J. Mod. Power Syst. Clean Energy (2018) 6(5):900–917
https://doi.org/10.1007/s40565-018-0425-1

Cyber-secure decentralized energy management for IoT-enabled active distribution networks

Zhiyi LI[1], Mohammad SHAHIDEHPOUR[1], Xuan LIU[2]

Abstract This paper provides a strategic solution for enhancing the cybersecurity of power distribution system operations when information and operation technologies converge in active distribution network (ADN). The paper first investigates the significance of Internet of Things (IoT) in enabling fine-grained observability and controllability of ADN in networked microgrids. Given severe cybersecurity vulnerabilities embedded in conventionally centralized energy management schemes, the paper then proposes a cyber-secure decentralized energy management framework that applies a distributed decision-making intelligence to networked microgrids while securing their individual mandates for optimal operation. In particular, the proposed framework takes advantage of software-defined networking technologies that can secure communications among IoT devices in individual microgrids, and exploits potentials for introducing blockchain technologies that can preserve the integrity of communications among networked microgrids in ADN. Furthermore, the paper presents the details of application scenarios where the proposed framework is employed to secure peer-to-peer transactive energy management based on a set of interoperable blockchains. It is finally concluded that the proposed framework can play a significant role in enhancing the efficiency, reliability, resilience, and sustainability of electricity services in ADN.

Keywords Cybersecurity, Active distribution network, Blockchain, Decentralized decision-making, Internet of Things, Networked microgrids, Transactive energy

1 Introduction

Distributed energy resources (DERs), which have progressively taken the place of centralized and large-scale generating facilities, have become active participants in the provision of electricity services for managing the state of electric power systems at steady state and extreme conditions. As larger populations in major metropolitan areas of the globe demand higher quantities, cleaner and more reliable electric energy services for sustaining a socioeconomic development, DERs dispersed in power distribution systems present logical solutions to address the growing concerns pertaining to a warmer climate by harvesting local and abundant energy resources [1].

However, a growing number of DERs would fundamentally change the way energy is generated, delivered, and consumed, and thereby put additional strain on the legacy power distribution infrastructure. In essence, power distribution systems penetrated by DERs feature multi-directional power flows (representing the interoperability among DERs, utilities, and customers) instead of traditional one-way power delivery directly from upstream

CrossCheck date: 5 June 2018

Received: 17 April 2018 / Accepted: 5 June 2018 / Published online: 6 July 2018

✉ Zhiyi LI
zhiyi.li@hawk.iit.edu

Mohammad SHAHIDEHPOUR
ms@iit.edu

Xuan LIU
xliu@hnu.edu.cn

[1] Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago 60616, USA

[2] College of Electrical and Information Engineering, Hunan University, Changsha 410006, China

centralized generating facilities to end customers. Moreover, a widespread adoption of DERs would drive and flourish distributed and controllable power systems (e.g., microgrids, nanogrids) in the near future and challenge the existing utility-based regulation models and policies [2–4]. These distributed power systems are expected to play an increasingly important role in extracting incremental values from DERs locally and improving power distribution system operations globally.

As grid modernization continues, power distribution systems themselves become a platform for social and technological innovations to enhance the efficiency, reliability, resilience, and sustainability of electricity services. A multitude of state-of-the-art information technologies are adopted to meet the technical challenges resulting from the widespread implementation of DERs across the legacy power distribution infrastructure, among which Internet of Things (IoT) plays the key part in filling the gap between control and monitoring applications and physical processes.

A myriad of physical objects (i.e., things) is increasingly connected to the Internet that would establish and enhance the connection of humans with things. However, the number of things connected to the Internet surpassed the globe's total population in 2008 [5]. The interconnected things are not only data sources that continuously harvest information from the residing environment through sensing, but also automated actors that make any requested change in effect through actuation. In this regard, IoT is viewed as a set of innovative technologies that instill intelligence to almost any such thing and link them to interact with the physical world. It is postulated that more than one trillion IoT devices would be connected to the Internet by 2022 [6] accounting for 45% of all Internet traffic [7].

The rapid growth in the number and diversity of IoT devices would benefit modern power distribution systems [8]. IoT technologies interconnect disparate devices, platforms, and services from virtually anywhere for managing the electricity generation, delivery, and consumption. As IoT devices are growing increasingly ubiquitous and powerful, they also expand their potentials collectively in active distribution network (ADN) [9–12].

Technically, ADN is a sophisticated cyber-physical system comprising a wide range of networked physical objects such as traditional utility assets (e.g., transformers, lines, capacitors) and DERs along with their coupling communication and control systems. In fact, modern power distribution systems are increasingly adopting strategic IoT solutions for enabling the transition toward ADN. ADN is increasingly viewed as a power distribution system which is inherent with IoT-enabled control, monitoring, and communication capabilities for optimizing and automating bidirectional flows of both electricity and information.

However, the proliferation of IoT devices will unavoidably produce massive volumes of raw data throughout ADN operations, which present significant difficulties in making rapid and shrewd decisions on energy management. Additionally, widespread implementations of IoT devices expand cyberattack surfaces exposed to disruptive agents, raising significant cybersecurity concerns in the context of ADN. Given that ADN operations depend heavily on the extended network of intelligent IoT devices across a power distribution infrastructure, any credible cyberattack on IoT devices may jeopardize the security of ADN operation and even lead to a system-wide blackout.

As cyberattacks manifest themselves with increasing sophistication, common cybersecurity solutions such as anti-virus software and firewalls will not be adequate to fend off cyberattacks [13]. ADN is therefore in need of cyber-secure energy management schemes that are tolerant of cyberattacks. Besides, most IoT devices have limited computation capabilities which render them incapable of running sophisticated encryption and authentication algorithms for securing communication systems, which further exacerbate ADN challenges for meeting evolving cybersecurity requirements.

To address potential cybersecurity issues in IoT-enabled ADN, this paper proposes a secure, scalable, and efficient energy management framework, which coordinates the application of prevalent cybersecurity technologies such as software-defined networking and blockchain to ensure the integrity and privacy of decentralized decision-making processes. The remainder of the paper is organized as follows. Section 2 investigates the role of IoT technologies in enabling ADN that will be formed by networked microgrids and discusses potential cybersecurity vulnerabilities in contemporary centralized energy management schemes. Section 3 develops a hierarchical framework for securing the ADN energy management by taking advantage of prevalent cybersecurity solutions. Section 4 provides a deep insight into cyber-secure decentralized transactive energy management based on the proposed cybersecurity enhancement framework. Section 5 concludes the paper and stresses the significance of cybersecurity in achieving the smart grid goals.

2 IoT-enabled ADNs

The development toward ADN has been driven by grid modernization requests for sustainable, flexible, secure, efficient, reliable, resilient electricity services at the power distribution level. As shown in Fig. 1, technological and

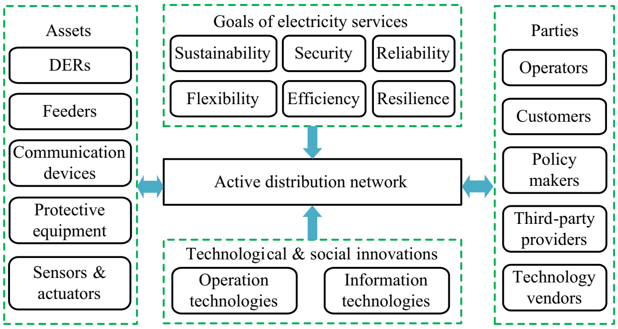

Fig. 1 ADN implementations driven by grid modernization requests

social innovations lay the foundation for ADN implementations where pertinent parties and assets are granted with a higher autonomy and a more proactive view of power system operations. In particular, the tight integration of IoT technologies and the legacy electric power distribution infrastructure acts as the fundamental enabler of ADN that will fuel economic prosperity, environmental protection, and social welfare in future smart cities [14].

2.1 IoT technologies for boosting ADN development

2.1.1 Convergence of IoT and ADN implementations

The emerging IoT technologies manage to instill intelligence, interconnection, and instrumentation into the legacy power distribution infrastructure with the supplement of advanced transducers (i.e., sensors and actuators), low-cost communication media, and fine-grained applications. Accordingly, those physical objects involved in power distribution system operations are turned to smart things that can sense continuous changes in the operating environment and implement autonomous actions resulting from intelligent data analytics.

The seamless integration of IoT technologies with ADN provides immense opportunities to realize fine-grained energy management decision making (e.g., operations, maintenance, planning) that capture full DER values in distributed power systems. A practical example applies to power electronic inverters which are enhanced with IoT technologies for achieving operational intelligence (e.g., automated reporting and control actions). The resulting smart inverters can elegantly regulate terminal voltage and output power of associated DERs [15]. Power utilities and third-party service providers harness IoT technologies to build a detailed view of power generation and consumption postures in ADN so as to offer a broad range of value-added electricity services to customers. Meanwhile, electricity customers will leverage IoT technologies to enjoy the benefits of being actively engaged with power distribution system operations through demand-side participation. Therefore, the ADN implementation is considered a leading real-world example of IoT [8].

IoT technologies play a critical role in interconnecting hardware-based devices and software-based applications across all facets of ADN operations, thereby facilitating the large-scale implementations of machine-to-machine communications and human–machine interactions. For example, a diversity of smart things enabled by the prevalence of radio frequency identification [16], near-field communications [17], and wireless sensor networks [18] has established close ties between information and physical processes in concert with efficient and reliable communication systems required in ADN operations. Figure 2 shows a representative case where various physical components pertinent to different domains of ADN operations are interlinked seamlessly by IoT technologies.

2.1.2 IoT technologies for enhancing observability and controllability of ADN operations

The adaptation of IoT technologies offers unique advantages in remote control and management, especially when locational sensing information is integrated into a geographical information system [19, 20]. As physical objects are inseparable from their digital counterpart, the development of IoT technologies eases the seamless integration of heterogeneous data sources for identifying a higher degree of observability and controllability. Accordingly, IoT ensures the multilateral interoperability of devices and applications with differentiated data formats and communication protocols. Therefore, power system operators would be able to exploit data stream potentials representing a volatile operating environment in IoT-based ADN operations and use data analytics to extract

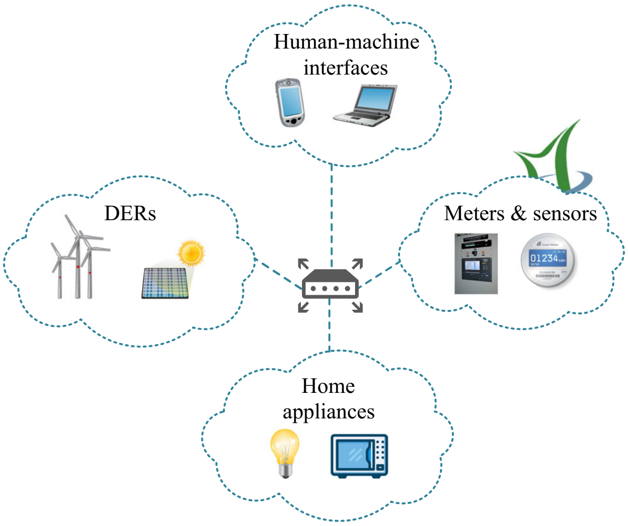

Fig. 2 Ubiquitous connection of smart things in ADN operations

actionable insights holistically for serving customers who mandate better electricity services. In such cases, ADN is provided with immense IoT-enabled opportunities for grid modernization (e.g., deepening renewable energy penetration, increasing customer convenience).

Considering the number of DERs that are often controlled remotely in ADN, it is impractical to control and manage them based on site visits. The significant costs due to on-site control and management will unnecessarily intensify the financial burden of installing DERs, thereby making DERs a less attractive option for exploiting renewable energy. IoT technologies provide a promising solution to perform remote real-time control, fault diagnosis, and predictive maintenance on DERs. For example, IoT devices embedded in DERs enable automated notifications when DERs are to be maintained or replaced, lessening the possibility of dispatching a crew to perform on-site inspection.

In comparison with traditional control options over utility assets (e.g., voltage regulators, capacitors) located at remote sites in which power system operators use a predefined configuration, IoT-driven solutions offer more efficient and flexible ADN operations. Advanced control entities (e.g., static var compensators, on-load tap-changing transformers, switchable lines) dispersed in ADN may initiate self-actuated control commands for a rapid network reconfiguration, following the instructive signals issued by power system operators [21]. For example, power system operators may reconfigure the ADN topology (normally designed with a meshed topology including redundant lines) at runtime by remotely manipulating the status of switchable lines in order to mitigate voltage rises and distribution line congestions caused by the renewable energy integration [22].

The widespread implementation of IoT technologies catalyzes the holistic situational awareness and the real-time decision making of ADN operations. Especially, IoT empowers power system operators to gain an unprecedented real-time visibility and understanding of multi-directional power flows and the functioning of underlying infrastructure so that power distribution system can be operated proactively as the primary promise of ADN. For example, a higher level of visibility into the management of power distribution system lays the foundation for understanding locational and temporal performance of DERs and tapping into their potentials more effectively.

Power system operators rely on IoT technologies for cognitive intelligence that adapt variable power supplies to demands and evolve electricity services (e.g., accelerated detection and restoration of power outages, faster response to customer inquiries, improved voltage and frequency regulation) to respond to a dynamic and uncertain operating environment. When the ADN operation is experiencing operational anomalies, power system operators can respond promptly and intelligently to tweak operating conditions and mitigate anomalies through a combination of automated control actions performed by IoT devices.

2.1.3 *IoT technologies for facilitating demand-side participation in ADN operations*

IoT technologies launch a wide variety of opportunities for customers to facilitate the demand-side participation in power distribution system operations. As IoT technologies become more affordable, customers can utilize them to enhance monitoring and control capabilities for local generation and consumption portfolios. Notably, smart home applications can substantially improve customer capabilities and willingness for optimizing their power consumptions, in response to dynamic electricity rates, with user-friendly control devices (e.g., phone, tablet, computer).

An example applies to the increasingly popular demand-side management. Given the ubiquitous connection of smart things (potentially through high-speed telecommunications and powerful cloud services), customers can conveniently and flexibly adjust appliance settings in wireless networks of their respective homes (e.g., changing lighting sequence and brightness and status of electric vehicle charging) for saving electricity bills.

Power system operators tend to collaborate with technology vendors to develop innovative platforms and applications for facilitating the demand-side participation in ADN. With a good knowledge of consumption behavior, power system operators could consider differentiated services (e.g., time-of-use rates, real-time pricing) for maximizing social welfare. The continuous flow of two-way information between customer sites and the control center ensures the transparency of such services offered to electricity customers.

Advanced metering infrastructure (AMI) [23] is an excellent example of how IoT technologies could lead to a win–win situation between system operators and customers. AMI employs smart meters to measure, transmit, and store high-fidelity demand-side information (e.g., active power consumption, voltage magnitude). Smart meters are by nature sophisticated IoT devices that support automated demand response for customers while facilitating voltage and outage management for power system operators. Smart meters are remotely accessible by power system operators which allow operators to get a more accurate information on energy usage and load patterns across ADN and locate outages at customer sites without the necessity of reporting by customers. Meanwhile, smart meters offer power system operators an ideal tool to track and guide customer participation in demand response.

More specifically, when power system operators implement dynamic pricing initiatives based on AMI, customers are motivated to reduce or shift their power demand based on the pricing information provided by smart meters without significantly impacting customer comfort or convenience [24, 25].

In the U.S., electric utilities have already converted the majority of 145 million electricity meters to smart meters [8]. The intelligent IoT implementation will lead to more comprehensive electricity service offerings in the context of ADN. Accordingly, customers will play a more active role in supporting power system operators' quest for addressing operational challenges introduced by the emergence of DERs.

2.2 Networked microgrids for facilitating energy management in ADN

2.2.1 Microgrids for refining local electricity services

As DERs proliferate in ADN, distributed power systems emerge as promising alternatives to traditionally centralized utility models so as to address inefficiencies and vulnerabilities embedded in long-distance power delivery from bulk generation plants to remote customer sites. Microgrids are commonly viewed as a powerful implementation of distributed power systems that are efficient, sustainable, reliable, and resilient. Microgrids can be deployed at commercial, industrial, and residential sites, and owned by utilities, communities, or individual customers.

Microgrids are small-scale self-controllable power systems localizing power generation and consumption through the interconnection of local DERs and loads. DERs clustered in a microgrid include conventional controllable generators (e.g., cogeneration systems, diesel generators), renewable-based non-controllable generators (e.g., using photovoltaic, wind, biofuel, small hydro, geothermal, wave, tidal energy), energy storage devices (e.g., batteries, pumped-hydro, electric vehicles with vehicle-to-grid capabilities).

Microgrids promise to dramatically improve the survivability and efficiency of local electricity services by taking advantage of on-site controllable resources [26, 27]. Each microgrid operates strategically for meeting local power demands and providing energy and auxiliary services to the rest of ADN. For example, microgrids can contribute to voltage security of ADN by locally generating or absorbing reactive power. Microgrids can help ADN mitigate the impacts of major disruptions resulting from extreme events (e.g., natural disasters [28, 29], cyber-physical attacks [30, 31]). When severe disruptions occur in ADN, microgrids are able to function in the island mode as self-contained entities. By taking full advantage of on-site resources, islanded microgrids manage to sustain local and critical electricity services at a satisfactory level and provide partial power to expedite the restoration of electricity services in ADN [32].

2.2.2 Networked microgrids for establishing foundation of ADN

Microgrids geographically located in a region can be networked to further improve the efficiency, sustainability, security, reliability, and resilience of electricity services in ADN [33]. First, networked microgrids act as a credible means of accommodating DERs scattered at diverse locations and reducing the total installed generation capacity by sharing available resources in individual microgrids. Second, networked microgrids operate in close coordination for enhancing the system-wide efficiency and security of electricity services. Third, networked microgrids feature an increased level of reliability, since each microgrid can provide backup power generation to other networked microgrids without putting critical loads in those microgrids on outage [34]. Last, networked microgrids are more likely to withstand disruptions due to extreme events, since the probability that multiple microgrids fail simultaneously is low.

Networked microgrids offer a highly scalable and flexible solution to fulfill the critical mission of ADN, namely, technology-driven, environment- and customer-friendly electricity service provisions. With the growing deployment and interconnection of microgrids, ADN will be logically identical to a network of interoperable and intelligent microgrids that are capable of handling two-way flows of electricity and information [35]. In Fig. 3, the modified 33-bus power distribution system [36] is sectionalized into four networked microgrids. These four microgrids can operate individually or in concert with each other. For example, each microgrid can supply its power demand not only by dispatching local resources but also by importing power from peer microgrids.

Figure 4 presents a detailed view of Microgrid #1 which is networked with neighboring microgrids in ADN. In this case, a nanogrid is a technologically simpler microgrid in a

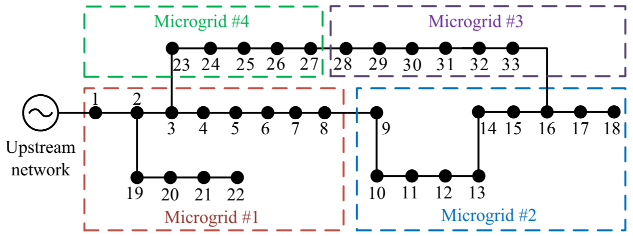

Fig. 3 Networked microgrids in power distribution network

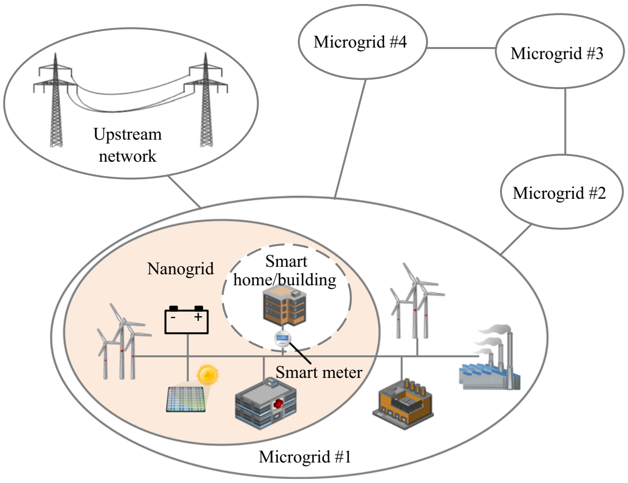

Fig. 4 Components in individual microgrids

much smaller geographic area with a more flexible implementation and operation strategy than a microgrid [37]. Smart home/buildings in Fig. 4 work in synergy with nanogrid/microgrid operations for managing energy usage (e.g., heating, ventilation, air conditioning, lighting) more efficiently [38]. The modularity of nanogrids and smart home/buildings makes them ideal for forming an islandable microgrid. In emergency cases, individual microgrids can be operated as islanded entities for maintaining the microgrid security. In such conditions, each microgrid will manage its resources, nanogrids and smart buildings for supplying energy to critical elements of local ADN.

2.3 Cybersecurity challenges of cloud-based centralized energy management

2.3.1 ADN energy management based on cloud services

The proliferation of DERs poses a host of techno economic challenges (e.g., higher cost and flow congestion) on the ADN operation. As networked micrograids collaborate for enhancing the operation efficiency and security of ADN, the energy management of ADN is entrenched into the management of networked microgrids. We consider that each ADN is supervised by a distribution system operator (DSO) which ties networked microgrids with bulk power transmission systems. Each microgrid is deployed with a microgrid master controller (MGMC) as a central command for communication with and control of on-site resources in various operating conditions.

As shown in Fig. 5, DSO interacts with associated MGMCs in ADN using bi-directional communication flows for managing networked microgrids, while participating in wholesale power market operations managed by an independent system operator (ISO). MGMCs report to DSO an aggregated set of monitoring and sensing data collected in their respective territories of ADN. Once ISO clears the market and makes coordination signals available to DSOs, individual DSOs make optimal decisions on ADN operations and issue supervisory control commands to MGMCs which manage local loads and on-site resources for portraying a holistic view of the ADN's operating state.

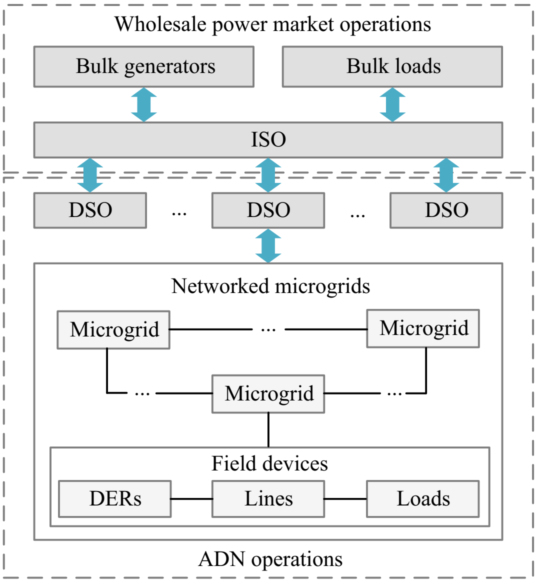

Fig. 5 Role of DSO in power system management

The implementation of IoT technologies in ADN could result in enormous data which are translated into actionable intelligence for realizing the ADN operation. The ever-growing volume and variety of data reported by MGMCs, would mandate cloud-based big data analyses [39, 40] for facilitating the DSO's proactive decision making process for energy management. Cloud computing signifies a group of servers linked over the Internet in a low-cost easily-accessible manner which allows large volumes of data to be retrieved and processed for big data analytics.

Cloud services are commonly regarded as promising solutions for data acquisition, processing, and storage which provide data-driven opportunities for the centralized energy management in ADN. Existing cloud platforms designed for IoT-based services include Amazon Web Services [41], GE Predix [42], Google CloudPlatform [43], Azure IoT Suite [44], and Salesforce IoT Cloud [45]. Figure 6 shows the cloud-based centralized energy management framework in ADN which is in accordance with the 33-bus distribution system depicted in Fig. 3. Here, DSO relies on cloud computing [46] to perform centralized decision making as MGMCs also communicate with the cloud via the Internet.

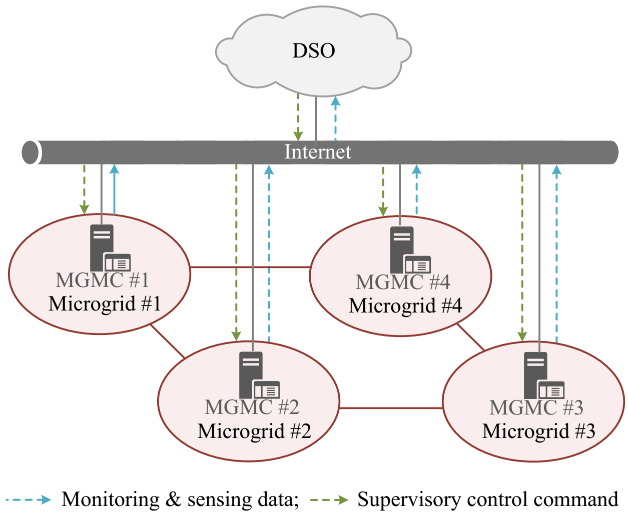

Fig. 6 Cloud-based centralized energy management

However, existing cloud-based centralized energy management schemes are often criticized for large communication overheads (i.e., severe data transmission delays due to limited bandwidth), single point of failure (i.e., breakdown of cloud servers leading to the collapse of the entire decision-making process), and poor physical scalability (i.e., substantial marginal costs for deploying additional communication links and upgrading cloud servers). The centralized cloud database is particularly vulnerable to sophisticated cyberattacks which can compromise and easily manipulate the stored information and jeopardize the ADN security. In addition, extensive communications among MGMCs and DSO are subject to a wide variety of cyberattacks including man-in-the-middle attacks (e.g., spoofing, eavesdropping) and denial-of-service attacks.

2.3.2 Common cybersecurity vulnerabilities of centralized energy management schemes

The privacy leakage is a common cybersecurity concern in cloud computing applied to the ADN energy management. The energy management decision making represents a complex optimization problem involving a variety of independent decision makers (MGMCs) that have separate objectives and control capabilities in the ADN operation. The centralized decision-making scheme of DSO requires MGMCs to disclose private monitoring and sensing results and grant decision-making capabilities to DSO for attaining a global observability and full controllability over corresponding components involved in the ADN operation. However, MGMCs with mutually-exclusive and independent regulation domains are less willing to expose their sensitive information (e.g., types, features, and states of their on-site resources) due to privacy and security considerations, especially when DSO has no direct control over generation assets in networked microgrids. Accordingly, DSO's centralized schemes could fail to find a globally optimal energy management solution, when DSO is blind to detailed configurations and operations within networked microgrids.

3 Cybersecurity enhancement in ADN

The inherent limitations of cloud-based centralized energy management schemes would block their widespread deployment in ADN. Alternatively, networked microgrids should rely on decentralized optimization schemes to get the global equilibrium of collaborative energy management without a central coordinator (DSO) when decision-making interactions among MGMCs can be directly executed in a peer-to-peer manner. Such a decentralization requires IoT-centric computing resources and cognitive intelligence to expand the edges of the cloud-based communication and control infrastructure so that collaborative data collection, processing, and storage in networked microgrids can be performed in a more localized manner.

3.1 Decentralized energy management enabled by edge computing

Edge computing [47] (also called fog computing [48]), acting as an extended edge of cloud computing, is a promising solution for realizing the decentralized energy management in ADN. Similar to cloud computing, edge computing utilizes semantic intelligence (e.g., natural language processing, machine learning) and computational intelligence (e.g., advanced mathematics). But different from cloud computing, edge computing enables more efficient data analyses by invoking local computing resources. As a new computing paradigm that focuses on enhancing the efficiency and cybersecurity of big data management, edge computing will undoubtedly give birth to a new breed of applications and services in accordance with the development of ADN.

Since most IoT devices enclosed in individual microgrids have inadequate commutating power, storage capacity, or communication bandwidth, MGMCs, which are normally powerful servers, are ideal candidates for taking the responsibility of performing edge computing in the context of ADN. To collaborate on the ADN-wide energy management, each MGMC would recursively optimize its microgrid-wide energy management based on technical and operational characteristics of on-site resources and share non-critical information with peer MGMCs for reaching a consensus. Accordingly, the decision-making intelligence is distributed from the cloud-based DSO to

MGMCs that would be dependent on the edge computing platform.

With ubiquitous high-speed communications with local IoT devices, each MGMC possesses secure, reliable, and accurate access to data sources dispersed across the microgrid. After turning the vast data into actionable intelligence, each MGMC makes data-driven decisions in a rapid and proactive manner for contributing to the economics and stability of the ADN operations. In particular, MGMCs with edge computing capabilities provide quick response to hazardous events (e.g., failure or malfunction of critical equipment) and criteria violations (e.g., frequency or voltage deviations) in the ADN operations. For example, when an unexpected ground fault occurs on a tie line interconnecting two microgrids, the pertinent MGMCs will respond cooperatively to isolate the fault by rerouting affected power flows in respective microgrids.

When decision-making is relegated by DSO to a distributed set of MGMCs equipped with numerous IoT devices, anticipated investments on data transmission, processing, and storage for the ADN energy management can be reduced considerably. By utilizing data produced by local IoT devices with maximized resolution and minimized latency, MGMCs host a rich set of sophisticated customized services (i.e., monitoring, analysis, and control) without having to send the traffic through a congested Internet to the remote cloud. The localized data processing is especially applicable to bandwidth-intensive applications with strict timeliness requirement (e.g., data analysis for phasor measurement units). Accordingly, microgrid operation data are stored in local MGMCs instead of cloud servers, which is essential for preserving the information privacy of networked microgrids. In such cases, critical and sensitive information for microgrid operation (e.g., production costs of DERs, customer metering information) would not be centrally stored by cloud services. Instead, the localized storage is applied which is a more economic strategy with reduced risk of privacy leakage.

3.2 Software-defined networking for securing intra-microgrid data flows

3.2.1 Need for software-defined networking technologies in hardening microgrid communication systems

There could be a variety of heterogeneous IoT devices (e.g., smart meters, smart inverters) clustered in a microgrid which represent extensive entry points and communication links that are unintentionally exposed to potential attackers. Without an inherent cybersecurity design, intra-microgrid communications are vulnerable to a multitude of cyber incidents. For example, attackers are likely to compromise smart meters they can easy access for discovering private power consumption profiles (e.g., by installing malware) [49]. Cyber incidents (e.g., malware infection, denial-of-service) originated in a compromised IoT device can quickly propagate and overwhelm the entire microgrid communication and control system due primarily to their ubiquitous connectivity. Consequently, traditional solutions designed for securing Internet services are deemed inadequate for protecting microgrid communications from potential cyber incidents. The diverse properties of hardware components and software applications further complicate the design and implementation of microgrid-specific cybersecurity enhancement solutions.

The emerging software-defined networking (SDN) technologies are effective in achieving cyber-secure communications inside microgrids. Conceptually, SDN is a novel communication paradigm that makes the control of a communication network globally visible and directly programmable. In particular, SDN breaks the conventional vertical integration of data and control planes by transferring the network control logic from switches to a logically centralized controller (i.e., SDN controller) [50]. The SDN controller guides the underlying switches to handle data flows via the OpenFlow communication protocol [51].

The global visibility and runtime programmability enabled by SDN technologies introduce unprecedented capabilities to guard a communication network adequately against cyber incidents. More specifically, the global visibility boosts the efficiency and effectiveness of network-wide traffic management, while the runtime programmability enables the SDN controller to adjust traffic management schedules on demand [52]. Besides, SDN technologies realize the per-flow micromanagement that is especially useful for checking the data integrity while ensuring the timeliness of data transmission. SDN technologies also make the implementation of security policies (i.e., access control, application whitelist) more convenient across the communication network.

3.2.2 Implementation of SDN technologies for realizing defense-in-depth cybersecurity goal

When SDN technologies are adopted to secure intra-microgrid communications, they promise to overcome the limitations of legacy communication infrastructure. On the one hand, SDN technologies facilitate the interactions among various IoT devices inherent with the plug-and-play capability and sustain their communication efficiency to meet specific operational requirements of individual microgrids. On the other hand, SDN technologies provide a wider range of opportunities for developing customized solutions to make intra-microgrid communications less susceptible to cyber incidents. In particular, SDN technologies have unique advantages in refining and evolving information and communication technologies for better supporting microgrid-wide monitoring and control applications which can tackle technical challenges (i.e., seamless integration of DERs) posed by the transition toward ADN.

The SDN controller can be integrated with MGMC for securing intra-microgrid communications in varying operating conditions [53]. In other words, MGMC can be configured to meet microgrid-wide electricity and communication service requirements in a well-coordinated manner. Figure 7 depicts the SDN-based communication and control architecture for individual microgrids, where the SDN controller acts as the interface between networking devices and microgrid applications. By taking full advantage of SDN technologies, an adaptive and holistic solution for cybersecurity enhancement can be developed that can fully address urgent cybersecurity concerns associated with intra-microgrid communications.

As stated in [13], SDN technologies can be configured to devise three lines of defense for minimizing the potential risks of cyberattacks in individual microgrid operations. These three lines take effect in close coordination for striving against cyberattacks. More specifically, the first line of defense including application-segmentation and online verification is aimed at restricting and detecting cyber intrusions which can deter attackers from executing cyberattacks on intra-microgrid communications; the second line of defense including moving-target defense and defensive deception is designed to make it difficult for attackers to achieve their goals in case attackers can successfully infiltrate the microgrid communication network; the third line of defense including self-healing communication networking plays a role in restoring cybersecurity when intra-microgrid communications are inevitably affected by cyberattacks. The communications would be secured such that attackers could have a minute chance for penetrating and compromising the communication network while the MGMC would have a better opportunity for mitigating the implications of cyberattacks effectively and promptly.

The microgrid-wide communication network will function properly as long as the SDN controller is protected from facing malfunction. In order to avoid the potential single-point failure of the SDN controller, additional SDN controllers can be deployed in addition to the one residing in MGMC. These multiple SDN controllers can work either in sequence (i.e., backup) or in parallel (i.e., in charge of data flow associated with a specific microgrid application) introduced by SDN technologies for enhancing the cybersecurity of intra-microgrid communications.

3.3 Smart contracts-aided blockchain for inter-microgrid data exchanges

3.3.1 *Blockchain as distributed secure database*

Blockchain, regarded as a powerful weapon to settle privacy and reliability concerns in the era of IoT [54, 55], can be employed to automate and record the communications between MGMCs in a cyber-secure manner. In principle, blockchain is a type of secure chronological database technology that maintains a continuously growing list of data records (i.e., blocks) secured by cryptographic signatures [56]. The database in the form of a blockchain is guaranteed to be verifiable, auditable, and immutable. In fact, blockchain technologies have already proven their merits in trustless peer-to-peer financial services that rely on Bitcoin [57] or other cryptocurrencies created with similar mechanisms.

Figure 8 shows a blockchain structure by linking a series of blocks. Each block records data in the form of a Merkle tree [58], when hash algorithms are used to encrypt

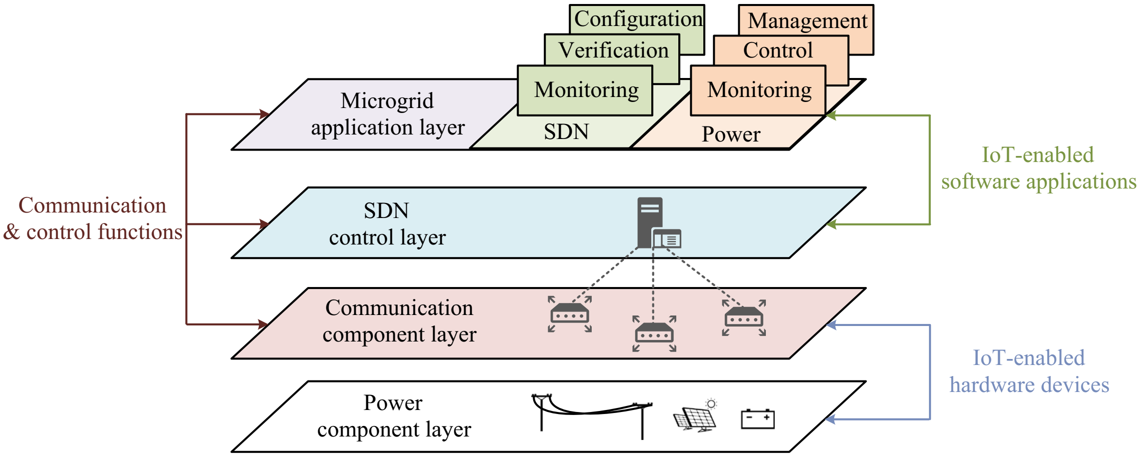
Configuration
Verification
Monitoring
Management
Control
Monitoring
Microgrid application layer
SDN
Power
IoT-enabled software applications
Communication & control functions
SDN control layer
Communication component layer
IoT-enabled hardware devices
Power component layer

Fig. 7 SDN-based microgrid communication and control architecture

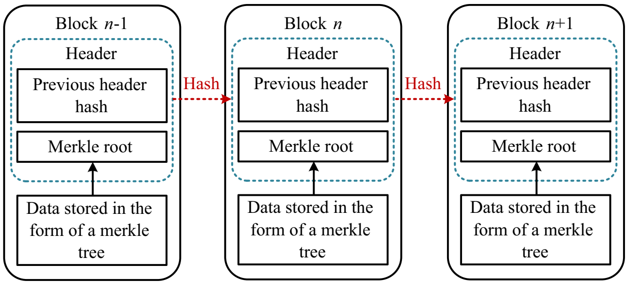

Fig. 8 Blockchain linked by data records

the recorded contents by converting the variable data size to a fixed length without proving any clue associated with the contents [59]. To form the Merkle tree, original contents are stored at the bottom nodes (i.e., leaf nodes) and hashes of children nodes are iteratively combined to form hashes of their parent node until the top node (i.e., root node) is obtained. Since the root node aggregates the encrypted information of the nodes contained in the Merkle tree, the header of each block only needs to store the root node for keeping track of the recorded content. Besides, each block is uniquely identified by the hash generated over the complete content or simply the header of the previous block. Therefore, the blockchain is formed by a chain of blocks linked recursively from the genesis block (i.e., initial block without referring to its previous block) to the current block.

Blockchain is a distributed database by nature. The blockchain providing a robust and reliable record of pertinent data exchanges regarding the ADN operation is automatically shared among a network of participants (i.e., MGMCs) such that the contained data records are synchronized globally. Each MGMC holding an up-to-date copy of the blockchain is permitted to update and validate data records without involving a trusted intermediary (i.e., DSO).

3.3.2 Inherent blockchain properties against cyberattacks

When MGMCs interact, their communications (e.g., power exchange requests) representing changes in the blockchain network state will be broadcasted to other MGMCs. Each MGMC continuously listens to changes in the network and verifies the changes using pre-specified mechanisms embedded in the blockchain. The validity is automatically determined by the consensus of all MGMCs. The change is considered valid only if the majority of MGMCs agree on verification results. During a pre-specified time interval, the inter-microgrid communication contents are ordered and bundled into a timestamped encrypted block which is then added to the end of the current blockchain by a designated party (e.g., MGMC).

Once a block is appended into the blockchain, it is computationally impractical to modify its content due to interlinking hashes of neighboring blocks. In other words, a change in the content of an existing block would force this block and all subsequent blocks to regenerate their cryptographic identifications (e.g., hashes in their headers). If attackers attempt to change, falsify, or delete the content of a block by compromising an MGMC, their suspicious behavior can be easily identified by other MGMCs with a commonly-acknowledged copy of the database. In other words, attackers can manipulate blockchain data records without being detected only when more than half of MGMCs can be compromised to change their consensus on the authenticity of the tampered blockchain. Accordingly, the content stored on blockchain is credible if the majority (rather than all) of MGMCs are trustworthy. Since data records are all replicated and shared over the blockchain network, the blockchain with adequate redundancy is resilient to failures and cyberattacks associated with MGMCs. Theoretically, the blockchain can complete its self-healing with the help of a single MGMC that can maintain an authentic copy of the database.

The blockchain is further protected by asymmetric cryptography. Each MGMC keeps a pair of private/public encryption keys for interaction with the blockchain. The public key makes each MGMC addressable when the private key is used to add a signature (i.e., ensuring authenticity) to the record initiated by each MGMC. The public key can be shared among MGMCs, but the private key is only held by the respective MGMC. Due to the asymmetry, the private key is hardly identified based on the prior knowledge of public key. Additionally, this encryption key pair facilitates the flexible implementation of access management policies. Each MGMC can read and validate the communication records pertinent to other MGMCs when their public keys are available but cannot extend the blockchain on behalf of them without their private keys. If the content recorded by an MGMC contains sensitive information, other MGMCs are granted access only with the knowledge of the pertinent public key to limited information which is solely for verification purposes. If another MGMC wishes to view the full content, it must obtain permission from the majority of MGMCs which will acknowledge with their private keys.

3.3.3 Blockchain functionality enhanced by smart contracts

Since the blockchain keeps a publicly verifiable and auditable proof of inter-microgrid communications, MGMCs are enforced to interact faithfully even if there was a previous mistrust. The emergence of smart contracts further makes it possible for MGMCs to realize decentralized consensus and optimization with a high degree of autonomy. Fundamentally, smart contracts are self-executable scripts allowing for distributed automation in a pre-specified manner [60]. Smart contracts are executed on the basis of clearly-defined specifications (e.g., events or times to take effect) determined individually or collectively by MGMCs. Similar to ordinary data records, smart contracts reside on blockchain with a unique address, and their logic can be transparently inspected by all MGMCs. Moreover, all MGMCs would have access to a cryptographically verifiable trace pertinent to the execution of smart contracts. Accordingly, smart contracts can be executed independently and flexibility by each MGMC and their execution behavior is guaranteed to be completely auditable and predictable.

Smart contracts are considered the silver bullet needed by the blockchain for automating microgrid interactions. The public blockchain platform, Ethereum [61], provides a built-in Turing-complete language (which is proved to solve any problem exactly if provided with sufficient time and storage space) for programming automated applications based on smart contracts. In practice, smart contract-aided blockchain technologies have shown disruptive potentials for securing decentralized energy management in ADN [62, 63]. A real-life peer-to-peer market for renewable energy trading was experimented in New York in April 2016, where the excess energy produced by solar panels was recorded securely on blockchain and traded with neighboring residents automatically via smart contracts. Accordingly, the integration of smart contracts with blockchain technologies presents a promising ADN strategy for optimizing and automating decentralized energy management (i.e., effected by MGMCs), while preserving the integrity and trustworthiness of data exchanges among MGMCs.

3.4 Cyber-secure framework for decentralized energy management

Both operation technologies (i.e., decentralized optimization performed by networked microgrids) and information technologies (i.e., edge computing, SDN, blockchain) offer effective solutions for improving the energy management performance of IoT-enabled ADN. The coordination of these technologies leads to a hierarchical energy management framework that decentralizes energy management decision making processes in a cyber-secure manner.

Figure 9 illustrates the framework based on the 33-bus distribution system depicted in Fig. 3, where operational and information technologies have converged to power cybersecurity enhancement solutions. Overall, this hierarchical framework strikes a balance between the efficiency of ADN operations and the privacy and independent decision-making of individual microgrids. MGMCs play a central role in the decentralized energy management of ADN. They are required to have strong data processing capabilities to perform edge computing, adequate storage space for implementing blockchain technologies, and flexible programmability to act as SDN controllers.

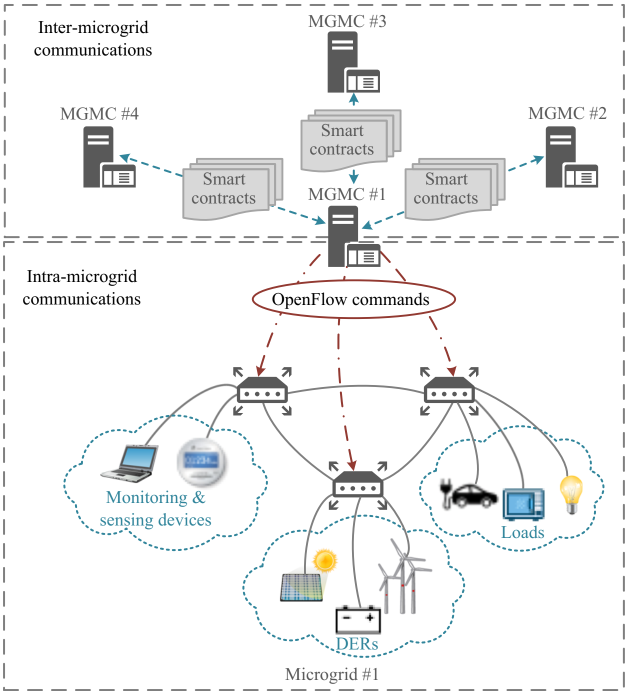

Fig. 9 Hierarchical cybersecurity enhancement framework

MGMCs form a mesh network for data exchanges. In contrast to the top-down regulation model which is dependent on a central coordinator (i.e., DSO), MGMCs interact directly in a peer-to-peer manner in order to address common cybersecurity concerns (e.g., privacy leakage, communication latency) in centralized energy management strategies. Without routing data traffic through DSO, each MGMC gather, integrate, analyze, and store data streams originated from local IoT devices. The strong edge computing capability enables each MGMC to perform sophisticated data-driven decision making. Meanwhile, MGMCs collaborate via sharing a set of non-critical information (e.g., available generation capacity, marginal generation cost) for aligning their local energy management decisions with a common goal (e.g., minimal costs for achieving ADN-wide power balance, fastest restoration of electricity services).

Blockchain provides a unique and powerful path for launching trustworthy distributed data storage. Decision-making interactions among MGMCs are recorded in the blockchain automatically and immutably, which is proved to be a more cost-effective way than cloud-based storage service. In fact, the storage cost for blockchain (about $2 per terabyte per month) is significantly lower than that for cloud services like Amazon S3 (25 per terabyte per month) [64]. As the size of the blockchain increases over time, only MGMCs are granted the access to the blockchain. IoT devices are not directly integrated with blockchain technologies due primarily to their constrained processing and storage capabilities. If data exchanges among MGMCs are of heterogeneity or over diverse timescales, a multitude of blockchain can be put into use instead of a single one (as will be detailed in Sect. 4.2).

In each microgrid, geographically-distributed IoT devices continuously communicate with MGMC for reporting monitoring information and receiving supervisory control commands. With adequate cybersecurity protection, MGMC is regarded as the trusted central authority to manage and store IoT data streams in a centralized manner. Furthermore, the adoption of SDN technologies manages to secure extensive communications inside the microgrid holistically and adaptively. In that regard, attackers can hardly intercept and manipulate these intra-microgrid communications for degrading the functionality of IoT devices, while MGMC can easily detect and mitigate the implications of cyberattacks for ensuring the robustness and effectiveness of its energy management decision making. Hence, SDN technologies boost the trustworthiness of MGMCs when they participate in the blockchain network.

The deployment of smart contracts on blockchain is consistent with the development of fully distributed and autonomous energy management for ADN. Smart contracts make it possible to automate sophisticated inter-microgrid decision-making interactions in a dependable way. Note that edge computing capabilities of MGMCs facilitate the encryption and verification of data records as well as the execution of smart contracts. Accordingly, each MGMC is identical to an autonomous agent with inherent intelligence that adapts energy management decisions to dynamic operating conditions. Hence, collaborative MGMCs are assured to accomplish the same energy management goal as that of centralized schemes with DSO.

The DSO's participation would not be required for decision-making processes performed by individual MGMCs. Rather, DSO specifies energy management goals for guiding the collaboration among MGMCs, considering the ADN's physical and financial constraints. In addition, DSO is assigned with tasks of auditing all the contents residing on the blockchain, supervising MGMCs to make smart contracts, and resolving disputes (if any) between MGMCs. If an MGMC's behavior is found to be suspicious by DSO, the MGMC will be temporally excluded from the blockchain network. Only when the majority of other MGMCs reach a consensus, can the MGMC be plugged back to the blockchain network.

4 Application scenario: cyber-secure transactive energy management in ADN

The proliferation of DERs along with widespread applications of IoT technologies allows customers to become prosumers who can switch smoothly and frequently between power production and consumption. Each prosumer makes intelligent decisions on when and how much to purchase, consume, store, or sell energy, thereby opening the door to competitive energy transactions among peer prosumers as they opt to trade energy directly and freely [65]. Accordingly, prosumers' enhanced market role lays the foundation for implementing a fully decentralized energy trading system [66].

4.1 Need for establishing transactive energy systems

Given presumes' diverse behavior and motivations for participating in direct energy transactions, ADN operations are faced with an overwhelm degree of diversity and complexity in sustaining presumes' objectives. A practical solution for easing the volume of energy trading is to aggregate prosumers within local communities by establishing transactive microgrids. Transactive microgrids are regarded as fundamental market entities which participate actively in energy trading [67]. Actually, networked microgrids often feature diversified profiles of renewable energy generation and power demand so that ADN operations have ample opportunities for reducing the total cost by coordinating energy exchanges among these networked microgrids [68].

Figure 10 presents a typical example where two neighboring microgrids trade energy for maintaining local power

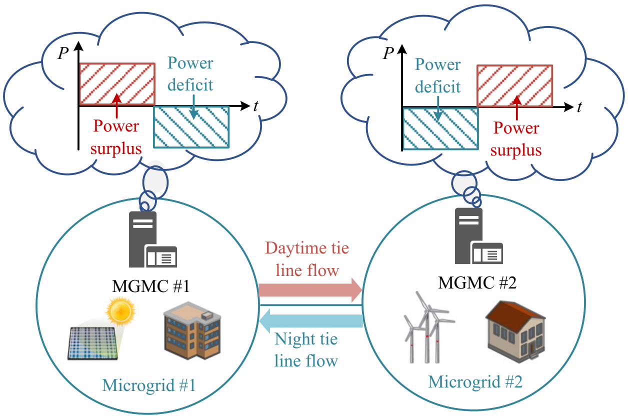

Fig. 10 Energy trading for local power balance

balance at their sites. It is assumed that Microgrids #1 and #2 are equipped with abundant solar and wind energy generation facilities, respectively. Microgrid #1 has excess local generation at daytime but suffers power shortage at night; on the contrary, Microgrid #2 suffers power shortage at daytime (when wind is weak) but has excess local generation at night (when wind is strong). Accordingly, these two microgrids would fail to balance the local power generation and consumption when they solely rely on their on-site resources. Energy trading between these microgrids signifies a win–win solution such that a microgrid could supply excess power strategically to compensate the other microgrid's power shortage. Therefore, each microgrid has a greater degree of flexibility in managing its operations by performing energy trading with the other.

DSO would accordingly set up a trustworthy transactive energy system for networked microgrids to carry out peer-to-peer non-discriminatory energy transactions in ADN [69, 70]. In this system, networked microgrids are granted the privilege to trade energy directly with their peers based on certain regulations (e.g., power balancing, peak demand management, line congestion management). In addition, decision-making is performed by MGMCs in a decentralized manner without the DSO's direct intervention. Hence, transactive energy management applies dynamic market signals to coordinate interactions among networked microgrids in accordance with the ADN's operational and environmental objectives.

Transactive energy management also expedites the proliferation of demand response programs for realizing the real-time load management. When on-site generation resources are inadequate to supply the total load and the market price for importing energy from ADN is high (i.e., higher than the current electricity rate set by utilities), microgrids are more willing to adjust or shift the timing and quantity of energy consumption for better shaping their net load profiles and save expenses on electricity usage.

Market operations for transactive energy trading are ideally regarded trustworthy and treated as transparent without distinctions to any microgrids in ADN. However, careless or malicious participants (e.g., potentially caused by cyberattacks or collusion among certain market participants) should be penalized or mitigated in order to minimize their adverse effects on market operations. Otherwise, false energy trading among networked microgrids could lead to unfair equilibria with reduced social welfare and even destabilize ADN operations when actual transactions fail to achieve a balance between energy production and consumption.

There are also privacy issues hampering the development of transactive energy management. When participating in the transactive energy systems, MGMCs should avoid exposing their trading behavior (e.g., amounts and patterns of energy generation and consumption) too frequently to their peers. Inadvertently, the completed energy transactions are rich information sources for inferring potential trading behavior of these networked microgrids. More importantly, sensitive commercial data (e.g., production cost coefficients of local generation) and critical operation information (e.g., operating states and security margin of local generation) of individual microgrids must be hidden from their peers for preserving their privacy to the greatest extent.

4.2 Blockchain-based transactive energy management

4.2.1 *Interoperable blockchains for facilitating transactive energy management*

A cyber-secure transactive energy management scheme can be easily realized within the hierarchical framework proposed in Sect. 3.4. SDN technologies are beneficial for managing on-site DERs within microgrids in the same trust domain, while the decentralized nature of transactive energy management lends itself to a blockchain implementation aided by smart contracts. In particular, the information exchanged between any two MGMCs is secured by cryptography applied to blockchain and stored identically in MGMCs for creating a set of publicly auditable records in the transactive energy management process.

Each microgrid needs to register with DSO in order to be authorized to participate in the transactive energy system. Then DSO will have a full knowledge of MGMC identities involved in transactive energy management. Accordingly, the blockchain can be configured as permissioned with no requirements for an energy-intensive proof-of-work mining process (e.g., the process of digging out Bitcoins) [71]. By contrast, the corresponding lightweight consensus consumes less energy and computation resources for appending blocks to blockchain.

Physical characteristics and operation requirements of ADN could render peer-to-peer energy trading impractical which ought to be simplified as is the case with that of other commodities. In fact, considering non-negligible power losses in networked microgrids, energy transactions cannot be determined simply by matching power generation offers with consumption bids. The direct applications of blockchain technologies designed for other commodities to transactive energy management may result in ADN violations of network security requirements (e.g., line overloading, voltage collapse). Accordingly, cyber-physical factors (e.g., power losses, network security) affecting the validity of energy transactions should be considered common market rules.

A heterogeneity of data is exchanged between MGMCs for transactive energy management. MGMCs may share a part of their real-time operation information collected periodically (e.g., every minute) by smart meters and phasor measurement units. They may also interact (e.g., every 30 min) for setting up energy transactions or settling existing transactions. In other words, data from heterogeneous sources normally have distinct resolution and play different roles in transactive energy management. Hence, multiple blockchains, each belonging to a specific data type for facilitating transactive energy management, are deployed for preventing any tampering and securing data exchanges.

Here we present a set of interoperable blockchains with embedded smart contracts, which are promising for optimizing and automating peer-to-peer energy trading among networked microgrids. As shown in Fig. 11, these blockchains execute distinct functionalities requested by the transactive energy system, when they offer interfaces for each other to achieve interoperability (represented by directed dashed lines). When working in tandem, these blockchains managed to get transactive energy management executed in a faithful and automatic manner. More specifically, the access management blockchain is maintained for enforcing access control rules in the transactive energy system; the energy trading, state estimation, and market settlement blockchains are responsible for storing all transactional, operational, and financial information involved in data exchanges between MGMCs, respectively.

4.2.2 Detailed process of blockchain-based transactive energy management

The use of blockchains in the transactive energy management process is detailed as follows. In each round, DSO appends the access management blockchain for broadcasting the registered information of networked microgrids as well as their properties in a peer-to-peer energy trading. The participants' properties include topological relations (i.e., tie connections), as the ADN network topology tends be reconfigured frequently for economic and security considerations. Each participant is also associated with a credit score that directly reflects the trustworthiness of its energy trading behavior. The participants' initial credit scores are set equally by DSO. Besides, DSO assigns each participant with a temporary pseudonym for concealing participants' actual identities and preventing other participants from inferring a participant's energy trading behavior. The decryption of pseudonym to the actual identity can only be realized by using a participant's private key. Accordingly, all participants remain pseudonymous to their peers and are only identified by DSO. The pseudonym of each participant is renewed after an agreed-upon time period when its credit score is reset to the initial value.

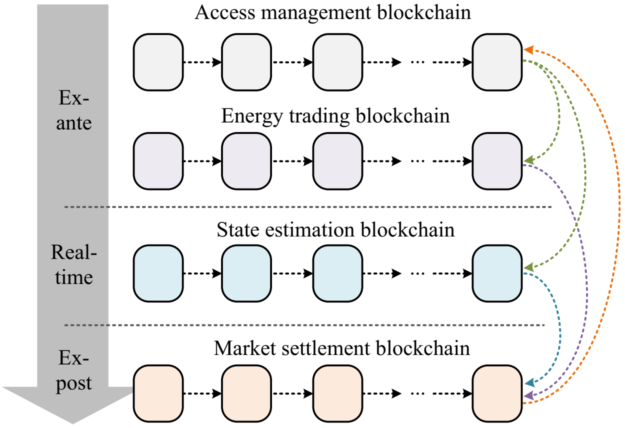
Access management blockchain
Ex-ante
Energy trading blockchain
Real-time
State estimation blockchain
Ex-post
Market settlement blockchain
···

Fig. 11 Interoperable blockchains for transactive energy management

The peer-to-peer energy trading is formulated as a comprehensive optimization problem, which is solved in a decentralized manner by smart contracts residing on the energy trading blockchain. To work toward the transactional consensus, each participant provides bidding information for its power generation or consumption. Note that a penalty term is added to the bids submitted by participants with a reduced credit score in order to lower these participants' priorities in the transactive energy system. More specifically, such participants' bidding prices for power consumption (or generation) would be automatically increased (or decreased) as enforced by smart contracts.

The decentralized consensus on optimal energy transactions could be obtained by applying the alternating direction method of multipliers [72, 73]. In that regard, each participant solves a local part of the original optimization problem and their optimization results are passed on to smart contracts that execute the aggregation step (e.g., return the average value of any coupling variable collected from neighboring participants) for evolving local optimal decisions toward the global equilibrium. After agreeing upon the scheduled energy trading, participants receive energy trading prices specific to their locations (e.g., distribution locational marginal prices). The optimal energy trading schedules and the corresponding locational prices are bundled to data blocks that are subsequently added to the energy trading blockchain by the participant with the highest credit score.

The state estimation blockchain keeps track of the ADN's operating states when energy trading continues in networked microgrids. All participants collaborate on the decentralized state estimation with the help of smart contracts. Each participant relies on local measurements and limited boundary information provided by its neighbors to calculate the local state estimation. As the differences in boundary information diminish in a finite number of iterations [74, 75], pertinent local estimates would be integrated seamlessly to represent the ADN's operating states. The full set of the converged ADN's operating states is then stored on the state estimation blockchain by the participant with the highest credit score. When all participants have access to actual energy trading information across ADN, the set of operating states local to a participant can only be decrypted by using the participant's private key.

After state estimation results become available, DSO settles the energy transactions completed by all participants. In an ideal case, all participants trade energy as scheduled, which is difficult to achieve due to a variety of uncertainties in the transactive energy management process. When there is a difference between the actual energy traded by a participant and the scheduled amount, the participant would pay additional fees for compensating the balancing quantity. When the difference is outside a predefined threshold, the participant will be penalized by lowing its credit score. The penalty will be higher as the difference increases.

A participant's payment or revenue is determined by a combination of penalty fee and expected value (i.e., scheduled amount times locational price). The DSO's net positive revenue (possibly due to tie line congestion) will be shared among participants in proportion to their credit scores. DSO will record payments and penalties on blockchain which could be further integrated with smart contracts for issuing automatic payments (via cryptocurrencies).

The interoperability among the four blockchains depicted in Fig. 11 are performed as follows. Energy trading and market settlement blockchains read participants' credit scores from the assess management blockchain in order to determine the miner for blockchain extension. The energy trading blockchain also reads the pseudonym and topological location of each participant from the assess management blockchain in order to formulate and solve the optimal peer-to-peer energy trading problem. The market settlement blockchain reads the scheduled energy trading information (i.e., trading amount, locational price) and the actual energy trading amount from the energy trading and state estimation blockchains, respectively, in order to determine a participant's payment or revenue. After determining the penalty for non-trustworthy participants, the market settlement blockchain notifies the access management blockchain of changes in credit scores.

These procedures are repeated in each round of transactive energy management process as networked microgrids are streamlined to exchange information and energy services autonomously. In particular, a limited amount of non-critical information will be exchanged for decision-making among networked microgrids, which would effectively overcome the privacy-leakage shortcomings of centralized schemes.

4.3 Outlook for a greater degree of cybersecurity

Although the proposed set of blockchains plays a significant role in balancing power generation and consumption as well as identifying abnormal energy transactions, additional cybersecurity measures are needed in order to enhance the cybersecurity of transactive energy management. These measures are listed as follows.

First, a microgrid participating in the transactive energy system would need to deposit a considerable level of currencies (or cryptocurrencies) with DSO. After the agreed-upon period for keeping the set of pseudonyms is over, the deposited currencies (or cryptocurrencies) in proportion to credit scores will be returned to microgrids. When an MGMC is compromised by attackers to execute a fraudulent energy trading that can be easily detected by blockchain technologies, the reduced credit score will lead to a sizeable penalty for the microgrid. Accordingly, the microgrid is enforced to upgrade its devices and applications more adequately for securing the MGMC and preventing it from executing additional malfunctions.

Second, each microgrid needs to enhance both hardware- and software-based cybersecurity for achieving its defense-in-depth goal in the case of cyberattacks. We should point out that the supply chain of IoT devices may be compromised by attackers. Especially, hardware-based Trojan horse [76] which emerges as a serious cybersecurity concern associated with IoT devices deployed across networked microgrids. Since these devices are normally procured from a multitude of vendors, attackers can easily gain access to the manufacturing process for inserting Trojan horse in the hardware device. Accordingly, the physical layer of IoT devices, especially processors and chipset, deserves special hardening against malwares. Only when hardware-based security solutions are implemented in concert with conventional software-based solutions, can the performance of mission-critical IoT applications be credible for transactive energy management.

Third, networked microgrids could also depend on blockchain technologies along with smart contracts for updating device firmware and software applications in a cyber-secure and automatic manner. Considering that there exist a host of IoT devices (e.g., smart meters, smart inverters) similar in each of networked microgrids, a dedicated database can be configured as a blockchain for keeping track of cybersecurity vulnerabilities and the corresponding patches. When a cybersecurity vulnerability is discovered and cured in a microgrid, all the other microgrids will also patch the vulnerability. Each microgrid monitors and validates the integrity and effectiveness of new patches which will ultimately be stored on the blockchain and made available automatically to networked microgrids. If a microgrid fails to patch the vulnerability, it will be marked as a potential target for lowing its credit score by a penalty, and eventually excluded from the transactive energy system if necessary. Hence, discovered vulnerabilities are to be assessed and patched promptly and faithfully.

5 Conclusion

Modern power distribution systems are undergoing a paradigm shift to ADN, which is driven by a collection of dynamic forces including the ever-growing penetration of DERs as well as an extensive quest for offering sustainable and resilient electricity services. As IoT continues to instil intelligence in power distribution system operations, ADN will evolve to become an ideal platform for adopting social and technological innovations that could realize the smart grid mandates. Bearing in mind that ADN is a cyber-physical system, cybersecurity vulnerabilities which are procured by IoT technologies may result in catastrophic physical impacts which could culminate in widespread power outages. Therefore, academic and industrial sectors should cooperate more proactively to identify innovative cybersecurity strategies that can preserve ADN's security while exploiting full benefits of IoT technologies.

This paper offers a vision for utilizing leading operation technologies (e.g., transactive energy, decentralized energy management) and information technologies (e.g., edge computing, soft-defined networking, and blockchain) to optimize and automate the ADN energy management in a scalable, efficient, and cyber-secure manner. On the one hand, networked microgrids shoulder the DSO's burden of managing ADN operations by taking advantage of edge computing. The ADN energy management will accordingly be determined in a decentralized manner without posing any concerns with single-point failures and latency associated with centralized cloud-based schemes. On the other hand, SDN and blockchain technologies are employed to secure intra- and inter-microgrid data flows, respectively. Accordingly, networked microgrids are considered trustworthy entities that participate in decentralized decision making for energy management while microgrid interactions are automated and recorded with cryptographic verifiability.

Under the proposed framework, networked microgrids in ADN interact in a credible and auditable manner for achieving a greater degree of efficiency, security, reliability, resilience, and sustainability in offering electricity services. The convergence of operation and information technologies is also expected to exhibit cyber-secure and decentralized energy management solutions for ADN by embracing IoT technologies.

References

[1] Lasseter RH (2011) Smart distribution: coupled microgrids. Proc IEEE 99(6):1074–1082

[2] Shahidehpour M, Khodayar M (2013) Cutting campus energy costs with hierarchical control: the economical and reliable operation of a microgrid. IEEE Electrif Mag 1(1):40–56

[3] Che L, Shahidehpour M (2014) DC microgrids: economic operation and enhancement of resilience by hierarchical control. IEEE Trans Smart Grid 5(5):2517–2526

[4] Che L, Khodayar M, Shahidehpour M (2014) Only connect: microgrids for distribution system restoration. IEEE Power Energy Mag 12(1):70–81

[5] Evans D (2011) The Internet of Things. https://blogs.cisco.com/diversity/the-internet-of-things-infographic. Accessed 15 January 2017

[6] Balda C, Mantooth A, Blum R et al (2017) Cybersecurity and power electronics: addressing the security vulnerabilities of the Internet of Things. IEEE Power Electron Mag 4(4):37–43

[7] Al-Fuqaha A, Guizani M, Mohammadi M et al (2015) Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Coummun Surv Tutor 17(4):2347–2376

[8] Pestridge C (2016) The emerging enernet: convergence of the smart grid with the Internet of Things. IEEE Ind Appl Mag 23(2):12–16

[9] Weng J, Liu D, Luo N et al (2015) Distributed processing based fault location, isolation, and service restoration method for active distribution network. J Mod Power Syst Clean Energy 3(4):494–503

[10] Martins VF, Borges CLT (2011) Active distribution network integrated planning incorporating distributed generation and load response uncertainties. IEEE Trans Power Syst 26(4):2164–2172

[11] Hu Z, Li F (2012) Cost-benefit analyses of active distribution network management, part I: annual benefit analysis. IEEE Trans Smart Grid 3(3):1067–1074

[12] Hu Z, Li F (2012) Cost-benefit analyses of active distribution network management, part II: investment reduction analysis. IEEE Trans Smart Grid 3(3):1075–1081

[13] Li Z, Shahidehpour M, Aminifar F (2017) Cybersecurity in distributed power systems. Proc IEEE 105(7):1367–1388

[14] Jin D, Hannon C, Li Z et al (2016) Smart street lighting system: a platform for innovative smart city applications and a new frontier for cyber-security. Electr J 29(10):28–35

[15] Emilio G, Pilo F (2015) Smart inverter operation in distribution networks with high penetration of photovoltaic systems. J Mod Power Syst Clean Energy 3(4):504–511

[16] Want R (2006) An introduction to RFID technology. IEEE Pervasive Comput 5(1):25–33

[17] Want R (2011) Near field communication. IEEE Pervasive Comput 10(3):4–7

[18] Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. Comput Netw 52(12):2292–2330

[19] Li F, Qiao W, Sun H et al (2010) Smart transmission grid: vision and framework. IEEE Trans Smart Grid 1(2):168–177

[20] Wu H, Shahidehpour M (2018) Applications of wireless sensor networks for area coverage in microgrids. IEEE Trans Smart Grid 9(3):1590–1598

[21] Feng C, Li Z, Shahidehpour M et al (2017) Decentralized short-term voltage control in active power distribution systems. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2663432

[22] Koutsoukis NC, DiO Siagkas, Georgilakis PS et al (2017) Online reconfiguration of active distribution networks for maximum integration of distributed generation. IEEE Trans Autom Sci Eng 14(2):437–448

[23] Mohassel RR, Fung A, Mohammadi F et al (2014) A survey on advanced metering infrastructure. Int J Electr Power Energy Syst 63(63):473–484

[24] Khodaei A, Shahidehpour M, Bahramirad S (2011) SCUC with hourly demand response considering intertemporal load characteristics. IEEE Trans Smart Grid 2(3):564–571

[25] Wu H, Shahidehpour M, Al-Abdulwahab A (2013) Hourly demand response in day-ahead scheduling for managing the variability of renewable energy. IET Gener Transm Distrib 7(3):226–234

[26] Li Y, Farzam N (2014) Overview of control, integration and energy management of microgrids. J Mod Power Syst Clean Energy 2(3):212–222

[27] Shahidehpour M, Clair JF (2012) A functional microgrid for enhancing reliability, sustainability, and energy efficiency. Electr J 25(8):21–28

[28] Ma S, Chen B, Wang Z (2018) Resilience enhancement strategy for distribution systems under extreme weather events. IEEE Trans Smart Grid 9(2):1442–1451

[29] Yuan W, Wang J, Qiu F et al (2016) Robust optimization based resilient distribution network planning against natural disasters. IEEE Trans Smart Grid 7(6):2817–2826

[30] Li Z, Shahidehpour M, Alabdulwahab A et al (2016) Bilevel model for analyzing coordinated cyber-physical attacks on power systems. IEEE Trans Smart Grid 7(5):2260–2272

[31] Li Z, Shahidehpour M, Abdulwhab A et al (2018) Analyzing locally coordinated cyber-physical attacks for undetectable line outages. IEEE Trans Smart Grid 9(1):35–47

[32] Liu Y, Fan R, Vladimir T (2016) Power system restoration: a literature review from 2006 to 2016. J Mod Power Syst Clean Energy 4(3):332–341

[33] Shahidehpour M, Li Z, Bahramirad S et al (2017) Networked microgrids: exploring the possibilities of the IIT-Bronzeville grid. IEEE Power Energy Mag 15(4):63–71

[34] Farzin H, Fotuhi-Firuzabad M, Moeini M (2016) Enhancing power system resilience through hierarchical outage management in multi-microgrids. IEEE Trans Smart Grid 7(6):2869–2879

[35] Li Z, Shahidehpour M, Aminifar F et al (2017) Networked microgrids for enhancing the power system resilience. Proc IEEE 105(7):1289–1310

[36] Baran ME, Wu FF (1989) Network reconfiguration in distribution systems for loss reduction and load balancing. IEEE Trans Power Deliv 4(2):1401–1407

[37] Shahidehpour M, Li Z, Gong W et al (2017) A hybrid ac/dc nanogrid: the Keating hall installation at the Illinois Institute of Technology. IEEE Electrif Mag 5(2):36–46

[38] Chen X, Wei T, Hu S (2013) Uncertainty-aware household appliance scheduling considering dynamic electricity pricing in smart home. IEEE Trans Smart Grid 4(2):932–941

[39] Simmhan Y, Aman S, Kumbhare A et al (2013) Cloud-based software platform for big data analytics in smart grids. Comput Sci Eng 15(4):38–47

[40] Baek J, Vu QH, Liu JK et al (2015) A secure cloud computing based framework for big data information management of smart grid. IEEE Trans Cloud Comput 3(2):233–244

[41] Amazon EC (2018) Amazon web services. https://aws.amazon.com/ec2/. Accessed 15 January 2018

[42] Morris HD, Ellis S, Feblowitz J et al (2014) A software platform for operational technology innovation. Int Data Corp 1–17. https://www.ge.com/digital/sites/default/files/IDC_OT_Final_whitepaper_249120.pdf

[43] Google Cloud (2018) Google Internet of Things (IoT) solutions. https://cloud.google.com/solutions/iot/. Accessed 15 January 2018

[44] Familiar B (2015) Microservices, IoT and Azure: leveraging DevOps and microservice architecture to deliver SaaS solutions. Apress, New York

[45] Salesforce IoT Cloud (2018) Connects the Internet of Things to the internet of customers. https://www.salesforce.com/products/salesforce-iot/overview/. Accessed 15 January 2018

[46] Armbrust M, Fox A, Griffith R et al (2010) A view of cloud computing. Commun ACM 53(4):50–58

[47] Shi W, Cao J, Zhang Q et al (2016) Edge computing: vision and challenges. IEEE Internet Things J 3(5):637–646

[48] Bonomi F, Milito R, Zhu J et al (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing, Helsinki, Finland, 17 August 2012, 4 pp

[49] Kalogridis G, Sooriyabandara M, Fan Z et al (2014) Toward unified security and privacy protection for smart meter networks. IEEE Syst J 8(2):641–654

[50] Kreutz D, Ramos FMV, Verı PE et al (2015) Software-defined networking: a comprehensive survey. Proc IEEE 103(1):14–76

[51] McKeown N, Anderson T, Balakrishnan H et al (2008) OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput Commun Rev 38(2):69–74

[52] Lin H, Chen C, Wang J et al (2018) Self-healing attack-resilient PMU network for power system operation. IEEE Trans Smart Grid 9(3):1551–1565

[53] Jin D, Li Z, Hannon C et al (2017) Toward a cyber resilient and secure microgrid using software-defined networking. IEEE Trans Smart Grid 8(5):2494–2504

[54] Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303

[55] Dorri A, Kanhere SS, Jurdak R et al (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of IEEE international conference on pervasive computing and communications workshops, Kona, USA, 13–17 March 2017, 6 pp

[56] Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media Inc, USA

[57] Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://doi.org/10.1007/s10838-008-9062-0

[58] Li H, Lu R, Zhou L et al (2014) An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst J 8(2):655–663

[59] Underwood S (2016) Blockchain beyond bitcoin. Commun ACM 59(11):15–17

[60] Hahn A, Singh R, Liu CC et al (2017) Smart contract-based campus demonstration of decentralized transactive energy auctions. In: Proceedings of 2017 IEEE power energy society innovative smart grid technologies conference, Washington, USA, 23–26 April 2017, 5 pp

[61] Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap 151:1–32

[62] Aitzhan NZ, Svetinovic D (2016) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secur Comput. https://doi.org/10.1109/TDSC.2016.2616861

[63] Basden J, Cottrell M (2017) How utilities are using blockchain to modernize the grid. Harv Bus Rev. https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid

[64] Sharma PK, Chen MY, Park JH (2018) A software defined Fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124

[65] Rahimi FA, Ipakchi A (2012) Transactive energy techniques: closing the gap between wholesale and retail markets. Electr J 25(8):29–35

[66] Chen S, Liu C-C (2017) From demand response to transactive energy: state of the art. J Mod Power Syst Clean Energy 5(1):10–19

[67] Khodayar ME, Manshadi SD, Vafamehr A (2016) The short-term operation of microgrids in a transactive energy architecture. Electr J 29(10):41–48

[68] Wang H, Huang J (2017) Incentivizing energy trading for interconnected microgrids. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2016.2614988

[69] Renani YK, Ehsan M, Shahidehpour M (2017) Optimal transactive market operations with distribution system operators. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2017.2718546

[70] Ye H (2018) Surrogate affine approximation based co-optimization of transactive flexibility, uncertainty, and energy. IEEE Trans Power Syst. https://doi.org/10.1109/TPWRS.2018.2790170

[71] Gervais A, Karame GO, Glykantzis V et al (2016) On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, Vienna, Austria, 24–28 October 2016, 14 pp

[72] Liu Y, Li Y, Gooi HB et al (2017) Distributed robust energy management of a multi-microgrid system in the real-time energy market. IEEE Trans Sustain Energy. https://doi.org/10.1109/TSTE.2017.2779827

[73] Gregoratti D, Matamoros J (2015) Distributed energy trading: the multiple-microgrid case. IEEE Trans Ind Electron 62(4):2551–2559

[74] Tai X, Lin Z, Fu M et al (2013) A new distributed state estimation technique for power networks. In: Proceedings of American control conference, Washington, USA, 17–19 June 2014, 6 pp

[75] Minot A, Lu YM, Li N (2016) A distributed Gauss–Newton method for power system state estimation. IEEE Trans Power Syst 31(5):3804–3815

[76] Bhunia S, Hsiao MS, Banga M et al (2014) Hardware Trojan attacks: threat analysis and countermeasures. Proc IEEE 102(8):1229–1247

Zhiyi LI received the B.S. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2011, the M.S. degree from Zhejiang University, Hangzhou, China, in 2014, and the Ph.D. degree from Illinois Institute of Technology, Chicago, USA, in 2017. His current research interests include cyber-physical power systems and power system optimization.

Mohammad SHAHIDEHPOUR received the Honorary Doctorate degree in electrical engineering from the Polytechnic University of Bucharest, Bucharest, Romania. He is the Bodine Chair Professor and the Director of the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, USA, and a Research Professor with King Abdulaziz University, Jeddah, Saudi Arabia. He is a member of the U.S. National Academy of Engineering.

Xuan LIU received the B.S. and M.S. degrees from Sichuan University, China, in 2008 and 2011, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2015, all in electrical engineering. He is currently a Professor in the College of Electrical and Information Engineering at Hunan University, China. His research interests include smart grid security, operation and economics of power systems.