A Game Theoretic Approach for Enhancing Data Privacy in SDN-based Smart Grids

Vignesh Sivaraman, *Student Member, IEEE* and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—Smart-grids rely on communication networks to connect the physical devices and the control and computation technologies. The transmission of sensitive data over the network induces the possibility of leakage of private and sensitive information about various entities and components in the grid. To address this issue, this paper proposes a privacy-preserving framework to enhance the privacy of smart-grids integrated with Software Defined Networks. The proposed framework uses two privacy metrics (mutual information and differential privacy) and formulates a privacy preserving distributed optimization algorithm with the objective of minimizing the network cost. We view the distributed optimization algorithm as an n-player, non-cooperative game and provide distributed techniques to solve the optimization problem efficiently. We prove that our algorithm converges to the Nash equilibrium of the game while preserving the data privacy. We validate the performance of our approach using three IEEE bus systems and realistic Internet Service Provider network topology.**

***Index Terms*—Smart grids, software defined networks, privacy**

I. Introduction

Cyber Physical Systems (CPSs) refer to system where a physical process is controlled remotely and, through feedback, adapts to varying real-time requirements. This goal is achieved by integrating physical processes, networking, and computation [1]. The data generated by sensors is used to determine the current operating conditions of the CPS and is sent over a network to the computing unit where the data is evaluated and decisions are made. The actuators are then updated of the new decisions (over the network) and they carry out the planned actions [2]. CPSs are complex and real-time systems, with large volumes of data and time-sensitive actuation commands. Therefore, the underlying communication network is expected to have low latency, high bandwidth, and high reliability.

Software Defined Networking (SDN) has revolutionized communication network by decoupling the control plane from the data plane. This flexibility of SDN has motivated its application in various domains like wide area networks [3], enterprises [4], data centers [5], [6], and wireless networks [7]. In the context of CPSs, SDNs find application in domains like industrial automation [8], vehicular CPSs [9], and power grids [10]–[12]. In particular, smart grids rely heavily on the network performance for the integration and synchronous functioning of its different components like distributed energy resources, Supervisory Control and Data Acquisition (SCADA) systems, automated meter reading, and customer energy management systems and SDN has been proposed as a solution to meet the network requirements of a smart power grid [13]–[16].

While SDNs provide enhanced networking capabilities to CPSs, the architecture of SDNs is vulnerable to various security threats that in turn affect the CPS. As the control plane and data plane are decoupled in SDN, the controller becomes a critical target for active and passive attacks by adversaries [17]. While active attacks on controller may allow the adversary to perform malicious actions, they are relatively easier to detect. On the other hand, a controller under a passive attack may be exploited by the adversary to infer critical, valuable, and private information about the CPS and its users. In such passive attacks, the adversary may analyze the traffic, identify the data source and destination, and the frequency of data generation. Such information may then be exploited to launch targeted attacks on CPS components or used for commercial advantage. A controller under passive attacks is difficult to detect since the adversary does not alter the data or affect the controller's operation. Hence, it is important to develop defenses against such threats to mitigate the loss of critical system information and privacy.

Preserving user privacy in CPSs is well explored in literature (see [18] for a survey). Specifically in the context of smart grids, mechanisms exists in the literature for privacy preserving data aggregation [19]–[21]. While these mechanisms are effective in conventional CPSs, they are not effective in the case of a passively compromised SDN controller because: (i) the compromised controller has sufficient side channel information like source and destination IP addresses to uniquely identify a flow and (ii) leakage of other system critical information (apart from user data) is still possible.

This paper addresses the problem of providing privacy to CPSs when the SDN controllers are subjected to passive attacks. The proposed solution formulates a non-cooperative game among the switches where each switch probabilistically chooses a controller such that the network cost it incurs is minimized and its (information theoretic) privacy bound is satisfied. We show that a Nash equilibrium exists in such a game and a Nash equilibrium can be achieved using an iterative best response algorithm. Moreover, we also formulate another game which incorporates differential privacy along

This research was supported in part by Singapore Ministry of Education Academic Research Fund Tier 1 (R-263-000-D62-114).

V. Sivaraman and B. Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583. Email: vignesh.sivaraman@u.nus.edu, bsikdar@nus.edu.sg.

with the information theoretic mutual information bound. This approach provides a framework for trade-off between the amount of information leaked by a compromised controller and network cost incurred in mitigating it in a SDN-based CPS. The proposed framework can be applied to any SDN-based CPS and for illustration, we consider the specific case of smart grids. The **contributions of this paper** can be summarized as:

- We propose a distributed switch-controller mapping scheme to mitigate passive information leakage via compromised controllers in SDN based CPSs.
- The proposed privacy framework is based on a non-cooperative game formulation among the switches. The privacy requirements are quantified using information theoretic mutual information and differential privacy. The Nash equilibrium of the game is computed using an iterative best response algorithm.
- The performance of the proposed scheme is compared with the globally optimal solution and exponential mechanism (for differential privacy). The proposed approach, in addition to being distributed, also achieves near optimal cost and better fairness compared to the global solutions.

The rest of the paper is organized as follows. The related literature is presented in Section II and Section III describes the system model and the required preliminaries. The proposed game model is presented in Section IV and Section V presents the game with differential privacy constraints. The Nash equilibrium of the game, an iterative best-response algorithm to solve it, and its convergence are discussed in Section VI. The performance evaluation of the proposed approach is discussed in Section VII and Section VIII concludes the paper.

II. Related Work

Game theoretic approaches for data privacy preservation are well explored in the literature and good surveys can be found in [22], [23]. The authors of [24] use anonymity to privately integrate the data of different users. In [25], authors obtain data privacy by perturbing the sensitive data. Authors of [26] use differential privacy and distortion privacy to achieve data privacy. Similarly, authors of [27] apply perturbation to location data. The approaches mentioned above discuss ways to make the user data more private. However, the privacy attack considered in this paper is not due to the leakage of the data itself, but based on observing the traffic patterns of different devices to infer sensitive and private information. Thus, the existing techniques for data privacy described above are not applicable in the scenario considered in this paper.

Security and privacy in CPSs has received considerable attention in literature [18]. As this paper considers SDN based CPSs and more specifically, SDN based smart grids, we focus our discussion on literature addressing security and privacy in smart grids and SDN-based smart grids.

The problem of privacy preserving data aggregation from smart meters has been well explored in existing literature. For example, authors in [28], [29] use anonymization where the data and its source are decoupled. Authors in [21], [30], [31] use trusted computation where either the data source or a trusted third party performs the computation. Approaches using data perturbation like differential privacy are discussed in [32]–[34]. The above mentioned techniques, in general, aim to preserve the privacy of the data source from the computing point of view and do not cater to privacy breaches possible in the communication network. For example, these anonymization techniques would fail in case of a compromised SDN controller as the adversary can still uniquely identify the data source using the IP addresses.

SDNs can be used to increase the resilience of the smart grids [14]. The authors of [14] use SDN to minimize the attack time window of the adversary, reset policies upon the detection of compromised switches, and hot-swap communication channels to the public Internet in the presence of attacks. In [13], the authors leverage SDN to model a flexible and dynamic network control to meet the communication requirements of smart grids. Similarly, authors of [16] use SDN for improving the resilience of Industrial Internet of Things by dynamically routing flows in the presence of a failure. While the literature mentioned above address different security threats to smart grids by leveraging the flexibility of SDNs, they do not consider the threats posed by SDN itself.

The scenario of a compromised SDN controller is considered in [35], [36]. Authors of [35] consider a smart grid with multiple SDN controllers and propose to deploy multiple intrusion detection systems (IDSs) to detect malicious activities. Specifically, local IDSs are placed at the substations and a global IDS runs at the control center which monitors the control commands of the SDN controller and SCADA master and generates an alarm whenever an unsteady state of the smart grid is detected. Such a scheme can detect malicious behavior of an actively compromised SDN controller but is unable to detect passively compromised controllers where system critical and private data is being leaked. In contrast, the proposed scheme aims to address this problem of passive information leakage.

The authors of [36] proposed a switch-controller mapping schedule to minimize information leakage via a passively compromised controller, albeit in a SDN-based Internet of Things scenario. The proposed solution is centralized and the network operator decides the privacy requirement and determines the mapping schedule. In comparison, we address a similar problem of information leakage in SDN based CPSs (or smart grids) using a distributed solution where the user (or the switch) decides the controller mapping based on its privacy requirements.

The existing privacy preserving methods for smart-grids primarily focus on the privacy of the user data like the data generated by smart meters. The existing approaches use data obfuscation techniques to preserve user privacy. However, even while using these data obfuscation techniques, the adversary can learn private (sensitive) user (system) data by observing the traffic flow patterns in the network. Our approach aims to mitigate such privacy attacks.

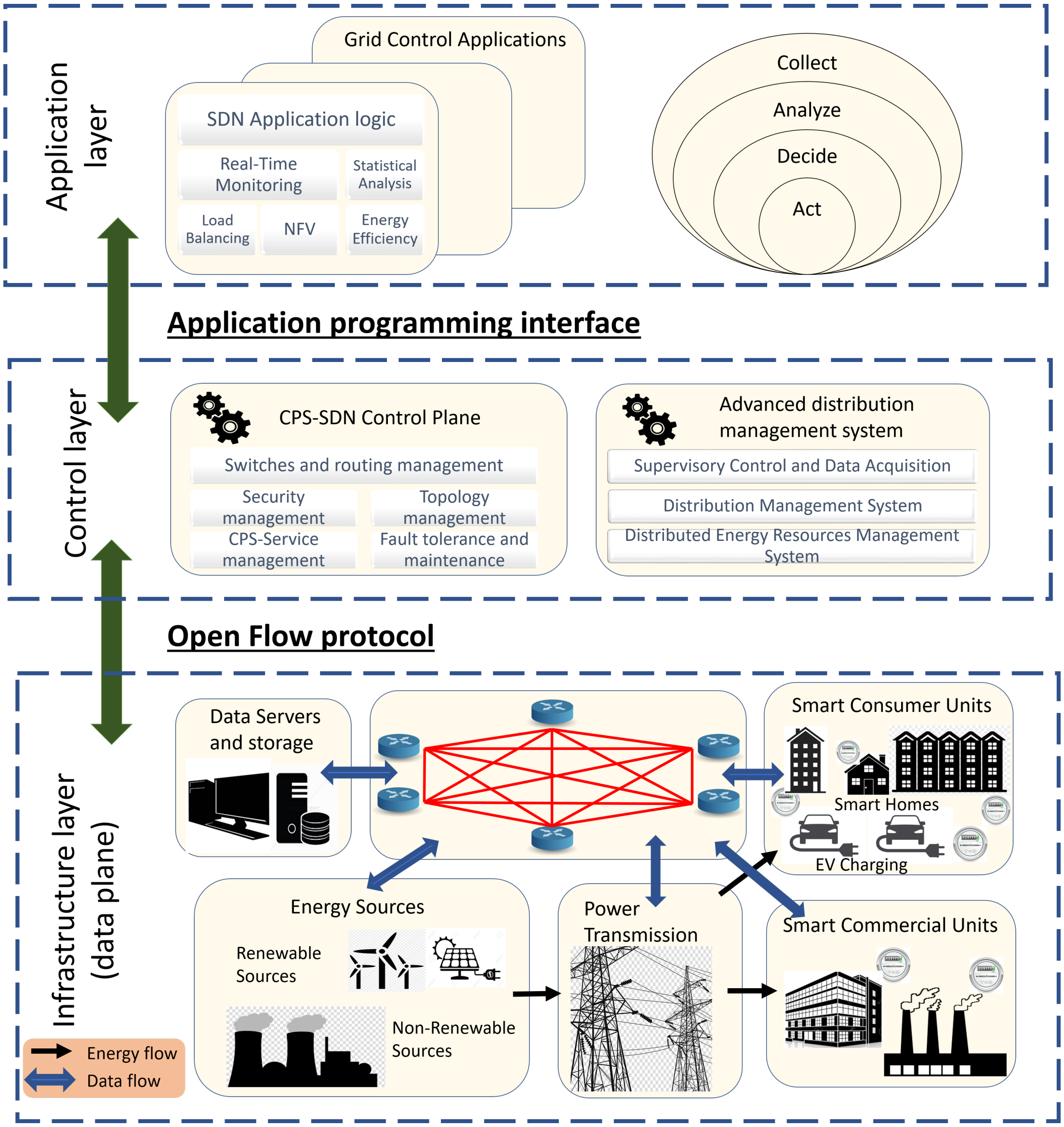

Fig. 1. SDN-based smart grid architecture.

III. Preliminaries

A. SDN based Smart-grid Architecture

SDN are capable of providing essential and enhanced networking services for smart-grids and SDN-based smart-grid architectures have been proposed in literature [14], [16], [37]. Here we briefly describe the architecture for completeness. The SDN-based smart-grid architecture can be viewed as a three-layered architecture as shown in Figure 1.

1) Infrastructure Layer: The infrastructure layer includes all the hardware, devices and physical equipment present in SDN-based smart-grids like SDN switches, gateways, access points, routers, data and computation servers, various sensors and actuators (deployed at the substations and power-plants), field-bus control, and smart-metering infrastructure installed at the user end. The primary function of this layer is data forwarding in the network. When a SDN switch receives a new traffic flow, the SDN switch notifies the control layer for routing decisions and further policy decisions by the application layer. In addition, it also monitors local information and gathers sensor data. Similar to the traffic data, the gathered sensor data is sent to the control layer for further processing.

2) Control Layer: The control layer functions as the interface between the application layer and the infrastructure layer. The control layer comprises of two components. The first is the network operating system which manages and secures the flow of data. It defines and controls different network operations like routing, topology management, and fault tolerance. The second component is the advanced distribution management system which controls and monitors the smart-grid system. It includes Supervisory Control And Data Acquisition (SCADA), Distribution Management System (DMS), and Distributed Energy Resource Management System (DERMS).

3) Application Layer: The application layer it the topmost layer where the data acquired by the infrastructure layer is processed and analyzed. This layer processes the traffic flow information obtained from the control layer and verifies that all the policies and standards are met. It also carries out functions like utility authentication, load balancing and rate monitoring. It also processes and analyzes the data generated by the advanced distribution management system and carries out various decisions with respect to power generation, transmission and distribution. To summarize, the application layer uses the data from the lower layers to form a abstract view of the data network and the smart-grid. Using this abstract view, it issues instructions to the control layer for proper functioning of the system as a whole.

B. Overview

To mitigate the impact of a passively compromised controller, we design a switch-controller mapping, $\mathcal{A}$, where a SDN switch (or the grid substation) is mapped to different controllers corresponding to the probability distribution output by $\mathcal{A}$. As we are concerned about the quality of service and the incurred network resource costs, we consider delay and controller resource consumption in our cost model. While requesting for privacy, a switch needs to decide on the appropriate mechanism $\mathcal{A}$. As the privacy of a switch depends not only on its own mechanism but also on the mechanisms chosen by other switches, we formulate the interactions between the switches as a game.

Solution Approach: We propose two solution approaches to address the problem of privacy in the presence of passive attacks on SDN controllers. The **first** approach formulates the problem as a non-cooperative game among the switches. Every switch solves an optimization problem with the objective to minimize the total cost incurred while achieving a minimum privacy level. The privacy level of a switch is quantified using the Shannon entropy of the system (i.e., mutual information). We show that a Nash equilibrium exists for this game and that it can be reached using a greedy iterative approach. While the **second** approach is similar to the first, here we also consider differential privacy constraints along with the Shannon entropy of the system.

Remark. The idea of switch probabilistically choosing a controller is a conceptual one. The main idea in our paper for providing privacy is to allow the switch-controller mapping to be chosen according to the privacy requirements. This mapping is done probabilistically and the computation of the probability vector that is used to determine the switch-controller mapping is done at the switches. The operator of the network performs the periodic switch-controller mapping on behalf of the switches [38], [39]. In the case of SDN based smart grids, this periodic mapping can be performed by the application layer (in Figure 1) [14], [37]. To facilitate such an implementation of the switch-controller mapping using the framework proposed in this paper, each switch computes its mapping $\mathcal{A}$ and updates the network operator (or application layer) with $\mathcal{A}$. Then, the network operator (or application layer) can carry out the required steps to modify the mapping based on the preferences of the switches. Note that switches generally have adequate processing capacity to compute $\mathcal{A}$ [38], [40], [41]. The switch needs to securely communicate the computed mapping probabilities to the network operator. The switch encrypts the message containing the controller-switch mapping probabilities before sending it to the network operator. Discussion on the possible encryption techniques is beyond the scope of this paper.

C. Differential privacy

Differential privacy was initially defined for two adjacent databases. Databases D and D' are said to be adjacent if they differ on a single row. Differential privacy is defined as:

Definition 1. *Differential Privacy.* A randomized algorithm $\mathcal{A}$ satisfies ϵ-differential privacy if for all adjacent databases D and D' and all $O \subseteq \text{Range}(\mathcal{A})$,

$$Pr[\mathcal{A}(D') \in O] \leq e^{\epsilon} \times Pr[\mathcal{A}(D) \in O]. \tag{1}$$

Exponential Mechanism. Let $\mathcal{D}$ and $\mathcal{R}$ be the arbitrary domain and range, respectively, of a randomized mechanism $\mathcal{A}$. Then, $\mathcal{A}$ is said to follow the exponential mechanism [42] if for any $d \in \mathcal{D}, \mathcal{A}$ selects an output $r \in \mathcal{R}$ with a probability proportional to $exp(\epsilon\frac{u(d,r)}{2\Delta u})$. Here $u : \{\mathcal{D} \times \mathcal{R}\} \rightarrow \mathbb{R}$ is the utility function and Δu is the largest possible difference in the utility when two inputs differ only on a single user's value, for any r.

IV. Switch-Controller Mapping Strategy Games

A. System Model

Consider a SDN based smart grid as depicted in Figure 1. We consider a multi-controller SDN network where each controller controls a subset of the switches. Since substations have a large number of SCADA devices (like sensors and actuators), we assume that each substation has an SDN switch.

Let the network consists of R controllers and U switches, indexed as $\mathcal{R} = \{1,\ 2, \cdots, R\}$ and $\mathcal{U} = \{1,\ 2, \cdots, U\}$. In the default scenario, a switch is mapped to one of the controllers and this mapping is static and deterministic. This forms a vulnerability since with this mapping information, the adversary can infer critical and private information by targeting the mapped controller of a given switch. Therefore, in our approach the switch is probabilistically mapped to a controller (which is changed periodically).

Let p_u^r be the probability with which switch u chooses controller r. Let $\mathbf{p}_u$ be the vector of probabilities of switch u corresponding to every controller, $\mathbf{p}_u = [p_u^1, p_u^2, \cdots, p_u^{|\mathcal{R}|}]^T$. The switch decides on $\mathbf{p}_u$ based upon the level of privacy required and the corresponding cost incurred for it. Let q_u be the prior knowledge of the adversary about switch u and we assume q_u is proportional to the amount of traffic generated by the switch (i.e., substation connected to it). Thus, $q_u = \frac{\lambda_u}{\sum_{u' \in \mathcal{U}} \lambda_{u'}}$ where λ_u is the amount of traffic generated by u.

B. Attack Model

The attack model assumed in this paper is that the adversary is capable of eavesdropping on the communication channel between a switch and its controller. While eavesdropping, the adversary does not modify any of the data, rather, the adversary just listens to the communication passively. Such eavesdropping enables the adversary to learn about the traffic patterns flowing through the different devices and the users connected to the switches that are managed by the controller. We also assume that the adversary is capable of identifying the source of the traffic using fingerprint techniques [43].

The objective of the adversary is to leverage the observed traffic patterns to predict the future behavior of the smart grid system and the users connected to it. Such predictions by the adversary can lead to serious security and privacy breaches. For example, the adversary can observe the traffic pattern of different devices at a substation (like sensors and actuators) to learn and predict about energy usage patterns at the substation. Similarly, by observing the traffic pattern of the users' smart-meters, the adversary can infer and predict about users' energy usage pattern. This information can be further used by the adversary to plan more serve attacks such as energy outage. We note that this type of attack by the adversary will be successful even when the existing privacy preserving techniques discussed in Section II are applied because in this attack the adversary does not need to know the exact data being communicated. Instead, the adversary learns just by observing the traffic patterns in the network [44].

C. Game Model

We first consider a game where a switch has complete knowledge of other switches' strategies and the network topology. Under these assumptions, we develop a non-cooperative game to capture the strategic interactions between the switches. Then, we extend the game model when these assumptions are relaxed.

We define a game $\mathcal{G}$ as a three tuple $\{\mathcal{P}, \mathcal{S}, \mathcal{F}\}$ where $\mathcal{P}$ is the set of players, $\mathcal{S}$ is the set of strategies, and $\mathcal{F}$ is the pay-off functions. The set of players correspond to $\mathcal{U}$, the set of all the switches in the network. The set of strategies for every switch is the different possible values of the probability vector $\mathbf{p}_u$. Hence, an instance of the strategies of all the switches can be viewed as a strategy matrix $\mathbf{P}$ ($\mathbf{P}$ is a $|\mathcal{R}| \times |\mathcal{U}|$ matrix).

Let $f_u(\mathbf{p}_u)$ be the cost incurred by switch u when its strategy is $\mathbf{p}_u$. Then, we have $f_u(\mathbf{p}_u) = \sum_{r \in \mathcal{R}} f_u^r(p_u^r)$, where f_u^r is the cost function of u corresponding to controller r. The cost function takes two factors into consideration: (i) the network resource consumed by choosing controller r, which intuitively is a function of the capacity of r and (ii) the delay incurred due to choosing r. This factor is independent of the capacity of r. We assume that f_u is a non-decreasing convex function. The assumption that f_u is non-decreasing is a natural one because when the privacy requirement increases, the cost incurred would tend to be higher and cannot decrease. Moreover, the intuition behind the convexity assumption is that when the privacy requirement is already high, any increase in the privacy requirement would incur a higher marginal cost (as compared to the case when privacy is lower). We also note that if the convexity assumption is relaxed, f_u is a non-decreasing function and therefore f_u is a quasi-convex function. When f_u is a quasi-convex function, $P0$ and $DP0$ are still solvable.

We solve the game for the case when the cost function is affine, i.e., $f_u^r(p_u^r) = (\hat{c}_r + d_u^r) q_u p_u^r$. Here, $\hat{c}_r$ corresponds to the network resource cost and d_u^r corresponds to the delay cost. Let $c_u^r = (\hat{c}_r + d_u^r) q_u$ and $\mathbf{c}_u = [c_u^1, c_u^2, \cdots, c_u^{|\mathcal{R}|}]$. Then, the cost function can be written in vector form as $\mathbf{c}_u^T \mathbf{p}$. We consider the negative cost to be the *pay-off function* of the game.

Let U be a random variable corresponding to the adversary's prior probability of any flow passing through u, i.e., $P[U = u] = q_u$. Let R be a random variable corresponding to the event that controller r is chosen by a switch. Note that $P[R = r|U = u] = p_u^r$ and thus we have:

$$P[U = u, R = r] = q_u p_u^r$$

$$\begin{aligned} P[R = r] &= \sum_{u' \in \mathcal{U}} P[R = r|U = u'] P[U = u'] \\ &= \sum_{u' \in \mathcal{U}} p_{u'}^r q_{u'} \end{aligned}$$

$$\begin{aligned} P[U = u|R = r] &= \frac{P[R = r|U = u] P[U = u]}{P[R = r]} \\ &= \frac{q_u p_u^r}{\sum_{u' \in \mathcal{U}} p_{u'}^r q_{u'}} \end{aligned}$$

The mutual information between U and R is then given by:

$$I(U, R) = -\sum_{u \in \mathcal{U}} q_u \log(q_u) + \sum_{u \in \mathcal{U}, r \in \mathcal{R}} q_u p_u^r \log \left[\frac{q_u p_u^r}{\sum_{u' \in \mathcal{U}} q_{u'} p_{u'}^r} \right]$$

The switch decides the level of privacy required by constraining the mutual information of the system to an upper bound. Since different substations may have different privacy requirements, each switch u decides on $\mathbf{p}_u$ accordingly.

D. Optimal Response

Let us denote the strategies of other switches by matrix $\mathbf{P}_{-u}$. Then, for any given strategy $\mathbf{P}_{-u}$ of other switches, the set $\mathcal{B}_u(\mathbf{P}_{-u})$ of the optimal response of switch u is given by

$$\mathcal{B}_u(\mathbf{P}_{-u}) = \underset{\mathbf{p}_u \in \mathcal{S}_u}{\arg\min} f_u(\mathbf{p}_u, \mathbf{P}_{-u}) \tag{2}$$

The optimal response $\overline{\mathbf{p}}_u$ of u in response to $\mathbf{P}_{-u}$ minimizes the total cost incurred for u while subjecting the mutual information of the system to an upper bound t_u. For a given $\mathbf{P}_{-u}$ and $\mathbf{q}$, $I(U, R)$ reduces to a function of $\mathbf{p}_u$ and for notational simplicity, we denote $I(U, R)$ as $I(\mathbf{p}_u)$. The optimal response of u can be formulated as the following optimization problem:

$$\begin{aligned} P0: \quad & \underset{\mathbf{p}_u}{\text{minimize}} && \mathbf{c}_u^T \mathbf{p}_u && (3) \\ & \text{subject to} && I(\mathbf{p}_u) \leq t_u && (4) \\ & && \mathbf{A}\mathbf{p}_u = \mathbf{b} && (5) \\ & && \mathbf{p}_u \geq \mathbf{0} && (6) \end{aligned}$$

Here, constraint (4) is the upper bound on the leaked mutual information. Constraint (5) includes the constraint $\mathbf{1}^T \mathbf{p}_u = 1$ which along with constraint (6) ensures that $\mathbf{p}_u$ is a probability distribution. Moreover, constraint (5) allows us to accommodate for any additional equality constraints. Here, $\mathbf{A}$ is an

$m \times |\mathcal{R}|$ coefficient matrix and $\mathbf{b}$ is a $m-$dimensional vector. We assume that $m \leq |\mathcal{R}|$ and that rank($\mathbf{A}$) $= m$, i.e., $P0$ is feasible and has at least one positive feasible solution. Moreover, we assume that $\mathbf{c}_u$ does not belong to the column space of $\mathbf{A}^T$, i.e., $\mathbf{c}_u \notin C(\mathbf{A}^T)$ (if $\mathbf{c}_u = \mathbf{A}^T y$, it would imply that $\mathbf{c}_u^T x = \mathbf{y}^T \mathbf{A} \mathbf{p}_u = \mathbf{y}^T \mathbf{b} =$ constant).

For problem $P0$, the objective function (3) is affine. Also, since the function $I(U, R)$ is convex in $\mathbf{p}_u$ for a given $\mathbf{q}$ and $\mathbf{P}_{-u}$, constraint (4) is convex. Finally, constraints (5) and (6) are affine. Therefore, $P0$ is a convex optimization problem. For completeness , the proof for the convexity of $I(U, R)$ is presented in Appendix A.

Consider a switch u with low privacy requirements and t_u chosen by it is large enough that the constraint (4) is inactive for all the feasible points. In this case, optimization problem $P1$ reduces to the following linear program:

$$
\begin{aligned}
P1: \quad & \underset{\mathbf{p}_u}{\text{minimize}} & & \mathbf{c}_u^T \mathbf{p}_u & (7)\\
& \text{subject to} & & \mathbf{A}\mathbf{p_u} = \mathbf{b} & (8)\\
& & & \mathbf{p}_u \geq \mathbf{0} & (9)
\end{aligned}
$$

Now, let us decrease the value of t_u and at some $t_u^{\max}$, constraint (4) becomes active, and remains active until a point $t_u^{\min}$. For any t_u less than $t_u^{\min}$, $P1$ becomes infeasible. Hence, when $t_u \in (t_u^{\min}, t_u^{\max})$, constraint (4) is active and this case is of interest to us. $t_u^{\max}$ is defined as $t_u^{\max} = I(\mathbf{p}_u^{LP}) = \min\{I(\mathbf{p}_u) | \mathbf{p}_u \text{ is an optimal solution to } P1\}$.

Now, consider the following optimization problem:

$$
\begin{aligned}
P2: \quad & \underset{\mathbf{p}_u}{\text{minimize}} & & I(\mathbf{p}_u) & (10)\\
& \text{subject to} & & \mathbf{A}\mathbf{p_u} = \mathbf{b} & (11)\\
& & & \mathbf{p}_u \geq \mathbf{0} & (12)
\end{aligned}
$$

Let $\mathbf{p}_u^{\min}$ be an optimal solution of $P2$. Then $I(\mathbf{p}_u^{\min})$ is the minimum possible mutual information. Hence, any t_u less than $I(\mathbf{p}_u^{\min})$ would make $P0$ infeasible, i.e., $t_u^{\min} = I(\mathbf{p}_u^{\min})$). Using the same arguments as used for $P0$, we note that $P2$ is a convex optimization problem.

Lemma 1. *For $t_u^{min} < t_u < t_u^{max}$, the optimal solution is strictly positive, i.e., $\mathbf{p}_u^* > \mathbf{0}$.*

Proof. As $t_u < t_u^{\max}$, we have $\mathbf{c}_u^T \mathbf{p}_u^* > \mathbf{c}_u^T \mathbf{p}_u^{LP}$ by construction. Let us consider $\mathbf{y} > \mathbf{0}$ such that $\mathbf{1}^T \mathbf{y} = 1$. For some $k \in [0, 1]$ and $l \in [0, 1]$, we define

$$\mathbf{s} = (1 - l)\mathbf{p}_u^* + l[k\mathbf{p}_u^{LP} + (1 - k)y]. \quad (13)$$

We can easily see that for $k < 1$ and $l > 0$, $z > \mathbf{0}$. If k is sufficiently close to 1 and $l > 0$, then $\mathbf{c}_u^T \mathbf{z} < \mathbf{c}_u^T \mathbf{p}_u^*$. As the slope of $I(\mathbf{p}_u)$ is infinite at the boundary of the feasible domain, if ${p_u^r}^* = 0$ we have $I(\mathbf{z}) < I(p_u^*)$ for $0 < k < 1$ and sufficiently small $t > 0$. Thus, we can construct a feasible solution $\mathbf{z}$ with $\mathbf{c}_u^T \mathbf{z} < \mathbf{c}_u^T \mathbf{p}_u^*$. This is a contradiction as $\mathbf{p}_u^*$ is an optimal solution. Hence ${p_u^r}^* > 0, \forall r \in \mathcal{R}$. □

Theorem 1. *The optimal solution of $P1$ is given by:*

(i) $t_u \geq t_u^{max}$: the optimal solution to the linear programming, $P1$, $\mathbf{p}_u^{LP}$,

(ii) $t_u^{min} < t_u < t_u^{max}$: the following solution of $P0$,

$$ {p^*}^r_u = \frac{1}{q_u}\left(\frac{\sum_{v \neq u} q_v p_v^r}{\exp((c_u^r + \boldsymbol{\beta}^T \mathbf{a}_r)/q_u\lambda) - 1}\right), \ \forall r \in \mathcal{R}, \quad (14)$$

(iii) $t_u = t_u^{min}$: the optimal solution to convex problem $P2$, $\mathbf{p}_u^{min}$,

(iv) $t_u < t_u^{min}$: no solution,

where $\boldsymbol{\beta} \in \mathbb{R}^m, \lambda \geq 0$, and $\mathbf{a}_r$ is the r^{th} column of $\mathbf{A}$.

Proof. **Case (i).** For the case $t_u > t_u^{\max}$, the result is immediate as constraint (4)is inactive for all the feasible points. For the case $t_u = t_u^{\max}$, we have $I(\mathbf{p}_u^{LP}) = t_u$, i.e., $\mathbf{p}_u^{LP}$ is feasible as well as optimal (as $\mathbf{c}_u^T \mathbf{p}_u$ cannot be further minimized even if constraint (4) is removed) and case (i) follows.

Case (ii). For $t_u^{\min} < t_u < t_u^{\max}$, $\mathbf{p}_u^{\min}$ is a feasible solution to $P1$ such that $I(\mathbf{p}_u^{\min}) < t_u$. This is immediate as $I(\mathbf{p}_u^{\min}) = t_u^{\min} < t_u$. As $I(\mathbf{p}_u)$ is strictly convex, there exists at least one optimal solution $\mathbf{p}_u^*$. For $t_u^{\min} < t_u < t_u^{\max}$, constraint (4) is active for an optimal solution $\mathbf{p}_u^*$. To prove this statement, assume that $I(\mathbf{p}_u^*) < t_u$. Then, as the constraint is inactive, $\mathbf{p}_u^{LP}$ is an optimal solution. Hence, $I(\mathbf{p}_u^{LP}) \leq t_u$. However, according to this case's assumption, $I(\mathbf{p}_u^{LP}) = t_u^{\max} > t_u$. This is a contradiction. Therefore, we conclude that constraint (4) is active and therefore $I(\mathbf{p}_u^*) = t_u$.

Now, we prove (14). The Lagrangian L of $P0$ is given by:

$$L(\mathbf{p}_u, \boldsymbol{\beta}, \lambda) = \mathbf{c}_u^T \mathbf{p}_u + \lambda\left(I(\mathbf{p}_u) - t_u\right) + \boldsymbol{\beta}^T(\mathbf{A}\mathbf{p}_u - \mathbf{b}). \quad (15)$$

From Lemma 1, we note that constraint (6) is satisfied with strict inequality (i.e., constraint is inactive) and thus, it is not included in the Lagrangian. The Lagrange dual function is:

$$g(\boldsymbol{\beta}, \lambda) = \inf_{\mathbf{p}_u} \mathbf{c}_u^T \mathbf{p}_u + \lambda\left(I(\mathbf{p}_u) - t_u\right) + \boldsymbol{\beta}^T(\mathbf{A}\mathbf{p}_u - \mathbf{b}) \quad (16)$$

From Lemma 1, we observe that when $t_u^{\min} < t_u < t_u^{\max}$, there exists a point in the feasible domain that is strictly feasible. Therefore Slater's condition is satisfied. As $P0$ is convex and satisfies Slater's condition, strong duality holds and the optimal duality gap is zero. Now, using the Karush-Kuhn-Tucker conditions, the gradient of L vanishes at $\mathbf{p}_u^*$. Therefore,

$$c_u^r + \boldsymbol{\beta}^T a_r + \lambda q_u \left[\log\left(\frac{q_u p_u^r}{q_u p_u^r + \sum_{v \neq u} q_v p_v^r}\right)\right] = 0, \quad (17)$$

$\forall r \in \mathcal{R}$. Here $\boldsymbol{\beta} \in \mathbb{R}^m$ and $\lambda > 0$ since constraint (4) is active. Solving (17) for p_u^r, we get (14). The Lagrangian multipliers $\boldsymbol{\beta}$ and λ in (14) are computed in Section IV-E.

Case(iii) and Case(iv). The results of case (iii) and case (iv) are immediate. □

E. Computing the Lagrangian Multipliers

Theorem 1 gives the form of the optimal solution, $\mathbf{p}_u^*$, for $P0$ in terms of the Lagrangian multipliers. This section focuses on case (ii) of Theorem 1 and computes the optimal values of the multipliers. Let $\mathbf{p}_u^*$ and $(\boldsymbol{\beta}^*, \lambda^*)$ be the primal and dual optimal points. Given that constraint (4) is active, we have the following from Karush-Kuhn-Tucker conditions:

$$c_u^r + {\boldsymbol{\beta}^*}^T a_r + \lambda^* q_u \left[\log\left(\frac{q_u {p_u^r}^*}{q_u {p_u^r}^* + \sum_{v \neq u} q_v p_v^r}\right)\right] = 0, \ \forall r \in \mathcal{R}, \quad (18)$$

$$I(\mathbf{p}_u^*) - t_u = 0, \quad (19)$$

$$\mathbf{A}\mathbf{p}_u^* - \mathbf{b} = 0, \quad (20)$$

$$\boldsymbol{\beta}^* \in \mathbb{R}^m, \ \lambda^* > 0. \quad (21)$$

Solving (18) for ${p_u^r}^*$, we get

$$ {p^*}_u^r = \frac{1}{q_u}\left(\frac{\sum_{v\neq u} q_v p_v^r}{\exp((c_u^r + {\boldsymbol{\beta}^*}^T\mathbf{a}_r)/q_u\lambda^*) - 1}\right), \ \forall r \in \mathcal{R}. \quad (22)$$

We have the primal optimal solution $\mathbf{p}_u^*$ as a function of the optimal dual solution $(\boldsymbol{\beta}^*, \lambda^*)$. As the optimal solution needs to satisfy the primal feasibility, i.e., (19) and (20), we determine the optimal dual solution $(\boldsymbol{\beta}^*, \lambda^*)$ by solving the primal feasibility equations. Here, we have $(m+1)$ equations and $(m+1)$ unknown multipliers.

Let us define the mapping $Q : \mathbb{R}^{m+1} \to \mathbb{R}^{m+1}$ as follows:

$$Q(\boldsymbol{\beta}, \lambda) = \begin{bmatrix} \mathbf{A}\mathbf{p}_u - \mathbf{b} \\ I(\mathbf{p}_u) - t_u \end{bmatrix}, \quad (23)$$

where $\mathbf{p}_u$ is given by (22). By solving the system $Q(\boldsymbol{\beta}, \lambda) = 0$, we obtain the optimal dual solution. We solve $Q(\boldsymbol{\beta}, \lambda) = 0$ using the Newton-Kantorovich method. To guarantee local convergence of this method, the Jacobian Q' needs to be continuous and non-singular. Let $P(\boldsymbol{\beta}, \lambda) = \mathbf{A}\mathbf{p}_u - \mathbf{b}$ and $I(\boldsymbol{\beta}, \lambda) = I(\mathbf{p}_u)$. Then, Q' is given by:

$$Q' = \begin{bmatrix} \frac{\partial P(\boldsymbol{\beta},\lambda)}{\partial \boldsymbol{\beta}} & \frac{\partial P(\boldsymbol{\beta},\lambda)}{\partial \lambda} \\ \frac{\partial I(\boldsymbol{\beta},\lambda)}{\partial \boldsymbol{\beta}} & \frac{\partial I(\boldsymbol{\beta},\lambda)}{\partial \lambda} \end{bmatrix}. \quad (24)$$

Now, we evaluate the partial derivatives as follows:

(i) The i^{th} row of $\frac{\partial P(\boldsymbol{\beta},\lambda)}{\partial \boldsymbol{\beta}}$ can be written as

$$\left(\frac{-1}{q_u\lambda}\right)\sum_r a_{ir} w_r a_r^T,$$

where w_r is given by:

$$w_r = \frac{1}{q_u \sum\limits_{v\neq u} q_v p_v^r}\left(q_u p_u^r (q_u p_u^r + \sum_{v\neq u} q_v p_v^r)\right).$$

Therefore, we get

$$\frac{\partial P(\boldsymbol{\beta}, \lambda)}{\partial \boldsymbol{\beta}} = \left(\frac{-1}{q_u\lambda}\right)\mathbf{A}\mathbf{W}\mathbf{A}^T \quad (25)$$

where $W = \text{diag}([w_1, w_2, \cdots, w_{|\mathcal{R}|}])$.

(ii) Similarly, $\frac{\partial P(\boldsymbol{\beta},\lambda)}{\partial \lambda}$ is given as follows:

$$\frac{\partial P(\boldsymbol{\beta}, \lambda)}{\partial \lambda} = \left(\frac{-1}{q_u\lambda}\right)\mathbf{A}\mathbf{y} \quad (26)$$

where y_r is given by

$$y_r = \frac{1}{\sum\limits_{v\neq u} q_v p_v^r}\left[q_u p_u^r (q_u p_u^r + \sum_{v\neq u} q_v p_v^r)\right]\log\left[\frac{q_u p_u^r}{q_u p_u^r + \sum\limits_{v\neq u} q_v p_v^r}\right].$$

(iii) Along the same lines, we get:

$$\frac{\partial I(\boldsymbol{\beta}, \lambda)}{\partial \boldsymbol{\beta}} = \left(\frac{-1}{q_u\lambda}\right)\mathbf{y}^T\mathbf{A}^T, \quad (27)$$

$$\frac{\partial I(\boldsymbol{\beta}, \lambda)}{\partial \lambda} = \left(\frac{-1}{q_u\lambda}\right)\mathbf{y}^T\mathbf{W}^{-1}\mathbf{y}. \quad (28)$$

Now, we can write Q' as follows:

$$Q'(\boldsymbol{\beta}, \lambda) = \frac{-1}{q_u\lambda}\begin{bmatrix} \mathbf{A}\mathbf{W}\mathbf{A}^T & \mathbf{A}\mathbf{y} \\ \mathbf{y}^T\mathbf{A}^T & \mathbf{y}^T\mathbf{W}^{-1}\mathbf{y} \end{bmatrix} \quad (29)$$

Theorem 2. *If* $\mathbf{c}$ *not in the column space of* $\mathbf{A}^T$*, i.e.,* $\mathbf{c}_u \notin C(\mathbf{A}^T)$ *then* $Q'(\boldsymbol{\beta}, \boldsymbol{\lambda})$ *is a non-singular matrix.*

Proof. A necessary and sufficient condition for Q' to be singular is that any row is a linear combination of the other m rows (or the rank of $Q' < m+1$). Let us assume that Q' is singular. Then, as the rows of $\mathbf{A}$ are linearly independent, the $(m+1)^{\text{th}}$ row of Q' is a linear combination of the first m rows. Performing row operations $(m+1)^{\text{th}}$ row of Q', we get:

$$s = \mathbf{y}^T[\mathbf{A}^T(\mathbf{A}\mathbf{W}\mathbf{A}^T)^{-1}\mathbf{A} - \mathbf{W}^{-1}]\mathbf{y} = 0. \quad (30)$$

Let $\hat{\mathbf{A}} = \mathbf{A}W^{1/2}$ and $\hat{\mathbf{y}} = \mathbf{W}^{-1/2}\mathbf{y}$, i.e., $\hat{y}_r = \left(q_u(q_u p_u^r(q_u p_u^r + \sum\limits_{v\neq u} q_v p_v^r))\right)^{1/2} \log\left(\frac{q_u p_u^r}{q_u p_u^r + \sum\limits_{v\neq u} q_v p_v^r}\right)$. From Lemma 1, we have $p_u^r > 0 \ \forall r$, hence

$$s = \hat{\mathbf{y}}^T[\hat{\mathbf{A}}^T(\hat{\mathbf{A}}\hat{\mathbf{A}}^T)^{-1}\hat{\mathbf{A}} - \mathbf{I}]\hat{\mathbf{y}} = -\hat{\mathbf{y}}^T\mathbf{P}\hat{\mathbf{y}}. \quad (31)$$

We note that $\mathbf{P}$ is the orthogonal projection onto the nullspace of $\hat{\mathbf{A}}$. Therefore,

$$s = 0 \Leftrightarrow \mathbf{P}\hat{\mathbf{y}} = 0 \Leftrightarrow \hat{\mathbf{y}} \in C(\hat{\mathbf{A}}^T) \Leftrightarrow \hat{\mathbf{y}} = \mathbf{X}^{1/2}\mathbf{A}^T\mathbf{k}, \text{ for some } \mathbf{k} \quad (32)$$

Simplifying Equation (18) and Equation (32), we get

$$\log\left(\frac{q_u p_u^r}{q_u p_u^r + \sum\limits_{v\neq u} q_v p_v^r}\right) = \frac{-c_u^r - \boldsymbol{\beta}^T\mathbf{a}_r}{q_u\lambda} = {\mathbf{a_r}}^T\mathbf{k'} \quad (33)$$

As $\boldsymbol{\beta}^T\mathbf{a}_r = \mathbf{a}_r^T\boldsymbol{\beta}$, we get

$$c_u^r = {\mathbf{a_r}}^T(-\boldsymbol{\beta} - q_u\lambda\mathbf{k}'), \text{ i.e.,} \quad (34)$$

$$\mathbf{c}_u = \mathbf{A}^T(-\boldsymbol{\beta} - q_u\lambda\mathbf{k}') \in C(\mathbf{A}^T) \quad (35)$$

Thus, $s = 0 \Leftrightarrow \mathbf{c}_u \in C(\mathbf{A}^T)$. But we have assumed $\mathbf{c}_u \notin C(\mathbf{A}^T$. Therefore, $s \neq 0$ and Q' is non-singular. □

Theorem 3. *Let* $(\boldsymbol{\beta}^*, \lambda^*)$ *be a solution to* $Q(\boldsymbol{\beta}, \lambda)$ *such that* $\lambda > 0$ *and* $\mathbf{c}_u \notin C(\mathbf{A}^T$*. Then* $(\boldsymbol{\beta}^*, \lambda^*)$ *is a point of attraction of the following Newton Kantorovich method:*

$$\begin{bmatrix} \boldsymbol{\beta}^{i+1} - \boldsymbol{\beta}^{i+1} \\ \lambda^{i+1} - \lambda^i \end{bmatrix} = \frac{-1}{q_u\lambda^i}\begin{bmatrix} \mathbf{A}\mathbf{W}^i\mathbf{A}^T & \mathbf{A}\mathbf{y}^i \\ (\mathbf{A}\mathbf{y}^i)^T & (\mathbf{y}^i)^T[\mathbf{W}^i]^{-1}\mathbf{y}^i \end{bmatrix}^{-1} \cdot \begin{bmatrix} \mathbf{A}{\mathbf{p_u}}^i - b \\ I(\mathbf{p}_u^i) - t_u \end{bmatrix} \quad (36)$$

where

$$w_r^i = \frac{1}{q_u \sum\limits_{v\neq u} q_v p_v^r}\left(q_u (p_u^r)^i (q_u (p_u^r)^i + \sum_{v\neq u} q_v p_v^r)\right) \quad (37)$$

$$y_r^i = \frac{1}{\sum\limits_{v\neq u} q_v p_v^r}\left(q_u (p_u^r)^i (q_u (p_u^r)^i + \sum_{v\neq u} q_v p_v^r)\right) . \log\left(\frac{q_u (p_u^r)^i}{q_u (p_u^r)^i + \sum\limits_{v\neq u} q_v p_v^r}\right) \quad (38)$$

$$(p_u^r)^i = \frac{1}{q_u}\left(\frac{\sum_{v\neq u} q_v p_v^r}{\exp((c_u^r + (\boldsymbol{\beta}^i)^T \mathbf{a}_r)/q_u\lambda^i) - 1}\right) \tag{39}$$

and i represents the values of the i^{th} of the method.

Proof. From Lemma 1 we have $\mathbf{p}_u > 0$. As we have $\lambda > 0$ and we assume $\mathbf{c}_u \notin C(\mathbf{A}^T$. Hence, from Theorem 2 the Jacobian Q' is continuous and non-singular. $\lambda > 0$ is in a neighborhood of λ^* as $\lambda* > 0$. Then $(\boldsymbol{\beta}^*, \lambda^*)$ is a point of attraction [45]. □

V. Differentially Private Mapping Games

This section enhances the mapping game discussed in Section IV. We add differential privacy constraints to the existing game model so that for a switch u, the probability of choosing two controllers with similar cost is similar. As in Section IV-D, we formulate the differentially private best response of u as an optimization problem with the objective to minimize the cost incurred subject to the mutual information **and** differential privacy constraints as follows:

$$\begin{aligned} DP0: \quad & \underset{\mathbf{p}_u}{\text{minimize}} && \mathbf{c}_u^T \mathbf{p}_u && (40)\\ & \text{subject to} && I(\mathbf{p}_u) \le t_u, && (41)\\ &&& \frac{p_u^r}{p_u^{r'}} \le e^{\epsilon_u |c_r - c_{r'}|} \quad \forall r, r' \in \mathcal{R}, && (42)\\ &&& \mathbf{1}^T \mathbf{p_u} = 1, && (43)\\ &&& \mathbf{p}_u \ge \mathbf{0}. && (44) \end{aligned}$$

Here, (42) ensures that differential privacy is satisfied for the choice of controllers for switch u. ϵ_u is the differential privacy parameter for switch u and the difference of the cost factors $|c_r - c_r'|$ is taken as the distinguishing metric between controllers r and r'. From (42), we can see that ϵ_u plays an important role in determining $\mathbf{p}_u$. Therefore, assuming ϵ_u as a given input parameter is not ideal. Rather, ϵ_u needs to be chosen such that the constraints of $DP0$ is satisfied. One approach to address this problem is to consider both $\mathbf{p}_u$ and ϵ_u as the decision variables of $DP0$. In this case, we can observe that $DP0$ is no longer a convex optimization problem and is difficult to solve.

We take the following **two step approach** to determine $\mathbf{p}_u$: **step 1:** determine a feasible value of ϵ_u by solving the equation $I(\mathbf{p}_u) = t_u$ and **step 2:** solve $DP0$ to obtain the best response of u using the feasible ϵ_u.

A. Determining ϵ_u

As the differential privacy constraint (42) holds for any mechanism that satisfies ϵ_u-differential privacy, we use the exponential mechanism [42] to solve $I(\mathbf{p}_u) = t_u$ and obtain a feasible ϵ_u. According to the exponential mechanism, $p_u^r \propto e^{-\epsilon_u c^r/2\Delta u}$, i.e., we consider the negative cost coefficient c^r as the utility. Therefore, using (43), we get

$$p_u^r = \frac{e^{-\epsilon_u c^r/2\Delta u}}{\sum\limits_{r'\in\mathcal{R}} e^{-\epsilon_u c^{r'}/2\Delta u}}. \tag{45}$$

Using $\mathbf{p}_u$ from (45), we solve $I(\mathbf{p}_u) = t_u$ for ϵ_u, e.g., by using the Netwon-Raphson method. It can be verified that the corresponding Jacobian is non-zero.

Remark. A vice versa relation also exists, i.e., for a given ϵ_u, we can identify a feasible value of t_u. To maintain consistency with the model in Section IV-D, we evaluate ϵ_u for a given t_u.

B. Optimal Response

Next, we solve $DP0$ using dual conjugate theory to determine the optimal response of u. Similar to Section IV-D, we focus on the case where $t_u^{\min} < t_u < t_u^{\max}$ (since a non-linear constraint exists in this case and the optimization problem is linearly constrained for other cases). First, we define the following:

Definition 2. *Conjugate function.* Let $f : \mathbb{R}^n \to \mathbb{R}$ and dom f be its domain. Then the conjugate function $f^* : \mathbb{R}^n \to \mathbb{R}$ is defined as follows:

$$f^*(\mathbf{y}) = \sup_{\mathbf{x}\in\text{dom } f} (\mathbf{y}^T\mathbf{x} - f(\mathbf{x})) \tag{46}$$

$$\text{dom } f^* = \{\mathbf{y} \mid \sup_{\mathbf{x}\in\text{dom } f} (\mathbf{y}^T\mathbf{x} - f(\mathbf{x})) < \infty, \ \mathbf{y} \in \mathbb{R}^n\} \tag{47}$$

Note that $f(\mathbf{x}) + f^*(\mathbf{y}) \ge \mathbf{y}^T\mathbf{x}, \ \forall \mathbf{x} \in \text{dom } f, \ \forall \mathbf{y} \in \text{dom } f^*$. Moreover, the equality occurs for the sub-gradient sets, i.e.,

$$f(\mathbf{x}) + f^*(\mathbf{y}) = \mathbf{y}^T\mathbf{x}, \text{ if } \mathbf{y} \in G(\mathbf{x}) \text{ or } \mathbf{x} \in G^*(\mathbf{y}) \tag{48}$$

where $G(\mathbf{x})$ and $G^*(\mathbf{y})$ are the sub-gradient of f and f^* at $\mathbf{x}$ and $\mathbf{y}$, respectively. Next, we define the positive homogeneous extension of f^* as follow:

Definition 3. *Positive homogeneous extension.* Let $f^* : \mathbb{R}^n \to \mathbb{R}$ and dom f^* be its domain. Then the positive homogeneous extension $f^+ : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$ is defined as

$$f^+(\mathbf{y}, \lambda) = \begin{cases} \lambda f^*(\mathbf{y}/\lambda), \ \lambda > 0 \\ \sup\limits_{\mathbf{x}\in\text{dom } f^*} \mathbf{y}^T\mathbf{x}, \ \lambda = 0 \end{cases} \tag{49}$$

$$\begin{aligned} \text{dom } f^+ = \{(\mathbf{y}, \lambda) | \lambda = 0, \ \sup_{\mathbf{x}\in\text{dom } f^*} (\mathbf{y}^T\mathbf{x}), \ \mathbf{y} \in \mathbb{R}^n\} \\ \cup \{(\mathbf{y}, \lambda) | \lambda > 0, \ \mathbf{y}/\lambda \in \text{dom } f^*\} \end{aligned} \tag{50}$$

In order to compute the dual of $DP0$, we first formulate the following equivalent optimization problem:

$$\begin{aligned} DP1: \quad & \underset{\mathbf{p}_u, \mathbf{x}, \mathbf{z}}{\text{minimize}} && \mathbf{c}_u^T \mathbf{p}_u && (51)\\ & \text{subject to} && I(\mathbf{x}) \le t_u, && (52)\\ &&& \mathbf{A}\mathbf{p}_u - \mathbf{z} \ge 0, && (53)\\ &&& \mathbf{z} = \mathbf{b}, && (54)\\ &&& \mathbf{p}_u - \mathbf{x} = 0, && (55)\\ &&& \mathbf{p}_u \ge \mathbf{0}. && (56) \end{aligned}$$

where $\mathbf{A}\mathbf{p}_u - \mathbf{b} \ge 0$ contains (42) and (43) (i.e., the differential privacy and probability distribution constraint, respectively).

The objective function of the dual program is computed as the sum of the conjugate function of the primal objective, (51), subject to constraint (54) and the positive homogeneous extension of constraint (52) which is given as:

$$f(\mathbf{z}', \mathbf{y}, \lambda) = \mathbf{b}^T\mathbf{z}'$$

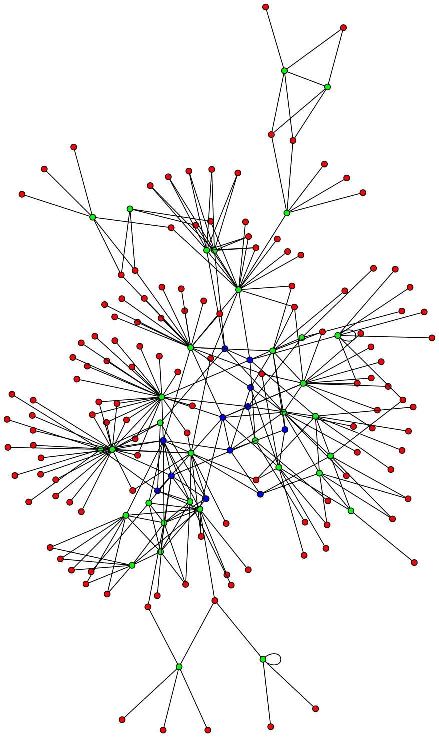

Fig. 2. Abovenet ISP topology. The blue and red nodes are backbone and access routers, respectively.

$$-\lambda\left[\sum_{r\in\mathcal{R}}\left[\sum_{\substack{v\in\mathcal{U}\\ v\neq u}} q_v p_v^r \log\left[\frac{q_v p_v^r(1-e^{y_r/\lambda q_u})}{\sum\limits_{v'\neq u} q'_v p'^r_v}\right]\right]+t_u\right]$$

subject to $\mathbf{s} = \mathbf{c}_u,\ \mathbf{z} = \mathbf{b},\ \lambda \geq 0$. Here $\mathbf{s}$ and $\mathbf{z}'$ are conjugate dual variables of $\mathbf{p}_u$ and $\mathbf{z}$, respectively and λ is the parameter from the positive homogeneous extension of constraint (52). For completeness, we derive the conjugate function of $I(x) - t_u$ in Appendix B. Further, from (48), the primal and dual variables are related as

$$s_r = \frac{\sum_{v\neq u} q_v p_v^r}{\lambda q_u(1 - e^{y_r/\lambda q_u})}. \tag{57}$$

Finally, the feasible set of the dual program is the dual cone of the primal cone generated by (53), (55) and (56). Let $\boldsymbol{\alpha}, \boldsymbol{\gamma}$ and $\boldsymbol{\delta}$ be the Lagrangian multipliers for constraints (53), (55), and (56), respectively. Then, using Definition 2, we have $\mathbf{s} = \mathbf{A}^T\boldsymbol{\alpha}+\boldsymbol{\delta}+\boldsymbol{\gamma}$, $\mathbf{y} = -\boldsymbol{\gamma}$, and $\mathbf{z}' = -\boldsymbol{\alpha}$. Here $\boldsymbol{\alpha} \geq \mathbf{0}$, $\boldsymbol{\gamma} \in \mathbb{R}^{|\mathcal{R}|}$, and $\boldsymbol{\delta} \geq \mathbf{0}$.

Now, we can form the dual program of $DP1$ as follows:

$$\begin{aligned} DP2: \quad & \underset{\boldsymbol{\alpha},\boldsymbol{\gamma},\lambda}{\text{minimize}} && f(-\boldsymbol{\alpha}, -\boldsymbol{\gamma}, \lambda) && (58)\\ & \text{subject to} && \mathbf{A}^T\boldsymbol{\alpha} - \mathbf{c}_u + \boldsymbol{\gamma} \leq 0, && (59)\\ & && \boldsymbol{\alpha} \geq 0, && (60)\\ & && \lambda \geq 0, && (61)\\ & && \boldsymbol{\gamma} \in \mathbb{R}^{|\mathcal{R}|}. && (62) \end{aligned}$$

$DP2$ is linearly constrained convex optimization problem and as it satisfies Slater's condition, strong duality holds and $\mathbf{p}_u^*$ can be computed using (57).

Algorithm 1: Iterative Best Response algorithm

```
Iterative Best Response Input: $\mathcal{G}$
Output: $\mathbf{p}_u^{NE}$ (Nash Equilibrium solution)
Randomly choose a feasible $\mathbf{p}_u^0$
$Update(\mathbf{P})$
do
    $Get(\mathbf{P}_{-u})$
    $\mathbf{P}_{prev} \leftarrow \mathbf{P}$
    $\mathbf{p}_u \leftarrow OptimalResponse(\mathbf{P}_{-u})$
    $Update(\mathbf{P})$
while $\mathbf{P} \neq \mathbf{P}_{prev}$;
```

VI. Nash Equilibrium

This section shows that Nash equilibrium exists for our games and presents an iterative best-response algorithm to compute it.

Definition 4. Nash Equilibrium. A mapping probability matrix $\mathbf{P}$ is a Nash equilibrium if and only if

$$f_u(\mathbf{p}_u, \mathbf{P}_{-u}) \leq f_u(\mathbf{p}'_u, \mathbf{P}_{-u}),\ \forall \mathbf{p}'_u \in \mathcal{S}_u,\ \forall u \in \mathcal{U} \tag{63}$$

Theorem 4. *For game $\mathcal{G}$, a pure strategy Nash equilibrium (PNE) exists.*

Proof. We can observe from $P2$ and $DP0$, that the strategy space of $\mathcal{G}$ is compact, convex, and non-empty and the cost function is convex. Hence, a pure strategy Nash equilibrium exists for $\mathcal{G}$ [46]. □

We use Algorithm 1 (IBR) to compute the pure strategy Nash equilibrium. Here, during the i^{th} update round, all switches compute their optimal response based on the strategies of other switches. This procedure is continued until the strategies converge to a Nash equilibrium. We observe that the optimal response of u does not depend directly on the strategy of the other individual switches. Rather, it depends on a few aggregate values (e.g., $\sum q_v p_v^r$ and $\sum q_v p_v^r \log(q_v p_v^r)$).

Theorem 5. *The iterative best response algorithm (IBR) converges to a pure strategy Nash equilibrium.*

Proof. The optimal response of u is subject to the constraint $I(\mathbf{p}_u) < t_u$. Hence, $\mathcal{G}$ is a game of strategic substitutes (with convex strategy sets) because if a switch with lower privacy requirement decreases the privacy of the system (to minimize its cost), then an another switch with higher privacy requirement substitutes for it (to meet its own privacy constraint). Moreover, the computation of best response in each round can be performed simultaneously in IBR. Then, under the assumption that all best response correspondences are single valued, IBR converges to a PNE [47]. □

VII. Performance Evaluation

This section evaluates the performance of the proposed mapping approaches. We abbreviate the solution of mapping game and differentially private mapping game as NM and NDM, respectively. For comparison we use the globally optimal solutions for the mapping game and differentially private

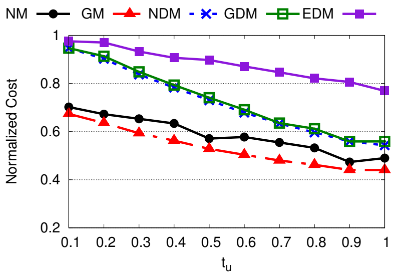

Fig. 3. Effect of t_u on the cost for IEEE 30 bus system.

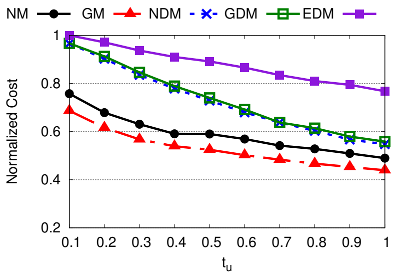

Fig. 4. Effect of t_u on the cost for IEEE 118 bus system.

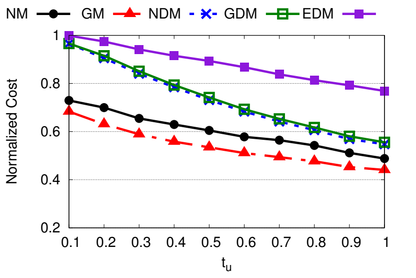

Fig. 5. Effect of t_u on the cost for IEEE 300 bus system.

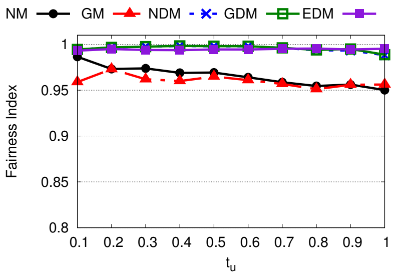

Fig. 6. Fairness index for IEEE 30 bus system.

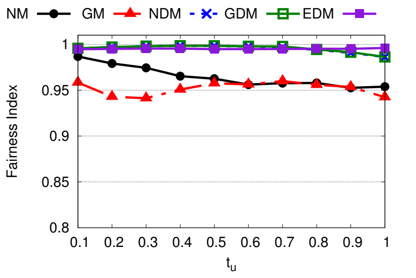

Fig. 7. Fairness index for IEEE 118 bus system.

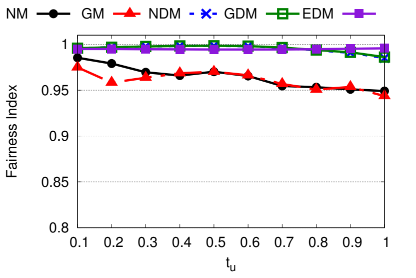

Fig. 8. Fairness index for IEEE 300 bus system.

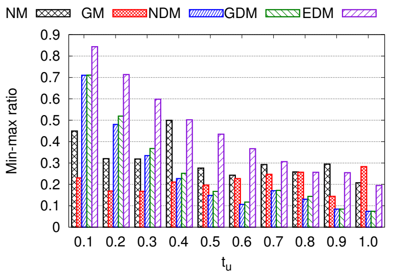

Fig. 9. Min-max load ratio for IEEE 30 bus system.

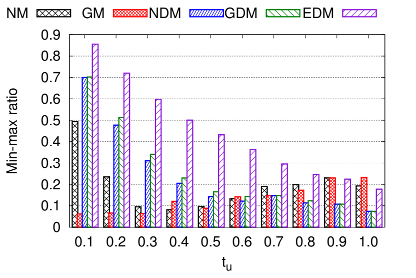

Fig. 10. Min-max load ratio for IEEE 118 bus system.

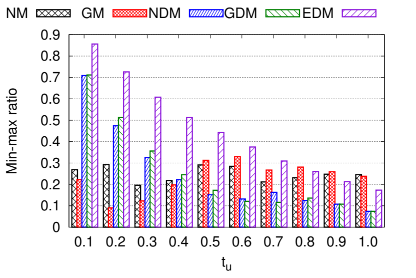

Fig. 11. Min-max load ratio for IEEE 300 bus system.

mapping game, abbreviated as GM and GDM, respectively. We also compare with the solution obtained using the exponential mechanism in (45), abbreviated as EDM.

We consider three power grids following the IEEE 30, 118 and 300 bus systems as our CPS [48]. The physical topology of the power grid (i.e., the connectivity of the buses and lines) is obtained using these topologies. An underlying and separate communication network interconnects the physical components (i.e., the substations which house the buses) of the smart grid. We adopt the network topology obtained from the Rocketfuel network topology traces for the SDN-based ISP, Abovenet [49], for the communication network to ensure that our evaluation uses a realistic network topology. The topology is depicted in Figure 2. We consider each substation (i.e., bus) to be a randomly chosen leaf-node in the Abovenet ISP network topology. Twelve backbone routers of the network are considered as the SDN controllers and the access routers of the network are considered as the SDN switches for the bus systems. We consider the prior probability on the switches to be uniformly distributed. The cost values in our evaluations are normalized such that the maximum cost is 1.

First, we examine the effect of t_u (i.e., the privacy requirement) on our mapping approach. We vary the value of t_u as $0.03, 0.06, \cdots, 0.3$ (lower value implies higher privacy). Figures (3)-(5) depict the average cost incurred per switch for the three power grid topologies. We observe that in general, as the value of t_u increases, the cost incurred decreases. For larger values of t_u, the switch chooses a controller with low cost with higher probability, thereby reducing the average cost incurred. We observe that the cost incurred for both NM and NDM is very close to their respective global solutions GM and GDM. The average difference in cost for NM and NDM is 10% and 1%, respectively. This extra cost is incurred due to the selfish behavior of the switches and the distributed nature of the solution when compared to GM and GDM. The difference in cost is lesser for DM because of the differential privacy constraint which renders both DM and GDM similar to each other. Moreover, due to the differential privacy constraint, the cost incurred by NDM and GDM is higher than that of NM and GM. As the value of t_u increases, we see that NM, GM, NDM and GDM tend to converge. This is intuitive as the mutual information and the differential privacy constraints relax with increasing t_u. We also note that on an average, EDM incurs an additional 66% and 24% cost compared to GM and GDM.

Next, we evaluate the fairness of the different approaches. We use Jain's fairness index, $FI = \frac{(\sum_{u\in\mathcal{U}} f_u)^2}{U\sum_{u\in\mathcal{U}} f_u^2}$, to quantify the fairness. Figures (6)-(8) show the fairness achieved for the three grid topologies. We observe that for smaller values of t_u (stricter privacy requirement), NM is fairer as compared to GM. For example, in the IEEE 118 bus system with $t_u = 0.2$, NM achieves a fairness of 0.98 while GM only achieves a fairness of 0.94. As the privacy constraint relaxes, NM and GM converge with respect to fairness. We observe that DM, GDM, and EDM achieve a fairness very close to 1 in almost all cases (with EDM being slightly less fair compared to DM and GDM). This fairness comes at a very high price. For example, for the IEEE 300 bus system with $t_u = 0.1$, DM, GDM and EDM incur an additional cost of 41%, 40.5%, and 47%, respectively. From Figures (6)-(8), we observe that NDM and GDM achieve better fairness compared to NM and GM for higher values of t_u while the cost incurred by the approaches tend to converge. Hence, NDM is preferred in this scenario to achieve better fairness for a little extra cost. For example, in the IEEE 300 bus system with $t_u = 1$, NM and NDM achieve a fairness of 0.95 and 0.99, respectively, with NDM incurring 12% extra cost.

Next, we examine the effect of our approaches on the traffic load at the controllers. We plot the ratio of the minimum controller load to that of the maximum controller load in Figures (9)-(11) for the three power grid systems. For smaller values of t_u, NDM, GDM and EDM are more balanced (i.e., higher min-max ratio) when compared to NM and GM. However, for higher values of t_u, NM and GM achieve better min-max ratio. For example, in the IEEE 30 bus system, when $t_u = 0.1$, NM and NDM achieve a ratio of 0.4 and 0.7, respectively, but when $t_u = 0.9$, the respective ratios are 0.3 and 0.1.

We would like to note that balancing the load at the controller is not the primary goal of our approaches but we observe an interesting trade-off between NM and NDM, especially for higher values of t_u. While NDM achieves better cost fairness than NM for a little extra cost, NM achieves better load balancing at the controllers and incurs lesser cost than NDM.

As the value of t_u decreases (i.e., mutual information constraint becomes stricter), the polytope formed (separately) by the differential privacy constraints (42) and the mutual information constraints (41) converge. For the limiting value of $t_u = 0$, both constraint (41) and constraint (42) have a single feasible point, $p_u^r = \frac{1}{|\mathcal{R}|}$, $\forall r \in \mathcal{R}$ (the uniform distribution). Therefore, when differential privacy constraints are added in NDM, the increase in cost incurred for switches with higher t_u is higher when compared to switches with lower t_u. As a result, the cost fairness for NDM is higher when compared to NM. Again, as the differential privacy constraints are stricter when compared to the mutual information constraint, the feasible region of the switches are more similar for NDM when compared to NM. As a result, the switches tend to prefer some controllers more (depending on the feasible region) that others, and hence, the load is less balanced for NDM when compared to NM.

VIII. Conclusion and Future Work

This paper proposed a switch-controller mapping scheme to mitigate passive information leakage from compromised controllers in SDN-based CPSs. The mapping is computed in a distributed manner by formulating a non-cooperative game among the SDN switches. The Nash equilibrium is computed using an iterative best response-algorithm. Our results shows that the proposed approach achieves near optimal results and better fairness when compared to the global solutions. The switch-controller mapping approach in this paper can be extended to include controller utilization and load balancing constraints to further improve the network performance. Also, currently we view the interactions between the switches as a non-cooperative game. Alternatively, we can explore the possibility of switches cooperating among themselves to achieve a socially private switch-controller mapping.

Appendix

A. Convexity of $I(U, R)$

The first order derivative of $I(U, R)$ with respect to p_u^r is evaluated as

$$\frac{\partial I(U,R)}{\partial p_u^r} = \tag{64}$$

$$\frac{\partial}{\partial p_u^r}\Bigg[q_u p_u^r \log\left(\frac{q_u p_u^r}{\sum_{u'\in\mathcal{U}} q'_u p_{u'}^r}\right) + \sum_{u'\neq u} q_{u'} p_{u'}^r \log\left(\frac{q_{u'} p_{u'}^r}{q_u p_u^r + \sum_{v\neq u} q_v p_v^r}\right)\Bigg]$$

$$= \frac{\partial}{\partial p_u^r}\Bigg[q_u p_u^r\bigg(\log(q_u p_u^r) - \log(q_u p_u^r + \sum_{v\neq u} q_v p_v^r)\bigg) + \sum_{u'\neq u} q_{u'} p_{u'}^r\bigg(\log(q_{u'} p_{u'}^r) - \log(q_u p_u^r + \sum_{v\neq u} q_v p_v^r)\bigg)\Bigg]$$

$$= q_u\Bigg[\log(q_u p_u^r) + 1 - \log(q_u p_u^r + \sum_{v\neq u} q_v p_v^r) - \frac{q_u p_u^r}{q_u p_u^r + \sum_{v\neq u} q_v p_v^r} - \sum_{u'\neq u}\frac{q_{u'} p_{u'}}{q_u p_u^r + \sum_{v\neq u} q_v p_v^r}\Bigg]$$

$$= q_u\Bigg[\log(q_u p_u^r) - \log(q_u p_u^r + \sum_{v\neq u} q_v p_v^r)\Bigg] \tag{65}$$

From Equation 65, we the following second order derivatives:

$$\frac{\partial^2 I(U,R)}{\partial {p_u^r}^2} = {q_u}^2\left(\frac{1}{q_u p_u^r} - \frac{1}{q_u p_u^r + \sum_{v\neq u} q_v p_v^r}\right),\ \forall r \in \mathcal{R} \tag{66}$$

$$\frac{\partial^2 I(U,R)}{\partial p_u^r \partial p_u^{r'}} = 0, \qquad \forall r \neq r'; r, r' \in \mathcal{R} \tag{67}$$

As $q_u p_u$ and $\sum_{v \neq u} q_v p_v^r$ are non negative, from Equation 66 $\frac{\partial^2 I(U,R)}{\partial {p_u^r}^2}$ is non negative for all r. Therefore, the Hessian matrix of $I(U,R)$ has non-negative diagonal elements. From Equation 67, the non-diagonal elements of the Hessian matrix are 0. Therefore the Hessian matrix is positive semi-definite and $I(U,R)$ is a convex function of $\mathbf{p}_u$.

B. Conjugate function of $I(x) - t_u$

Let $I^*(y)$ be conjugate of $I(x) - t_u$, then $I^*(y)$is given by:

$$I^*(\mathbf{y}) = \sup_{\mathbf{x}} (\mathbf{y}^T \mathbf{x} - (I(x) - t_u)) \tag{68}$$

$$\begin{aligned} &= \sup_{\mathbf{x}} \Bigg[\mathbf{y}^T \mathbf{x} - \Bigg(- \sum_{u \in \mathcal{U}} q_u \log(q_u) \\ &\quad + \sum_{u \in \mathcal{U}} \sum_{r \in \mathcal{R}} q_u x_r \log \left(\frac{q_u x_r}{\sum_{u' \in \mathcal{U}} q_{u'} p_{u'}^r} \right) - t_u \Bigg) \Bigg] \end{aligned} \tag{69}$$

Using the first order derivative, the supremum occurs at

$$x_r = \frac{\sum_{u' \in \mathcal{U}} q_{u'} p_{u'}^r}{q_u (e^{-y_r / q_u} - 1)} \tag{70}$$

Substituting the value of x_r in (69), we get

$$\begin{aligned} I^*(\mathbf{y}) = &-\sum_{r \in \mathcal{R}} \Bigg(\sum_{\substack{v \in \mathcal{U} \\ v \neq u}} q_v p_v^r \Bigg[\log(1 - e^{y_r / q_u}) \\ &+ \log \Bigg(\frac{q_v p_v^r}{\sum\limits_{v' \neq u} q_v' p_v'^r} \Bigg) \Bigg] \Bigg) + \sum_{u \in \mathcal{U}} q_u \log(q_u) + t_u \end{aligned} \tag{71}$$

Computing the positive homogeneous extension is straightforward by replacing y_r with y_r / λ for $\lambda > 0$.

References

[1] R. Sabella, "What do cyber-physical systems have in store for us?" Ericsson, Tech. Rep., 2019. [Online]. Available: https://www.ericsson.com/en/blog/2019/12/cyber-physical-systems-technology-trend

[2] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2014.

[3] R. Ahmed and R. Boutaba, "Design considerations for managing wide area software defined networks," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 116–123, 2014.

[4] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, T. Zinner, and P. Tran-Gia, "An SDN/NFV-enabled enterprise network architecture offering fine-grained security policy enforcement," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 217–223, 2017.

[5] Y. Cui, S. Xiao, C. Liao, I. Stojmenovic, and M. Li, "Data centers as software defined networks: Traffic redundancy elimination with wireless cards at routers," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 12, pp. 2658–2672, 2013.

[6] R. Cziva, S. Jouët, D. Stapleton, F. P. Tso, and D. P. Pezaros, "SDN-based virtual machine management for cloud data centers," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 212–225, 2016.

[7] I. T. Haque and N. Abu-Ghazaleh, "Wireless software defined networking: A survey and taxonomy," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2713–2737, 2016.

[8] K. Ahmed, J. O. Blech, M. A. Gregory, and H. Schmidt, "Software defined networking for communication and control of cyber-physical systems," in *IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, 2015, pp. 803–808.

[9] A. Jindal, G. S. Aujla, N. Kumar, R. Chaudhary, M. S. Obaidat, and I. You, "SeDaTiVe: SDN-Enabled Deep Learning Architecture for Network Traffic Control in Vehicular Cyber-Physical Systems," *IEEE Network*, vol. 32, no. 6, pp. 66–73, 2018.

[10] M. Cabral, M. Silveira, and R. Urie, "SDN Advantages for Ethernet-Based Control," Schweitzer Engineering Laboratories, Inc., Tech. Rep., 2019. [Online]. Available: {https://cdn.selinc.com/assets/Literature/Publications/White%20Papers/0030_SDNAdvantages_SW_20190627.pdf}

[11] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814–2825, 2018.

[12] D. Bendouda, A. Rachedi, and H. Haffaf, "Programmable architecture based on software defined network for internet of things: Connected dominated sets approach," *Future Generation Computer Systems*, vol. 80, pp. 188 – 197, 2018.

[13] N. Dorsch, F. Kurtz, H. Georg, C. Hägerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in *2014 IEEE international conference on smart grid communications (smart gridComm)*. IEEE, 2014, pp. 422–427.

[14] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 61–68.

[15] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 3, pp. 1220–1231, 2017.

[16] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial internet of things driven by SDN platform for smart grid resiliency," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 267–277, 2017.

[17] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 623–654, 2015.

[18] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, 2017.

[19] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 238–243.

[20] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[21] P. Gope and B. Sikdar, "An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3126–3135, 2018.

[22] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–28, 2019.

[23] 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," vol. 50, no. 2, May 2017.

[24] N. Mohammed, B. C. Fung, and M. Debbabi, "Anonymity meets game theory: secure data integration with malicious participants," *The VLDB Journal*, vol. 20, no. 4, pp. 567–588, 2011.

[25] M. Chessa, J. Grossklags, and P. Loiseau, "A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications," in *2015 IEEE 28th Computer Security Foundations Symposium*, 2015, pp. 90–104.

[26] R. Shokri, "Privacy games: Optimal user-centric data obfuscation," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 299–315, 2015.

[27] G. Theodorakopoulos, R. Shokri, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Prolonging the hide-and-seek game: Optimal trajectory privacy for location-based services," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014, pp. 73–82.

[28] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010, p. 61–66.

[29] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 238–243.

[30] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 327–332.

[31] A. Saleem, A. Khan, S. U. R. Malik, H. Pervaiz, H. Malik, M. Alam, and A. Jindal, "Fesda: Fog-enabled secure data aggregation in smart grid iot network," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6132–6142, 2020.

[32] G. Ács and C. Castelluccia, "I have a dream!(differentially private smart metering)," in *International Workshop on Information Hiding*. Springer, 2011, pp. 118–132.

[33] J. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *2010 IEEE International Conference on Communications Workshops*, 2010, pp. 1–5.

[34] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 248–258, 2015.

[35] U. Ghosh, P. Chatterjee, and S. Shetty, "A Security Framework for SDN-Enabled Smart Power Grids," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2017, pp. 113–118.

[36] V. Sridharan, K. S. K. Liyanage, and M. Gurusamy, "Privacy-Aware Switch-Controller Mapping in SDN-Based IoT Networks," in *2020 International Conference on COMmunication Systems NETworkS (COMSNETS)*, 2020, pp. 1–6.

[37] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, 2018.

[38] T. Wang, F. Liu, J. Guo, and H. Xu, "Dynamic SDN controller assignment in data center networks: Stable matching with transfers," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[39] M. F. Bari, A. R. Roy, S. R. Chowdhury, Q. Zhang, M. F. Zhani, R. Ahmed, and R. Boutaba, "Dynamic controller provisioning in software defined networks," in *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, 2013, pp. 18–25.

[40] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, "Devoflow: Scaling flow management for high-performance networks," in *Proceedings of the ACM SIGCOMM 2011 conference*, 2011, pp. 254–265.

[41] J. G. Mohanasundaram, T. Truong-Huu, and M. Gurusamy, "Game Theoretic Switch-controller Mapping with Traffic Variations in Software Defined Networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[42] 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.

[43] V. Thangavelu, D. M. Divakaran, R. Sairam, S. S. Bhunia, and M. Gurusamy, "Deft: A distributed IoT fingerprinting technique," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 940–952, 2018.

[44] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[45] *7. General Iterative Methods*. Society for Industrial and Applied Mathematics, 2000, pp. 181–239.

[46] S. Cachon, Gérard P.and Netessine, *Game Theory in Supply Chain Analysis*. Boston, MA: Springer US, 2004, pp. 13–65.

[47] P. Dubey, O. Haimanko, and A. Zapechelnyuk, "Strategic complements and substitutes, and potential games," *Games and Economic Behavior*, vol. 54, no. 1, pp. 77–94, 2006.

[48] X.-P. Zhang, C. Rehtanz, and B. Pal, *Flexible AC Transmission Systems: Modelling and Control*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 31–66.

[49] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP topologies with Rocketfuel," *ACM SIGCOMM Comput. Commun. Rev*, 2002.