IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 14, 2019, accepted December 4, 2019, date of publication December 31, 2019,
date of current version January 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2963325

Secured Energy Trading Using Byzantine-Based Blockchain Consensus

A. SHEIKH, V. KAMUNI, A. UROOJ, S. WAGH, (Senior Member, IEEE), N. SINGH, AND DHIREN PATEL

Veermata Jijabai Technological Institute, Mumbai 400019, India

Corresponding author: A. Sheikh (masheikh_p17@ee.vjti.ac.in)

ABSTRACT To mitigate the problems of demand-supply mismatch in the future grid the solution of renewable energy source (RES) integration results in a bidirectional flow of information and transactions, which are prone to different kinds of cyber attacks, especially in energy trading where the security of financial transactions is of most concern. Electric vehicle (EV) having the advantage of mobility can play a significant role in maintaining demand-supply balance at any location unlike their peers (conventional compensator). For deciding entire system security, securing EVs charging-discharging transactions at all charging stations or connecting points is most important. The system can be made more secure against cyber-attacks with the introduction of the blockchain framework. Hence, in view of secured transactions, the paper focuses on the energy trading process between EVs and distribution network (DN) in a Byzantine based blockchain consensus framework. During peak load period DN initiates the energy trading process by demanding additional power from the EVs. This process of energy trading results in energy and information exchange which needs to be secured through blockchain from vulnerable attacks and threats. Possible scenarios of various cyber-attacks on different nodes of the system are visualized in the form of false data. To highlight the application of blockchain, the Byzantine general problem framework is used which states that for successful attack 33% of information is to be manipulated, in other words, decreasing the probability of attack confirms the system security. Numerical results based on various operating scenarios for the standard IEEE 33 bus system are in agreement with the Byzantine consensus problem indicating improvement in system security.

INDEX TERMS Blockchain, Byzantine general problem, consensus, energy trading, security.

I. INTRODUCTION

For traditional power system operation security has become a pivotal factor which comprises of two main aspects, physical security, and cybersecurity [1]–[3]. Physical security implicates the ability of the system to continue a normal working state in the existence of severe disturbances. Cyber security supports the power system operation with its inherent property of securing the communication networks and computer systems. The process operations and tasks related to its control are performed in the power system with the help of information and communications technology (ICT) [4], [5] which are still susceptible to exposure of threats even with the integration of the cyber-physical system and renewable energy sources (RES). As discussed in [6]–[8], this integration opens the access to the communication link between the cyber and physical layer, leading to increased probability of occurrence of cyber attack.

In the future grid, the integration of RES is strengthened to mitigate the problem of conventional power sources and demand-supply mismatch. However, such grid integration results in the unbalanced distribution network (DN) resulting in various issues such as voltage regulation, high system losses and consequently may lead to blackout [9], [10]. The future grid has various energy storage and supply elements such as solar photovoltaic (PV) cells, wind turbines, electric vehicles (EV), and super-capacitors. EV having the advantage of mobility over solar PV cells and wind turbines can provide solutions to the problem of demand-supply mismatch in DN. With recent advancements in the automobile industry and trends of the smart grid, EV is expected to be one of the major players for distributed energy consumption, storage, and supply system. EVs operate in two modes, one in which vehicle recharges from the grid power i.e. grid-to-vehicle

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

mode (G2V) and other in which vehicle discharges power to grid i.e vehicle-to-grid (V2G) mode [11].

The vehicle to grid systems (V2G) has many benefits and cost issues [12]–[16], although increasing the number of EVs may impact power distribution system dynamics and its performance. The residual state of charge in each EVs can be utilized and transmitted to a DN to suffice the need and thus facilitating the demand response. In [17]–[20] energy trading among EVs with a major focus on charging/discharging coordination was reported. The energy trading process between EVs and aggregator was modeled as a non-cooperative game among EVs and a linear price function was proposed by [17]. The authors of [18] also used a non-cooperative game for the energy trading market with the inclusion of multiple sellers and buyers. The process of energy trading in [17] and [18] was carried out considering single time-slots, however, in [19] and [20] the multiple time-slots were considered. For a number of EVs, the authors of [19] developed a coordinated charging/discharging scheduling algorithm with the aim of minimizing the total cost at the aggregator. Based on a Markov Chain, for energy trading market price uncertainty was considered in [20]. To reduce the impact of EV charging on the power system during office working hours, trading between two sets of EVs in a peer-to-peer (P2P) manner is proposed in [21]. In [22] the energy exchange between two isolated microgrids is addressed in the context of minimizing the total cost in generation and transportation of energy. An optimal contract-based scheme was designed in [23] and also incentive-based energy trading mechanisms in the smart grid are investigated. The authors of [24] proposed an electricity trading model in the consortium blockchain framework, where charging/discharging EVs can trade electricity without the need of any trusted intermediary. The authors of [25] explored blockchain and edge computing for secure and efficient V2G energy trading process. For a decentralized blockchain-enabled smart grid system, a novel EV participation charging scheme is proposed in [26], with the objective of minimizing charging the cost of EV users as well as minimizing power fluctuation level in the grid. The aforementioned literature's considered energy trading either between vehicle and grid or two EVs or between two microgrids and majorly focused on charging and discharging issues of EVs.

In [27] an energy trading between EV and charging station (CS) is proposed in the blockchain framework. Further, this work was extended in [28], where the authors considered the energy trading process in presence of Sybil attack and highlighted the effectiveness of blockchain framework defense mechanism against Sybil attack. The energy trading between EV and CS was also emphasized in [29], the authors presented the idea of securing energy trading process against different cyber attacks by using blockchain. The energy trading between EV and CS is proposed by [30] in software-defined networking (SDN) enabled V2G environment. For securing the transactions of energy trading a blockchain mechanism is also designed in a distributed edge-as-a-service environment. In view of the intelligent transportation system, the authors of [31] proposed BEST, an energy trading scheme based on blockchain for securing the energy trading process. The proposed scheme for improving the quality of service (QoS) in the network utilized vehicular networking architecture based on SDN. The authors of [32] proposed EnergyChain, a blockchain model for securing the data generated by smart homes. The work carried out in [27]–[32] utilized Proof-of-Work (PoW) consensus in the blockchain framework, the limitations of using PoW consensus is discussed in later Sections.

For the secure charging of EV in smart communities, a contract-based energy blockchain is proposed in [33]. The authors also proposed an energy allocation mechanism for allocating limited energy available from renewables to EVs. However, the work majorly focused on the charging issues of EVs. A Byzantine fault tolerance (BFT) based real-time electricity pricing is proposed in [34], where the security of communication between the utility and smart meters is enhanced. In contrast to [34], homomorphic encryption (HE) technology is proposed by [35] in which the data available from meters are aggregated and then verified using a blockchain system based on BFT consensus. The authors of [36] highlighted the need of BFT mechanism, for monitoring and control of the power grid. The major task of the BFT mechanism was to handle the data of phasor measurement units (PMU) and thus leading to an overall improvement in the security and reliability of the power grid. A Byzantine consensus based on gossip protocol and time sequence was proposed in [37], with the aim of eliminating a central node in the Internet of Vehicles (IoV) structure. In [38], the attack on smart grids is prevented by generating blocks with short signatures and hash function. For achieving high throughput a practical BFT algorithm is employed in the P2P system. A Proof-of-Concept (PoC) was implemented by [39] for securing transactions in a decentralized energy trading system. In the aforementioned literature's the implementation of BFT was majorly carried out for securing data of smart meters, grid monitoring and also energy trading by securing transactions irrespective of the energy flow information in the smart grids. The security of energy flow information is crucial as in the future grid with bidirectional energy flow and consumer-utility interaction there is a tremendous increase in security issues with the influence of multiple entities. In view of this, the paper proposes a blockchain framework for securing not only transaction details but also energy flow information.

Security issues are important in the communication network at public charging facilities hence a reliable two-way communication infrastructure network is needed. However, this issue can be seen analogous to a Byzantine general problem (BGP), in which security of the message given by the commander to the lieutenants is of at most importance [40]. The risk of misinformation or miscommunication between the generals can be seen similarly in real-life practical applications, whether accidental or deliberate. To evade these risks, blockchain proves to be one of the most promising solutions. In a decentralized P2P system like a public blockchain, a consensus has to be achieved. The individual parts of the system have to agree on the history of the blockchain up until the present moment as well as on how to move forward since there is no central authority to assume responsibility for it.

There is a tremendous change in infrastructures and social form due to the breakneck development in Internet technology and large data [41]. Similarly, the advancement and development in electric vehicle technology, energy market, energy storage, the demand-side response have resulted in the growth of a transparent system with no central trusted entity for irrevocable transactions between machines or persons. The various problems associated with the centralized approach can be thus solved using a decentralized blockchain approach [42]. The authors of [43] present an overview of the blockchain technologies with detailed discussion on architecture and key characteristics of the blockchain. Different consensus algorithms used in the blockchain are also described in [43] and finally, the authors analyze and compare these protocols in different respects.

The attack on a modern power system is considered to be successful if the attacker tampers the sensor data at a node or manipulates the data through transmission channels or attacks the control room. However, with the introduction of blockchain, the probability of attack reduces as the attacker needs to manipulate more than 51% nodes data which is hard to achieve. The network will face major collisions if the attackers want to modify data of a particular block as for executing the same all the subsequent blocks should be modified too. The complete data collected is eventually stored in the form of a ledger of connected blocks that exist in the distributed form in each node memory. For storing the data in blocks the data is encrypted, mined, then block is generated, and finally, the data is decrypted and verified, details of each process are discussed in the sections below. The major contributions of the paper are as follows:

(i) The blockchain is applied to a centralized energy trading process between EV and DN resulting in decentralized operation which leads to the elimination of untrusted intermediary and enhances the transparency of the system.

(ii) For verification of blocks in the blockchain, a Byzantine based consensus algorithm for energy trading between EV and DN is proposed which states that for successful attack 33% of information is to be manipulated, in other words, decreasing the probability of attack confirms the system security.

(iii) To emphasize the system security, the impact of Byzantine based blockchain consensus is illustrated by considering various possible attack scenarios on different nodes of the system.

(iv) The effectiveness of the proposed method is validated using standard IEEE test feeder and results show improvement in security, as well as the privacy of the system, is maintained after the inclusion of blockchain.

The rest of the paper is organized as follows: Section II focuses on the preliminaries of BGP and blockchain. Section III introduces the system model of energy trading. Section IV presents the proposed framework for energy trading between EV and DN. Section V describes the Byzantine based consensus in the blockchain for verification and validation of information and energy exchange. Section VI provides supporting case studies and results to confirm the claim and Section VII concludes with the possible future extension of the work.

II. PRELIMINARIES

A. BYZANTINE GENERAL PROBLEM

Every system has to cope with its own failures and attack components, where one of the well-known consensus algorithm dealing with the intrusion of conflict information into the system is BGP. The BGP is a way of admitting the problem of misalignment between users of a decentralized system and its solution, without which decentralized distributed ledger technology would fail to function properly. The BGP gets its name from a 1982 paper [40] in which Leslie Lamport and two co-authors described the problems of decentralized decision-making. The analogy goes like this, the night before a battle, a group of Byzantine generals in different camps, each with command over a portion of the army, try to decide whether to attack or retreat. Messages between the generals are passed by messengers. However, some generals and some messengers may be traitors to the cause. Traitorous generals would be interested in sabotaging the plans of loyal generals, and traitorous messengers would be interested in altering the messages entrusted to them by loyal generals. Thus there is a need to find a way to reach consensus even with the knowledge that betrayal was possible. In [40] the algorithm is proposed in which the Byzantine army decides the action to be taken in order to overcome the malicious messages from disturbing the system. Lamport *et. al* have assessed the problem of survival from failures of computer systems in terms of BGP assuming few divisions in the Byzantine army camped outside the enemy city, with each division commanded by its own general. All generals need to come up with a common plan of action with the majority, in the presence of traitors. Suppose there are n generals, the commanding general must send an order to his n-1 subordinates such that [40]

1) All loyal subordinates obey the same order.
2) If the commanding general is loyal, then every loyal subordinate obey the order he sends.

The above condition 1 follows 2 only if the commander is loyal whereas on the other hand, if it is not then, few of the generals may be traitors trying to manipulate the loyal ones. In such situations, the loyal generals should survive with traitors in the network. However, it is shown that no solution with fewer than a total of $3m + 1$ generals can subsist the situation with m as the number of traitors [40].

An algorithm called Oral Message algorithm $OM(m)$ is proposed in [40] as a solution to the BGP to cope with m

traitors and with at least $3m + 1$ generals. This principle assumes the property of function *majority* with n generals obtaining a value v_i equals v, then n-1 subordinates obtaining the *majority* $(v_1, \ldots, v_{n-1})$ equals v. The algorithm follows as,

a. Algorithm *OM(0)*
   1) The commander sends his value to every subordinate,
   2) Each subordinate uses the value he receives from the commander or uses the default value if he receives no value.

b. Algorithm *OM(m)*, $m > 0$
   1) The commander sends his value to every subordinate.
   2) For each i, let v_i be the value (ATTACK or RETREAT) that subordinate i receives from the commander or else RETREAT if no value returned. Subordinate i acts as the commander in the algorithm *OM(m-1)* to send the value v_i to each of the n-2 other subordinates.
   3) For each i and $j \neq i$, let v_i be the value, the subordinate i receives from subordinate j in 2, (using Algorithm *OM(m-1)*) or else RETREAT if no such value received. Subordinate i uses the value *majority*$(v_1, \ldots, v_{n-1})$.

B. ARCHITECTURE OF BLOCKCHAIN

In current structures, data manipulation is possible because present data storing and collection mechanism yields a centralized framework which results in an increase of probability of attack. In contrast, a basic structure is provided by blockchain framework for gathering data from various units, the transmission of plain text from communication channels and information storage in some database [44]. The blockchain is a distributed data structure, can be viewed as a data log whose records are grouped together in timestamped blocks. The blockchain formulation and data storage operation is described in this section. Fig. 1 and 2 explain the signing and verification process using a hash function and also highlights the storing of data in the nodes.

1) DATA SIGNING

The data signing mechanism is a part of cryptography which contributes towards the confidentiality of data. It may not be a complete solution but can be treated as an important building block with a large security system in creating a secure environment. Cipher data is an encrypted data, which even an adversary unable to retrieve without valid decryption.

In the network, each node is designated with a private and public key. For message decryption, a private key also known as the secret key is needed and for system security, it should not be divulged to the adversary. The lengths of key vary in accordance with the class of algorithm [45]. A public key is a piece of information publicly available to all the nodes available in the network. In the first step, data is encrypted and then in next, it is broadcasted to all the nodes as seen from Fig. 1.

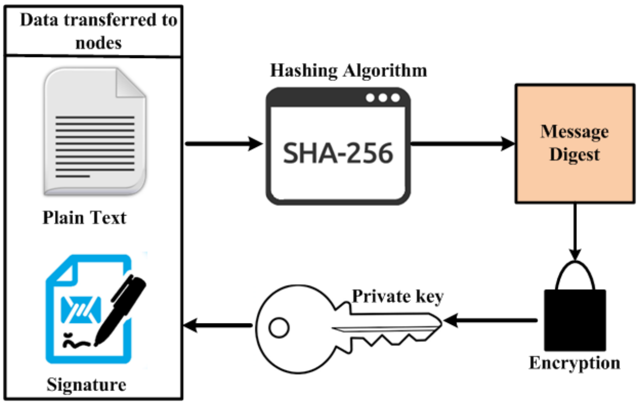

FIGURE 1. Data signing process in the network.

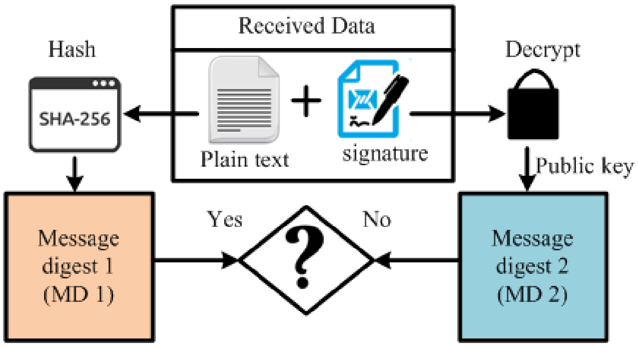

FIGURE 2. Data verification process.

The stored data within each node consist of two parts, all nodes public key information, node-specific private key information, accumulated blocks, and pre-set consensus. The transferred data consists of signatures and plaintext which is broadcasted to all the other nodes. A message digest (MD) is generated by processing collected plaintext with the help of a secure hash algorithm (SHA). To prevent different types of cyber-attacks and securing sensitive data, a set of algorithm known as SHA was developed by the National Institutes of Standards and Technology (NIST) and private parties and other government. With the help of private key MD is encrypted as a digital signature, the decryption of which is executed with the help of the same node public key [44]. The communication link broadcasts the transferred data to all other nodes.

2) DATA VERIFICATION AND AUTHENTICATION

The node receives encrypted data which needs to be verified by hashing the plaintext into message digest1 (MD1) and the signature to message digest 2 (MD2) with the help of sender's public key as shown in Fig. 2. For checking the authenticity of the information received the MD1 and MD2 are compared and finally if both the information is analogous then the received information is considered true otherwise it is concluded to be false [44]. Each node for verification should follow consensus i.e. each node should

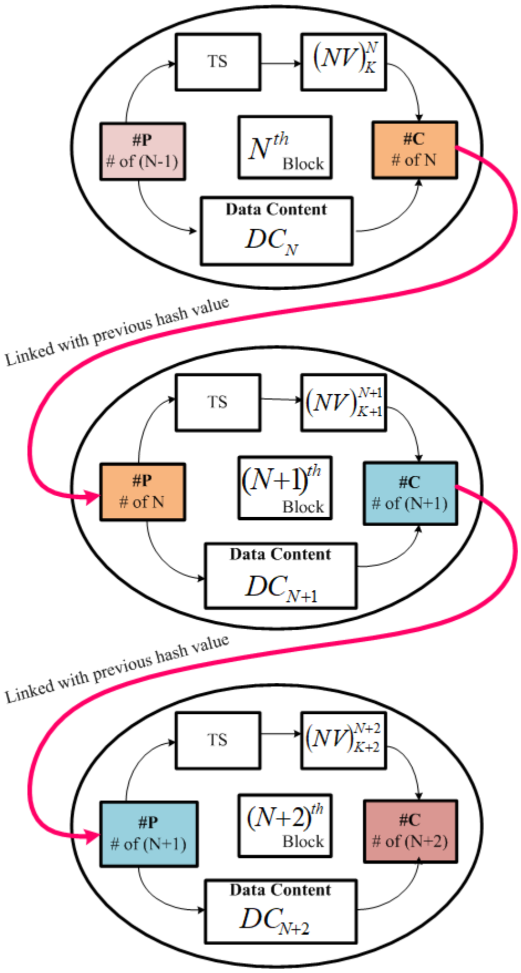

FIGURE 3. Block content and chain connections.

agree to a single conclusion. For achieving consensus the total number of nodes agreeing to a single conclusion should be approximately more than 51%.

3) DATA MINING AND GENERATION OF BLOCKS

As seen in Fig. 3 the information stored in the chain network is linked by cryptographically encoded data blocks. The hash function of various types are accessible and mostly used in message authentication codes and digital signatures.

With the help of SHA−256 the process of block generation and mining is executed. In the blockchain network, each block consists of the block number, data content, timestamp, previous hash value, current hash value, and nonce. The description of all the elements of the blocks in the blockchain is described in Table 1.

SHA−256 has a block size of 512−bits, the message size of less than 2^{64}−bits and word size of 32−bits. The output is a 256-bit digest. The compression function processes a 512-bit message block and a 256-bit intermediate hash value [44].

The algorithm has two interdependent parts,

1) Pre−processing and
2) Hash computation

TABLE 1. Various Attributes of block content.

Factors	Definition
N	The title of the blocks or Block number .
DC	Data Content- Block transaction details
TS	Time Stamp, the time instant of update in the block.
#P	Hash value of previous block
#C	Hash value of present(or current) block
NV	Nonce value is a number incremented by one every time a transaction is completed and it is a solution to the puzzle problem.

The pre−processing step deals with the overall message (S) including all the attributes of a block i.e. block number (N), data content (DC_N), time instant (TS_N) plus nonce (NV_N^K) which is nothing but a random value and lastly previous nonce value ($\#P_{N-1}$) [44].

$$S = N + DC_N + TS_N + NV_N^K + \#P_{N-1} \tag{1}$$

In the process of mining, all the miners or nodes find appropriate nonce value for hashing the output to a current block by solving a puzzle problem. The value of the present hash typically depends on the current block data content and the previous hash value. For example, if the current block is J^{th} then its data content and the previous block $(J-1)^{th}$ hash value will yield the current hash value [44].

In the next step i.e. the hash computation step the generation of puzzle problem is carried out. The overall message (S) is hashed twice with help of SHA−256 making it more secure to produce MD. This requires a target value which should be set greater than or equal to the final hash, as stated in (2):

$$F_{\#} = \#(\text{SHA} - 256, \#(\text{SHA} - 256, S)) \tag{2}$$

The computational difficulty of the problem increases if the value of the target hash is small resulting in the complexity of finding a preferable nonce. For validating the condition of the target hash, the miner has to find the nonce value and broadcast it to other miners or nodes. The resultant hash value is updated in the block if after verification consensus is achieved by more than 51% of nodes and only then it is allowed to be cryptographically linked to the previous ledger.

C. ROLE OF SMART CONTRACT IN BLOCKCHAIN

The smart contracts were introduced by Nick Szabo in 1994 and it is defined as "A computerized transaction protocol that executes the terms of a contract" [45]. Smart contracts are the codes executed to express the logic of transactions in the blockchain, such as solidity which is a higher-level language for writing smart contracts. These Ethereum blocks thus contain both smart contract and the final state produced by executing the contracts. The contracts are stored as byte-codes. Once the parties have looked upon the contract and are satisfied only when the smart contract is linked to the blockchain in the form of program code. It is then validated

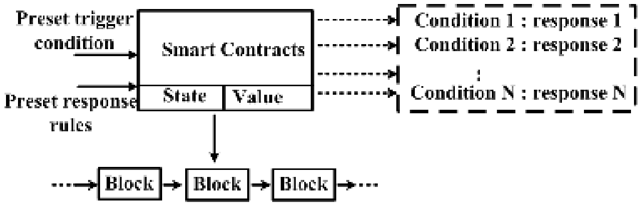

FIGURE 4. Smart contract configuration.

and received by each node of the network and deployed to a specific block of the blockchain and it can monitor the status of smart contracts in real-time.

The consensus will not be reached if the results between nodes are inconsistent i.e. smart contracts should be deterministic in nature. With this feature, it can be ensured that the same output will be produced for a specific input by a smart contract. The principle of operation of the smart contract is shown in Fig. 4 The contracts as byte-code instructions are stored in the blockchain for the Ethereum Virtual Machine (EVM) [46]. For writing such contracts a higher level language like Solidity is used. The contract in the form of program code is added to the blockchain once all the parties sign the contract [46].

III. BLOCKCHAIN BASED COMMUNICATION BETWEEN EV PARKING LOT AND DN

In this paper, a commercial parking lot is considered which can accommodate hundreds of EVs, e.g. multistorey office building. The DN experiences peak load on the system during 24 hours' load cycle. This intermittent peak demand requirement is fulfilled by switching on additional generators or by shedding load on priority basis which leads to customer dissatisfaction. In order to address the demand-supply mismatch problem in a modern distribution system, EVs being one of the energy consumption as well as energy storage elements can act as an energy supplying element in a duration of peak load hours. During office working hours, EVs remain idle for nearly entire day time and also their parking patterns remain relatively fixed. For the energy exchange process, the SCADA (supervisory control and data acquisition system) is the bridging element between the DN and parking lot.

The role of a SCADA system is to develop a communication link between EVs and DN for communicating the amount of power required during peak load hours. The EVs in a parking lot can engage in energy trading process with DN depending on its battery capacity and charging constraints as shown in Fig. 5. It is assumed that EVs entering into parking lot are charged around 75% of its rated capacity so that it can easily discharge some of the power and in return earn revenue for discharged power. The selling and buying of power and also information exchange can be viewed as a "virtual" trading process between EVs and DN with the help of the SCADA system. EVs, respond by setting the amount of energy it wants to sell back for earning revenues. The EVs start supplying for the decided time frame and the corresponding reward is given to the EV owner as shown in Fig. 6.

When the demand on the grid increases, the additional power required to supply the peak load is taken from the EVs which necessitates two-way communication between DN and EVs. Once a bidirectional link is set in between them, the communication process may become prone to various vulnerabilities and acts as an open window for the attackers. Thus, the safety and security of the bidirectional link is an important consideration. To ensure that the malicious activities do not affect the P2P network operations, an immutable data ledger has to be formed. This can be achieved through the chain of blocks, i.e blockchain. The P2P network is the part of the process in which each node has an equal role to play. The decisions taken by a node affects the upcoming stages in the process of energy trading, thereby, affecting the total performance of the system. In similar terms, the judgment of a commander of the Byzantine army to attack or retreat will affect the future of the subordinates and his kingdom. This enlightens the similarities between a P2P network and BGP.

The scenario of energy trading between DN and parking lot can be considered as the BGP. There is always the possibility of attacks or intrusion of malicious data into the system, which disturbs the network from fulfilling the load demand. Here, the DN demanding the energy is considered as the commander and the EVs in the parking lot as subordinates. In the proposed energy trading scenario there are more than $(3m + 1)$ generals. Thus, the problem of no solution for three generals with m traitors are not identified. However, the issue of secure message transfer between the generals of the Byzantine army can be solved in similar terms as that of EVs and DN using blockchain. This implies that the messages of the generals (acting as the nodes of the networked system) will be the data to be stored in the ledger. For the confirmation of these blocks, a BGP based consensus is applied in between the army generals i.e. the EV and DN.

The recorded data and the virtual trading process in between the EV parking lot and DN is illustrated in Fig. 5. Furthermore, it exemplifies the process of block formation during energy exchange as per the demand-supply.

IV. PROPOSED FRAMEWORK FOR ENERGY TRADING

As discussed in Section III the energy exchange process is initiated between EVs and DN with the help of the SCADA system to overcome the problem of demand-supply mismatch. The communication between DN and EVs for energy exchange with the SCADA as a communication layer is formulated in this section. The DN supplies energy to various residential, commercial, as well as industrial consumers. However, the demand for energy from consumers is intermittent in nature which may lead to unstable operation of DN. During peak load hours the power grid is overloaded, this additional load on the grid can be supplied by additional power from EVs connected in the parking lot. The number of EVs, in the parking lot act as energy storage system where additional discharged power of EVs is available and can be

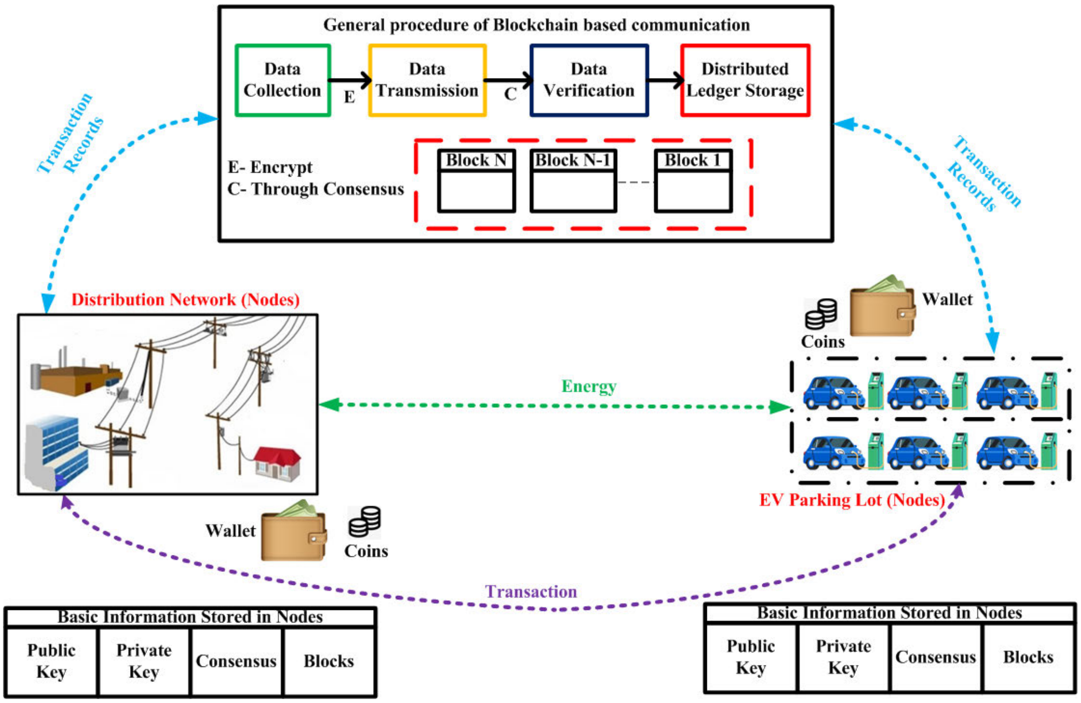

FIGURE 5. The representation of the Blockchain based communication with DN and EV parking lot as a P2P network.

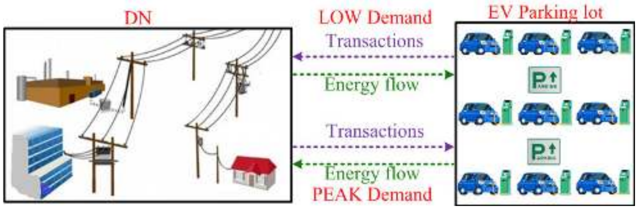

FIGURE 6. Energy and transactions flow during low and peak demand.

utilized during peak load hours to support the grid from partially overloading.

A. MATHEMATICAL FORMULATION OF ENERGY TRADING BETWEEN DN AND EV

The EVs with a minimum initial state of charge (SOC) i.e. SOC^i_{init} greater than or equal to 75% of EVs full charge, denoted as C^i_F, will only participate in the process.

$$SOC^i_{init} \geq 0.75C_F, \quad i = 1, 2, \ldots, EV_p, \ldots, EV_n \tag{3}$$

where EV_n is the number of EVs in the parking lot and EV_p is the total number of participating EVs in energy trading process. Let the distance from the parking lot to the next charging point destination for an EV be d^i_{EV} and state of charge required per *km* be SOC^i_{km}. The SOC required to travel from the parking lot to the destination is denoted as,

$$SOC^i_{reach} = d^i_{EV} \times SOC^i_{km} \tag{4}$$

The charge left C^i_{rem} after excluding the SOC^i_{reach} and a tolerance of ±10% of full charge, C^i_F is represented in (5) which is the energy that an EV contributes to the DN,

$$C^i_{rem} = SOC^i_{init} - SOC^i_{reach} - 0.1C^i_F \tag{5}$$

The nodes in the P2P network are the number of EVs participating in satisfying the demand of the DN. The energy demand is assumed to be evenly distributed among the number of participating EVs and not extracted from a single EV as it may result into battery degradation if the same EV is asked to discharge and meet the requirements every day. Let the energy demand from DN be D_{dem}, the amount of energy needed from each EV, E^i, is given by,

$$E^i = \frac{D_{dem}}{EV_p} \tag{6}$$

All the participating EV_p may not have the desired SOC to deliver i.e. $C^i_{rem} \leq E^i_n$ and if this is the case then the minimum C^i_{rem} among the EVs will be the aggregate value which will be contributed by all of them.

The $C^r_{rem} = \min\{C^i_{rem}\}$ where C^r_{rem} is the minimum charge among all participating EVs. This will lead to the discharge of one of the EVs with only SOC^i_{reach} left for utilization and $(EV_p - 1)$ number of EVs to suffice the remaining demand. The energy left to be supplied will again be equally distributed among the $(EV_p - 1)$ vehicles.

The E_{sup} is energy supplied by the participating EVs represented by,

$$E_{sup} = C^r_{rem} \times EV_p \tag{7}$$

The energy left to be supplied is given as,

$$D_{left} = D_{dem} - E_{sup} \tag{8}$$

This will continue until the DN requirements are met.

B. ROLE OF BLOCKCHAIN IN SECURING ENERGY TRADING BETWEEN EVs AND DN

The energy trading between EVs and DN can be considered equivalent to traditional trading between consumers and merchant. In contrast to the traditional trading of any commodity, electricity market needs to produce the energy at the same instance when it is required and storing has limited options. Similarly, in the traditional market, for any financial transactions, the secure payment system will protect any financial loss for a person or organization. Contrary to this, in the energy market, not only transactional details are important but also energy flow information is important, as any attack on data, may lead to paralyzed grid affecting larger population with no electricity, in turn causing huge loss equivalent to a blackout.

The major difference between the traditional trading and EV-DN trading is that here the role of merchant-consumers keeps on interchanging depending on the load condition of the grid. The EVs act as a merchant and DN act as consumers during peak demand on the grid whereas EVs act as a consumer and DN act as a merchant during low demand on the grid as shown in Fig. 6. The scenario of energy trading is initiated between EV and DN when demand on grid increases which results in a bidirectional flow of information between EVs and DN. This bidirectional trading takes place according to the load demand on both sides. At the time of peak load demand on DN, the energy is given to DN from EVs surplus charge as indicated in Fig. 6. Accordingly, at low load demand on DN, the EV is charged by DN as shown in Fig. 6. This two-way communication requires the exchange of energy and transactional data resulting in an increase of probabilities of malicious attack. To avoid the malicious attack on the system, blockchain plays an important role in both side trading process because of its inherent properties of security. In energy trading process any mislead in energy demand or supply may severely affect the grid, which can be protected by using the blockchain, where each energy and transactional details are stored in blocks. The blockchain store all the data with it and link every stored data details cryptographically using SHA-256 algorithm, which makes the system immutable. The stored data in local blocks of blockchain is verified by different consensus protocols, out of which Byzantine based consensus is considered in this paper. As shown in Fig. 7 DN and EV form the nodes of the P2P network. The energy trading between EV and DN is secured using Byzantine based consensus. Once the consensus is reached between the nodes of the network, the block is appended to the blockchain indicating no false data. The detail description of the achievement of consensus between nodes is explained in the next section.

V. BYZANTINE FAULT TOLERANCE (BFT) BASED CONSENSUS WITHIN BLOCKCHAIN

All nodes of the distribution system and participating EVs in the parking lot will together make the nodes of the P2P network. These nodes of the P2P network are connected and secured through blockchain, where the data content of each node is stored in immutable blocks. The data content such as the load profile of DN with respect to time, weak nodes of the system, load demand at weak node D_{dem}, the number of EVs participating in energy trading EV_p, initial charge SOC_{init}, EVs required SOC to reach a next destination SOC_{reach}, the amount of SOC that each EV can provide to a weak node of distribution system C^i_{rem}. These data contents are cryptographically encrypted using a hash function (SHA-256), as conveyed in Section II-B and its validation using BFT based consensus mechanism is discussed as follows. A copy of each node data is stored with all the other nodes for its validation among the peers of the network as shown in Fig. 8 and Fig. 9. As discussed in Section II-A and Section III, the DN and EVs act as a general and lieutenant respectively. Fig. 8 explains the BGP with DN as a traitor. According to the Byzantine algorithm at first, the DN act as a commander and sends its value to each EV. However, considering DN being a traitor the message passed to EVs may vary from one another. Let the original demand from DN to EVs be ‘1’, the message ‘1’ is sent to some of the EVs whereas some of the EVs receive the message ‘0’ from DN due to cyber-attack. All the EVs participating in energy trading act as a lieutenant communicating with each other for verification of the message received. It can be seen from Fig. 8 that EV_1 after

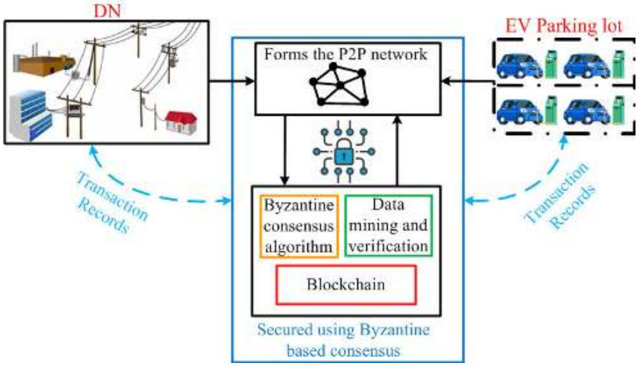
DN
EV Parking lot
Forms the P2P network
Transaction Records
Transaction Records
Byzantine consensus algorithm
Data mining and verification
Blockchain
Secured using Byzantine based consensus

FIGURE 7. Securing energy trading between EV and DN using Byzantine based consensus.

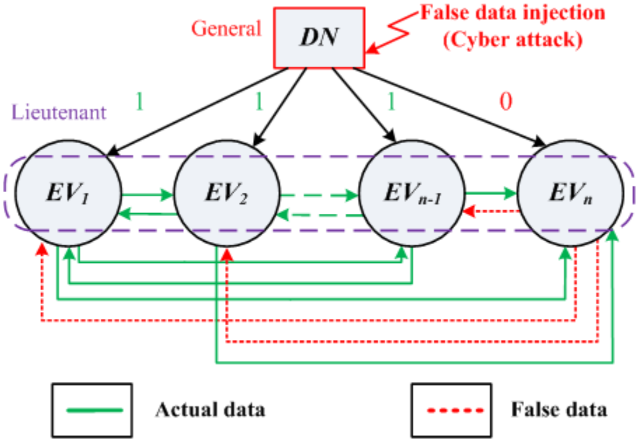

FIGURE 8. False data attack on DN resulting in DN being traitor.

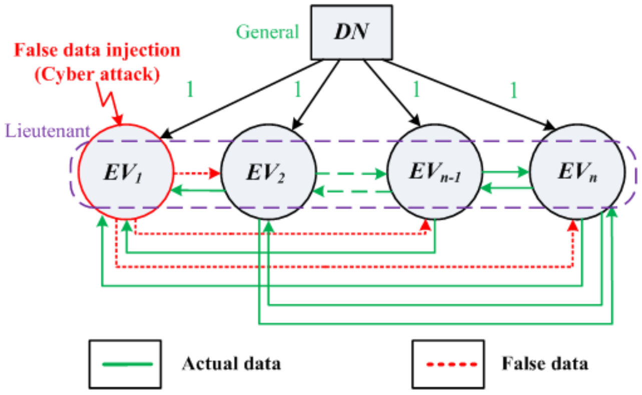

FIGURE 9. False data attack on EV resulting in EV being traitor.

communicating with EV_2 confirms that message received from DN is '1' represented by the green line. However, if EV_n communicates with EV_1, EV_2, and EV_{n-1} it can easily predict that DN communicated wrong information represented by a red dotted line. In this way, all the participating EVs in the energy trading process can identify any manipulated information communicated by the attacker instead of the correct information from DN.

Similarly, it is considered that out of all participating EVs one of the EV is a traitor which will mislead the information in energy trading process as shown in Fig. 9. The message communicated by DN to all the EVs is '1'. As seen in Fig. 9 that EV_1 being traitor communicates message '0' to EV_2, EV_{n-1}, and EV_n represented by the red dotted line. However, other EVs in energy trading process i.e. EV_2, EV_{n-1}, and EV_n after communicating with each other can easily predict that message given by DN is '1' as represented by the green line. EVs after communicating with each other can finally conclude that EV_1 is communicating manipulated information. This manipulated information by DN being traitor or EV being traitor can be verified with Algorithm $OM(m)$, $m > 0$ as described in Section II-A. After the collection of all values, the EV uses the value of majority for energy trading process. Thus, with the help of BFT based consensus between the EVs and DN the erroneous data can be verified and the valid block is appended.

In the process of Byzantine based consensus, the peer with the least block execution time becomes the leader node and the rest of the peer nodes will receive the request of the transaction i.e. the local block, for its corresponding verification. From here the validated transactions are broadcasted to other peers including the leader node [47]. This local block is now a Genesis Block of the chain. However, there can be a number of transactional rounds to be appended to the block. Then in order to make sure that the received block is valid, the leftover nodes double-check the same procedure and re-execute the block. If the proposed block is the same as the $2/3^{rd}$ of calculated blocks, the consensus is reached between the nodes. Thus the block gets appended to the chain. However, in the presence of an attack scenario, where the data is corrupted, this consensus algorithm between nodes helps to recover from plausible attacks. An important role of the chain of blocks is to make the data secure, safe and immutable, thus making the attack difficult. For the attacker to get into the system data, more than 33% of data should be hacked, which is relatively very difficult for intrusion and time-consuming. Fig. 10 represents the flow of the proposed framework. At the start, the DN initialize its demand and communicate with EVs in the parking lot. The EVs with SOC more than 75% are allowed to participate in the trading process else the EVs are declined to participate. The DN nodes and participating EVs forms the peers of the network. For the participating EV_p vehicles, each EV SOC^i_{reach}, C^i_{rem}, C^r_rem, SOC^i_init, and E^i are calculated. This calculated data copy is given to each node of the network. Using this data content, the blocks are mined and each node forms their own local block. The overall message S is hashed using SHA 256 as $F_{\#}$. The target value is set by defining the mining difficulty. After that the $F_{\#}$ and target value T is compared with the condition $F_{\#} \leq T$. If the condition is satisfied the local block is formed else the

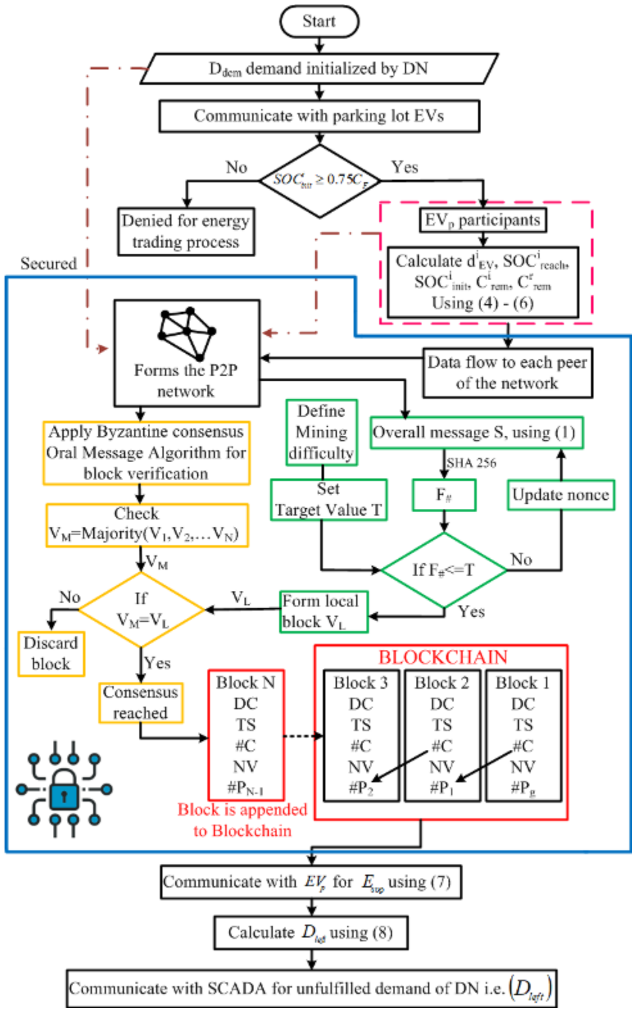
Start
D_dem demand initialized by DN
Communicate with parking lot EVs
No
Yes
SOC_init ≥ 0.75C_r
Denied for energy trading process
EV_p participants
Calculate d^i_EV, SOC^i_reach, SOC^i_init, C^i_rem, C^r_rem Using (4) - (6)
Secured
Forms the P2P network
Data flow to each peer of the network
Apply Byzantine consensus Oral Message Algorithm for block verification
Define Mining difficulty
Overall message S, using (1)
SHA 256
Check V_M=Majority(V_1,V_2,...V_N)
Set Target Value T
F_#
Update nonce
V_M
If F_#<=T
No
No
If V_M=V_L
V_L
Form local block V_L
Yes
Discard block
Yes
Consensus reached
Block N DC TS #C NV #P_N-1
BLOCKCHAIN
Block 3 DC TS #C NV #P_2
Block 2 DC TS #C NV #P_1
Block 1 DC TS #C NV #P_g
Block is appended to Blockchain
Communicate with EV_p for E_sup using (7)
Calculate D_left using (8)
Communicate with SCADA for unfulfilled demand of DN i.e. (D_left)

FIGURE 10. Flowchart for secured energy trading process between DN and EV.

nonce value is incremented by 1. This local block is sent to each node and verified using Byzantine based oral message algorithm. If the consensus is matched the block is appended to the blockchain. Thus, energy trading process is secured and protected from cyber-attacks.

VI. REPRESENTATIVE CASE-STUDY FOR IEEE 33 NODE TEST FEEDER

In the field of the control system, the security-related issues have significantly increased in the past few years that include various types of attacks, which may replace the data package or inject malicious information into the network. The different possible attack scenarios are visualized in the form of false data for which BGP framework could be used which states that for successful attack $2/3^{rd}$ of information is to be manipulated. The various case studies were conducted on the different IEEE bus system and the results obtained from IEEE 33 bus system is presented. IEEE 33 bus system consists of one feeder with four different laterals, 32 branches, and a peak load of 3715 kW and 2300 $kVAr$ [48]. The representative case study for highlighting the impact of blockchain is carried out in two parts;

- Case 1: Securing energy and information data exchange during energy trading between EVs and DN.
- Case 2: Securing different nodes of the system.

The details of different cases and scenarios are summarized in Table 2.

TABLE 2. **Summary of different cases and scenarios considered for representative case study.**

Cases	Scenarios
Case 1: Securing energy and information data exchange during energy trading between EVs and DN.	Scenario I- Communication between EVs and DN without false data
	Scenario II- Communication between EVs and DN with false data (When $\sum C^i_{rem} > D_{atk}$)
	Scenario III- Communication between EVs and DN with false data (When $\sum C^i_{rem} < D_{atk}$)
Case 2: Securing different nodes of the proposed model	Scenario I- Attack scenario for the system with no security i) Attack on sensor data/sender node ii) Attack on Communication links iii) Manipulation in the SCADA information iv) Attack on actuators/receiver end
	Scenario II-Attack scenario for the system with the inclusion of blockchain i) Attack on sensor data/sender node ii) Attack on Communication links iii) Manipulation in the SCADA information iv) Attack on actuators/receiver end

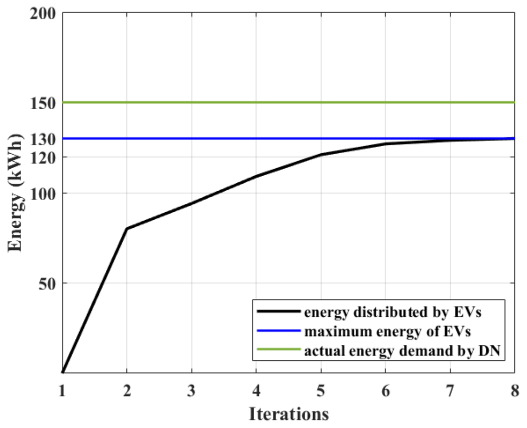

FIGURE 11. **Energy demand requirements by DN without any false data.**

A. CASE 1: SECURING ENERGY AND INFORMATION EXCHANGE PROCESS BETWEEN EVs AND DN.

The energy trading between EVs and DN is illustrated in Section IV. However, if the demand for DN increases the SCADA communicates with EVs for additional demand required. EVs depending on their battery capacity will start the trading process by discharging their batteries. In case if demand on DN is more than the available power from EVs batteries, SCADA will communicate with other energy supply sources. The role of blockchain in securing this energy and information exchange process between EVs and DN is described considering three scenarios. One in which the communication between EVs and DN is described without any false data and others in which communication between EVs and DN is considered with false data.

1) SCENARIO I- COMMUNICATION BETWEEN EVs AND DN WITHOUT FALSE DATA

Considering an operating scenario as described in Table 3 the actual demand by DN is 150 kWh whereas the total energy available from EV_p ($\sum C^i_{rem}$) is 130 kWh. As seen from Fig. 11 EVs supply the available 130 kWh and the remaining 20 kWh is arranged by SCADA. Thus it can be seen that even though EVs are not able to completely satisfy the requirements of DN then also partial requirements of DN are met in the absence of false data. This process of energy and information exchange is prone to malicious attack which may lead to manipulated data. If total energy available from EV_p ($\sum C^i_{rem}$) is considered 150 kWh then it can completely satisfy the DN requirement of 150 kWh. In such a case, there is no need for the arrangement of additional power through SCADA.

2) SCENARIO II- COMMUNICATION BETWEEN EVs AND DN WITH FALSE DATA (WHEN $\sum C^i_{rem} > D_{atk}$)

In this scenario it is considered that the actual demand on DN is same i.e. 150 kWh, however, if there is an attack on the system the false data communicated (D_{atk}) to EVs shows DN requirement as 50 kWh. As mentioned in Scenario I, EVs total

TABLE 3. Energy demand requirements with and without false data present in the system model.

Factors	Scenario I	Scenario II	Scenario III
Actual demand by DN (D_{dem})	150 kWh	150 kWh	100 kWh
Maximum energy EVs can provide ($\sum C^i_{rem}$)	130 kWh	130 kWh	130 kWh
False demand by attackers (D_{atk})	0 kWh	50 kWh	250 kWh
Amount of energy EV supplied (EV_{sup})	130 kWh	50 kWh	130 kWh
Energy left to be supplied (D_{left})	20 kWh power deficiency	100 kWh power deficiency	30 kWh surplus power

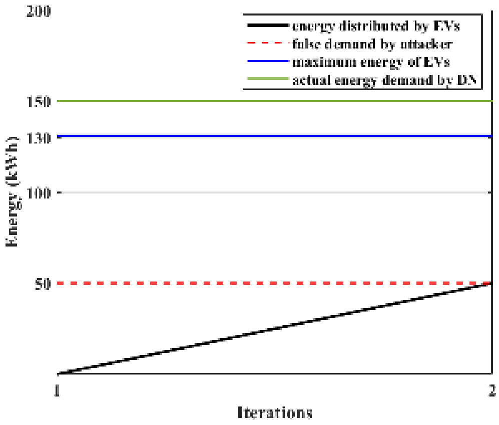

FIGURE 12. Energy demand requirements by DN with false data for scenario II.

energy available is 130 kWh which can easily satisfy the D_{atk} i.e. 50 kWh. EVs starts to feed the required power and satisfy the false requirements of DN. However, it can be seen that due to manipulated demand the requirement of DN remains unsatisfied as shown in Fig 12. This may give rise to the adversarial effect on the system which results in performance deterioration of the system and may consequently lead to a blackout.

3) SCENARIO III- COMMUNICATION BETWEEN EVs AND DN WITH FALSE DATA (WHEN $\sum C^i_{rem} < D_{atk}$)

Considering the operating scenario with D_{dem} from DN as 100 kWh and the false data communicated (D_{atk}) to EVs indicating DN requirement as 250 kWh. As the total power available by EVs is 130 kWh it would be obviously utilized to fulfill (false) grid requirement. It can be seen from Fig. 13 that the DN requirement of 100 kWh is satisfied, however, surplus power fed by EVs leads to over-compensation of DN which is responsible for frequency deviation and may result in synchronization issues.

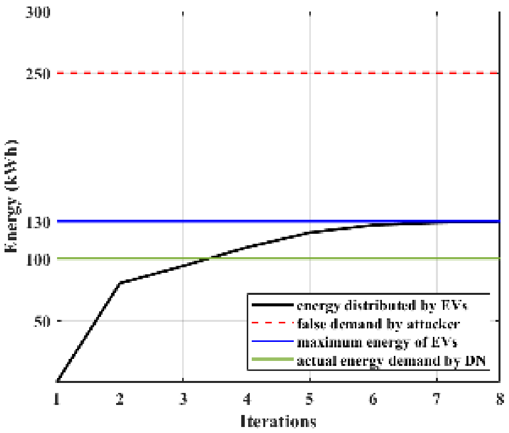

FIGURE 13. Energy demand requirements by DN with false data for scenario III.

With the introduction of the blockchain, this energy-related information exchange between DN and EVs is secured. However, the complexity of energy trading process will increase with the number of EVs. As each node data is stored with all the other nodes of the network, the peer with the least block execution time will become the leader node. The data exchanged between the two parties i.e the DN and EVs undergoes the process of encryption so as to form a block i.e. leader block. For this local block to be a part of chain validation, all the nodes of the network are queried and are double-checked through Byzantine based consensus as discussed in Section V. In the blockchain, the data is exchanged in encrypted form and each block is cryptographically connected to its previous block. It makes system computationally more strong. The attack in the presence of blockchain is difficult because the hacker needs to manipulate more than 33% of data which is a challenging calculation. This aspect of blockchain assures system security.

B. CASE 2: SECURING DIFFERENT NODES OF THE PROPOSED MODEL

Considering the N-node system and possible attacks at four different points in the proposed network system. As shown in Fig. 14 the attack can occur as follows,

i) Attack on sensor data/sender node
ii) Attack on Communication links
iii) Manipulation in the SCADA information
iv) Attack on actuators/receiver end

The IEEE 33 bus system consists of 33-nodes and 32 branches. It is assumed that the parking lot has 50 EVs parked at the time of energy trading. The total number of sensors in this networked system is calculated by considering the total number of sensors required for DN (n^{DN}_{sen}) as well as considering the total number of sensors required for EVs parking lot (n^{EV}_{sen}). While calculating (n^{DN}_{sen}) the following features are considered [44]: For reading parameters such as voltage, current, power etc. a sensor is placed at each node

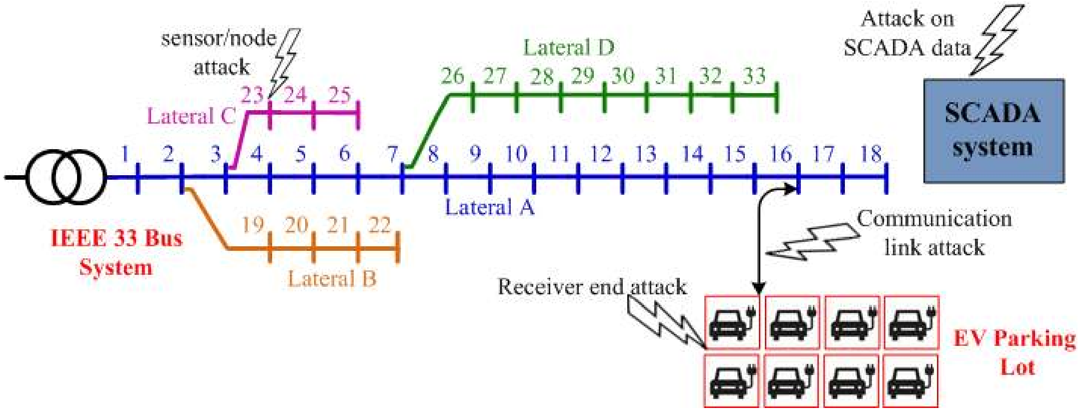

FIGURE 14. Attack on different nodes of P2P network.

(N_{DN}^{read}); for checking line status (open/close) each branch has a sensor (B_{DN}^{status}); and for reading parameters such as voltage, current, power etc. two sensors are placed at both ends of line (B_{DN}^{read}).

$$n_{sen}^{DN} = N_{DN}^{read} + B_{DN}^{status} + B_{DN}^{read} \quad (9)$$
$$n_{sen}^{DN} = 33 + 32 + (32 \times 2) \quad (10)$$

Similarly, while calculating (n_{sen}^{EV}) the following features are considered [44]: For reading parameters such as voltage, current, power etc. a sensor is placed at each node (N_{EV}^{read}); for checking communication links status (open/close) each links has a sensor (L_{EV}^{status}); and for reading parameters such as voltage, current, power etc. two sensors are placed at both ends of communication channels (L_{EV}^{read}).

$$n_{sen}^{EV} = N_{EV}^{read} + L_{EV}^{status} + L_{EV}^{read} \quad (11)$$
$$n_{sen}^{EV} = 50 + 1225 + (1225 \times 2) \quad (12)$$

Finally, the total number of sensors is given by,

$$n_{sen} = n_{sen}^{DN} + n_{sen}^{EV} = 3854 \quad (13)$$

The detail description of attack scenario for the system with and without security is explained in the preceding section.

1) SCENARIO I-ATTACK SCENARIO FOR THE SYSTEM WITH NO SECURITY

The possible attacks on system model without any protection system is illustrated in this scenario. In this case, hacking into a few data may lead to a successful attack. The probabilities of attack at each point are as follows,

(i) Tampering on sensors data information or physically manipulating the sensor nodes. The probability of attacker to hack into n_{sen} sensors is denoted by P_{SA}, wherein α_i is the probability of attack each sensor $(0 \leq \alpha_i \leq 1)$, $i = (1, 2, \ldots, n_{sen}, ..N)$.

$$P_{SA} = \frac{1}{S}\prod_{i=1}^{n_{sen}} \alpha_i \quad (14)$$

where S is the number of sample size

(ii) Attack on communication links, considering n_{sen} sensors to be linked with communication channels, the probability of attack to replace the data packages on communication links given by β_i and denoted by P_{CA}, wherein $(0 \leq \beta_i \leq 1)$, $i = (1, 2, \ldots, n_{sen}, ..N)$.

$$P_{CA} = \frac{1}{S}\prod_{i=1}^{n_{sen}} \beta_i \quad (15)$$

(iii) The information disclosure attack on the SCADA system, where the network provides many redundant data since during certain period of time all registered sensors in the network have a collection of all measured nodes data. Let the probability of an attack on SCADA system information be P_{SCADA}, with the range [0.01, 0.05] [44].

(iv) The attack at the receiver end where idle EVs are parked in the parking lot. The attacker may manipulate the action of actuators. Let the probability of an attack on receiving end denoted by P_R, with the range [0.01, 0.05] [44].

Let the overall probability for an attacker to attack the system be P_{TA}, which is the sum of all possibilities of attack at four different points of the system. It is assumed that for an attacker to manipulate any information (control center information excluded) the attacking probability is equal and selected to be x i.e. $\alpha_i = \beta_i = x$. The value of x lies in the range of 0.9 to 0.999, which indicates the proposed system to be exposed to the highest vulnerabilities. Then, the overall success probability P_{TA} of this attack launch without the inclusion of blockchain can be calculated as:

$$P_{TA} = \frac{1}{4}(\prod_{i=1}^{n_{sen}} \alpha_i + \prod_{i=1}^{n_{sen}} \beta_i + P_{SCADA} + P_R) \quad (16)$$
$$= \frac{1}{4}(2x^{n_{sen}} + 0.01 + 0.01)$$

The success probability of attacks without any security application is represented in Fig.15.

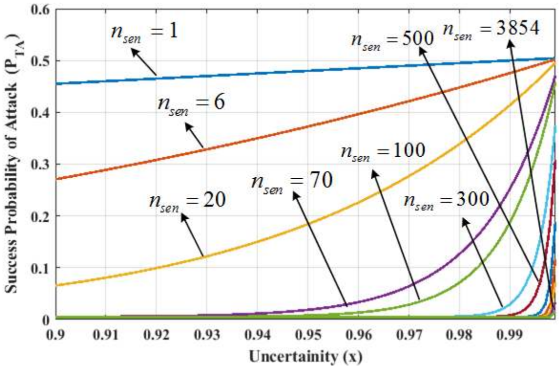

FIGURE 15. The success probability of attack without inclusion of blockchain.

2) SCENARIO II-ATTACK SCENARIO FOR THE SYSTEM WITH THE INCLUSION OF BLOCKCHAIN

The attack possibilities in presence of blockchain are formulated in order to mitigate the attacks on the network. In this scenario, the attacker needs to steal n_{sen} corresponding key information so as to hash the data used in data transmission and data verification. Thus, leading to an increase in the number of information to be manipulated for an attacker to intrude into the system. Stealing this n_{sen} key information is difficult because it takes large computational time and the Byzantine condition of hacking more than 33% data is proven to be challenging to accomplish. Considering the same possible attack points as in Section VI-B1 with n_{sen} key data to be hacked in each point of attack.

(i) When there is an attack on sensors the attacker has to hack into n_{sen} sensors data as well as has to steal n_{sen} key information such as hash values, public key or private key so as to hash the data. The probability of stealing n_{sen} key information is γ_i, wherein $(0 \leq \gamma_i \leq 1)$. Let the probability of launching this attack be,

$$P_{SA_b} = \frac{1}{S}(\prod_{i=1}^{n_{sen}} \alpha_i \times \prod_{i=1}^{n_{sen}} \gamma_i) \tag{17}$$

(ii) The second situation where the probability of an attack to replace the data when data is transmitting from one node to other nodes. Let the number of communication channels be $k = n_{sen}(n_{sen}-1)/2$, the attack probability of hacking into k communication channels denoted by P_{CA_b}. As known, for any attacker to intrude into the system which is secured by blockchain, it has to hack at least 33% information. Therefore, $k_1 = k \times 33\%$ has to be attacked for success and also n_{sen} key information to be attacked.

$$P_{CA_b} = \frac{1}{S}(\prod_{i=1}^{k_i} \beta_i \times \prod_{i=1}^{n_{sen}} \gamma_i) \tag{18}$$

(iii) The attack on SCADA leads to manipulated information as explained in Section VI-B1. The probability of attack is given as P_{SCADA_b}, with the range [0.01, 0.05] [44] and also with n_{sen} corresponding key data to manipulate. Thus, the attack probability on SCADA is given as,

$$P_{SCADA_b} = \frac{1}{S}(P_{SCADA} \times \prod_{i=1}^{n_{sen}} \gamma_i) \tag{19}$$

(iv) The probability of attack at the receiver end, that is after completion of data verification process, the attacker needs to hack into majority of the nodes, that is $k_2 = n_{sen} \times 33\%$, to reach on false consensus. Therefore, the attack probability is given as,

$$P_{R_b} = \frac{1}{S}(\prod_{i=1}^{k_2} P_{R_i} \times \prod_{i=1}^{n_{sen}} \gamma_i) \tag{20}$$

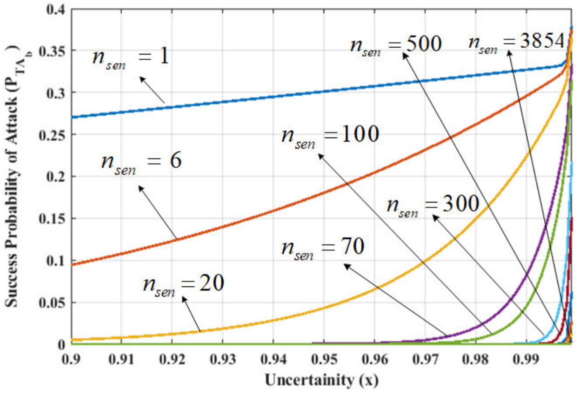

FIGURE 16. The success probability of attack with the inclusion of blockchain.

The overall success probability of an attack is represented as, P_{TA_b}. It is assumed that for an attacker to manipulate any information (control center information excluded) the attacking probability is equal and selected to be x i.e. $\alpha_i = \beta_i = \gamma_i = P_{R_i} = x$. The value of x lies in the range of 0.9 to 0.999, which indicates the proposed system to be exposed to highest vulnerabilities. Therefore for launching the attack in scenario B is calculated as,

$$P_{TA_b} = \frac{1}{4}[\underbrace{(\prod_{i=1}^{n_{sen}} \alpha_i \times \prod_{i=1}^{n_{sen}} \gamma_i)}_{P_{SA_b}} + \underbrace{(\prod_{i=1}^{k_1} \beta_i \times \prod_{i=1}^{n_{sen}} \gamma_i)}_{P_{CA_b}}$$
$$+ \underbrace{(\prod_{i=1}^{k_2} P_{R_i} \times \prod_{i=1}^{n_{sen}} \gamma_i)}_{P_{R_b}} + \underbrace{(P_{SCADA_b} \times \prod_{i=1}^{n_{sen}} \gamma_i)}_{P_{SCADA_b}}] \tag{21}$$

$$P_{TA_b} = \frac{1}{4}x^{n_{sen}}[x^{n_{sen}} + x^{3786613} + x^{1966} + P_{SCADA_b}] \tag{22}$$

In Fig. 16 the success probability of attack with the inclusion of blockchain is demonstrated, where the success rate of attacks is considerably reduced.

In Fig. 15 the success probability of attack is high as compared to Fig. 16. It is known that, the lesser the number of sensors, more is the probability of attack. Similarly, as the number of sensors increases the success probability of attack

TABLE 4. Possible system attacks and their success probabilities.

Possible attack points	Success probability of attack	
	System without security	System with security
Sensor attack	$\frac{1}{S}\prod_{i=1}^{n_{sen}} \alpha_i$	$\frac{1}{S}(\prod_{i=1}^{n_{sen}} \alpha_i \times \prod_{i=1}^{n_{sen}} \gamma_i)$
Communication Links	$\frac{1}{S}\prod_{i=1}^{n_{sen}} \beta_i$	$\frac{1}{S}(\prod_{i=1}^{k_1} \beta_i \times \prod_{i=1}^{n_{sen}} \gamma_i)$
SCADA	$\frac{1}{S}P_{SCADA}$	$\frac{1}{S}(\prod_{i=1}^{n_{sen}} \gamma_i \times P_{SCADA_b})$
At receivers end	$\frac{1}{S}P_{R_i}$	$\frac{1}{S}(\prod_{i=1}^{k_2} P_{R_i} \times \prod_{i=1}^{n_{sen}} \gamma_i)$

TABLE 5. Comparative analysis of proposed scheme with existing approaches.

References	Consensus	Hash Algorithm	Application
Survivor [30]	PoW	SHA 256	Energy Trading (EV and CS)
Best [31]	PoW	SHA 1	Smart Transportation
Energychain [32]	PoW	SHA 1	Smart Homes
Proposed	BFT	SHA 256	Energy Trading (EV and DN)

TABLE 6. Comparison of hash algorithm.

Parameters	SHA 1	SHA 256
Encryption		480 ms
Power Consumption (Wh)	17.5	14.8
Latency (ms)	60	62
Prone to attack	Yes	Secure
Size of hash value	160	256
Complexity of the best attack	2^{80}	2^{128}
Message size	$<2^{64}$	$<2^{64}$
Message block size	512	512
Word size	32	32
Number of words	5	8
Number of digest rounds	80	64
Number of constants	4	64

is relatively decreased. However, in case of attack scenario for the system with no security, even though with high number of sensors the chance of data manipulation is high in the range of low uncertainty. As seen from Fig. 16 with the inclusion of blockchain the success probability of attack is comparatively low and it is more reliable with an increased number of sensors or nodes in the network. The success probability of an attack with and without the inclusion of blockchain is summarized in Table 4. It may be claimed that the success probability of attack is approximately half with the inclusion of blockchain as shown in Fig. 16 as compared to Fig. 15. The range of x is selected between 0.9 and 0.999 in the representative case study is very high which implies that the energy trading process is completely prone to attacks.

C. OBSERVATIONS/COMPARISON WITH EXISTING METHODS

A comparative analysis of the proposed scheme with existing approaches is given in Table 5. It can be seen from the Table 5 that authors of [31] and [32] employs SHA 1 algorithm for a hash process whereas the authors of [30] and the proposed scheme utilized SHA 256 algorithm for the hash process. The advantage of using the SHA 256 algorithm over SHA 1 algorithm is given in Table 6. As seen from Table 6 SHA 256 algorithm is more secure as compared to SHA 1 algorithm when there is an attack on the system also the power consumed for SHA 256 algorithm is 14.8 *Wh* whereas for SHA 1 it is 17.5 *Wh*. Thus with the help of Table 6 it can be concluded that the SHA 256 algorithm employed in the proposed scheme is more efficient as compared to SHA 1.

The next important feature of the proposed scheme is that it employs Byzantine consensus for energy trading application as compared to literature [30]–[32]. The advantages of BFT consensus over PoW are as follows:

1) IDENTITY MANAGEMENT OF NODES

The key feature of PoW is that the node identity management is entirely decentralized, where any nodes can participate without permission. In contrast, the Byzantine consensus is entirely centralized where each participating node is issued a cryptographic as well as identity certificate with the help of a trusted party. This results in an overall improvement in the safety of Byzantine consensus as only "permissioned" nodes are allowed to participate in the consensus process.

2) CONSENSUS FINALITY

The consensus finality has a property that once the block is appended to the blockchain at some time instant, by a valid block, will never be removed from the chain. In PoW the block frequency is regulated to avoid the block collisions known as a randomized concurrency control mechanism. With concurrency control, the block generation takes some time and collisions do happen, eventually leading to temporary splits (forks) on the blockchain. The presence of these temporary splits results into no consensus finality, the absence of consensus finality introduces the latency in the transaction process. Thus the PoW does not satisfy the consensus finality. In contrast, the consensus finality is satisfied by BFT where the protocols are built upon consensus.

3) SCALABILITY

The scalability of both PoW and BFT based blockchain in terms of number of clients is scale well and provide support to thousands of clients.

TABLE 7. Comparison of PoW and Byzantine based consensus.

Parameters	PoW consensus	BFT consensus
Identity management of nodes	Decentralized, Open	IDs of all other nodes should be known to existing nodes, Permissioned
Consensus finality	No (presence of temporary forks)	Yes
Scalability (number of clients)	Excellent (thousands of clients)	Excellent (thousands of clients)
Performance (throughput)	Limited (presence of temporary forks)	Excellent (transactions rates in tens of thousands)
Performance (latency)	High latency (confirmations of multi-block)	Excellent (equals to network latency)
Power consumption	Very poor (energy is wasted by PoW)	Good
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g. for block validity)	None for consensus safety (synchrony needed for liveness)
Correctness proofs	No	Yes

4) PERFORMANCE

The block frequency and block size are the two most important parameters for analyzing the performance of a PoW blockchain. The increase in block size for boosting the throughput results in an increase of latency because larger blocks lead to propagation delay across the Internet. These longer delays may lead to security issues because with longer delays there is an increase in the number of forks and also the possibility of attacks increases. Even with the increase of block frequency for reducing the latency results in similar security challenges. However, in case of BFT protocols as prototypes and also practical systems can support transactions in range of tens of thousands with latencies equal to network-speed [49]–[52].

5) ADVERSARY

The important features of PoW blockchain is how much computational (hash) power can be controlled by an adversary. In the initial phase of Bitcoin, it was assumed that if less than 50% of hash power is controlled by adversary than it remains invulnerable. However, years later it was claimed by [53] that Bitcoin is vulnerable even if 25% of hash power is controlled by an adversary. In contradictory BFT can tolerate at the most corrupted nodes whose value is equal to $1/3$ nodes. For this condition to remain true the network should be fully asynchronous on a timely basis.

TABLE 8. Symbols and abbreviations description.

Notation	Description
BFT	Byzantine fault tolerance
BGP	Byzantine general problem
B_{DN}^{Status}	Number of sensor for detecting status of line
B_{DN}^{read}	Number of sensor for reading line data
CS	Charging Station
C_F	Total full charge of EVs
C_{rem}^{i}	Charge left after excluding SOC_{reach}^{i}
C_{rem}^{r}	Minimum charge EVs can provide
DN	Distribution Network
D_{dem}	Demand from DN
D_{left}	Energy left to be supplied after E_{sup}
D_{atk}	False data communicated to EVs by the attackers
d_{EV}^{i}	Distance from parking lot to next charging point
EV	Electric Vehicle
EV_n	Number of EVs in the parking lot
EV_p	Number of EVs participating in the energy trading
E^i	Amount of energy needed from each EV
E_{sup}	Energy supplied by participating EVs
G2V	Grid to vehicle
ICT	Information and communications technology
k	Number of communication channels
L_{EV}^{status}	Number of sensor for detecting status of links
L_{EV}^{read}	Number of sensor for reading link data
N	Total number of nodes in an IEEE bus system
n_{sen}	Number of sensors to be manipulated
n_{sen}^{DN}	Number of sensors in DN
n_{sen}^{EV}	Number of sensors in EVs parking lot
N_{DN}^{read}	Number of sensors at each node of DN
N_{EV}^{read}	Number of sensors at each node of EVs parking lot
P2P	Peer-to-peer
PoW	Proof-of-Work
PV	Photo-voltaic

6) NETWORK SYNCHRONY

A timestamp plays an important role in Bitcoin, where the block is acceptable only if it's timestamp is greater than the

TABLE 8. ***(Continued)*** **Symbols and abbreviations description.**

Notation	Description
P_{SA}	Probability of attacker to hack into n_{sen} sensors
P_{CA}	Attack probability of replacing data packages on communication links
P_{SCADA}	Probability of attack on SCADA system
P_R	Attack probability on the receiver side
P_{TA}	Total probability of attack on the overall system
P_{SA_b}	Attack probability of key information from each sensor
P_{CA_b}	Attack probability of hacking into k channels
P_{SCADA_b}	Probability of attack on SCADA system with inclusion of blockchain
P_{R_b}	Attack probability on the receiver side with inclusion of blockchain
P_{TA_b}	Total probability of attack on the overall system with inclusion of blockchain
QoS	Quality of service
RES	Renewable energy sources
S	The number of sample size
SOC_{km}^{i}	State of charge required per km
SOC_{reach}^{i}	SOC need from parking lot to the destination
SOC_{init}^{i}	Initial state of charge of i^{th} PEV
SDN	Software-defined networking
SCADA	Supervisory control and data acquisition system
V2G	Vehicle to grid
α_i	Probability of attack on each sensor
β_i	Probability of attack on communication links
γ_i	Probability of stealing n_{sen} key information

median of the last 11 blocks. However, timestamp involves the major role to calculate mining difficulty and for maintaining block frequency. Therefore, to maintain the liveness loose synchrony is needed. On another hand, in the BFT the physical clock for consensus is obsolete. In this, the consensus is difficult to achieve in the presence of a faulty node in an asynchronous system.

The advantages of BFT consensus over PoW are summarized in Table 7.

VII. CONCLUSION

In this paper, a Byzantine based blockchain consensus framework for the enhancement of data security of the energy trading process between EVs and DN is proposed. The system first formulates the energy trading process in terms of BGP and then blockchain is applied to the system for securing the trading process. The effectiveness of blockchain is investigated in two cases with different operating scenarios. In the first one, the energy and information exchange process between EVs and DN is secured and in the other different nodes of the system are secured. The representative case study conducted on IEEE 33 bus system confirms the system security; as for successful attack, 33% of information is to be manipulated in BGP. It is claimed from results that the success probability of an attack on the system reduces with the application of Byzantine based blockchain consensus framework. In future research, refinement in consensus algorithm will be considered and assessment of performance with additional physical constraints of DN and EVs will be evaluated.

APPENDIX

See Table 8.

REFERENCES

[1] T. Baumeister, "Literature review on smart grid cyber security," Collaborative Softw. Develop. Lab. at Univ. Hawaii, Honolulu, HI, USA, Tech. Rep., 2010.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[4] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[5] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[6] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[7] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tinshhua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, Apr. 2014.

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[9] W. Bower, S. Kuszmaul, S. Gonzalez, and A. Akhil, "Solar energy grid integration systems (SEGIS) proactive intelligent advances for photovotaic systems," in *Proc. 35th IEEE Photovoltaic Spec. Conf.*, Jun. 2010, pp. 523–528.

[10] J. D. Dogger, B. Roossien, and F. D. J. Nieuwenhout, "Characterization of li–ion batteries for intelligent management of distributed grid–connected storage," *IEEE Trans. Energy Convers.*, vol. 26, no. 1, pp. 256–263, Mar. 2011.

[11] W. Kempton and J. Tomić, "Vehicle-to-grid power implementation: From stabilizing the grid to supporting large-scale renewable energy," *J. Power Sour.*, vol. 144, no. 1, pp. 280–294, Jun. 2005.

[12] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, Nov. 2009.

[13] E. Sortomme and M. A. El-Sharkawi, "Optimal scheduling of vehicle-to-grid energy and ancillary services," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 351–359, Mar. 2012.

[14] E. Keane and D. Flynn, "Potential for electric vehicles to provide power system reserve," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–7.

[15] A. K. Srivastava, B. Annabathina, and S. Kamalasadan, "The challenges and policy options for integrating plug-in hybrid electric vehicle into the electric grid," *Electr. J.*, vol. 23, no. 3, pp. 83–91, Apr. 2010.

[16] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug–in hybrid electric vehicles on a residential distribution grid," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 371–380, Feb. 2010.

[17] C. Wu, H. Mohsenian-Rad, and J. Huang, "Vehicle-to-aggregator interaction game," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 434–442, Mar. 2012.

[18] W. Saad, Z. Han, H. V. Poor, and T. Basar, "A noncooperative game for double auction-based energy trading between PHEVs and distribution grids," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 267–272.

[19] J. Xu and V. W. Wong, "An approximate dynamic programming approach for coordinated charging control at vehicle-to-grid aggregator," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 279–284.

[20] W. Shi and V. W. Wong, "Real-time vehicle-to-grid control algorithm under price uncertainty," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 261–266.

[21] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 8, no. 3, pp. 33–44, 2016.

[22] J. Matamoros, D. Gregoratti, and M. Dohler, "Microgrids energy trading in islanding mode," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 49–54.

[23] K. Zhang, Y. Mao, S. Leng, S. Maharjan, Y. Zhang, A. Vinel, and M. Jonsson, "Incentive–driven energy trading in the smart grid," *IEEE Access*, vol. 4, pp. 1243–1257, 2016.

[24] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[25] Z. Zhou, L. Tan, and G. Xu, "Blockchain and edge computing based vehicle-to-grid energy trading in energy Internet," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI)*, Oct. 2018, pp. 1–5.

[26] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain–based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[27] U. Asfia, V. Kamuni, A. Sheikh, S. Wagh, and D. Patel, "Energy trading of electric vehicles using blockchain and smart contracts," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 3958–3963.

[28] U. Asfia, V. Kamuni, S. Sutavani, A. Sheikh, S. Wagh, and N. M. Singh, "A blockchain construct for energy trading against sybil attacks," in *Proc. 27th Medit. Conf. Control Autom. (MED)*, Jul. 2019, pp. 422–427.

[29] V. Kamuni, U. Asfia, S. Sutavani, A. Sheikh, and D. Patel, "Secure energy market against cyber attacks using blockchain," in *Proc. 6th Int. Conf. Control, Decis. Inf. Technol. (CoDIT)*, Apr. 2019, pp. 1792–1797.

[30] A. Jindal, G. S. Aujla, and N. Kumar, "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Comput. Netw.*, vol. 153, pp. 36–48, Apr. 2019.

[31] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K.-R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, Aug. 2019.

[32] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. 1st ACM MobiHoc Workshop Netw. Cybersecur. Smart Cities*, 2018, p. 1.

[33] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[34] D. Durgvanshi, B. P. Singh, and M. M. Gore, "Byzantine fault tolerance for real time price in hierarchical smart grid communication infrastructure," in *Proc. IEEE 7th Power India Int. Conf. (PIICON)*, Nov. 2016, pp. 1–6.

[35] Y. Wang, F. Luo, Z. Dong, Z. Tong, and Y. Qiao, "Distributed meter data aggregation framework based on blockchain and homomorphic encryption," *IET Cyber Phys. Syst., Theory Appl.*, vol. 4, no. 1, pp. 30–37, Mar. 2019.

[36] W. Zhao and F. E. Villaseca, "Byzantine fault tolerance for electric power grid monitoring and control," in *Proc. Int. Conf. Embedded Softw. Syst.*, 2008, pp. 129–135.

[37] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain–based byzantine consensus algorithm for information authentication of the Internet of vehicles," *IEEE Access*, vol. 7, pp. 139703–139711, 2019.

[38] M. A. Ferrag and L. Maglaras, "Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, to be published.

[39] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi–signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[40] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[41] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[42] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, May 2018.

[43] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[44] 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 Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[45] I. Bashir, *Mastering Blockchain*. Birmingham, U.K.: Packt, 2017.

[46] S. Hua, E. Zhou, B. Pi, J. Sun, Y. Nomura, and H. Kurihara, "Apply blockchain technology to electric vehicle battery refueling," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018.

[47] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, Jan. 2018.

[48] D. Q. Hung, N. Mithulananthan, and K. Y. Lee, "Determining PV penetration for distribution systems with time–varying load models," *IEEE Trans. Power Syst.*, vol. 29, no. 6, pp. 3048–3057, Nov. 2014.

[49] R. Kotla, A. Clement, E. Wong, L. Alvisi, and M. Dahlin, "Zyzzyva: Speculative byzantine fault tolerance," *Commun. ACM*, vol. 51, no. 11, p. 86, Nov. 2008.

[50] A. Clement, E. L. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making Byzantine fault tolerant systems tolerate Byzantine faults," in *Proc. NSDI*, vol. 9, 2009, pp. 153–168.

[51] R. Guerraoui, "The next 700 BFT protocols," in *Proc. 5th Eur. Conf. Comput. Syst.*, 2008, pp. 363–376.

[52] A. Bessani, J. Sousa, and E. E. Alchieri, "State machine replication for the masses with BFT-SMART," in *Proc. 44th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun. 2014, pp. 355–362.

[53] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.

A. SHEIKH received the B.E. degree in electrical engineering and the M.E. degree in power systems from Mumbai University, India, in 2013 and 2017, respectively. He is currently pursuing the Ph.D. degree in electrical engineering from the Veermata Jijabai Technological Institute, Mumbai, India. His current research interests include blockchain, electric vehicles, smart buildings, and cyber security.

V. KAMUNI received the B.E. degree in instrumentation engineering from Mumbai University, India, in 2016. She is currently pursuing the M.Tech. degree in electrical engineering (specialization in control systems) with the Veermata Jijabai Technological Institute, Mumbai, India. Her current research interests include blockchain, electric vehicles, and cyber physical systems.

A. UROOJ received the B.E. degree in instrumentation engineering from Mumbai University, India, in 2016. She is currently pursuing the M.Tech. degree in electrical engineering (specialization in control systems) with the Veermata Jijabai Technological Institute, Mumbai, India. Her current research interests include blockchain, electric vehicles, cyber physical systems, and security.

S. WAGH (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from The University of Western Australia, Perth, WA, Australia, in 2012. From 2015 to 2016, she was a Visiting Scholar with Tufts University, Medford, MA, USA. She is currently an Assistant Professor with the Veermata Jijabai Technological Institute, Mumbai, India. Her current research interests include power system dynamics, stability and control, and smart grid.

N. SINGH received the Ph.D. degree in electrical engineering from IIT Bombay, Mumbai, India, in 1990. He is currently an Adjunct Professor with the Veermata Jijabai Technological Institute, Mumbai. His current research interests include geometric control theory, complex networks, and stochastic control.

DHIREN PATEL currently heads the Veermata Jijabai Technological Institute, Mumbai, India. He is a Professor of computer engineering, where he is involving in cyber security, blockchain, the IoT, and AI for Global Good. He leads the Blockchain Research Group, Veermata Jijabai Technological Institute, Mumbai.