomorphic encryption [43], etc.) with DP to provide more data privacy. In those settings, trusted third parties or key management center can be another player of the game. Nevertheless, in the proposed setting, the players play the game sequentially. Also, in a single game, the defender makes move twice while the attacker makes his moves only once.

C. Strategies

The strategies of both the attacker and defender depend on application requirements and thus can be varied accordingly for changing circumstances. For example, the mission-critical operations (e.g., state estimation for distributed generator synchronization) require high data utility (alternatively, less noisy differentially private data) whereas day ahead energy consumption prediction application, which carries sensitive information of the user, require high data privacy (alternatively, more noisy differentially private data). Therefore, based on these changing scenarios, the attacker and the defender chooses their optimal strategies and try to maximize their profits. In the proposed game model, we consider the strategies for both players as follows:

1) Adversarial Strategies: In general, the adversary follows two conflicting strategies to achieve his objectives that are – (1) Maximum damage, or, (2) minimum disclosure. More specifically, if the adversary is A, the set of adversarial strategy is S_A, maximum damage is $max(A_i)$, and the minimum disclosure is $min(D_c)$, then the adversarial strategies can be described as follows:

$$S_A = \{max(A_i), min(D_c)\} \tag{1}$$

2) Defender's Strategies: In the first stage of the game (i.e., designing the DP mechanism and selecting privacy loss, ε), the defender considers the data privacy, utility, and security. Since all of these (i.e., data privacy, utility, and security) are highly correlated with the privacy loss, ε, the defender has two strategies two follow to maximize his payoff – (1) selecting small ε ($\varepsilon = 0.1$), or, (2) selecting large ε ($\varepsilon = 1.0$. For this particular game, we are not considering the moderate or optimal level of ε since the optimal level of ε is not known in advance; rather we are focusing on computing the equilibrium strategies of the game based on boundary conditions (i.e., maximum data utility as upper bound and maximum privacy as lower bound of ε). We are selecting ε value within $[0.1, 1.0]$ since previous studies suggest to keep the ε between 0.1 to 1.0 [44]. Accordingly, the defender's strategy in the first stage can be described as follows:

$$\begin{aligned} S_D^1 = \{&\varepsilon = 0.1 : [P_{max}, U_{min}, S_{min}], \\ &\varepsilon = 1.0 : [P_{min}, U_{max}, S_{max}]\} \end{aligned} \tag{2}$$

where, S_D^1 is the strategy set of the defender in first stage, P_{max} is maximum privacy, P_{min} is minimum privacy, U_{max} is maximum utility, U_{min} is minimum utility, S_{max} is maximum security, S_{min} is minimum security.

After the attacker plays in the second stage of the game, the defender plays again sequentially in the third stage of the game. In this third stage, the defender has again two strategies to follow– (1) maximum resource deployment, or (2) minimum resource deployment. Defender either selects the maximum resource (e.g., IDSs, anomaly detectors, etc.) deployment strategy to detect the malicious activity, generally in expense of monetary value and computational burden, or selects the minimum resource deployment strategy to reduce the cost and computational overhead. Therefore, the strategy of the defender in the third stage of the game can be expressed as follows:

$$S_D^2 = \{R_{max}, R_{min}\} \tag{3}$$

where S_D^2 denotes the strategy set of the defender in second stage, R_{max} is the maximum resource utilization, and R_{min} is the minimum resource utilization.

D. Utilities

Albeit there can be several parties (e.g., data providers, adversary, master node, customers as depicted in Fig. 1) interacting among themselves, the proposed game is being played only between the adversary (or attacker) and the

TABLE II
TAXONOMY OF THE PROPOSED GAME

Classification	Description (Players: Attacker-A, Defender-D)
Dynamic game	A and D make their moves multiple times in contrast to single move in static games
Non-cooperative game	A and D are playing against each other and trying to maximize their own payoff in a non-cooperative manner
Non-zero-sum game	The payoffs of A and D are not opposite and equal in value all the time due to varying scenarios
Two-person game	Though there can be multiple other parties (e.g., edge devices or data providers, customers, etc.), the game is played between the defender and the attacker
Sequential interaction game	The proposed game follows defense-attack-defense model where each player plays one after another
Complete information game	Both A and D makes their moves knowing each others ultimate goals, strategies and payoffs
Imperfect information game	After a certain stage of the game (more specifically after 2^{nd} stage), no one has information about other's strategy

master node (defender). Nevertheless, the payoffs of both the attacker and the defender significantly depend on the payments and rewards from the data providers and customers.

1) Defender's Utility: In our proposed setting, we are considering the data providers as the physical layer components of a smart grid network (e.g., smart houses, smart meters, PMUs-Phasor Measurement Units, RTUs-Remote Terminal Units, IEDs, etc.). The data providers provide data to the master node (i.e., defender). We are assuming the data providers pay some incentives to the defender (i.e., $I_p = \sum_{i=0}^{N} I_p^i \ \forall i \in N\ where\ N\ denotes\ the\ number\ of\ data\ providers$) if they obtain a certain level of data privacy guarantee from the defender as shown in Fig. 1 (step-1 to step-3).

In parallel, we consider the customers as the individuals or organizations who need grid data for their specific applications (e.g., data analytics, research, disturbance analysis, demand prediction, etc.). The defender utilizes his resources to sanitize the differentially private data (either manipulated or not) and send it to the customers. The customers pay incentives to the defender (i.e., $I_c = \sum_{i=0}^{N} I_c^i$ $\forall i \in N\ where\ N\ denotes\ the\ number\ of\ customers$) if they obtain a certain level of data utility and data security (alternatively, data integrity) guarantee from the defender as shown in Fig. 1 (step-1 to step-3). The incentive from each customers can be divided into two parts: I_{cu} and I_{cs}; where I_{cu} is the incentive regarding data quality and I_{cs} is the incentive regarding data integrity. Moreover, in case of any attack incident, if the defender can successfully disclose the attack and the attacker's identity, he will earn the penalty from the attacker as a form of incentive. Therefore, defender's total incentive from data providers and customers is–

$$I_D = \begin{cases} I_P + I_{cu} + I_{cs} + V_{pen} & \text{attack detected} \\ I_P + I_{cu} + I_{cs} & \text{otherwise} \end{cases} \tag{4}$$

The defender has some fixed costs and some variable costs. We define the defender's fixed cost incurred from deploying the resources (for simplicity, we consider two resources, IDS and bad data filters). The variable costs can be portrayed as penalties due to the data privacy leakage, data utility degradation and data security breach incident under any successful attack. This penalties are paid to the attacker from the defender according to the particular incident. Therefore, the expenditure of the defender can be described as–

$$E_D = \begin{cases} F_B + F_I + V_p + V_q + V_s & \text{attack not detected;} \\ F_B + F_I & \text{otherwise} \end{cases} \tag{5}$$

where E_d is the total expenditure of the defender, F_B and F_I are the fixed cost for bad data filtration and IDS respectively, V_p, V_q, V_s are the variable cost for data privacy leakage, data utility degradation and data security breach in the form of penalty. Therefore, the total utility (G_D) of the defender is-

$$G_D = I_D - E_D \tag{6}$$

2) Attacker's Utility: The attacker makes his incentives through devastating attacks and successful hideout. In other words, the attacker earns what the defender looses. However, the attacker also has the fixed cost and variable cost. We consider the attacker's fixed cost due to the apparatus cost for attack setup and the variable cost due to the penalty in case of successful attack disclosure by the defender. In short, the attacker's total utility (G_A) can be described as follows:

$$\begin{gathered} G_A = I_A - E_A\ s.t. \\ I_A = \begin{cases} I_D + (E_D - F_B - F_I) & \text{attack not detected} \\ 0 & \text{otherwise} \end{cases} \\ and\ E_A = F_S + V_{pen} \end{gathered} \tag{7}$$

where I_A and E_A are the total incentive and expenditure of the attacker, F_S is the fixed cost for attack setup (i.e., apparatus cost), V_{pen} is the variable cost for attack disclosure by the defender as a form of penalty. However, the utilities of the defender and the attacker vary based on their selected strategies; we will elaborate this in Section IV-E.

E. Game Rules: Strategies vs Utilities

In our proposed model, we consider defense-attack-defense scenario where the defender will play first, then the attacker, and finally the defender will play again. From (1) to (3), it can be inferred that the attacker has two strategies to choose whereas the defender has a set of total four strategies to choose throughout the game. Both attacker's and defender's strategies are shown in Table III. Based on these strategies, the payoffs of both player (defender: G_D^{xy}, attacker: G_A^{xy}) will vary. Here, we can consider four different cases from defender's perspective as follows:

TABLE III
PAYOFF MATRIX OFF THE GAME

Players / Strategies / Utilities		**Attacker**	
		$max(A_i)$	$min(D_c)$
Defender	$(\varepsilon = 0.1, R_{max})$	(G_D^{11}, G_A^{11})	(G_D^{12}, G_A^{12})
	$(\varepsilon = 0.1, R_{min})$	(G_D^{21}, G_A^{21})	(G_D^{22}, G_A^{22})
	$(\varepsilon = 1.0, R_{max})$	(G_D^{31}, G_A^{31})	(G_D^{32}, G_A^{32})
	$(\varepsilon = 1.0, R_{min})$	(G_D^{41}, G_A^{41})	(G_D^{42}, G_A^{42})

1) Case-01 ($\varepsilon = 0.1, R_{max}$): As the defender is selecting minimum privacy loss, the data privacy is preserved regardless of whatever strategy the attacker chooses. If the attacker chooses maximum attack strategy while defender deploys his full resources (both IDSs and Bad data filters), the attack is identified (data security guarantee provided) and bad data is filtered (data utility is preserved). Since the attack is disclosed, the attacker is punished with the penalty fee, V_{pen}. Both the player bears their fixed cost in the process. Therefore, the payoffs of the defender and the attacker are–

$$G_D^{11} = (I_P + I_{cu} + I_{cs} + V_{pen}) - (F_B + F_I) \tag{8}$$

$$G_A^{11} = -(V_{pen} + F_S) \tag{9}$$

However, if the attacker chooses minimum disclosure strategy, the defender cannot identify the adversarial presence (security breached). But, he can still filter the bad data (data utility preserved). As the attack is not identified, the attacker needs not to pay any penalty; rather he earns incentives from data security breach. In that scenario, the payoffs of the defender and the attacker are-

$$G_D^{12} = (I_P + I_{cu}) - (V_s + F_B + F_I) \tag{10}$$

$$G_A^{12} = (I_{cs} + V_s) - (F_S) \tag{11}$$

2) Case-02 ($\varepsilon = 0.1, R_{min}$): Similar to the Case-01, the defender is selecting minimum privacy loss; so, the data privacy is preserved regardless of whatever strategy the attacker chooses. If the defender goes for the minimum resources, the attack will still be identified (data security guarantee provided) as the attacker makes maximum attack without paying much attention to the attack disclosure to maximize his payoff. However, due to minimum resource utilization, bad data is not filtered (data utility degraded). Since the attack is disclosed, the attacker is punished with the penalty fee, V_{pen}. Both the player bears their fixed cost in the process. Therefore, the payoffs of the defender and the attacker are–

$$G_D^{21} = (I_P + I_{cs} + V_{pen}) - (V_q + F_B) \tag{12}$$

$$G_A^{21} = (I_{cu} + V_q) - (V_{pen} + F_S) \tag{13}$$

However, if the attacker chooses minimum disclosure strategy, the defender cannot identify the adversarial presence (security breached). At the same time, due to minimum resource utilization, the defender cannot filter the bad data (data utility degraded) also. As the attack is not identified, the attacker needs not to pay any penalty; rather he earns incentives from data security breach and data utility degradation. In that scenario, the payoffs of the defender and the attacker are-

$$G_D^{22} = (I_P) - (V_q + V_s + F_I) \tag{14}$$

$$G_A^{22} = (I_{cs} + I_{cu} + V_s + V_q) - (F_S) \tag{15}$$

3) Case-03 ($\varepsilon = 1.0, R_{max}$): In this case, the defender selects maximum privacy loss; so, the data privacy is not preserved any more due to the small noise regardless of whatever strategy the attacker chooses. For this, the defender bears a penalty for data privacy leakage (V_p). If the attacker chooses maximum attack strategy while defender deploys his full resources (both IDSs and Bad data filters), the attack is identified (data security guarantee provided) and bad data is filtered (data utility is preserved). Since the attack is disclosed, the attacker is punished with the penalty fee, V_{pen}. Both the player bears their fixed cost in the process. Therefore, the payoffs of the defender and the attacker are–

$$G_D^{31} = (I_{cu} + I_{cs} + V_{pen}) - (V_p + F_B + F_I) \tag{16}$$

$$G_A^{31} = (I_P + V_p) - (V_{pen} + F_S) \tag{17}$$

However, if the attacker chooses minimum disclosure strategy, the defender cannot identify the adversarial presence (security breached). But, he can still filter the bad data (data utility preserved). As the attack is not identified, the attacker needs not to pay any penalty; rather he earns incentives from data security breach and data privacy leakage. In that scenario, the payoffs of the defender and the attacker are-

$$G_D^{32} = (I_{cu}) - (V_p + V_s + F_B + F_I) \tag{18}$$

$$G_A^{32} = (I_{cs} + I_p + V_p + V_s) - (F_S) \tag{19}$$

4) Case-04 ($\varepsilon = 1.0, R_{min}$): In this case, the defender selects maximum privacy loss; so, the data privacy is not preserved any more due to the small noise regardless of whatever strategy the attacker chooses. For this, the defender bears a penalty for data privacy leakage (V_p). If the defender goes for the minimum resources, the attack will still be identified (data security guarantee provided) as the attacker makes maximum attack without paying much attention to the attack disclosure to maximize his payoff. However, due to minimum resource utilization, bad data is not filtered (data utility degraded). Since the attack is disclosed, the attacker is punished with the penalty fee, V_{pen}. Both the player bears their fixed cost in the process. Therefore, the payoffs of the defender and the attacker are–

$$G_D^{41} = (I_{cs} + V_{pen}) - (V_p + V_q + F_I) \tag{20}$$

$$G_A^{41} = (I_P + I_{cu} + V_p + V_q) - (V_{pen} + F_S) \tag{21}$$

However, if the attacker chooses minimum disclosure strategy, the defender cannot identify the adversarial presence (security breached). At the same time, due to minimum resource utilization, the defender cannot filter the bad data

(data utility degraded) also. As the attack is not identified, the attacker needs not to pay any penalty; rather he earns incentives from data security breach, data privacy leakage and data utility degradation. In that scenario, the payoffs of the defender and the attacker are-

$$G_D^{42} = -(V_p + V_q + V_s + F_I) \tag{22}$$

$$G_A^{42} = (I_p + I_{cu} + I_{cs} + V_p + V_q + V_s) - (F_S) \tag{23}$$

V. Subgame Perfect Nash Equilibrium (SPNE) Strategy

In this section, we focus on finding out the equilibrium strategies (SPNE-Subgame Perfect Nash Equilibrium) through backward induction method. Moreover, we discuss and evaluate the applicability of our proposed model from an economic and practical point of view. The extensive form of the game has been depicted in Fig. 2.

For each choice of the defender (i.e., $\varepsilon = 0.1$ or $\varepsilon = 1.0$) in the first stage, the attacker has two choices (i.e., $max(A_i)$ or $min(D_c)$). However, the attacker at this stage of the game does not know the strategy of the defender. Thus this game is an imperfect information game which can be solved using a concept called 'subgame perfection' suggested by Selten [45], [46]. In Fig. 2(a), the game of trade-off in differential privacy under adversarial presence has been depicted where we can find two proper subgames (Subgame-1 and Subgame-2) along with their nodes. Let us now give the formal definition of a proper subgame.

Definition 1 *The game G' is a proper subgame of an extensive-form game G if it consists of a single node in the extensive-form tree and all of its successors down to the leaves. Therefore, if a node $n_s \in G'$ then also $n_s \in G$ s.t. $G' \subset G$.* The subgame perfection concept also introduces subgame perfect Nash equilibrium (SPNE) strategy which can be understand through the following definition.

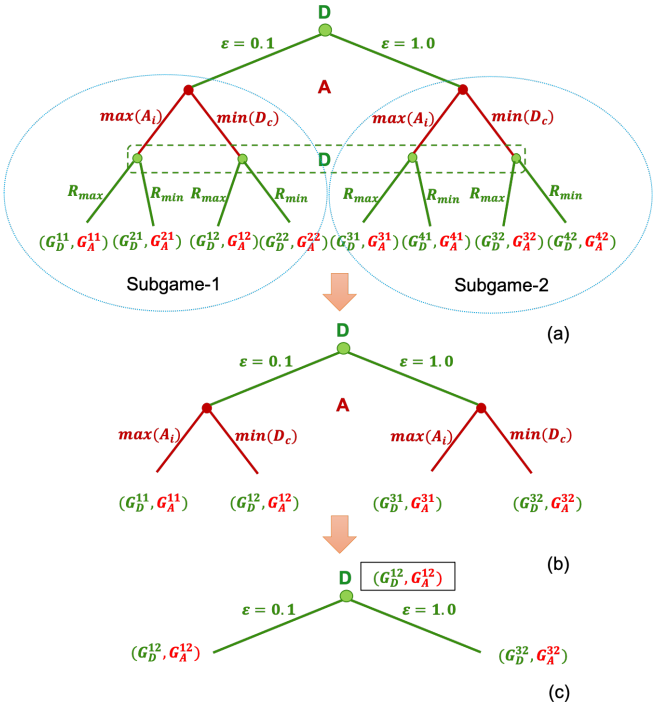

Fig. 2. Extensive form of the proposed dynamic game

Definition 2 *A strategy profile s can be called a subgame perfect Nash equilibrium (SPNE) strategy of an extensive-form game G if it specifies a Nash equilibrium in each of its subgames, ($G'_i \subset G$).*

A. Game Tree Representation

The game tree representation of Fig. 2(a) contains important information regarding our proposed game including *root of the tree, labels, choice nodes, dotted line, information set, terminal nodes*. We assume that the defender publishes the privacy loss level (i.e., the value of ε) he has deployed. This assumption is also practical as it will increase the trustworthiness of the DP-based applications among the stakeholders as suggested by Dwork et al. [47]. Based on this assumption, the attacker already knows the defender's strategy taken in the first stage of the game. However, as the game unfolds to multiple stages, the attacker and the defender do not have any more information about each other's move onwards.

B. Methodology for Computing SPNE

The steps to solve the game through backward induction process has been shown through Fig. 2(a)-(c). In both subgames, the defender, having no information of attacker's move, will try to maximize his payoff by selecting R_{max} strategies in every cases. This is because the R_{max} strategy provides more payoff to the defender than R_{min} that can be understood through analyzing the payoff expressions stated in section IV-E. For instance, the defender's payoff from (8), G_D^{11} is certainly greater than his payoff from (12), G_D^{21} since in the first case the defender obtains all the incentives whereas in the later case he looses incentive from data utility. Similarly, analyzing other relevant correlations, we can reach to below rationality constraints.

$$G_D^{11} \geq G_D^{21}, G_D^{12} \geq G_D^{22}, G_D^{31} \geq G_D^{41}, G_D^{32} \geq G_D^{42} \tag{24}$$

As the game progresses, we can compute the Nash equilibrium points (NEP) through backward induction method for both the subgames as illustrated in Fig. 2(b) and (c). From the reduced form of the game tree representation (Fig. 2(b)), the NEP for the subgames (from the attacker's point of view) are (G_D^{12}, G_A^{12}) and (G_D^{32}, G_A^{32}). Here, (G_D^{12}, G_A^{12}) and (G_D^{32}, G_A^{32}) supports the definition of Nash equilibrium which dictates- '*An outcome O^* of a game is a NEP if no player can unilaterally change its strategy and increase its payoff*'. This is so due to the below rationality constraints.

$$G_A^{11} \leq G_A^{12}, G_A^{31} \leq G_A^{32} \tag{25}$$

In other words, for G_A^{12} and G_A^{32}, the attacker can attack successfully and earn incentives from the attack impact whereas for G_A^{11} and G_A^{31}, the attack is disclosed and the attacker pays penalties as expressed by (9), (11), (17) and (19).

Successively, the Nash equilibrium point for the entire game can be computed from the further reduced form of the game tree (Fig. 2(c)). Comparing (10) and (18), we can say that the defender's payoff from (10) is greater than his payoff from (18). This is because in (18), the defender losses two incentives (i.e., incentives from privacy and security guarantee) whereas in (10), he only losses one incentive (i.e., the incentive from security guarantee) using same amount of resources. Formally, it can be expressed as below rationality constraint.

$$G_D^{12} \geq G_D^{32} \tag{26}$$

So, the Nash equilibrium point of the proposed game model is (G_D^{12}, G_A^{12}) which is also the Nash equilibrium point of subgame-1. Therefore, (G_D^{12}, G_A^{12}) is a subgame perfect Nash equilibrium (SPNE) solution of the game and it's corresponding strategy, $(\varepsilon = 0.1, max(A_i), R_{max})$ can be called as the SPNE strategy.

C. Discussion

The SPNE computed in section V is practical and reflects the best possible choices of both the players. Certainly, the defender can change his strategy to increase his payoff and obtain G_D^{11} instead of G_D^{12}. However, in that case the attacker's payoff (G_A^{12}) will decrease as he has to pay the penalty for attack disclosure (i.e., V_{pen}). Moreover, analyzing the cases stated in section IV-E, it is comprehensible that no other strategies can be found which will increase the payoff of both the players at the same time. In other words, '*given the SPNE strategy, no other strategy can be better off without making at least one player worse off or without any loss thereof*'. Therefore, the computed SPNE is also a Pareto-optimal point.

Although the game theoretic approach can solve many existing problems, specially in optimization or trade-off scenarios, one major criticism of game theory, as applied to the modelling of human strategies and decisions, is that human beings are, in practice, rarely fully rational. Therefore, modelling the human decision process by means of a few equations and parameters is questionable [48]. However, in the modern CPSs such as smart grids, the operators and the stakeholders do not interact with each other on such a fine-grained basis; rather they design their applications based on some well-agreed protocols (i.e., strategies). The applications may also capture the variations and dynamically adjust the protocols. Here, the applications play as the rational decision makers. Therefore, in the dynamic situations where applications and machines are interacting among themselves to choose the required data privacy, utility, and security level, our proposed game theoretic approach to find the equilibrium strategy will certainly assist the grid-controller to make rational decisions considering adversarial presence.

VI. Conclusion and Future works

In this paper, we formulate the trade-off problem among the data privacy, utility, and security in DP-based applications of a smart grid network as an attack-defender (more specifically, defense-attack-defense) non-zero-sum, dynamic, sequential and imperfect information game. We model this game in a resource-constraint and adversarial environment. Existing related works on the inter-section of DP-mechanism and smart grid only focused on the privacy-utility trade-off part and missed the data security along with resource utilization considerations. From this point of view, we devise a novel game-theoretic model for solving the trade-off among data privacy, utility, security and resource utilization. We also develop the methodology for solving the game and computing the subgame perfect Nash equilibrium (SPNE) under some realistic observations and feasible assumptions. Finally, through our discussion, we show that our solution of the game (i.e., SPNE) also achieves Pareto-optimality and so, provides the best optimal solution for the defender and the attacker playing in resource-constrained DP-based smart grid environment.

References

[1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography conference*. Springer, 2006, pp. 265–284.

[2] J. Tang, A. Korolova, X. Bai, X. Wang, and X. Wang, "Privacy loss in apple's implementation of differential privacy on macos 10.12," *arXiv preprint arXiv:1709.02753*, 2017.

[3] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 1054–1067.

[4] J. Near, "Differential privacy at scale: Uber and berkeley collaboration," in *Enigma 2018 (Enigma 2018)*, 2018.

[5] J. Giraldo, A. A. Cardenas, and M. Kantarcioglu, "Security vs. privacy: How integrity attacks can be masked by the noise of differential privacy," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 1679–1684.

[6] J. Giraldo, A. Cardenas, M. Kantarcioglu, and J. Katz, "Adversarial classification under differential privacy," in *Network and Distributed Systems Security (NDSS) Symposium 2020*, 2020.

[7] R. B. Myerson, *Game theory*. Harvard university press, 2013.

[8] M. J. Osborne *et al.*, *An introduction to game theory*. Oxford university press New York, 2004, vol. 3, no. 3.

[9] X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, "Service pricing decision in cyber-physical systems: Insights from game theory," *IEEE Transactions on Services Computing*, vol. 9, no. 2, pp. 186–198, 2015.

[10] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Computing Surveys (CSUR)*, vol. 50, no. 2, pp. 1–37, 2017.

[11] L. Cui, Y. Qu, M. R. Nosouhi, S. Yu, J.-W. Niu, and G. Xie, "Improving data utility through game theory in personalized differential privacy," *Journal of Computer Science and Technology*, vol. 34, no. 2, pp. 272–286, 2019.

[12] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, 2007, pp. 94–103.

[13] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Transactions on Big Data*, 2017.

[14] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[15] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[16] A. Friedman and A. Schuster, "Data mining with differential privacy," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2010, pp. 493–502.

[17] J. Bambauer, K. Muralidhar, and R. Sarathy, "Fool's gold: an illustrated critique of differential privacy," *Vand. J. Ent. & Tech. L.*, vol. 16, p. 701, 2013.

[18] A. Machanavajjhala, X. He, and M. Hay, "Differential privacy in the wild: A tutorial on current practices & open challenges," in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1727–1730.

[19] S. L. Garfinkel, J. M. Abowd, and S. Powazek, "Issues encountered deploying differential privacy," in *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, 2018, pp. 133–137.

[20] J. Zhao, Y. Chen, and W. Zhang, "Differential privacy preservation in deep learning: Challenges, opportunities and solutions," *IEEE Access*, vol. 7, pp. 48 901–48 911, 2019.

[21] S. E. Fienberg, A. Rinaldo, and X. Yang, "Differential privacy and the risk-utility tradeoff for multi-dimensional contingency tables," in *International Conference on Privacy in Statistical Databases*. Springer, 2010, pp. 187–199.

[22] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *2014 IEEE international symposium on information theory*. IEEE, 2014, pp. 2371–2375.

[23] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy: on the trade-off between utility and information leakage," in *International Workshop on Formal Aspects in Security and Trust*. Springer, 2011, pp. 39–54.

[24] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[25] J. Tian, B. Wang, and X. Li, "Data-driven and low-sparsity false data injection attacks in smart grid," *Security and Communication Networks*, vol. 2018, 2018.

[26] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *2013 IEEE Power & Energy Society General Meeting*. IEEE, 2013, pp. 1–5.

[27] A. Bhattacharjee, S. Badsha, A. R. Shahid, H. Livani, and S. Sengupta, "Block-phasor: A decentralized blockchain framework to enhance security of synchrophasor," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*. IEEE, 2020, pp. 1–6.

[28] A. Bhattacharjee, S. Badsha, and S. Sengupta, "Blockchain-based secure and reliable manufacturing system," in *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*. IEEE, 2020, pp. 228–233.

[29] M. T. Hossain, S. Badsha, and H. Shen, "Porch: A novel consensus mechanism for blockchain-enabled future scada systems in smart grids and industry 4.0," in *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. IEEE, 2020, pp. 1–7.

[30] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. S. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2483–2493, 2017.

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

[32] 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," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169–177, 2019.

[33] L. Niu and A. Clark, "A framework for joint attack detection and control under false data injection," in *International Conference on Decision and Game Theory for Security*. Springer, 2019, pp. 352–363.

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

[35] P. Xun, P. Zhu, Z. Zhang, P. Cui, and Y. Xiong, "Detectors on edge nodes against false data injection on transmission lines of smart grid," *Electronics*, vol. 7, no. 6, p. 89, 2018.

[36] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[37] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[38] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[39] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access*, vol. 5, pp. 13 787–13 798, 2017.

[40] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy*, 2016, pp. 81–92.

[41] NCCIC/ICS-CERT, "Cyber-attack against ukrainian critical infrastructure," Feb 2016. [Online]. Available: https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

[42] X. Liu, A. Liu, X. Zhang, Z. Li, G. Liu, L. Zhao, and X. Zhou, "When differential privacy meets randomized perturbation: a hybrid approach for privacy-preserving recommender system," in *International Conference on database systems for advanced applications*. Springer, 2017, pp. 576–591.

[43] X. Tang, L. Zhu, M. Shen, and X. Du, "When homomorphic cryptosystem meets differential privacy: training machine learning classifier with privacy protection," *arXiv preprint arXiv:1812.02292*, 2018.

[44] A. Wood, M. Altman, A. Bembenek, M. Bun, M. Gaboardi, J. Honaker, K. Nissim, D. R. O'Brien, T. Steinke, and S. Vadhan, "Differential privacy: A primer for a non-technical audience," *Vand. J. Ent. & Tech. L.*, vol. 21, p. 209, 2018.

[45] R. Selten, "Spieltheoretische behandlung eines oligopolmodells mit nachfrageträgheit: Teil i: Bestimmung des dynamischen preisgleichgewichts," *Zeitschrift für die gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics*, no. H. 2, pp. 301–324, 1965.

[46] J. C. Harsanyi, R. Selten *et al.*, "A general theory of equilibrium selection in games," *MIT Press Books*, vol. 1, 1988.

[47] C. Dwork, N. Kohli, and D. Mulligan, "Differential privacy in practice: Expose your epsilons!" *Journal of Privacy and Confidentiality*, vol. 9, no. 2, 2019.

[48] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: A tutorial," 2006.