published online on 26 April 2019. DOI: 10.1109/TSMC.2019.2911548

A Collaborative Intrusion Detection Approach using Blockchain for Multi-microgrid Systems

Bowen Hu, Chunjie Zhou, Yu-Chu Tian, Yuanqing Qin, Junping Xing

***Abstract*—Multi-microgrid (MMG) systems have the potential to play an increasingly important role in the transformation of existing power grid to smart grid. However, the open and distributed connectivity of MMGs exposes the systems into various cyber-attacks, which may cause serious failures or physical damages, such as power supply interruption and human casualties. Therefore, ensuring the security of MMGs is of paramount importance. To address this issue, a new collaborative intrusion detection (CID) approach using blockchain is proposed in this paper for MMG systems in smart grid. Due to the consensus mechanism of blockchain, the approach is designed without the need of a trusted authority or central server while improving the accuracy of intrusion detection in a collaborative way. It is equipped with a proposal generation method that combines periodic and trigger patterns to generate the detection target of CID, i.e., a proposal. From the generated proposals together with the correlation model of MMGs, a CID is achieved by using the consensus mechanism. The final detection results of CID are stored on blockchain in sequence. The use of an incentive mechanism motivates a single microgrid to participate in consensus. The effectiveness of the presented approach is demonstrated through a case study on an MMG system.**

***Index Terms*—Collaborative intrusion detection (CID); multi-microgrid (MMG); blockchain; consensus mechanism; incentive mechanism.**

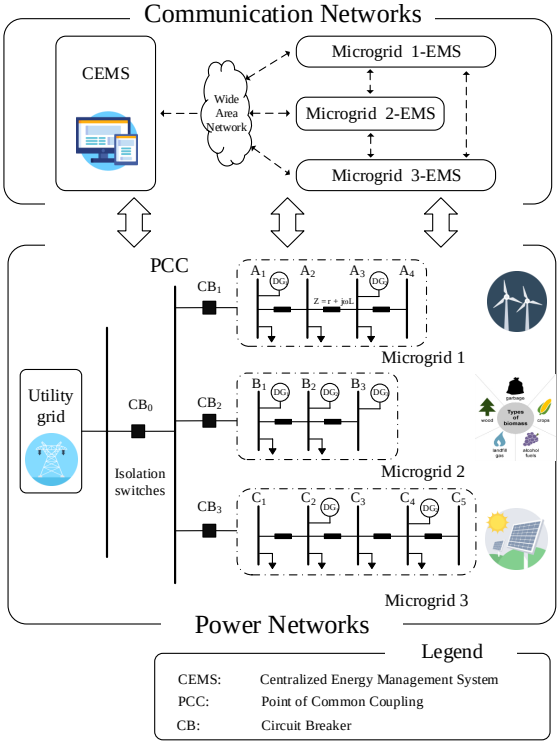

Figure 1. A typical MMG system.

I. Introduction

In today's power grid, energy is most generated in large and centralized power plants. Meanwhile, various new energy technologies are being introduced to the power grid such as distributed generators, multi-agent systems and cloud computing. Among these new technologies, multi-microgrid (MMG) systems have the potential to play an increasingly important role in the future power grid [1]. They can be operated in either grid-connected or islanded mode [2]. New trading models such as trading with the power grid, and purchasing from a controllable distributed generation plant, will coexist [3], [4]. The typical structure of an MMG system is shown in Fig. 1. While the vulnerability of traditional power systems has been exposed in recent years [5], the open and distributed connection of MMG systems exposes the systems to serious cyber-security problems. Therefore, it is of critical importance to ensure the security in addition to the stability for MMG systems. As the initial protective barrier, intrusion detection system (IDS) playes a critical role in overall security protection. The results from IDS can be used in self-adaptive decisions and real-time response [6], or help safety operator with the detection result of abnormal state in time [7], [8]. However, traditional host-based or network-based IDS that works independently [9], [10] is not entirely adopted to MMG systems. In comparison, collaborative intrusion detection system (CIDS) can analyze the evidence from multiple domains simultaneously and consider the alerts of distributed detector synthetically for promoting the efficiency of IDS [11]. Therefore, it is more appropriate for distributed architecture as in MMG systems.

Recently, efforts have been made in the applications of CIDS in smart grid. This includes a fully distributed

CIDS management structure [12]. For constrained resources in smart meters, a CIDS is proposed against false data injection attack [13]. A scalable and elastic architecture is also presented with a Peer-to-Peer (P2P) solution for grid and cloud computing [14]. In addition, considering the problem of how to operate a CIDS when these assumptions of trust and security are relaxed, some proposed methods have partially addressed this problem. Such as several CIDSs [15], [16] use message authentication to guarantee that alerts come from a trusted participant by using a central certification authority (CA) or certifying happens among peers [1], [17]. However, the central certificate authority can become a bottleneck for scalability as the number of participants increases. Furthermore, these approaches cannot protect against a legitimate participant who is sending malicious data, and prevent misbehavior by a peer who has taken the time to first build a high reputation.

Therefore, a new CID approach using blockchain is presented in this paper for MMG systems. More specifically, the target of CID, called a proposal, is generated from periodic and trigger patterns. From these generated proposals together with the correlation model of MMGs, a CID is achieved by using the consensus mechanism in blockchain. The final detection results are stored on each block. The recording node that proposes the consensus-reached block will be awarded according to an incentive mechanism. Overall, the paper makes the following three main contributions:

1) A distributed CID approach incorporating with the consensus and incentive mechanisms of blockchain is proposed for MMG systems without a trusted authority or central server;
2) As a part of the approach, a proposal generation method that combines periodic and trigger patterns is designed to enhance the accuracy of intrusion detection;
3) An improved algorithm of delegated proof of stake (DPoS) is devised for consensus on the distributed detection results by the utilization of the degree of correlation and the detection coefficient.

The rest of this paper is organized as follows. Section II provides some background knowledge about CIDS and blockchain. Section III presents the architecture of our CID approach using blockchain. This is followed by Section IV on the process of generating proposals based on multiple patterns. Section V shows the process of collaborative detection based on an improved DPoS algorithm and incentive mechanism. Experiments are conducted in Section VI to demonstrate our approach. Finally, Section VII concludes the paper.

TABLE I
A COMPARISON OF THE THREE CLASSES OF CIDS.

Species	Advantage	Shortcoming
Centralized CIDS [20]	1) High detection accuracy 2) Simple implementation	1) Poor scalability 2) Unsuitable for large-scale scenarios
Hierarchical CIDS [21]	1) Better scalability 2) Suitable for large-scale scenarios	1) Lower detection accuracy 2) Loss of detection information 3) Single-Point-of-Failure
Fully Distributed CIDS [15]	1) Peer to peer suits to transfer data	1) Lacking detector from a global perspective 2) Low detection accuracy

II. BACKGROUND AND RELATED WORK

A. A Brief Review of CIDS

A skilled intruder can slowly change his or her behavior to avoid being detected by IDS. Thus, it is worth achieving collaboration among MMGs to increase the difficulty of intrusion. According to the network topology of each detection unit and ways of the information interaction, a classical CIDS falls into one of the three classes [11], [18]: centralized, hierarchical [19], and distributed. A comparison of these three classes is shown in Table I.

However, the survey [11] also point out that the another important aspect is the problem of security and trust for CID, and the trustworthiness of the alerts generated by each single anomaly detection unit is the premise of accurate results of CIDS.

Thus, the immutability and reliability of information transfer and dissemination are worthy to be considered, more so in fully distributed systems.

B. Blockchain and Security

Since Satoshi Nakamoto founded Bitcoin in 2008 [22], blockchain, the underlying technology architecture of Bitcoin, has attracted widespread interest. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. When a new block is added to the blockchain, it must be approved by the verification of all nodes. The schematic diagram of a blockchain is shown in Fig. 2.

As a typical distributed data storage technology, blockchain covers a variety of technologies, such as decentralization, cryptography, and consensus algorithms.

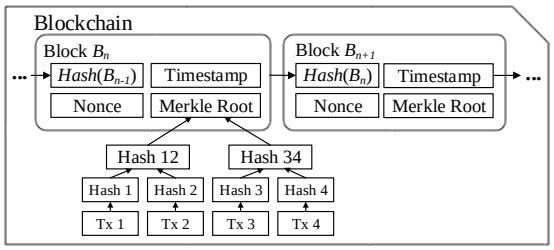

Figure 2. A schematic diagram of a blockchain.

In the absence of a trusted third party or centralized node, a new consensus mechanism is formed. Due to the advantage of establishing the secured, trusted, and decentralized autonomous ecosystems for various scenarios, blockchain has been investigated in both research and applications [23].

As a novel and fundamental technical framework, blockchain is suitable for applications in the security protection of cyber-physical systems (CPSs). Most current applications of blockchain are in the field of data security for ensuring that data is traceable and not easily tampered. For example, it is demonstrated [24] that the integration of blockchain, smart contracts and Internet of Things (IoT) technologies is powerful. With the ability to interact with peers in a trustless, auditable manner, blockchain could give us resilient, truly distributed peer-to-peer systems. Blockchain has the fundamental role to register and authenticate all operations performed on Internet of Things (IoT) devices data [25]. Consortium blockchain is explored for a secure energy trading system named energy blockchain [26]. It is suitable for P2P energy trading, such as microgrids.

Other research efforts use the consensus mechanism to implement distributed and collaborative scheduling decisions or intrusion detection. For managing billions of devices deployed worldwide, a fully distributed access control system based on blockchain is proposed for arbitrating roles and permissions in IoT [27]. As the operation of the future Energy Internet would also be more decentralized and self-executing, it is suggested that blockchain be applied in operational framework of Energy Internet [28]. This could promote a consensus among the decentralized institutions of various energy entities. A distributed blockchain-based protection framework is proposed to enhance the self-defensive capability of modern power systems against cyber-attacks [29]. Moreover, a blockchain framework is discussed in [30] for collaborative intrusion detection.

In summary, blockchain has been used in several domains to date. This motivates us to investigate this technique in the security of MMG systems by using the the consensus and incentive mechanisms. Similar to the storage of transaction information in cryptocurrency, the detection results of CID with consensus will be stored on the blockchain.

III. The Proposed Architecture of our CID using Blockchain

The architecture of our CID using blockchain is shown in Fig. 3. In each microgrid, our CID approach has a proposal generation component and a CID component. Their functions are described below.

The proposal generation component aims to propose proposals for CID. The proposals are obtained periodically under normal circumstances. They can also be triggered when abnormal state of microgrid is found out by its own IDS, whose content is defined as the state of a microgrid.

The CID component realizes the transmission and consensus of detection results among MMGs. Firstly, as the microgrid involved in the proposal is the detection target, each microgrid that has energy or cyber interdependency with it obtains the result of detection independently based on One-Class SVM. Secondly, a consensus on the proposal is reached based on an improved DPoS algorithm, which utilizes the degree of correlation and detection coefficient instead of stake in this paper. The results of CID are obtained and stored on blockchain in sequence to ensure its immutability and reliability. Thirdly, with the help of an incentive mechanism, when the Block B_n proposed by a microgrid is recorded, the level of the detection coefficient of a microgrid is promoted, so as to make it be accepted more easily in the next Block B_{n+1} generation process. In contrast, other microgrids which put forward the orphan blocks will be suspected as attacked nodes.

IV. Multi-Pattern Based Proposal Generation

This section presents the process of generating the object of consensus in the proposal generation component. It begins with an introduction of multi-pattern including trigger pattern and periodic pattern. Then, an algorithm is developed to implement the whole process.

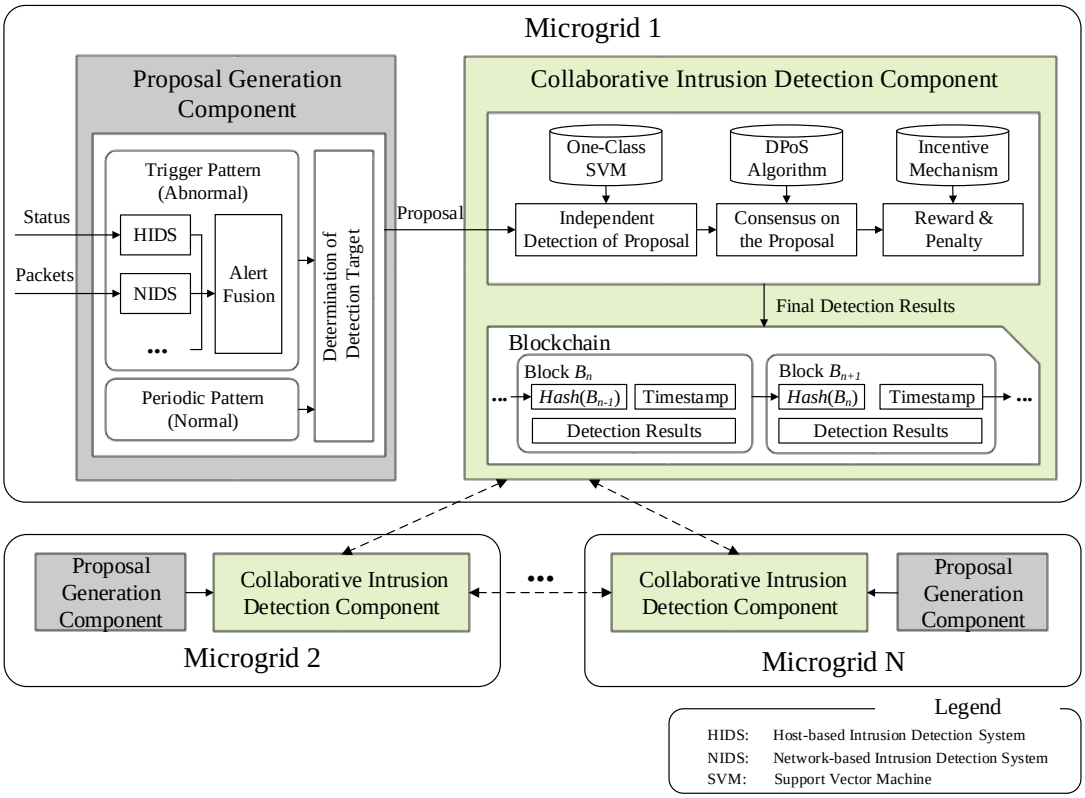

Figure 3. The architecture of our CID using blockchain.

A. *Multi-Pattern*

The initial proposal is not only triggered when abnormal event is detected by each microgrid's IDS under trigger pattern, but also generated in turn under periodic pattern.

1) Trigger Pattern: The IDS of each microgrid detects the abnormal state mainly from the perspective of communication and power flows. The alert, context of proposal, will be generated at the same time.

Detection of Communication Flow: The white list of access-control mainly monitors medium-access control (MAC) addresses, IP addresses and ports in the data link, network and transport layers, respectively.

$$\boldsymbol{ac} \nsubseteq \boldsymbol{AC}_{wl} \rightarrow Alert, \tag{1}$$

where $\boldsymbol{ac}$ indicates the set of $\{MAC_{src}, MAC_{dst}, IP_{src}, IP_{dst}, Port_{src}, Port_{dst}\}$, and $\boldsymbol{AC}_{wl}$ represents the white list of access-control. In addition, because MAC and IP addresses are unique when identifying a communication subject, there is an unique match $\langle IP, MAC\rangle$ generally. If the match $\langle IP, MAC\rangle$ has been changed, a spoofing attack , e.g., an address resolution protocol (ARP) attack, may take place.

The white list of protocol-based mainly confirms that the protocol used is suitable for the grid in the application layer, such as DNP3, IEC61850, IEC61870 and other proprietary protocols.

$$\boldsymbol{pb} \nsubseteq \boldsymbol{PB}_{wl} \rightarrow Alert, \tag{2}$$

where $\boldsymbol{pb}$ indicates the used communication protocol, and $\boldsymbol{PB}_{wl}$ represents the white list of protocol-based.

Detection of Power Flow: Unknown and new attack types will be detected by behavior-based rules [31], which are mainly reflected in the constraints of power flow. For instance, there is an upper limit $(v_{i.max})$ and a lower limit $(v_{i.min})$ of each nodal voltage (v_i), and a maximum allowable apparent power $(s_{l.max})$ of the branch.

$$v \notin \{v_i \mid v_i \in (v_{i.min}, v_{i.max})\} \rightarrow Alert, \tag{3}$$

$$s \notin \{s_l \mid s_l \in (0, s_{l.max})\} \rightarrow Alert, \tag{4}$$

where s_l represents the apparent power of branch l.

2) Periodic Pattern: Due to the existence of false negatives, it is insufficient to rely on its own IDS. To tackle this problem, periodic pattern is integrated. This allows the state of a microgrid to regularly become the target of detection and also enables other microgrids to judge it.

Under periodic pattern, as system runtime T_{run} is an integer multiple of polling cycle time T_{period}, we select a relevant microgrid m as a new proposal. Different from a proposal generated under trigger pattern, the content of this proposal is 'Microgrid m: normal'.

$$m = (T_{run}/T_{period}) \bmod N, \tag{5}$$

where N represents the total number of microgrids.

B. Algorithm for the Proposal Generation

The detailed steps of the proposal generation process is shown in Algorithm 1. In the pseudo code of the algorithm, Pro' and Pro represents pre-proposal and proposal, separately. Firstly, each microgrid is detected from the perspective of communication flow and power flow according to Section IV-A1. Then, the judgement $(Pro \neq Pro')$ aims to remove redundant results. As soon as $T_{run}/T_{period} \in \mathbb{Z}$, the proposal (Microgrid m: normal) is generated.

Finally, through fusion and de-redundancy, the ultimate proposal is obtained and delivered to the CID component for the determination of the detection target.

Algorithm 1 Multi-Pattern Based Proposal Generation.

Input: Detect information of microgrids, Pro'
Output: Pro

$Pro \leftarrow \varnothing$
while $T_{run}/T_{period} \notin \mathbb{Z}$ **do**
  for each $n \in \{1, 2, ..., N\}$ **do**
    $a \leftarrow \boldsymbol{ac} \nsubseteq \boldsymbol{AC}_{wl} \mid \boldsymbol{pb} \nsubseteq \boldsymbol{PB}_{wl}$
    $b \leftarrow v \notin (v_{i.min}, v_{i.max}) \mid s \notin (0, s_{l.max})$
    if $a \,\&\, (Pro \neq Pro')$ **then**
      Pro = 'Microgrid n: abnormal comm.'
    else if $b \,\&\, (Pro \neq Pro')$ **then**
      Pro = 'Microgrid n: abnormal power'
    end if
  end for
end while
$m \leftarrow (T_{run}/T_{period}) \bmod N$
Pro = 'Microgrid m: normal'

V. Consensus-Based CID

After generating the proposal, the next step is to achieve CID. This section begins with an introduction of independent detection of proposal by each microgrid. This is followed by discussions of the achievement of consensus. Then, the application of an incentive mechanism is developed to reward or punish the recording microgrid.

A. Independent Detection of Proposal

The smart grid is a complex cyber-physical system (CPS) [32]. The interaction between MMGs is mainly reflected in both energy and cyber interdependencies, which are chosen as the basis of intrusion detection in this paper. Through a calculation of load flow [33] [34], we aim to judge whether the voltage magnitude, current, power and other interactive electrical quantities are within the normal range from the perspective of power flow. If not, the detection target will be suspected to have been attacked.

In view of intrusion detection at the communication system, the rationality of the control strategy as well as the real-time synchronization of information transmission are mainly considered. For instance, it is judged whether or not the breaking of the line breaker is unreasonable under the goal of optimal scheduling, and whether or not the transmission delay of data between the nodes exceeds the threshold. An abnormal alarm is issued once discovered.

Normal behaviors are modelled by one-class SVM in this paper. This is because abnormal data of the grid is more difficult to obtain during actual operations, and one-class SVM is suitable as an unsupervised learning algorithm. Moreover, the algorithm has been widely accepted as a classification algorithm for detecting abnormal states [35].

The detection process can be divided into three parts: data training, model establishment, and data testing.

The one-class SVM algorithm can be summarized as mapping the data into a feature space, and then trying to separate the mapped vectors from the origin with maximum margin, because the origin is the only original member of the second class [36]. In the modelling process of power system, there is no hyperplane in the original sample space that can correctly classify two types of samples. Thus, we use a nonlinear kernel function $(\Phi(x))$ to map samples from the original space to a higher-dimensional feature space [37], such as radial basis function

$$\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j) = exp(-\frac{\|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2}{2\sigma^2}). \tag{6}$$

It is always possible to find a hyperplane that solves the separation problem. Finding the maximum margin

to separate the dataset can be converted to the following optimization problem:

$$\min_{w,\zeta_i,\rho} \frac{1}{2}\|w\|^2 + \frac{1}{\nu n}\sum_{i=1}^{n}\zeta_i - \rho \tag{7}$$

$$\text{s.t. } w^T\Phi(x_i) > \rho - \zeta_i,\ i = 1, \cdots, n,\ \zeta_i > 0 \tag{8}$$

where parameters w is a vector orthogonal to the hyperplane, ρ represents the margin, ζ_i is the slack variables, the role of ν is similar to penalty factor C in Two-class SVM, representing the fraction of training patterns that are allowed to be rejected, and n is the total number of training patterns.

This optimization problem can be solved by using the Lagrange multiplier method to transform (7) to a dual optimization problem as follows

$$\min_{\alpha} \frac{1}{2}\sum_{ij}\alpha_i\alpha_j\kappa(\boldsymbol{x}_i, \boldsymbol{x}_j), \tag{9}$$

$$\text{s.t. } 0 \le \alpha_i \le \frac{1}{\nu n},\ \sum_i \alpha_i = 1. \tag{10}$$

Finally, the decision function of one-class SVM can be expressed as

$$\begin{aligned} f(x) &= \text{sgn}\left((w^T\Phi(x) - \rho)\right) \\ &= \text{sgn}\left(\sum_i \alpha_i\kappa(\boldsymbol{x}_i, \boldsymbol{x}) - \rho\right), \end{aligned} \tag{11}$$

The types of data collected and analyzed include measurement information, state information, transaction log, etc. Thus, one detection model based on one-class SVM has finished. If N is the number of microgrids, we will get at most $N(N-1)$ models according to the relationship matrix between microgrids for intrusion detection. It is worth mentioning that the detected data which is different from data of microgrid's own IDS.

B. Consensus on the Proposal

Considering that each detector has its own insight about the proposal, these distributed detection results need to achieve consensus. In order to achieve this purpose without any trusted authorities or central servers, one microgrid is selected as the recording node firstly. Its detection results will be stored in a new block and be submitted to the network as the process of 'mining' in Bitcoin [22].

Then, as every node in a decentralized system has a copy of the blockchain, a microgrid with similar insights for detection results will confirm that the detection result is correct and add the new block to the end of the chain.

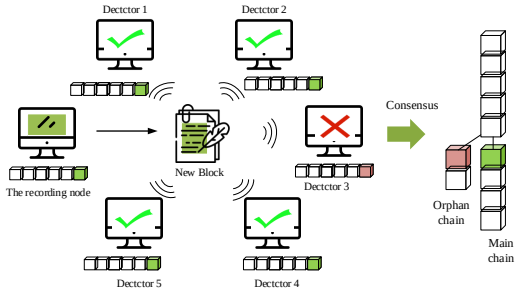

Figure 4. A schematic diagram of the consensus process.

On the other side, the microgrid that has objection to the detection results will generate another block and add the block to the end of its own chain. The schematic diagram of the consensus process is shown in Fig. 4.

Finally, as main chain consists of the longest series of blocks which require a consensus of the network majority, wrong detection results will be meaningless to become an orphan block. In other words, there is a reward for generating each block. The corresponding incentive mechanism will be described in detail later.

According to the different selection ways of recording node, the algorithms aiming to achieve consensus mainly include: Proof of Work (PoW), Proof of Stake (PoS) and DPoS [23]. Combining system characteristics and application requirements, the DPoS algorithm is adopted to achieve CID in MMGs due to its lower energy consumption and shorter time in the process of reaching consensus.

Each microgrid has a different probability of being selected as a recording node based on the stake it owns. In the hash operation process of generating a new block, it is embodied in the difference of target and difficulty. A different recording node k has a different value of the difficulty indicator $D(k)$. A modified version of DPoS algorithm uses a condition of

$$\begin{aligned} &SHA256(SHA256(Hash\boldsymbol{B}_{n-1}) + Timestamp \\ &+ Nonce + MerkleRoot) \\ &< ST(k)Targetmax/D(k), \end{aligned} \tag{12}$$

where $ST(k)$ means the elapsed time holding these stakes by recording node k, and its maximum value cannot exceed 72 hours. The larger the value of $ST(k)$ or the smaller the value of $D(k)$, the easier the Inequality (12) can be established. To ensure real-time detection, $Targetmax$ can be set to 0xFFFF0000 $\times 2^{4\times 56}$.

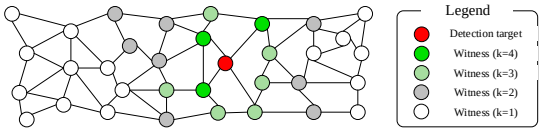

Figure 5. DPoS based electing nodes for participation in consensus.

TABLE II
CORRESPONDENCE BETWEEN P_{ij} AND $\hat{P}_{ij}$

P_{ij}	[0.6,1]	[0.3,0.6)	[0.1,0.3)	[0,0.1)
$\hat{P}_{ij}$	1	2	3	4
$D(\hat{P}_{ij})$	16	16^2	16^3	16^4

$D(\hat{P}_{ij})$ is the corresponding difficulty indicator in Inequality (12).

DPoS selects a recording node by trusting a small number of honest nodes as representatives. For example, in the rating of 1 to 4, the honest nodes of level 2 and above could be selected as representatives, as shown in Fig. 5 intuitively. However, stake-based selection will result in undesirable centralization. This is because the single richest member may have a permanent advantage. To overcome this defect, in this paper, the degree of correlation as well as the detection coefficient are utilized as the basis for electing nodes instead of stake innovatively.

By adopting this method, the greater energy or cyber interdependency with the target of detection, the larger probability of the microgrid will be selected as a recording node. This is experssed as

$$\begin{aligned} P_{ij} &= \frac{\int_0^T \theta_{ij}(t)dt}{T} \times I_{ij} \\ &= \frac{\int_0^T \theta_{ij}(t)dt}{T} \times (\gamma E_{ij} + (1-\gamma)C_{ij}), \end{aligned} \quad (13)$$

where P_{ij} means probability of selecting node i as a recording node, j means the target node for detection, θ_{ij} represents the detection coefficient of node i on j which is related to the accuracy of previous detection results, $\int_0^T \theta_{ij}(t)dt/T$ means the cumulative mean of θ_{ij} over time, I_{ij} indicates interdependency of microgrid node i on j, and E_{ij}, C_{ij} represent energy and cyber interdependency of microgrid node i on j, respectively. A detailed example of correlation model, and the formation of E_{ij}, C_{ij}, can be seen in Section VI-B. γ indicates the adjustment factor, which is different in different conditions. For instance, γ is 0.8 in the case of abnormality of communication flow, is 0.2 on condition of abnormality of power flow, and is 0.5 when proposal is normality. All above-mentioned index coefficients are within the interval $[0, 1]$. The correspondence between selection probability (P_{ij}) and the level of difficulty $(\hat{P}_{ij})$ is shown in Table II.

C. Rewards and Penalties

Analogous to the fact that cryptocurrency can be obtained by the behaviour of mining in Bitcoin, the incentive mechanism of blockchain when a new block reaches consensus is also modified and adopted in this paper. The form of reward is expressed not only by financial incentives but also the improvement of detection coefficient θ_{ij}. Therefore, the probability that the node will be selected as a recording node in the next block generation process will increase. A higher coefficient θ_{ij} will bring benefits and more influence on distributed management and decision-making for a microgrid. Conversely, if the detection result presented by i for target j does not reach consensus, the level of detection coefficient θ_{ij} will decrease in a similar way.

$$\theta'_{ij} = \begin{cases} \max\{-\theta_{ij}^2 + 2\theta_{ij} + \alpha I_{ij}, 1\}, & \text{consensus-reached,} \\ \min\{1 - \sqrt{1 - \theta_{ij} + \beta I_{ij}}, 0\}, & \text{consensus-unreached,} \end{cases} \quad (14)$$

where θ_{ij} means the previous detection coefficient whereas θ'_{ij} signifies the detection coefficient after exaltation. The greater interdependency I_{ij}, the faster the change in detection coefficient θ_{ij}. Parameters α and β are added as adjustment factors.

VI. EXPERIMENTAL STUDIES

To evaluate the detection performance of our CID approach using blockchain, this section conducts simulation experiments on a typical MMG platform.

A. Simulation Setup

A typical MMG scenario is set up in this section. The co-simulation platform of a cyber-physical power system is depicted in Fig. 6. The power distribution system is considered to be a set of interconnected microgrids that may be connected to the utility grid through PCC and CB. The radial distribution feeders contain 6 microgrids, which are divided according to different laterals. Each microgrid has corresponding renewable energy resources and distributed load.

In order to establish a decentralized experimental environment, we presume that the isolation switch (CB_0) is open and interconnected microgrids are running in island mode without the support of the utility grid. The microgrid adopt the master-slave control method. This implies that there is one distributed grid adopts U/f

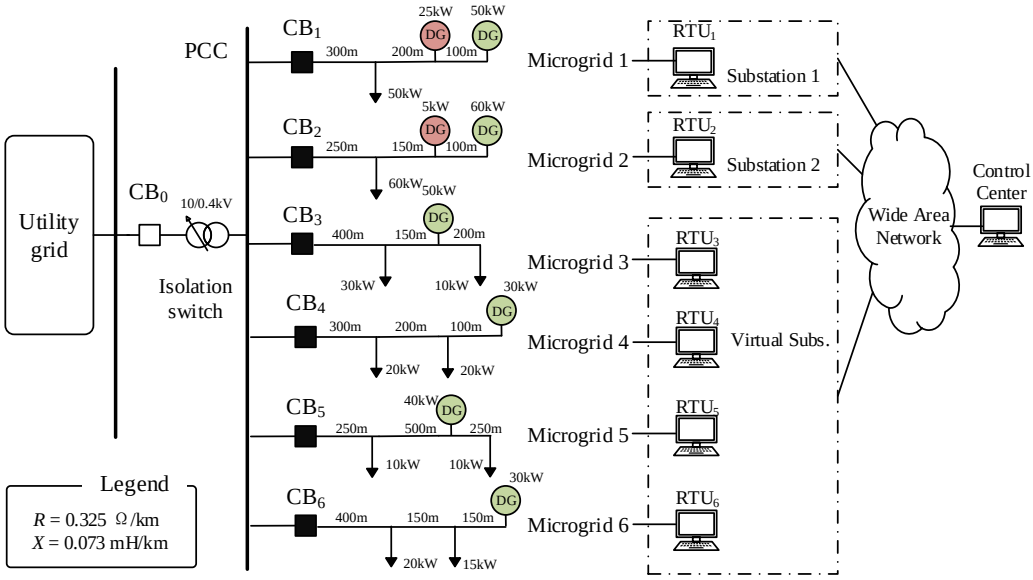

Figure 6. Typical MMG model of the simulation.

control to guarantee not only the balance of power supplies and demand but also the uniformity of frequency as the master unit in each microgrid. All other microgrids adopt P/Q control to make the active power and reactive power of the inverter output equal to the reference. Two color nodes, green and red, are used to represent master unit and slave unit, respectively.

To build a communication environment of the power system, the function of remote terminal unit (RTU) and power management unit (PMU) is simulated on the host in a substation. Overall scheduling is achieved in the control center, which is not used actually due to island mode without the support of the utility grid. The transmission of measurement information and operating instructions is via a wide area network (WAN).

In this paper, four common types of attacks [38] are considered, and the attack secnarios are described in details as below.

1) Tampering Attack: Typical tamper attack, such as false data injection [39], is often occured in power systems. In our simulations, control instructions of load switch is set as being tampered in microgrid.

2) Man-in-the-Middle (MITM) Attack: MITM attack means that the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Which is conducted by ARP poisoning and the modification of operating instructions.

3) Replay Attack: Replay attack is a form of attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. To conduct this kind of attack, the machine of substation is hacked into by an attacker who continues to intercept all data sequence from sensors and then retransmits it.

4) Denial of Service (DoS) Attack: This type of attack is simulated by totally obstructing the communication channels of sensor nodes, such as RTU.

B. Establishment of the Correlation Model

For achieving consensus and CID among MMGs, a correlation model is established according to the energy and cyber interdependency of microgrids. Relationship matrix EM and CM are formed, respectively. Energy relationship matrix EM means the magnitude of the impact of one microgrid on another. With the MMG platform, the experimental data is generated by the floating load up and down below 10% in each single microgrid. Active power and reactive power are selected as features. For instance, we fit the active power of the microgrid whose load is dynamically changing with active power of other microgrids, and get the linear regression equation $y = a_i x + b_i, (i = 1, \cdots, N)$ and

$\sum_{i=1}^{N} a_i = 1$. So, E_{ij} is defined as the correlation coefficient a_i for microgrid j.

$$EM = \begin{Bmatrix} 1 & 0.287 & 0.208 & 0.191 & 0.151 & 0.163 \\ 0.242 & 1 & 0.221 & 0.203 & 0.161 & 0.173 \\ 0.224 & 0.281 & 1 & 0.187 & 0.148 & 0.160 \\ 0.220 & 0.276 & 0.200 & 1 & 0.146 & 0.158 \\ 0.211 & 0.265 & 0.192 & 0.177 & 1 & 0.155 \\ 0.214 & 0.269 & 0.196 & 0.179 & 0.142 & 1 \end{Bmatrix}.$$

The cyber relationship matrix CM reflects the transmission of measurement information (MI) and operating instructions (OI) between microgrids. It is also related to the geographical location ($Distance$) of the microgrid in the radial distribution feeders.

$$C_{ij} = \frac{\sigma_1 MI_{ij}/MI_i + \sigma_2 OI_{ij}/OI_i}{Distance}, \tag{15}$$

where MI_i and OI_i indicate the total of measurement information and operate instructions from other microgrids. For example, CM_1 is calculated according to Eq. (15) as $\sigma_1 = \sigma_2 = 1.5$

$$CM_1 = \{1, \frac{0.45}{\sqrt{1}}, \frac{0.45}{\sqrt{2}}, \frac{0.3}{\sqrt{3}}, \frac{0.15}{\sqrt{4}}, \frac{0.15}{\sqrt{5}}\}.$$

The CM of the MMG model in Fig. 6 is

$$CM = \begin{Bmatrix} 1 & 0.450 & 0.318 & 0.173 & 0.075 & 0.067 \\ 0.450 & 1 & 0.450 & 0.318 & 0.173 & 0.075 \\ 0.318 & 0.450 & 1 & 0.450 & 0.318 & 0.173 \\ 0.173 & 0.318 & 0.450 & 1 & 0.450 & 0.318 \\ 0.075 & 0.173 & 0.318 & 0.450 & 1 & 0.450 \\ 0.067 & 0.075 & 0.173 & 0.318 & 0.450 & 1 \end{Bmatrix}.$$

The relationship matrix between microgrids is obtained as $IM = \gamma EM + (1-\gamma)CM$, and the correlation model is established.

C. Reach Consensus Based on DPoS Algorithm

Now, let us explain the implementation process of the DPoS algorithm through three typical attack scenarios: tampering attack on microgrid 4, MITM attack on microgrid 6, and replay attack on microgrid 6. Due to the different characteristics of attack types, tampering control instructions and the change in match $\langle IP, MAC \rangle$ may be easily found by the abnormality of power flow and communication flow, while replay attack could spoof the monitor of substation. Thus, after ignoring other insignificant proposals, these three proposals are considered in our experiments: $\mathcal{A}$) Microgrid 4: abnormal power, $\mathcal{B}$) Microgrid 6: abnormal comm., and $\mathcal{C}$) Microgrid 6: normal.

1) Proposal $\mathcal{A}$: Using the consensus algorithm of DPoS, the recording node needs to be selected. For proposal $\mathcal{A}$, the relationship is $I_{ij} = \gamma E_{ij} + (1-\gamma)C_{ij}$ where γ is 0.8. For Microgrid 4, its relationship vector

$$IM_4 = \{0.211, 0.284, 0.250, 1.000, 0.207, 0.190\}.$$

Only some representative nodes whose relationship is beyond 0.2 will be selected to participate in the process of consensus. As the initial value of detection coefficient (θ_{ij}) of node j on i all is 0.5, microgrid 2 will be selected as the recording node due to its maximum relationship. Then, for proving its computing power, microgrid 2 has to put forward the new block in a limit time by hash operation process (12). Otherwise, it will be replaced by the microgrid whose relationship after its relationship. The selection probability

$$P_{24} = \frac{\int_0^T \theta_{24}(t)dt}{T} \times I_{24} = 0.142 \in [0.1, 0.3).$$

$D(\hat{P}_{24})$ given in Table II is 16^3 and the initial value of $ST(2)$ is 72. On the basis of Inequality (12),

$$SHA256(SHA256(HashB_{n-1}) + Timestamp + Nonce + MerkleRoot) < 72 \times Targetmax/16^3,$$

where $HashB_{n-1}$ is $0\text{x}\underbrace{00\ldots00}_{64}$ as the genesis block, and timestamp is the generation time of block. By the anomaly detection model based on one-class SVM, microgrids 1, 2, 3 and 5 all believe power flow of microgrid 4 is indeed abnormal by confirming the abnormal action of load switch and abnormal nodal voltage. So the block proposed by microgrid 2 will reach a consensus and these two abnormal states will be recorded as a and b, respectively. Since Merkle Root is implemented by using algorithm SHA-256 twice, the stored detection results are shown in Fig. 7.

$$Merkle\ Root = dhash(dhash(a)\ concat\ dhash(b)). \tag{16}$$

Then, based on the incentive mechanism, the detection coefficient (θ_{24}) of microgrids 2 on 4 will get an upgrade from 0.5 according to (14) when coefficient $\alpha = 0.1$.

$$\theta'_{24} = max\{-\theta_{24}^2 + 2\theta_{24} + \alpha I_{24}, 1\} = 0.7784,$$

2) Proposal $\mathcal{B}$: In contrast to proposal $\mathcal{A}$, the content of proposal $\mathcal{B}$ is an abnormal communication flow. As γ is 0.2, the relationship vector IM_6 of microgrid 6 is

$$IM_6 = \{0.097, 0.114, 0.177, 0.290, 0.388, 1.000\}.$$

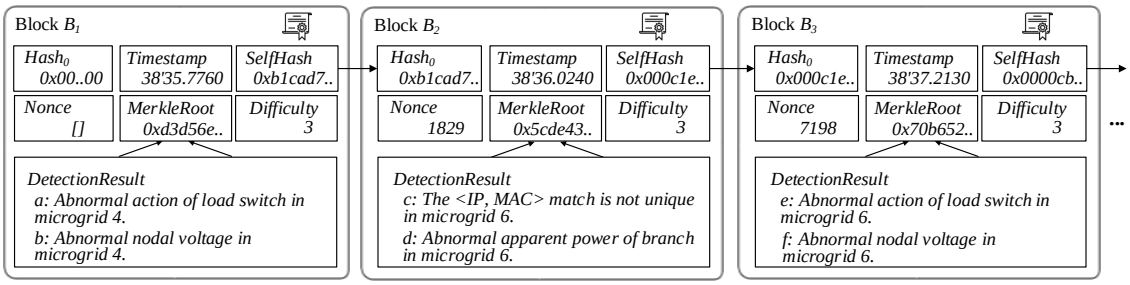

Figure 7. Consensus-induced detection results are stored on blockchain.

Similar to the previous process, nodes 4 and 5 whose relationship beyond 0.2 are selected as representative. Microgrid 5 is chosen as the recording node. The selection probability

$$P_{56} = \frac{\int_0^T \theta_{56}(t)dt}{T} \times I_{56} = 0.194 \in [0.1, 0.3).$$

$D(\hat{P}_{56})$ given in Table II is 16^3, too. According to the collaborative anomaly detection model, microgrids 4 and 5 justify the abnormal communication flow of detection target. The results will be recorded as abnormal states c. Moreover, they also dig out that the abnormal apparent power of branch still exists in microgrid 6 (abnormal states d). Analogous to the generation of block 1, detection coefficient (θ_{56}) will also get an upgrade as

$$\theta'_{56} = max\{-\theta_{56}^2 + 2\theta_{56} + \alpha I_{56}, 1\} = 0.7888,$$

3) Proposal $\mathcal{C}$: About the proposal $\mathcal{C}$ 'Microgrid 6 is normal', similar to the previous analysis process, they will put forward their own different opinions and reach a consensus since not being deceived. The detection results will be stored as 'e: Abnormal action of load switch in microgrid 6' and 'f: Abnormal nodal voltage in microgrid 6'. The new detection coefficient (θ_{56}) of microgrid 5 on 6 will changed to

$$\theta'_{56} = max\{-\theta_{56}^2 + 2\theta_{56} + \alpha I_{56}, 1\} = 1,$$

which means when detection object is microgrid 4, the probability of microgrid 2 as the recording node will increase.

D. CID Performance Evaluation

First, we test the detection rates of our CID approach for different types of attacks. The overall accuracy (OA) depends on true positive rate (TPR) and false positive rate (FPR). It describes how correctly an IDS works by $OA = (TPR + 1 - FPR)/2$ [40]. Based on the various attack scenarios introduced in Section VI-A, the results of the experiment are shown in Table III.

TABLE III
THE OA FOR DIFFERENT TYPES OF ATTACKS.

Category	Tampering	MITM	Replay	DoS
Single IDS	90.3%	85.6%	×	100%
CID	97.9%	94.3%	91.2%	100%

It is seen from Table III that the OA of our CID approach has improvement over traditional single IDS for different types of attacks. In particular, in the MITM attacks scenario, CID not only verifies the abnormality of communication flow in microgrid 6, but also checks out its power abnormality. In the replay attacks scenario, CID is able to detect the abnormal state whereas a single IDS fails to do so. Furthermore, the results suggest that replay attacks and MITM attacks are more difficult to detect than others. That may be interpreted by the fact that the attacks sometimes do not cause abnormal state of power grid.

Then, we evaluate the real-time performance of our CID approach. The real-time performance of our CID mainly depends on the execution time of the DPoS consensus algorithm. Thus, we plan to analyze the relationship between the influencing factors ($\hat{P}_{ij}$, $ST(k)$) and the computing time of generating a new block, and find the apposite setting of difficulty.

By running the 'mining' process for 500 times at different $\hat{P}_{ij}$ values under $ST(k) = 1$, the minimum, mean, and maximum computing times are displayed in Fig. 8. It is noted that the expression of the correlation is shown in (17). This correlation indicates that with the increase of difficulty ($\hat{P}_{ij}$), the computing time grows exponentially. To ensure the real-time performance of our CID approach, the nodes with a difficulty of 3 or

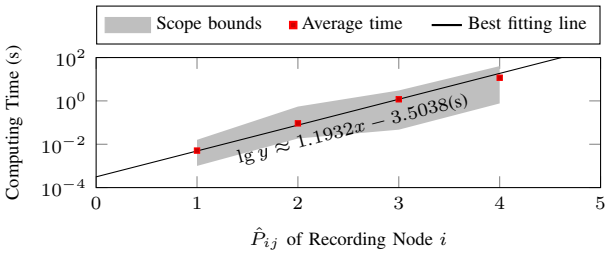

Figure 8. Computing time versus Difficulty Indicator.

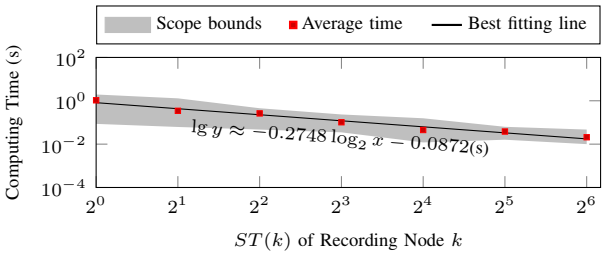

Figure 9. Computing time versus Elapsed Time.

less are generally selected as recording node.

$$\lg y \approx 1.1932x - 3.5038. \tag{17}$$

As a difficulty of 3 remains unchanged, running 500 times at different $ST(k)$ values, the computing time display in Fig. 9. The elapsed time ($ST(k)$) holding detection coefficient (θ_{ij}) exponential growth with base 2, the computing time will also grow exponentially. The exponential correlation is expressed as

$$\lg y \approx -0.2748 \log_2 x - 0.0872. \tag{18}$$

E. Discussions

Through the above experiments, the proposed CID approach is able to efficiently detect intrusions for MMGs in island mode. Using blockchain well solves the collaborative problem of IDS in distributed systems through consensus of detection results. Proposal generation based on multi-pattern reduces the false negative rate (FNR) by generating new proposals constantly. The achievement of consensus could increase the OA. Table IV presents the comparison of our CID with several previous studies on CID. According to Table IV, it suggests that our approach can achieve CID in the absence of a trusted third party or centralized node by using the consensus and incentive mechanisms of blockchain, more so in MMG systems, the representative of fully distributed scenario.

TABLE IV
PERFORMANCE COMPARISON OF CID APPROACHES.

CID	Category	Year	TPR	System architecture	Incentive	Participant safety	Without CA
[12]	Smart grid	2017	88.9%	Fully distributed	×	×	–
[13]	AMI	2015	100%	Centralized	×	×	–
[15]	Internet	2004	–	Fully distributed	√	×	–
[17]	Computer networks	2013	>93%	Fully distributed	√	√	×
[41]	HIDS network	2010	–	Fully distributed	√	√	×
Our CID	MMG	2019	96.3%	Fully distributed	√	√	√

Note: '√' shows that the ability was considered in the literature;
'×' indicates that the ability was not available;
'–' means that the item was not mentioned and could not be inferred.

VII. CONCLUSION

A new CID approach using blockchain has been presented in this paper for distributed intrusion detection in MMG systems without a trusted authority or central server. It guarantees the consistency and non-repudiability of detection results of IDS in each microgrid in the process of distributed data transmission. The novelty of this paper lies in the following three aspects. Firstly, a new CID approach is proposed for MMG systems by incorporating the consensus and incentive mechanisms in blockchain. Secondly, a multi-pattern proposal generation method is developed to reduce the FNR of intrusion detection. Thirdly, an improved DPoS algorithm is designed as the consensus mechanism to overcome the defect of one single richest member.

There are a few aspects worth investigating in our future work. Our method utilizes consensus and incentive mechanisms of blockchain to achieve CID. To address the uncertainties in the propagation of distributed detection results, how to design a fuzzy consensus algorithm is a direction for future work. In addition, in response to the increasingly complex and distributed attacks, the above method proposed for intrusion detection can be considered in collaborative risk assessment and decision making.

REFERENCES

[1] K. Boroojeni, M. H. Amini, A. Nejadpak, T. Dragievi, S. S. Iyengar, and F. Blaabjerg, "A novel cloud-based platform for implementation of oblivious power routing for clusters of microgrids," *IEEE Access*, vol. 5, no. 99, pp. 607–619, 2017.

[2] Q. Jiang, M. Xue, and G. Geng, "Energy management of microgrid in grid-connected and stand-alone modes," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3380–3389, 2013.

[3] D. An, Q. Yang, W. Yu, X. Yang, X. Fu, and W. Zhao, "Soda: Strategy-proof online double auction scheme for multimicrogrids bidding," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 7, pp. 1177–1190, 2018.

[4] D. Gregoratti and J. Matamoros, "Distributed energy trading: The multiple-microgrid case," *Industrial Electronics IEEE Transactions on*, vol. 62, no. 4, pp. 2551–2559, 2013.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[6] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[7] I. Ullah and Q. H. Mahmoud, "An intrusion detection framework for the smart grid," in *Electrical and Computer Engineering*, 2017, pp. 1–5.

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

[9] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, and S. Smith, "Intrusion detection for resource-constrained embedded control systems in the power grid," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 2, pp. 74–83, 2012.

[10] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2018.

[11] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Computers & Security*, vol. 29, no. 1, pp. 124–140, 2010.

[12] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Jnior, and S. Katsikas, "A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems," *Computers & Security*, vol. 64, no. C, pp. 92–109, 2017.

[13] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, Sept 2015.

[14] H. A. Kholidy and F. Baiardi, "Cids: A framework for intrusion detection in cloud systems," in *International Conference on Information Technology-New Generations*, 2012, pp. 379–385.

[15] V. Yegneswaran, P. Barford, and S. Jha, "Global intrusion detection in the domino overlay system," in *In Proceedings of Network and Distributed System Security Symposium (NDSS)*, 2004.

[16] S. Shaik and S. G. John, "A novel distributed trust model for peer-to-peer networks," *IJCER*, vol. 3, no. 5, pp. 267–270, 2014.

[17] M. G. Pérez, F. G. Mármol, G. M. Pérez, and A. F. S. Gómez, "Repcidn: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms," *Journal of Network and Systems Management*, vol. 21, no. 1, pp. 128–167, 2013.

[18] E. Vasilomanolakis, S. Karuppayah, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *Acm Computing Surveys*, vol. 47, no. 4, pp. 1–33, 2015.

[19] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2018.

[20] F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework," in *Proceedings 2002 IEEE Symposium on Security and Privacy*, May 2002, pp. 202–215.

[21] E. Vasilomanolakis, M. Fischer, M. Mhlhuser, P. Ebinger, P. Kikiras, and S. Schmerl, "Collaborative intrusion detection in smart energy grids," in *International Symposium for ICS & Scada Cyber Security*, 2013.

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, 2008.

[23] Y. Yuan and F. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, Sept 2018.

[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[25] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *Computer Systems and Applications*, 2017.

[26] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, Aug 2018.

[27] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, April 2018.

[28] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin, "Applying blockchain technology to decentralized operation in future energy internet," in *Energy Internet and Energy System Integration*, 2018, pp. 1–5.

[29] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2018.

[30] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, no. 99, pp. 10 179–10 188, 2018.

[31] Y. Yang, K. Mclaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute scada-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092–1102, 2014.

[32] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2017.

[33] N. Qin, *Voltage control in the future power transmission systems*. Springer, 2017.

[34] A. Elrayyah, Y. Sozer, and M. E. Elbuluk, "A novel load-flow analysis for stable and optimized microgrid operation," *IEEE Transactions on Power Delivery*, vol. 29, no. 4, pp. 1709–1717, 2014.

[35] R. Perdisci, G. Gu, and W. Lee, "Using an ensemble of one-class svm classifiers to harden payload-based anomaly detection systems," in *International Conference on Data Mining*, 2007, pp. 488–498.

[36] L. M. Manevitz and M. Yousef, "One-class svms for document classification," *Journal of Machine Learning Research*, vol. 2, no. 1, pp. 139–154, 2001.

[37] S. Lecomte, R. Lengelle, C. Richard, F. Capman, and B. Ravera, "Abnormal events detection using unsupervised one-class svm - application to audio surveillance and evaluation -," in *IEEE International Conference on Advanced Video and Signal-Based Surveillance*, 2011, pp. 124–129.

[38] A. A. Cardenas, T. Roosta, and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor net-

works: A case study in scada systems," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1434–1447, 2009.

[39] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[40] K. Huang, Q. Zhang, C. Zhou, N. Xiong, and Y. Qin, "An efficient intrusion detection approach for visual sensor networks based on traffic pattern learning," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 47, pp. 2704–2713, May 2017.

[41] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Trust management and admission control for host-based collaborative intrusion detection," *Journal of Network and Systems Management*, vol. 19, no. 2, pp. 257–277, 2011.