## Incentive mechanisms

برگرفته از مقاله:‌ Incentive Mechanisms for Smart Grid: State of the Art, Challenges, Open Issues, Future Directions

Although SG can provide significant services and applications, attracting consumers/ producers to participate in several operations of SG is still a significant challenge. Consumers/ producers and grid operators may have to be provided with some incentive to improve the operations of the SG. For instance, demand response is a crucial operation in an SG, where the customers may have to shed/reduce their power consumption in peak periods to balance the supply and demand of electricity. To motivate the consumers to shed/reduce their energy consumption during peak hours, grid operators can provide them with incentives such as reduced pricing based on their energy consumption [6]. Another example is the government incentivizing grid operators who provide electric charging at a lesser price to electric vehicles (EV) by providing some subsidies or reducing taxes and so on [7]. Similarly, the producers can be motivated by providing incentives for renewable energy generation so that the emission of poisonous gases can be reduced to a great extent [8].

Hence, developing incentive mechanisms using several technologies, such as game theory, artificial intelligence (AI)/ ML algorithms, blockchain, and federated learning (FL), to motivate the SG operators, producers, and consumers of electricity plays a vital role in maintaining the supply/demand balance of electricity, optimizing resource utilization, providing a fair price to the consumers, reducing carbon emissions, and so on. Considering the aforementioned aspects, a comprehensive survey on the incentive mechanisms for SG is provided in this paper.

### Game Theory

Game theory deals with modelling strategies through which the players can make interdependent decisions by considering their competitor’s decisions [48]. This science of strategies helps the player determine various mathematical and logical actions that need to be performed to reach the optimum outcome in the game. Games in game theory can be categorized into five types: (i) cooperative and non-cooperative games; (ii) normal form and extensive form games; (iii) simultaneous move and sequential move games; (iv) constant sum, zero-sum, and non-zero-sum games; and (v) symmetric and asymmetric games. Game theory provides noteworthy analytical benefits in various disciplines such as finance, military, energy, operations research, and more.

Various games in game theory can also be used to solve critical issues in the SG. Out of these, cooperation in the non-cooperative setting is best suited for designing incentive mechanisms in the SG. Players have partial or total conflicting interests in deciding the case of non-cooperative games, whereas an incentive is provided for players to act together in the case of cooperative games. SG constitutes various micro-grid elements, in which some grids may require excess energy, whereas some other grids have unused energy to share. A cooperative strategy can be applied here for exchanging energy between microgrids without requesting it from the main grid [49]. Demand-side management (DSM) is a significant part of the SG, as energy consumption can be controlled on the consumer side. Incentives can also be provided to those consumers who adjust energy consumption by considering the peak hours and using power when it is least loaded in the grid. Monetary incentives can also be provided for consumers who voluntarily shift their energy usage during the non-peak hours, thus balancing the energy load.

A scheduling mechanism based on incentives for energy consumption was proposed by [50]. The “energy consumption scheduler” is provided in the smart meter, thus enabling optimal energy consumption for every user. Smart meters are connected to both the power lines and communication networks. With the help of a flexible and appropriate pricing mechanism, the Nash equilibrium can be achieved by not deviating from the actual strategy, and by making sure that the strategy of every component is also optimal when considering the decisions made by other components. A detailed study on incentive mechanisms is carried out by [15]. Similarly, anonymous rewarding schemes in the SG were studied by [51].

A framework named “REWARDS” was proposed for assigning rewards in SG [52]. This privacy-preserving mechanism can provide incentives to consumers by assigning rewards anonymously to the token, which can be redeemed at any time. A hybrid demand response mechanism that combines real-time incentives and pricing using a 3-level Stackelberg game was also proposed. This model proved beneficial for the power grid, retailers, and users. Similarly, a demand response model based on a 2-level Stackelberg game that understands consumer–company interaction was proposed. This allows the consumers to be provided with benefits based on the power consumed [53]. In addition, a dynamic pricing model was proposed to ensure SG robustness.

### Reinforcement learning algorithms can also be used for designing efficient energy trading games by providing the day-ahead details of pricing, thus enabling every player to understand strategies for energy trading that further increase average revenue [54,55]. In addition, incentive-based models from the viewpoint of grid operators were proposed. A two-loop Stackelberg game model was used by [56] to understand the interaction between different participants. The model considers different levels in the hierarchy, such as grid operators, service providers, and consumers. This incentive-based model works by the interaction between three hierarchical levels, which can help make significant demand reduction possible at the consumer end by assigning incentives based on their cooperation. The work was further extended in [57] by considering the intra-day market with demand response resources from multiple sectors. The Stackelberg approach could yield the best trading results and minimum procurement cost. Liu et al. [58] formulated a bi-level game that benefits both the consumer and aggregator by playing the game at the community level and the market level. An “energy demand partition-based market purchasing algorithm” is also proposed for solving the game formulated. Even though different games, in theory, can be used for formulating incentive mechanisms in SG, most of the research has been carried out with Stackelberg games, as they prove to be efficient in modelling decisionmaking problems.

### Blockchain

Blockchain can be defined as a digital ledger of decentralized transactions in a peerto-peer network. Due to the decentralized nature of blockchain, it offers various other advantages, such as transparency, security, privacy, traceability, cost reduction, efficiency, immutability, tokenization, and more [59]. Blockchain proves to be efficient in various domains, such as healthcare, SG, voting, real estate, banking, and insurance. The integration of blockchain with SG proves to be efficient in handling security, privacy, incentive mechanisms, penalty mechanisms, and standardization issues. Various use cases related to the use of blockchain have been carried out by [25]. Similarly, Mollah et al. provide an extensive study on the use of blockchain in SG [60]. In addition, Aderibole et al. surveyed the applicability of blockchain technology in SG about three important features: decentralization, incentives, and trust [61]. This section provides an overview of various research works on designing incentive schemes for SG using blockchain technology.

Incentive and penalty mechanisms are often related but complementary. Incentive schemes benefit customers by providing rewards in terms of cryptocurrency, reputation value, and carbon credit, whereas penalty schemes aid in preventing malicious activity by participating entities. Each electricity unit can be considered a virtual currency in blockchain technology. Wang et al. [62] proposed a blockchain-based energy system involving various energy trading transactions and crowdsourcing. This is carried out using a two-phase algorithm, where the initial phase focuses on grid operation and the second phase aids in balancing energy surplus or deficit using monetary incentivizing schemes. This system is implemented using the “IBM Hyperledger Fabric platform”. As wireless networks can further improve the efficiency of an energy trading system, [63] proposed an energy management system for SG using wireless networks and blockchain technology. The smart contracts enabled in this system allow the producers to gain fair incentives for providing quality power generation.

A security-aware demand response management system named “*e*-Sutra” was proposed by [64], which includes an “Ethereum-based smart contract” for incentivizing consumers as an effort to improve their energy-saving behaviour. Energy and carbon markets were also considered in a decentralized energy trading system proposed by [65]. In addition, incentive mechanisms prove to be useful in enhancing the grid connection behaviour of P2P trading systems [66]. Another breakthrough in the field was the introduction of a fully public blockchain to deal with the energy trading market [67]. A proof-of-stake consensus protocol alleviates the price gaps, thus rewarding the concerned party according to their energy behaviour. The integration of blockchain technology in the SG is still a hot research topic in energy systems, as more transparent and secure systems that benefit consumers and producers can be built using this. Figure 2 depicts the blockchain-based incentive mechanism for SG. Here, the data server publishes the task, the data owners upload their data, and the data miners verify the quality of data and the transactions. Based on the data uploaded by the users, appropriate incentives will be provided.

## Trust: State of the Art in Smart Grid

برگرفته از مقاله:‌ **A Trust-Influenced Smart Grid: A Survey and a Proposal**

In this section, we present literature on trust within the Smart Grid, categorized by the priority areas, conceptual domains, and trust definitions—after which we briefly discuss our observations. We searched the IEEE, Science Direct, Scopus, Web of Science, ACM, and Springer Link databases to find literature by using the keywords trust, reputation, trust management, mistrust, and trust model. We further reduced the papers by pairing each keyword with each of the following keywords: cyber-physical systems, critical infrastructure, distributed energy resources, micro-grids, smart grid, smart meters, substations, advanced metering infrastructure, building automation and control systems, distribution automation, and industrial control systems. We streamlined the list by reading the abstracts to ensure that the papers were relevant to the subject matter. The remaining papers were scrutinized and categorized or left out if they were not relevant to the subject matter.

Cheng et al. sought to detect the credibility of data from different sources by establishing trust from the said sources [29]. Though they were not specific about which part of Smart Grid they were working on, their work implied that it could be used in all areas of the Smart Grid because it deals with big data. In their paper, they used trust and credibility interchangeably. Even though the knowledge component exists in terms of previous trust values and a forgetting rate, the measure of risk on the data from the data source and the data source itself was not computed. There were no tests against trust-based attacks.

Moving away from big data to secure routing, another paper sought to compute trust for secured routing in wireless-based communications in the Smart Grid [30]. Networkbased features such as the average transmission rate, buffering capacity and time-to-live (TTL) are used to compute trust. Their algorithm first computes direct trust between nodes; indirect trust based on recommendations from other nodes; and finally uses that information to compute how to route information from one node to another within the Smart Grid communication infrastructure. This algorithm would work best in AMI but not in the generation and distribution domains of the Smart Grid where communications are more wired than wireless. This paper improved their previous trust model to identify benign and malicious nodes based on various features using a combination of Bayes, Dempster–Schafer and Fuzzy theory [31]. They employed a water cycle algorithm (WCA) to improve its efficiency and tested it using an NS-2 simulator. The parameters used are clear indicators of the knowledge component of trust; however, there was no measurement for risk to show the impact should a node be wrongfully trusted. The algorithm was also not tested against trust-based attacks.

Another paper also proposed a fuzzy logic-based trust model to ensure secure routing in the network [32]. It computes a global trust value by computing direct and indirect trust to allow nodes to make decisions on compromised nodes. They tested their work against trust-based attacks, but their algorithm had no risk component.

Still focusing on routing, Xiang et al. presented a trust-based geographical routing protocol which placed trusted nodes in a trust list [33–35]. To be part of the trusted list, the node was required to have a good performance ratio as well as a good recommendation from other nodes. Based on that list, a routing algorithm is implemented to route from one trusted node to another. Their work did not include a risk component and was not tested against trust-based attacks, even though it was tested against WSN-based DOS attacks. Their experiment was simulated using a Java-based simulator called J-Sim.

Though not creating their trust model, Bello et al. explored the impact of transitivity in network topology in the performance evaluation of the famous EigenTrust model [36]. They demonstrated that a network containing established transitivity connections implied that a benevolent node was quickly identified by a node, thereby reducing the average energy consumption. An improved version was tested against trust-based attacks and showed that structural similarity has an impact on robustness against trust-based attacks and malicious nodes [37].

In trying to detect a compromised node in a network, a trust management model was proposed based on fuzzy logic using the packet error rate, interaction duration and packet loss rate as features [38] to compute trust. There was no risk component in the calculation, and neither was the algorithm tested against trust-based attacks. The trust model was simulated using Xfuzzy-3.5.

Moving away from networks, and still within AMI, Pliatsios et al. computed trust based on three features, namely consumption, polling, and connection to detect malicious devices [39]. The continuous-time Markov chain was utilized to compute the trust value of a node. It was purely tested with numerical parameters. The trust value of a device was decreased or increased in unit steps within the range of 1–3 (inclusive) depending on the behaviour of the device. The state of the Markov chain stores the state of a previous interaction. However, the risk component does not exist to determine the extent of a possible threat on or from the device. Furthermore, an on–off attack can be used to ensure that the device’s trust value is maintained.

In tackling meter tampering within the AMI, Pradhan et al. did the reverse of calculating trust by using mistrust [40]. Their algorithm involved comparing the presented data with houses and actual data from smart meters to see whether a house is being truthful or not. A dishonest house is added to a mistrust table. Their algorithm has no risk component and was not tested against trust-based attacks.

In tackling cascading power failures, a trust management toolkit was proposed, which computes a trust value using the simple trust algorithm [41] which uses the threshold of grid values as input [42]. With the trust values being attained and Djikstra’s shortest path algorithm, it allows the flow of power in an optimal direction to prevent cascading failures. This work was improved upon to create a special protection system (SPS) that implemented a trust mechanism that is con-resistant and mitigates transient instabilities (being aperiodic of time) within the grid by using load-shedding strategies [43]. One of the key features in calculating trust values was ensuring that a node reports a frequency value around a specific threshold. There was no risk component, and their work was not tested against trust-based attacks.

Other papers assume that trust is already manifest in firewalls, intrusion detection systems (IDSs) and other security devices and therefore apply the term trust nodes for these devices. Thus, their research involves placing them in vantage points within the AMI [44–48] or SCADA network [49] and computing an optimal routing algorithm for them, especially when a node is compromised. These papers do not include any computations of trust because they assume that trust is already embedded in the devices.