An Enhanced Blockchain-Based Data Management Scheme for Microgrids

Chapter · March 2020

DOI: 10.1007/978-3-030-44038-1_70

4 authors:

Bacem Mbarek
Masaryk University
16 PUBLICATIONS **38** CITATIONS
SEE PROFILE

Stanislav Chren
Masaryk University
19 PUBLICATIONS **90** CITATIONS
SEE PROFILE

Bruno Rossi
Masaryk University
57 PUBLICATIONS **383** CITATIONS
SEE PROFILE

Tomáš Pitner
Masaryk University
101 PUBLICATIONS **295** CITATIONS
SEE PROFILE

An Enhanced Blockchain-Based Data Management Scheme for Microgrids

Bacem Mbarek, Stanislav Chren, Bruno Rossi, Tomás Pitner

Abstract Trading of distributed energy resources is an important aspect to fully achieve energy efficiency. Modern microgrids and consumer/prosumer energy transactions are such kind of enablers. The blockchain has been proposed as a solution to aid microgrid applications with the support of a decentralized trading model, operations processing, computation and storage. However, microgrids trading is still vulnerable to so-called False Data Injection (FDI) attacks, that is the attempt by malicious participating nodes to distribute false measurements to the peers to gain personal advantages. In this paper, we propose an enhanced blockchain mechanism to counteract possible FDI attacks by means of mobile software agents to control and detect malicious activities of sellers nodes.

Keywords: Microgrid, Blockchain, FDI attacks.

1 Introduction

Blockchains have emerged over time as a reliable and secure way to record transactions in an immutable manner, with their applicability that has been extended to many domains. In the smart grids context, blockchains have been adopted also for sharing and protecting electricity suppliers due to their scalability, interoperabil-

Bacem Mbarek
Faculty of Informatics, Masaryk University, Brno, Czech Republic, e-mail: bacem.mbarek@mail.muni.cz

Stanislav Chren
Faculty of Informatics, Masaryk University, Brno, Czech Republic, e-mail: chren@mail.muni.cz

Bruno Rossi
Faculty of Informatics, Masaryk University, Brno, Czech Republic, e-mail: brossi@mail.muni.cz

Tomas Pitner
Faculty of Informatics, Masaryk University, Brno, Czech Republic, e-mail: tomp@fi.muni.cz

ity and sustainability when connected to the microgrid [13]. The blockchain has been used to manage energy transactions between energy suppliers and neighbouring houses connected to the microgrid distribution system. We can exemplify how microgrids transactions have been adopting blockchain-based systems. Households can be considered as either energy consumers or prosumers (both providing excess energy and demanding energy). Each household has a quantity of electricity that it can sell to other members of the channel. Each seller sends to the blockchain its current state of stored energy reserves.

However, one of the well-known attacks in the microgrids context is the False Data Injection (FDI) attack [26], in which an attacker tries to inject false data within the system, for example by altering a subset of measurements either from sensors/devices or from the network. The final goal of the attacker is either to observe the behaviour based on the injected data or to force actors to take specific actions based on the tampered data, in this case selling/buying energy. Thus, several blockchain approaches have been proposed to support microgrids trading (e.g., [17]). However, such approaches focus more on the whole blockchain platform and are not specifically targeted at the prevention and detection of FDI attacks.

In this paper, we address the issue of FDI attacks by proposing a secure and efficient blockchain scheme for the microgrids, specifically tailored to identify and counteract FDI attacks. In particular, we present a distributed blockchain platform based on mobile agents to efficiently detect FDI attacks in microgrids. The mobile agent helps the blockchain peers to improve the identification of malicious nodes during the trading process.

The remainder of the paper is organized as follows. Section 2 presents an overview of microgrids systems with common definitions. Section 3 proposes our approach of integrating the blockchain with an agent-based system. To evaluate the proposed solution, Section 4 discusses the state-of-the-art solutions that have been proposed to implement blockchain in microgrids and approaches adopted for FDI attacks identification. Finally, Section 5 concludes the paper and outlines future directions for this work.

2 Background - Microgrids

The traditional power grid faced difficulties with issues such as increasing demand for uninterrupted power supply, pressure on environment protection and efficiency of power distribution. To tackle these challenges, the traditional power grid has begun its transformation to a smart grid. A smart grid (SG) is an infrastructure which utilizes the existing power network, enhanced with modern information and communication technologies. SG covers all the segments of power infrastructure from power generation, power distribution to power consumption in household, business and industry premises. One of the integral part of SG are Distributed Energy Resources (DERs). DERs are typically represented by renewable power sources, such as photovoltaics (PV)s or wind turbines which have become more accessible also to the household customers. Being able to locally produce and consume the electric power has lead to the introduction of new localised power grid infrastructure called

microgrid which allows to move the power generation closer to the loads [16]. The benefits of microgrids include the reduction of power losses in energy distribution, local regulation of power load, increased reliability and reduction of the high investments for network upgrades [16]. Microgrids can be controlled autonomously, and may operate in both grid-connected and self-sufficient modes [20]. Surveys of approaches to microgrid management can be found in [10], [15]. The overall architecture of a microgrid is shown in Fig. 1.

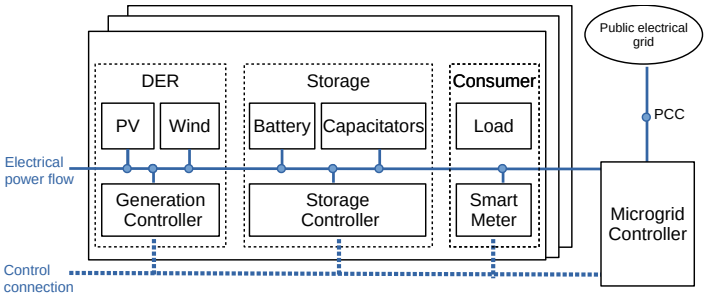

Fig. 1 Microgrid architecture

The main components of a microgrid are [12]: i) the power distribution system, ii) the DERs, iii) energy storage units and iv) communication and control modules. The responsibility of the distribution system is to transmit the power from the power between power generation, storage units, consumers as well as provides connection to the external power infrastructure. The structure of the distribution system depends on the type of the electrical current that is being transmitted: the alternating current (AC), the direct current (DC) or the combination of both. The storage component usually represents different types of batteries, capacitators or fuel cells. Their main purpose is to balance the load in the grid to increase its stability. The potential imbalance can be caused by the fluctuations of the power production output from DERs, such as PVs or wind turbines that are largely dependent on the current weather conditions. Additional fluctuations can be related to variety of consumer behaviour, i.e. their power consumption profile may vary depending on the time period in a day, week, year etc. There are many open issues in microgrids energy trading. Wang et al. [21] cover several of these aspects. On one side, the centralized management may lead to a single point of failure, and other risks related to transparency and data tampering. Furthermore, there can be privacy-related issues, as transaction traces can be used to derive patterns about energy generation and usage, especially if big data analysis platforms are adopted. Other issues can be related to the security of the communication of the infrastructure during energy transaction, as well as the resilience to cyber attacks. Other aspects might be related to encouraging the support of renewable resources, and granting flexibility to meet power demand.

The operation of microgrid depends on the up-to-date measurements of energy supply and demand. The measurements are collected from smart meters, sensors and controllers which are deployed at the customer premises. These components are

often deployed in open environment and communicate with each other using wireless technologies which makes them vulnerable to potential cyber attacks. From the power grid perspective, false data injection (FDI) attacks can have a serious impact on stability of power network [8]. In general, injecting false data may increase the risk of power grid instability by allowing injection (or consumption) of more or less energy than is safe – based on decisions made on the basis of falsified data [18]. In the microgrid context, the FDI attack can be viewed as forgery or modification of measurements for energy supply and demand from customers. For example, a compromised customer can claim less energy available than what can be provided, or they can claim more energy needed than what is required or combination of both [26].

3 Microgrid Electricity Transaction Mode Based on Blockchain

3.1 Overview of our layered design

Each household has specific quantities of energy that can be produced and stored and will bid excess energy to be traded by means of microgrid energy transactions. Each seller responds to the blockchain by letting it know the current amount of stored energy. As discussed, False Data Injection (FDI) attacks are one of the main threats faced by microgrids, making the whole transaction process less trustful, as they introduce uncertainty about the values of energy bids. We therefore describe an enhanced blockchain-scheme called Microgrid Blockchain Platform (MBP) based on mobile agents to enable the trusted and secure settlement of electricity trading transactions. Each agent monitors the activities of sellers in the network. The blockchain peer nodes use the mobile agent report to improve the decision making process, and make better decisions in the verification of the sellers declared information.

3.1.1 System Design

In our proposal, the blockchain is composed of three elements: 1) endorsing peers, 2) the ordering service, and 3) committing peers. As shown in Figure 2, each householder is a transmitter/receiver that sends requests/information to neighbour houses in the channel through the blockchain platform. In blockchain, the smart contract is a code fragment that executes the terms of a contract [25]. A channel can be defined as a sub-network for peers communication, if it is necessary to divide transactions according to different boundaries according to some service logic. Channels can represent others groups of neighbouring electricity producers and consumers.

- **Endorsing peers** are a predefined number of households that will endorse a transaction proposal, as defined in specified policies. When enough endorsing peers support a transaction proposal, it can be submitted to the ordering service to be added as a block. During the commissioning and configuration of the

blockchain network, the developers should select a number of households that are defined as the endorsing peers.

- **Ordering service** collects transactions for a channel into proposed blocks for distribution to peers. Blocks can be delivered for each defined channel. The task of the ordering service is to gather all the endorsed transactions, perform the ordering in a block, and then send the ordered blocks to the committing peers.
- **Committing peers** (including endorsing peers) run the validation and update their copy of the blockchain and status of transactions. Each peer receiving the block, as a committing peer, can now attach the new block to its copy of the transactions. Committing peers have also the responsibility of updating the shared ledger with the list of transactions.

3.1.2 Order-execute architecture in microgrid blockchain platform

When a seller agrees to enter into a transaction, he determines the parameters of this transaction by specifying its energy supply value, its location, price. Each transaction is stored in a smart contract and transmitted to the endorsing peers of the blockchain platform. The received transaction is verified by checking their smart contract. After the reception of N providers transactions, the endorsing peers can choose one provider by their own preferences (provider/consumer locations and distance report, supply value, price) to serve a consumer. Then, the endorsing peers verifies the selected provider by using a mobile agent that attempts to detect the quantity of the electricity supply stored in the selected seller and will be acting as a local FDI detector. Moreover, the mobile agent will migrate from the Blockchain platform to the selected seller to check the storage, power balance, smart meters behaviour, and historical transactions. To improve the decision making process, the endorsing peers use the mobile agent for detecting the wrong declared power supply by the selected seller. Any malicious activity will be sent to the endorsing peers. The mobile agents are able to autonomously migrate from the peers to a selected house, transferring their code and data, which allows them to efficiently perform computations, gather information and accomplish tasks.

Figure 2 depicts an example of execution of transaction in the blockchain-enabled microgrid system. The seller adds the current stored amount of energy to a smart contract and sends it to the blockchain platform. Once the smart contract is received by the blockchain platform, the endorsing peers checks and verifies the authenticity of the smart contract and sends a mobile agent to the selected seller. The mobile agent will migrate to seller and verifies its data (battery storage, meters functionalities, encryption protocols, network communication, historical transactions) and creates a reports about the gathered information and returns back to the endorsing peers. When the report is received, the endorsing peers start the verification of the received information and then decide to accept or reject the seller's transaction.

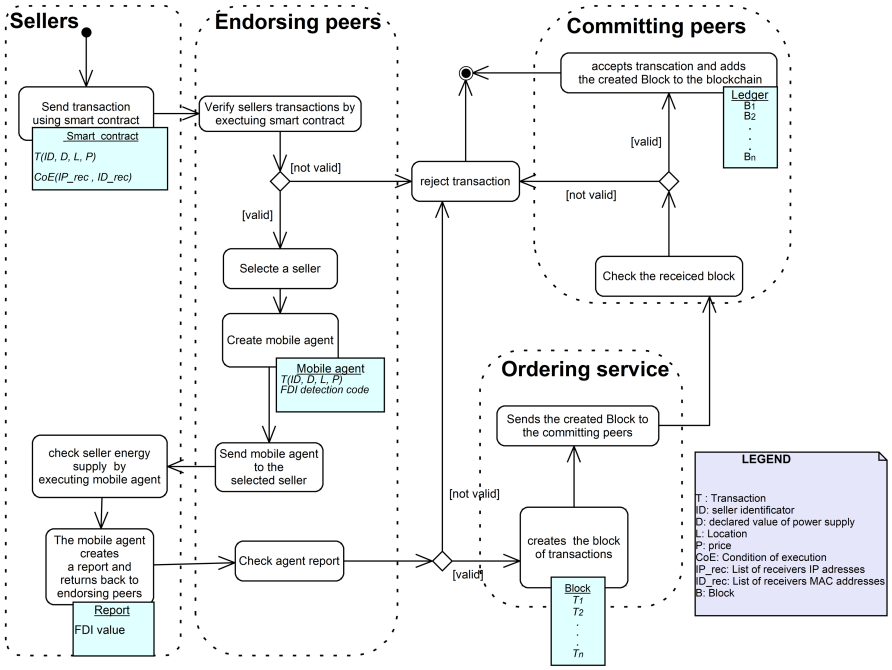

Fig. 2 Order-execute architecture in microgrid blockchain platform

3.1.3 Agent-based policy for an enhanced blockchain management

In our context, a mobile agent is a standalone software entity that can start various tasks when visiting different computing nodes: such as collecting data, doing some computation, as well as visiting other computing nodes [1].

The Battery Management System (BMS) sensors are coupled to all batteries storage in the smart grids to monitor and control power density, battery life such as charge and discharge process, which all are important parameters for battery storage. BMS sensor consists of measuring devices to collect parameters such as battery voltage, current, and temperature. These parameters can be used to calculate an estimation of batteries state of charge (SOC) and state of health (SOH) [5] [22]. The mobile agent can visit each of the microgrid nodes involved in energy transactions and execute customized code on each BMS sensor. The mobile agent can detect anomalies in the communicated data, compared to what detected by the BMS sensor. Of course, such approach cannot detect cases in which the BMS sensor itself has been tampered with, like modifications of firmwares or complete substitution of the equipment (as long as the tampered hardware complies with the contract to interface with the software compoments).

3.1.4 System Implementation

In the implemented platform, the blockchain platform will create a mobile agent dedicated to every selected seller. The mobile agent will migrate to the selected seller. Then, the mobile agent will execute its code in the battery management sensor. The mobile agent computes the volume of energy V that is produced by each seller and reported by the sensors. Then the mobile agent compares V with D, where D is the declared value of power supply submitted to the blockchain. If $D < V \pm \varepsilon$, then a potential FDI attack is suspected. The mobile agent also checks if the seller is a member of other blockchain channels, and computes the supply transactions C which will be delivered to those channels. If $D < (V - C) \pm \varepsilon$, then a potential FDI attack can be reported. The mobile agent detects the FDI attacks as depicted in Equation (1), where ε represents some measurement error threshold.

$$FDI = \begin{cases} 1, & \text{if } D < V \pm \varepsilon \text{ or } D < (V - C) \pm \varepsilon \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

We have implemented a preliminary prototype of our approach in the open source blockchain platform called Hyperledger Fabric [7] which has been reported as one of the most suitable platforms for the smart grid sector [24]. All nodes (both sellers and buyers) on the network use the SHA-1 hash algorithm and 2MB as data block sizes. With Battery Management home devices linked by the hyperledger blockchain, the foundation of blockchain equipped smart home was designed to control electricity trading between neighbour houses. For this system to work, sellers should be a blockchain channel member. Besides that, there are two ways for endorsing peers to verify and check the authenticity of the sellers transactions, by their smart contract and by the mobile agent report. We created a smart contract program that is used by the seller to send its transaction to the endorsing peers. We deployed the initial prototype to test the feasibility of the solution, we planned further tests by running simulations of different scenarios of energy trading and data tampering activities.

4 Related Work

Related works go into two directions: the application of blockchains in the context of microgrids, and the detection of FDI attacks disrupting microgrids transactions.

Usage of the Blockchain in Microgrids. The decentralized nature of the blockchain has gathered wide interest for its application in the smart grids context, making energy trading the most interesting area of adoption, with several solutions that were proposed over time [4]. Blockchains have been applied to overcome many of the issues in energy trading. According to Mengelkamp et al. [14], the adoption of blockchains can bring a series of advantages. First of all, building distributed systems that are more secure and built bottom-up, increasing transparency, reliability and equality between different actors. Another advantage is no need for central in-

termediaries, as well as cost-efficient micro-transactions in a fully distributed and decentralized system with transactions that are irreversible (which can sometimes be considered an issue). On the other side, the correct application of blockchains can also bring drawbacks such as scalability issues, high energy consumption, and potentially the adoption of technologies that are not yet mature for a wide adoption.

Several platforms for the adoption of the blockchain in microgrids and energy trading have been proposed over time. Mengelkamp et al. [14] provide the simulation of a decentralized energy platform based on the Ethreum blockchain. Agent-based systems are used to model prosumers bidding energy. Overall, the simulated scenarios show the real-time behaviour of such energy trading mechanisms, however, more concrete implementations are necessary to evaluate the feasibility. Kang et al. [9] propose an energy trading platform based on the Ethereum blockchain. Authors discuss the implementation of smart contracts, to allow prosumers perform transactions. The scenario shown applies to only two nodes, so scalability of the solution is a future work. While previous work focuses on the general application of the blockchain for energy trading in the migrogrids, our research focuses more on how the inclusion of an agent-based system, together with the blockchain, can bring benefits in terms of control of data tampering activities.

Microgrids FDI Attacks Identification & Countermeasures. The identification of FDI activites and application of proper countermeasures in the area of microgrids is a widely discussed topic (e.g., [26, 8]). False data injection attacks have gathered large attention in the context of the Smart Grids infrastructure, as false data can propagate through the network bringing to wrong decisions and failures. In the context of microgrids, FDI attacks can be exploited by malicious users to gather the maximum benefits from the transactions between authorized participants [8]. Countermeasures about FDI go typically in three directions: protecting critical measurements, detecting FDI attacks, and increasing uncertainties in power systems (to make data injection activities more difficult) [11].

Various approaches have been proposed to deal with FDI attacks in microgrids. Beg et al. formalized the problem as properties that do not change over time in microgrids (invariants), with dynamic analysis aimed at identifying mismatches [2]. Chlela et al. proposed a real-time hardware-in-the-loop testing platform to detect FDI attacks and study mitigation strategies [3]. Talebi et al. proposed to address coordinated FDI attacks by dynamically changing the information structure of microgrids [19]. Yu et al. coupled a threshold-based anomaly detection approach with a watermarking-based scheme to avoid data tampering of measurement information [23]. Furthermore, many authors focused on different machine learning approaches for the identification of FDI attacks, like He et al. examining the application of deep learning for real-time injection events identification [6]. While various FDI detection techniques in the literature address the problem of false data injection in the microgrids, there is still a lack on providing practical and secure FDI detection methods. Our blockchain agent-based proposal is more based on the higher level, but some of the approaches from related works can be applied either at the single agent level or at the level of information aggregation by several agents.

5 Conclusion

In this paper, we proposed a new blockchain mechanism based on a mobile agent system to address the problem of False Data Injection (FDI) attacks in microgrids energy trading. The proposed platform allows to detect FDI attacks as the blockchain system does not have to wait for the distribution of the sharing supply and the verification of the channel peers. The blockchain platform in collaboration with endorsing peers sends a mobile agent to detect the possible FDI attacks in each household location. By using and integrating mobile agents in the blockchain, the FDI attacks are identified and isolated from the network. Thus, this will significantly reduce the impact of tampered data and help the endorsing peers to make a decision about the distributed transactions. As a future work, we plan to to conduct set of experiments of simulated runs according to various microgrid topologies and type of data tampering attacks, testing how the blockchain platform can behave. Furthermore, we plan to handle the challenge of interoperability and the cost of implementing such new framework compared to traditional approaches.

Acknowledgements The research was supported from ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

References

1. Arekete, S.A., Oguntunde, B.O., Ore-Adewole, O.G.: Development of a mobile agent system for monitoring memory usage in a network. The International Journal of Engineering and Science (IJES) **6**, 1–13 (2017)
2. Beg, O.A., Johnson, T.T., Davoudi, A.: Detection of false-data injection attacks in cyber-physical dc microgrids. IEEE Transactions on industrial informatics **13**(5), 2693–2703 (2017)
3. Chlela, M., Joos, G., Kassouf, M., Brissette, Y.: Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In: 2016 IEEE Power and Energy Society General Meeting (PESGM), pp. 1–5. IEEE (2016)
4. Goranović, A., Meisel, M., Fotiadis, L., Wilker, S., Treytl, A., Sauter, T.: Blockchain applications in microgrids an overview of current projects and concepts. In: IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 6153–6158. IEEE (2017)
5. Haq, I.N., Leksono, E., Iqbal, M., Sodami, F.N., Kurniadi, D., Yuliarto, B., et al.: Development of battery management system for cell monitoring and protection. In: 2014 international conference on electrical engineering and computer science (ICEECS), pp. 203–208. IEEE (2014)
6. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Transactions on Smart Grid **8**(5), 2505–2516 (2017)
7. Hyperledger: Hyperledger fabric (2019). URL https://github.com/hyperledger/fabric
8. Islam, S.N., Mahmud, M., Oo, A.: Impact of optimal false data injection attacks on local energy trading in a residential microgrid. Ict Express **4**(1), 30–34 (2018)
9. Kang, E.S., Pee, S.J., Song, J.G., Jang, J.W.: A blockchain-based energy trading platform for smart homes in a microgrid. In: 2018 3rd International Conference on Computer and Communication Systems (ICCCS), pp. 472–476. IEEE (2018)
10. Khan, A.A., Naeem, M., Iqbal, M., Qaisar, S., Anpalagan, A.: A compendium of optimization objectives, constraints, tools and algorithms for energy management in microgrids. Renewable and Sustainable Energy Reviews **58**, 1664–1683 (2016)

11. Liu, X., Li, Z.: False data attack models, impact analyses and defense strategies in the electricity grid. The Electricity Journal **30**(4), 35–42 (2017)
12. Mariam, L., Basu, M., Conlon, M.F.: Microgrid: Architecture, policy and future trends. Renewable and Sustainable Energy Reviews **64**, 477 – 489 (2016). DOI https://doi.org/10.1016/j.rser.2016.06.037. URL http://www.sciencedirect.com/science/article/pii/S1364032116302635
13. Mbarek, B., Jabeur, N., Pitner, T., et al.: Mbs: Multilevel blockchain system for iot. Personal and Ubiquitous Computing pp. 1–8 (2019)
14. Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., Weinhardt, C.: A blockchain-based smart grid: towards sustainable local energy markets. Computer Science-Research and Development **33**(1-2), 207–214 (2018)
15. Minchala-Avila, L.I., Garza-Castañón, L.E., Vargas-Martínez, A., Zhang, Y.: A review of optimal control techniques applied to the energy management and control of microgrids. Procedia Computer Science **52**, 780–787 (2015)
16. Patrao, I., Figueres, E., Garcer, G., Gonzlez-Medina, R.: Microgrid architectures for low voltage distributed generation. Renewable and Sustainable Energy Reviews **43**, 415 – 424 (2015). DOI https://doi.org/10.1016/j.rser.2014.11.054. URL http://www.sciencedirect.com/science/article/pii/S1364032114009939
17. Sabounchi, M., Wei, J., et al.: Blockchain-enabled peer-to-peer data trading mechanism. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1410–1416. IEEE (2018)
18. Stelec, M., Hering, P., Janeek, P., Georgiev, D., Vor, P.: Optimal procurement of ancillary services considering balance and system security criteria. In: 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), pp. 1–5 (2019). DOI 10.1109/ISGTEurope.2019.8905458
19. Talebi, M., Li, C., Qu, Z.: Enhanced protection against false data injection by dynamically changing information structure of microgrids. In: 2012 IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM), pp. 393–396. IEEE (2012)
20. Ton, D.T., Smith, M.A.: The us department of energy's microgrid initiative. The Electricity Journal **25**(8), 84–94 (2012)
21. Wang, N., Zhou, X., Lu, X., Guan, Z., Wu, L., Du, X., Guizani, M.: When energy trading meets blockchain in electrical power system: The state of the art. Applied Sciences **9**(8), 1561 (2019)
22. Xing, Y., Ma, E.W., Tsui, K.L., Pecht, M.: Battery management systems in electric and hybrid vehicles. Energies **4**(11), 1840–1857 (2011)
23. Yu, W., Griffith, D., Ge, L., Bhattarai, S., Golmie, N.: An integrated detection system against false data injection attacks in the smart grid. Security and Communication Networks **8**(2), 91–109 (2015)
24. Yu, Y., Guo, Y., Min, W., Zeng, F.: Trusted transactions in micro-grid based on blockchain. Energies **12**(10), 1952 (2019)
25. Yuan, Y., Wang, F.Y.: Towards blockchain-based intelligent transportation systems. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pp. 2663–2668. IEEE (2016)
26. Zhang, X., Yang, X., Lin, J., Yu, W.: On false data injection attacks against the dynamic microgrid partition in the smart grid. In: 2015 IEEE International Conference on Communications (ICC), pp. 7222–7227. IEEE (2015)