Accepted Manuscript

BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System

Rajat Chaudhary, Anish Jindal, Gagangeet Singh Aujla, Shubhani Aggarwal, Neeraj Kumar, Kim-Kwang Raymond Choo

PII: S0167-4048(18)31201-X
DOI: https://doi.org/10.1016/j.cose.2019.05.006
Reference: COSE 1529

To appear in: *Computers & Security*

Received date: 23 October 2018
Revised date: 30 March 2019
Accepted date: 10 May 2019

Please cite this article as: Rajat Chaudhary, Anish Jindal, Gagangeet Singh Aujla, Shubhani Aggarwal, Neeraj Kumar, Kim-Kwang Raymond Choo, BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.05.006

Highlights

- Blockchain-based secure energy trading in intelligent transportation system
- SDN- and blockchain-based secure energy trading
- Distributed secure system for authenticating and validating participating EVs

BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System

Rajat Chaudhary[a], Anish Jindal[b], Gagangeet Singh Aujla[c], Shubhani Aggarwal[a], Neeraj Kumar[a], Kim-Kwang Raymond Choo[d,e]

[a] *Computer Science and Engineering Department, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India*
[b] *School of Computing and Communications, Lancaster University, Lancaster, UK*
[c] *Computer Science and Engineering Department, Chandigarh University, Mohali (India)*
[d] *Department of Information Systems and Cyber Security and Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249, USA*
[e] *School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5095, Australia*

Abstract

Tactile Internet is a fairly recent technological tren associated with the Internet-of-Things (IoT) era, with potential applications in a broad range of industrial, societal and business use cases. The real-time machine-to-machine and human-to-machine interactions (e.g., in unmanned vehicles and the underpinning infrastructure within the smart city ecosystem) in the intelligent transportation sector, for example, contribute to the potential utility of Tactile Internet in this particular sector (and the broader smart city). In the context of unmanned vehicles, such as unmanned aerial vehicles and electric (ground) vehicles, one of several key challenges to its broader utility is how to design a secure energy trading ecosystem that can be used for purposes such as charging and discharging from the supporting smart grids. Most existing approaches in the literature focused on conventional and centralized security mechanisms, which may not be applicable for energy trading in a smart city environment. Moreover, the need for real-time processing for energy trading computation is one of the essential requirements of Tactile Internet. Therefore, to address these challenges, *BEST*: a Blockchain-based secure energy trading scheme for electric vehicles (EVs) is proposed in this paper. Specifi-

Email address: raymond.choo@fulbrightmail.org (Kim-Kwang Raymond Choo)

cally, in *BEST*, blockchain is used to validate EVs' requests in a distributed manner; thus, ensuring resilience against the single point of failure. The miner nodes are selected to validate the requests on the basis of energy requirements, time of stay, dynamic pricing, and connectivity record, as well as other factors that are crucial for the operator at the time of operation. Moreover, to provide low latency and real-time services, software-defined networking is used as the network's backbone to transfer EVs' requests to a global software defined network controller. Finally, *BEST* is evaluated on the basis of the communication and computation costs incurred during various transactions between the EVs and the smart grid. A case study is also provided to demonstrate the potential deployment of *BEST* in energy trading.

Keywords: Blockchain, energy trading, software-defined networking, intelligent transportation system, smart city, smart nation, tactile Internet, 5G.

1. Introduction

Tactile Internet has many industrial, societal and business use cases, such as intelligent transportation systems (ITS) and the broader smart city (e.g., Texas Innovation Alliance[1] or smart nation[2]. In such a setting, smart and electric vehicles (including unmanned aerial and ground vehicles) are equipped with sensors to sense the real-time data about their surroundings and different communication technologies (e.g., bluetooth, WiFi, and 5G) to transmit the sensed data to an external source for further processing. Moreover, the in-built communication technologies allow the vehicles to interact with each other and share information (e.g., with the other infrastructure within the smart city / nation); thus, facilitating collaborative decision-making since tactile Internet enables real-time human to machine interactions on the move within a specific range [1].

One key benefit of using electric vehicles (EV) is reducing carbon emissions / footprints [2, 3, 4]; hence, its increasing popularity in our society. For example, a survey by Global EV outlook estimated that 20 million EVs will be on our road by the end of 2020 [5]. In other words, these EVs will

[1] `http://txinnovationalliance.org/`, last accessed Mar 30, 2019.
[2] `https://www.smartnation.sg/`, last accessed Mar 30, 2019.

potentially form a large networks of vehicles on the road, connected via the Internet or other available technologies (e.g., 5G). EVs can use the available information and communication technologies (ICT) to share energy (and other) information among themselves or with the service provider / utility, in order to make and optimize energy trading decisions for better management of their battery / energy. The information from the EVs to the utility and *vice-versa*, clearly, needs to be secured, so that both EVs and utility can trust the information used in energy trading decision-making. However, if there is a financially-motivated attacker in the network who can modify the pricing information or the energy requests, then there are potential security and privacy implications as well as financial and legal consequences (e.g., due to grid breakdown and fatalities).

While there are a number of conventional security solutions such as centralized key management scheme, a key limitation in many of these solutions is the single point of failure, where the trusted gateway can be targeted and successfully compromised by the attacker, including a malicious insider [6, 7]. To address these challenges, we posit the potential of a decentralized secure energy trading scheme in software defined networking (SDN)-enabled ITS. The benefits of the blockchain technology (e.g., low transaction costs, faster transactions, transparency, and immutability) have attracted attention from researchers in different domains and for different applications [8, 9, 10, 11, 12, 13, 14]. Blockchain provides a transparent solution, where any changes to the blockchain or the transaction received in the public wallet address are globally displayed by all communication parties. Such changes are immutable in nature, which means that the transactions cannot be deleted or changed. However, there are a number of challenges in the distributed system, such as the significant communication overheads incurred during transaction synchronization. The inconsistency of state synchronization arises because of frequent transactions among peer-to-peer (P2P) nodes. To address such challenges, a SDN framework is suitable as it can facilitate efficient resource distribution and its logically centralized architecture helps to maintain global consistency of transaction synchronization among all the authorized nodes. The SDN architecture also overcomes redundancy as the global controller performs transactions once only, rather than the same transaction been processed independently by each node.

1.1. Contribution

The key contribution of this paper is our proposed blockchain-based technique for secure energy trading for EVs or to the utilities, *BEST*. To minimize network latency and improve the quality of service (QoS) in this network, a SDN architecture is used in the proposed scheme. The advantage of using SDN-enabled network over conventional TCP/IP is that SDN is autonomous and allows the complete network topology to be managed efficiently and dynamically [15]. A summary of our proposed approach in this paper is as follows:

- The design of a SDN-based vehicular networking architecture to transfer energy trading requests from EVs to the global controller, and *vice-versa* for improving QoS in the network.
- The design of a miner node selection algorithm, based on vehicle mobility, the energy requirement of EVs, time of stay, and energy pricing (and in the future, any other factors deem necessary by the service provider).
- The design of a secure blockchain technique to facilitate energy trading in the ITS, allowing EVs to trade among themselves or with the utility.

1.2. Related Work

A number of solutions have been proposed in the literature to address transaction security and to achieve privacy protection for EVs deployment in ITS. For instance, Roberts *et al.* [16] proposed an authentication framework for authorizing EVs to charge the required amount of energy from the charging stations. The proposed scheme uses a key-exchange protocol to perform secure energy trading using a peer-to-peer connection via Wi-Fi or Bluetooth among EVs, however without using digital certificates. Specifically, the participating EVs send a random challenge to each other in plaintext, as well as in hashed form, using a shared secret key. The receiving EV re-computes the hashed value of the plaintext using the secret key and if both hash values match, then the EVs are successfully authenticated. Shen *et al.* [17] also proposed a lightweight key agreement protocol for vehicle-to-grid (V2G) environment to carry out mutual authentication, without disclosing the real identity of the participating users. The authors only used bit-wise exclusive OR operations and hash values to make their scheme lightweight. In another work, Han and Xiao [18] surveyed existing privacy preservation techniques in

V2G environment and presented a number of research challenges. Saxena *et al.* [19] also discussed a number of open challenges and issues related to network security and privacy preservation in the smart V2G environment. To solve these challenges, the authors proposed a V2G network security architecture for authentication, confidentiality, and integrity. However, the drawback of this scheme is that all transaction decisions are made by the centralized control center, authentication server and trusted server; thus suffering from a single point of failure.

This necessitates the design of a distributed security system, in order to authenticate and validate participating EVs without relying on any single centralized entity. Hence, as previously discussed in this paper, we posit the potential of blockchain in such an application. In addition to its success in cryptocurrency transactions such as Bitcoin [20], blockchain has been used in many other applications, ranging from dataset sharing to authentication, and so on [21, 22, 23, 10, 24, 25]. For example, in the context of this paper, blockchain contracts deployed in a smart grid (SG) can remove the reliance on some trusted third party to facilitate energy-related transactions, as well as improving the resilience of the system against cyber attacks [26].

There have also been attempts to introduce blockchain in a smart city environment. For example, a blockchain-based conceptual framework was proposed in [27] to facilitate interactions between humans, technology, and organizations by providing a secure way of information sharing. A distributed blockchain mechanism in the smart vehicular environment to preserve the privacy of the users was also proposed in [28]. Dynamic public keys were used to ensure user privacy; however, these keys may put an additional burden on the capacity and computation requirements of the vehicles. Yuan and Wang [29] identified a number of challenges in blockchain-based ITS-based framework. To address such challenges, Lei *et al.* [30] proposed a blockchain-based mechanism for key-sharing among security managers in a decentralized network. Sharma *et al.* [31] proposed a distributed framework based on the blockchain technology for a specific case of automotive technology in a smart city. The authors designed a minor node selection scheme and evaluated it on the Ethereum platform. Jindal *et al.* [32] designed a blockchain-based framework to support secure energy trading in a vehicle-to-grid setting. More recently in 2019, Zhang *et al.* [13] also explained how blockchain can be used to facilitate data sharing in a smart city environment. Specifically, they proposed a method using both fair blind signatures and threshold secret sharing to realize conditional privacy in participating vehicles, and designed

a reward mechanism to incentivize the participating vehicles to broadcast announcement messages and maintain the blockchain(s).

1.3. Layout

In Section 2, we present the SDN-based vehicular networking architecture. Sections 3 and 4 present the proposed blockchain-based secure energy trading scheme and its security and performance evaluations. Finally, the paper is concluded in Section 5.

2. Software Defined Vehicular Networking Architecture

To deal with network latency and ensure security when receiving and responding to requests from highly mobile vehicles in the ITS environment, SDN is used in our approach, since SDN can provide flexibility for applying various rules to facilitate network management [33]. Another reason that contributes to the popularity of SDN in supporting networking services in various application domains is because it separates the control and data planes. In other words, SDN provides users the flexibility to build an efficient control system with logical centralization of the network intelligence at the control plane [34, 35, 36]. Our proposed SDN architecture is presented in Fig. 1, which has a layered top-down structure and divided into three planes (i.e., application, control, and data planes).

- *Application Plane* is the uppermost layer in the SDN architecture, which is responsible for providing a set of services and applications to the end users. These services and applications are developed by a third-party, and are executed remotely and concurrently at the application plane of the SDN. These applications include mobility, routing, traffic engineering, network virtualization, network topology, and security.

- *Control Plane* is the second layer and comprises the software platform that represents the centralized core of the overall network intelligence. The SDN controller software is installed in the network operating system (NOS) responsible for making decisions regarding the global network topology. The global network policies are implemented and modified in this plane, which maintains a global database of node placement, information about the requests, and data flow path in the entire network. Moreover, using hypervisor, the control plane creates virtual

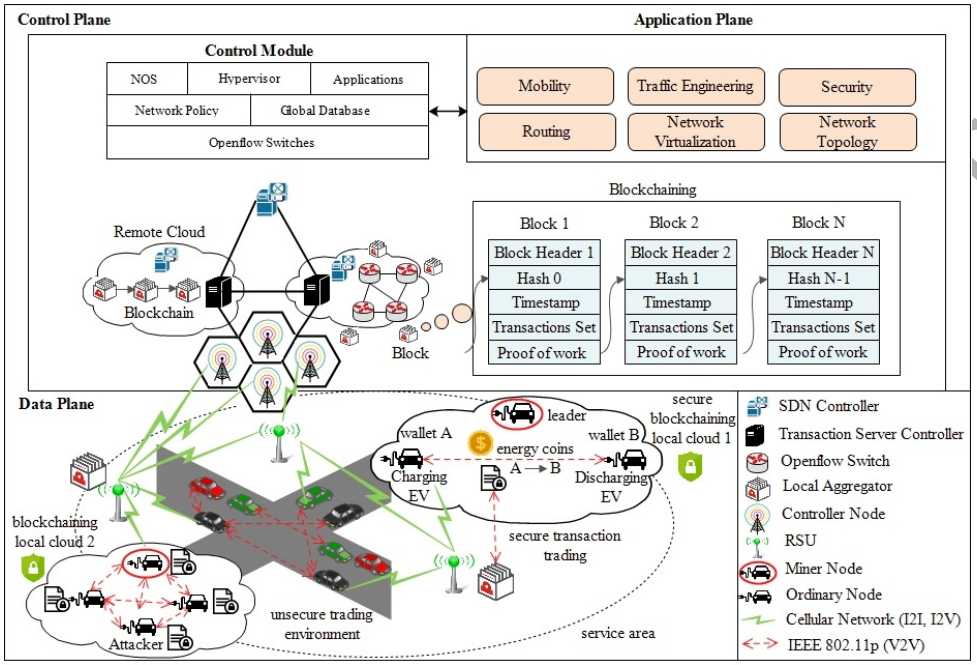


Figure 1: Proposed blockchain-based secure energy trading in SDN-enabled ITS system.

instances of the physical controller so as to serve the maximum number of requests in a minimum time without compromising the QoS. In addition, the control plane has multiple physical controllers (to avoid the single point of failure); thus, ensuring the utility of the SDN for distributed applications.

- *Data Plane* comprises physical entities such as OpenFlow switches, routers, base station, roadside units (RSUs), and EVs. The EV nodes are connected in a peer-to-peer manner amongst themselves, to the base station controller node, and the RSUs using a short/medium range communication protocol such as IEEE 802.11p. These RSUs and controller nodes are connected to the global SDN controller using long-range communication protocols such as LTE-A.

The underlying SDN architecture is used in the proposed scheme to improve the overall communication in the network to facilitate energy transfer between EVs and the utility. The SDN architecture improves the network latency by decreasing the end-to-end delay and increasing the throughput of

a large EV network. This helps in localized P2P electricity trading among multiple EVs and the capability to balance the real-time energy demands of the EVs. However, the EVs and utility communicate their trading requests and decisions with one another in an insecure environment. Fig. 1 shows one example attack model, depicting an insecure trading environment, where attackers are mainly targeting the data plane of the SDN architecture. Energy trading among EVs can be vulnerable to man-in-the-middle (MiTM) attacks as an active attacker can comprise some intermediate device, say local cloud 2 in Fig. 1. For instance, if the utility provider exchanges the secret key for authenticating its identity, then an attacker can acquire the exchanged key. In other words, an attacker simply creates his/her own key exchange parameters and broadcasts this information to the communication entities; thus, impersonating as a legitimate user. MiTM attacks can also occur during the plaintext message exchange among EVs through Wi-Fi or Bluetooth. Generally, a MiTM attacker will seek to impersonate as a legitimate participant and, for example authorize the EV to charge energy from the charging station. This allows such an attacker to acquire energy from the grid operator without paying for the consumed energy.

The second scenario is a secure transaction trading environment comprising local cloud 1. In order to make the network resilient against MiTM attacker, a blockchain consortium is used. This, in turn, provides transaction security and privacy protection without relying on a trusted third-party to carry out verification. In this scenario, each remote cloud comprises three entities, namely: the local SDN controller, a transaction server controller (TSC), and the local aggregators. The task of the local controller is to share up-to-date information of the transaction records to the global controller. The task of the TSC is to maintain the transaction record and meet the energy demands of the users. The local aggregators are multiple authorized nodes, which validate the transactions. Here, all the miner nodes play the role of a local aggregator on the particular local cloud. Initially, the TSC collects the energy requests of both the sellers and buyers from the local cloud. After this, the TSC selects the miner nodes based on the maximum time-of-stay. Here, the miner nodes act as an energy broker and start the energy bidding. The final trading pairs are selected based on the highest auction price announced by all the energy sellers on which the corresponding buyer has agreed for energy trading. So, the charging EVs compute their proof-of-work (PoW) as an encrypted transaction record. The computed PoW with the digital signature of the associated EV is sent to all the miner nodes for

public auditing of the transaction records. Next, all the miner nodes compete with each other to obtain a hash value with a certain difficulty and match the hash output with the received PoW. The fastest miner node to compute a matching PoW is rewarded with some energy coins.

Each EV maintains a wallet as an account for energy trading to store the digital cryptocurrency in the form of energy coins. Therefore, the discharging EV sends his/her public wallet address to the charging EV. The public wallet address is created for privacy protection, and is generated by adding a random pseudonym (salt value) to the true wallet address. The charging EV transfers the energy coin to the discharging EV in his/her public wallet. This public wallet address is changed every time the payment is received (to minimize the risk of account compromise). The local aggregator stores the validated PoW and sends one copy to TSC and the local controller. At last, the local aggregator stores the validated transaction into the shared ledger connected to a blockchain consortium and is accessible by all EVs. The advantage of using blockchain is that it is not prone to single point of failure, unlike other schemes which make use of some trusted third-party for securing the transactions.

In the next section, we will explain how the blockchain consortium works.

3. Blockchain Consortium for Secure Energy Trading

A blockchain consortium is a distributed public ledger in which all the communicating nodes are connected in a P2P manner for sharing of information without depending on a trusted third-party. The blockchain consists of multiple blocks chained together with each block comprising multiple energy trading transactions. The primary functions performed by the blockchain technique are secure identity and transaction management, event recording, and fault provenance. The reason for implementing blockchain consortium in an ITS is that EVs perform energy trading at the charging stations (CSs) for local buying and selling of energy from other EVs or the utility. These transactions need to be secured so as to maintain the energy balance at the utility, as well as the proper distribution of energy to legitimate participating EVs. Therefore, secure energy trading transactions in the form of cryptocurrency, referred to as *energy coins* in this paper, are created and stored in a public ledger before communicating any useful information. These energy coins, in a non-human readable format, is accepted as a payment system in energy

trading between multiple EVs, and EVs with the utility, without involving a centralized intermediary – see Fig. 1.

In this secure energy trading scheme, the communicating nodes are responsible for the maintenance of the blockchains and energy coins. A brief description of how this scheme works is given below. The participating EVs involved in the communication send a service request to the global SDN controller node. The role of the local SDN controller is to provide statistical information of the local electricity demands to store the local network state of all transactional records. The replicated local network state is sent periodically to the global controller to store in the global database. The global SDN controller is deployed on the control plane connected with all the distributed local controllers. The global controller performs three tasks, namely: to reduce the communication overhead during synchronization between controllers, to create the replication mechanism, and to maintain global consistency of the database. It ensures that all the local controllers have up-to-date trading information, and not out-dated local network state. The miner node is selected for the transaction validation process in the local cloud. The third step is to create the blocks which are performed using digital signatures or (PoW) of the participating EV(s). In the last step, the blocks are validated with the help of miner nodes, which perform independent validation of blocks for exchanging the energy coins. In the case where the validation is successful, the blocks are added and updated in the overall blockchain of the RSUs, which can be accessed by any participating node for secure transaction. The blockchain consortium consists of the following entities: miner node, ordinary node, a controller node, and TSC in the form of a distributed model, as illustrated in Fig. 1. In this figure, the miner node is circled as red.

The ordinary node sends a service request for energy trading to the miner node, which performs the validation of every transaction in the block. The requests coming from miner nodes would be validated by other miner nodes in the network. The selection criteria of the miner node is another major task in the blockchain, which is carried out by the TSC as described below.

3.1. Miner node selection

The procedure for miner node selection is explained in Algorithm 1. Initially, a scenario is shown in which numerous EV nodes send the request/response requests to the TSC as shown in Fig. 2.

The TSC selects the miner nodes to validate the requests from the ordinary nodes. Fig. 3 shows the steps performed for the selection of miner

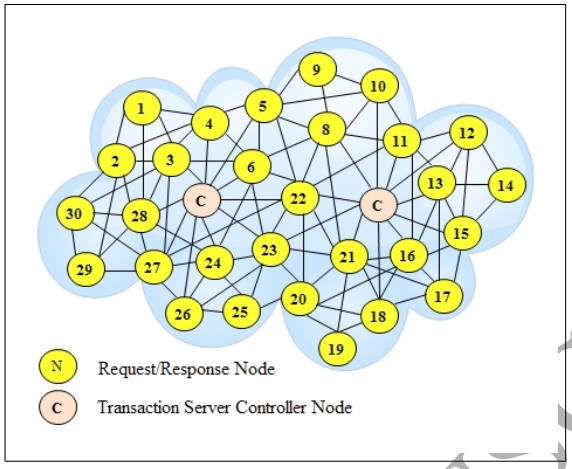


Figure 2: Request / response from EV nodes

nodes. In the first step, the number of EVs (i) send the request for the energy required (E_i) to the controller node. In the second step, the TSC calculates the energy required by these EVs and announces the selling price to all EVs in the service area. In the last step, the EVs confirm the buying price.

The entire process is described in Algorithm 1, where the TSC computes the time of stay of every EV node. Based on the particular threshold, it chooses some nodes as the miner nodes and the remaining as ordinary nodes. The algorithm is described as follows.

This algorithm takes the values of the maximum SOC of the respective EV's batteries (SoC_i^{max}), threshold SoC (SoC^{Th}), maximum SoC of the CS (SoC_j^{max}), dynamic pricing (P_i^s), and distance of EV from charging station ($D_{i \to j}$). Initially, the present SoC (SoC_i^{prs}) of all EVs is checked. If this value is less than a threshold value (SoC_i^{Th}), then the required SoC (SoC_i^{req}) to charge their batteries is calculated. Based on this value, the energy required (E_i^{rq}) by the EVs is computed. This energy is to be charged from the available CSs using secure energy trading requests. For this purpose, E_i^{req} requests are forwarded to the TSC, which checks the present energy at m available CSs. For a single CS, its available SoC value (SoC_j^{avl}) is checked and the available energy at this CS (E_j^{avl}) is computed. Based on these values, the dynamic price (P_j^s) is computed that should be more than the price at which the CS bought the energy (i.e., P_j^{buy}). Finally, this price is announced to the EVs by the global SDN controller. The EVs which agree

Algorithm 1 Election of Miner Node(s)

Input: $n, m, SoC_i^{max}, SoC^{Th}, E_i^{rated}, SoC_j^{max}, P_i^s$
Output: I, MN, ON

procedure FUNCTION(EV, CS)
  for $(i = 1; i \leq n; i++)$ **do** ▷ $i:$ EV
    Check SoC_i^{prs}
    if $(SoC_i^{prs} < SoC_i^{Th})$ **then**
      $(SoC_i^{rq}) : SoC_i^{rq} = (SoC_i^{max} - SoC_i^{pr})$
      Compute $(E_i^{rq}) : E_i^{rq} = SoC_i^{rq} \times E_i^{rated}$
      Forward request for (E_i^{rq}) to the TSC
      TSC checks the list of $'m'$ CS
      for $(j = 1; j \leq m; j++)$ **do** ▷ $j:$ CS
        Checks SoC_j^{prs}
        if $(SoC_j^{prs} > SoC_j^{Th})$ **then**
          $(SoC_j^{avl}) = (SoC_j^{prs} - SoC_j^{Th})$
          $(E_j^{avl}) : E_j^{avl} = SoC_j^{avl} \times E_j^{rated}$
          CS broadcasts (P_j^s) to all EVs
          $P_j^s = \zeta \left\{ \frac{SoC_j^{max}}{SoC_j^{avl} - SoC_j^{Th}} \right\} s.t. P_j^s > P_j^{buy}$
        end if
      end for
      $\forall(\ i,\ j)$, EVs confirm the price (P_{ij}^s)
      TSC checks EV location and computes $D_{i \to j}^{trv}$
      $D_{i \to j} = |\frac{D_i}{D}|D + |\frac{D_j}{D}|D + n_{i \to j}\ D$ ▷ D : Distance of a block,
      ▷ $n_{i \to j}$: Number of blocks
      TSC Computes $SoC_{i \to j}^{trv}, E_{i \to j}^{trv}$
      $SoC_{i \to j}^{trv} = SoC_i^{max}(\frac{D_{i \to j}}{D_{max}})$
      $E_{i \to j}^{trv} = SoC_{i \to j}^{trv} \times E_i^{rated}$
      TSC computes the TOS of every EV node
      $TOS = \frac{T_{chr}^{rated}}{B_{capacity}} \times E_i^{rq}$
      Check γ as the previous connectivity record
      $C_I = (\gamma_{i,j} \times T_{i,j}); s.t. (\gamma \geq 1)$
      $M_I = \frac{TOS}{T_{i \to j}^{trv}} \times C_I$
      TSC sorts M_I in descending order
      if $(M_I > \tau)$ **then** ▷ $\tau \leftarrow$ Threshold value
        Select MN ▷ $MN \leftarrow$ Miner node
      else
        Select ON ▷ $ON \leftarrow$ Ordinary node
      end if
    end if
  end for
end procedure

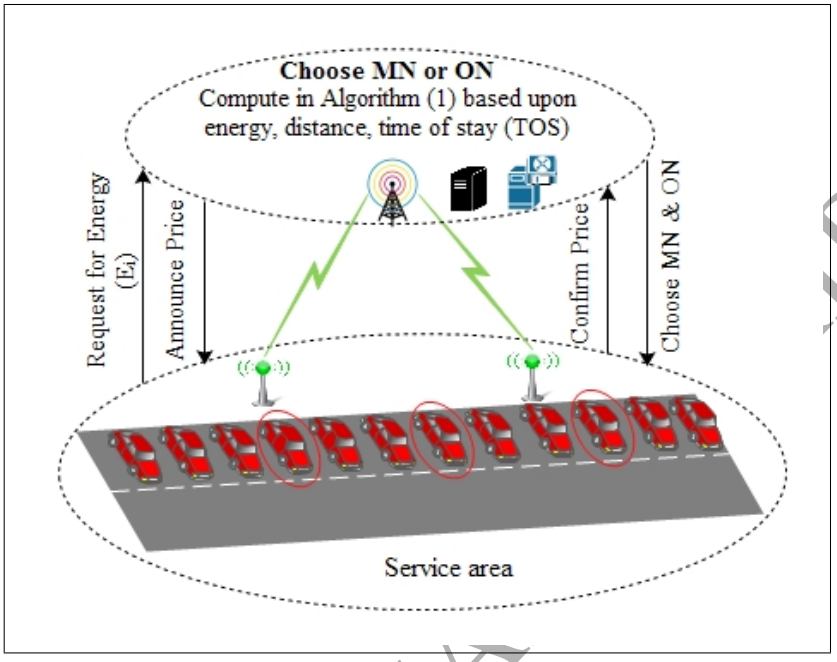


Figure 3: Miner node and ordinary node election

to transact at this price confirm this to the controller.

The TSC then checks for the distance between the EVs and the CSs. Based on this value, it computes the values of SoC ($SoC^{trv}_{i\to j}$) and energy required ($E^{trv}_{i\to j}$) for traveling this distance. It also calculates the time of stay (TOS) for each EV at the CS for charging their batteries. This TOS is based upon the rated energy battery capacity ($B_{capacity}$), time required to charge the rated capacity (T^{rated}_{chr}), and required energy (E^{rq}_i). A connectivity index (C_I) is then computed, which is based on the previous connectivity record of i^{th} EV with j^{th} CS ($\gamma_{i,j}$) and time for which the energy was traded ($T_{i,j}$) between this EV and the CS. A miner index M_I of these EVs is computed on the basis of C_I, TOS, and time required to travel from EV to CS ($T_{i\to}j$). This M_I is sorted in the descending order and the EVs which have their index values above a threshold value (τ), are selected as miner nodes. All the other nodes are selected as ordinary nodes. The selected miner nodes are then used for validating all the requests in the network.

Complexity Analysis: The overall time complexity for Algorithm 1 is computed as follows. The algorithm is executed for n EVs and m CSs,

so the algorithm takes $O(n.m)$ to forward the transaction requests of n EVs to m CSs. The sorting of M_I by the TSC takes $O(n.logn)$. The remaining computations can be carried out in $O(1)$ time. So, the overall complexity of this algorithm is $O(n.m) + O(nlogn) = O(n.m)$.

3.2. Block Creation and Validation

The tasks involved in exchanging blocks for energy trading are shown in Fig. 4. The requesting EV node first creates an encrypted block and broadcasts the encrypted block to the intermediary communicating nodes through the RSU. The RSU then forwards the request for validation to the miner nodes and also maintains a micro cloud to store the validated blocks. The miner nodes perform three activities, namely: sensing, computing, and storage during the validation processing. If the block is authenticated successfully by a miner node, then it is added to the blockchain with the previous hash index; otherwise, the block validation request is sent to the other miner nodes. These miner nodes then perform the same tasks to validate the request. If the request is validated, then the transaction initiated by the EVs is deemed authentic; else, it is invalidated.

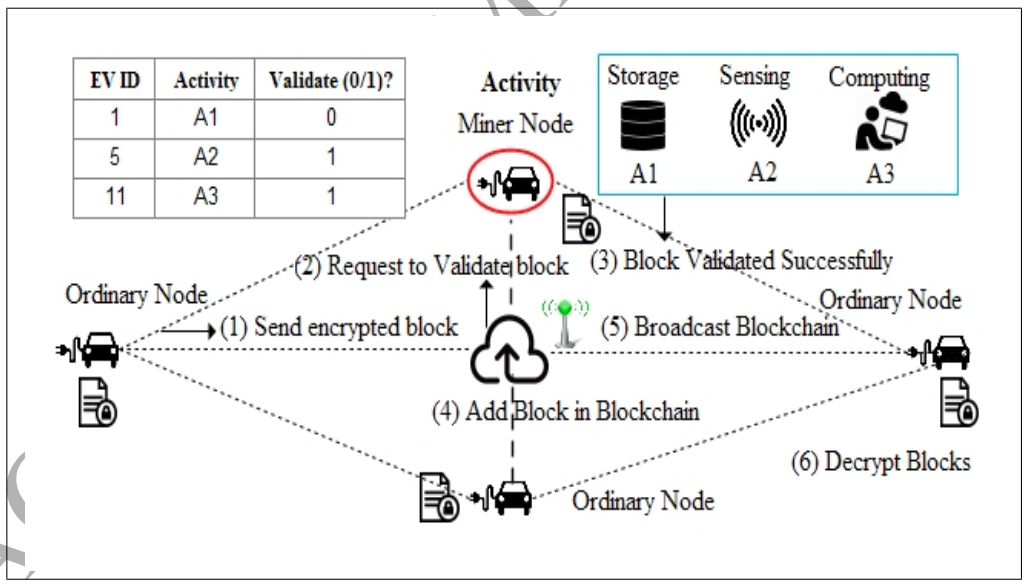


Figure 4: Miner node function

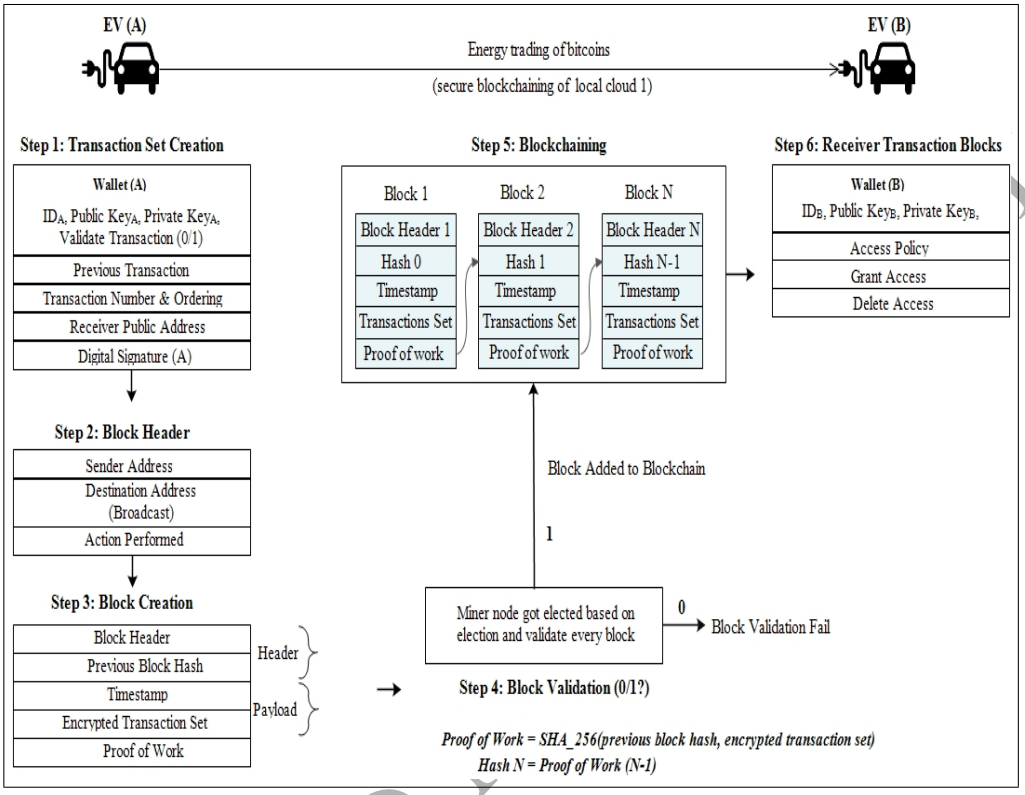


Figure 5: Blockchain structure of localized P2P energy trading in EVs.

Fig. 5 shows the step-by-step workings of a secure blockchain energy trading mechanism between two EVs nodes (A) and (B). Based on Fig. 5, the PoW is generated and validation process between three entities, namely: EVs (A), transaction server (B), and miner node (C) – see Fig. 6. The steps used during energy trading request validation are as follows:

1. Entity (A) transmits a list L to the entity (B) through SSL/TLS connection, which contains the credentials of A such as identity (ID_A), vehicle location longitudinal on X axis, latitudinal on Y axis (A_X, A_Y) from the origin, vehicle rotation angle (A_θ), scale (s), and skew for the origin (ζ).
2. Entity (B) computes a wallet address (WID_A) based on list L and appends a salt value ($salt_A$) of 32-bit to increase the complexity for an attacker. In addition to the wallet address, the TSC is connected with the database of the vehicle registration numbers to create a valid

certificate for (A).

3. (A) receives the wallet address and certificate (WID_A, Cer_A) and creates a combined hash address (MHT_{Root}) of all the transactions using a merkle hash tree. The hash root (MHT_{Root}) is calculated by hashing individual transaction $H(T_i)$ and then a hash code is computed after combining the pair of left and right child hash indexes. Now, (A) creates a block header (B_H) in a random order to provide an extent of stochasticity by appending previous block hash index (H_{Pre}), (MHT_{Root}), time stamp (T_S) of the block creation, block version (B_V), and a random difficult number (d) chosen between the range 0 to 2^{32}. Next step is the addition of a nonce and padding bits to create a message length of a fixed size. Initially, the nonce is set as zero, i.e., $N = 0$ and is incremented by 1 after each iteration. Then, a message digest (H_C) of the input block is computed using SHA-1 to generate the hash output of 160 bits. The block value is repeatedly hashed with different values of N to create a complicated hash index. Finally, PoW which is a digital receipt for (A), is generated by combining (WID_A, H_C, Cer_A). The entity (A) sends the PoW to the entity (C) through RSUs.
4. Entity (C) initially has the inputs as (H_Pre, B_V, d). It first mines and extract the nonce from (B_H). Then, (C) computes the similar (B_H) at its end and calculates the hash output (H_{out}) using SHA-1 on the block header as well as payload (V). Finally, it generates the hash result by appending the wallet address, certificate, and hash result of (A). Moreover, (C) validates a transaction by checking whether $(PoW = H_{result})$. If the PoW matches the H_{result}, then C sends a transaction validation message to (A) (i.e., 1); else transaction invalid message is sent (i.e., 0).

4. Security Evaluation

The performance evaluation of the proposed scheme is described as below.

4.1. Communication cost

A 128 bits identity (ID_A) key of EV node is used, which generates a message digest (hash output) of 160 bits using SHA-1. Using these values, the communication cost for each entity, i.e., EV (A), TSC (B), and MN (C) is computed as below.

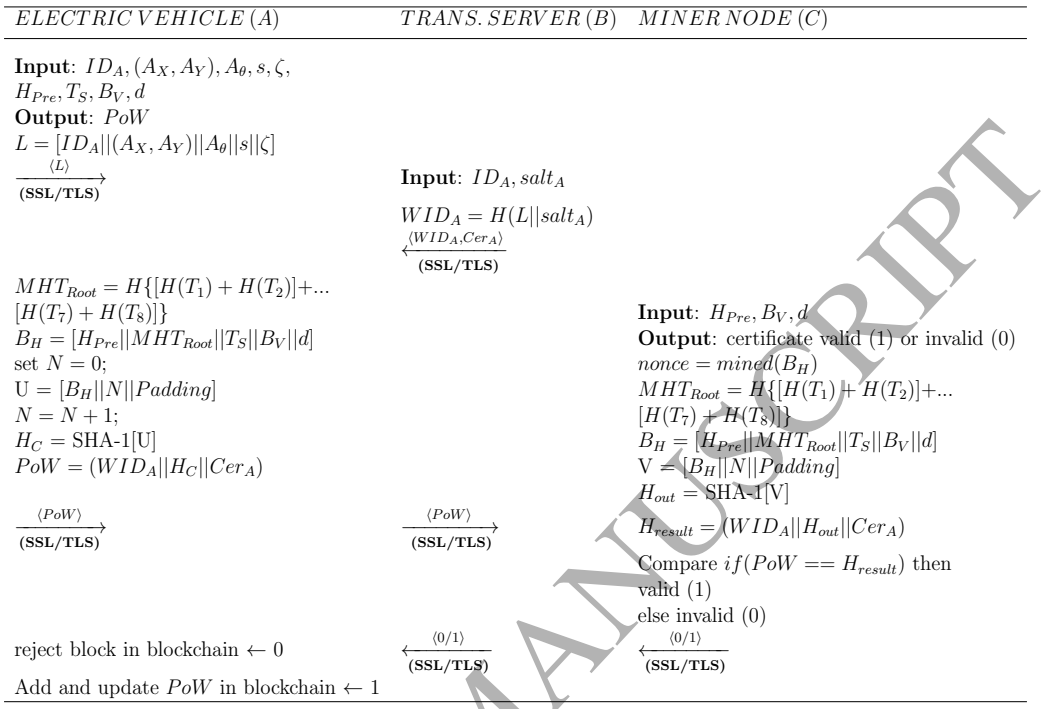


Figure 6: PoW generation for block creation and validation process

- **Electric Vehicle (A)**: Initially, the location of (A) is computed in a list L (128+8+8+8+8), which is 160 bits; where the values of $[(A_X, A_Y)$, $A_\theta, s, \zeta]$ are of 8 bits each. The bits processed at B_H (160+160+32+32+32) are of 416 bits; where (H_{Pre}, MHT_{Root}) is of 160 bits each, and (T_S, B_V, d) are of 32 bits, respectively. The nonce N is of 32-bits and 64 padding bits are appended to B_H for creation of a message input of 512 bits. Therefore, in order to generate the overall message digest, H_C returns the hash output as 160 bits using SHA-1.

- **Transaction Server (B)**: The communication bits processed at B are calculated as: WID_A= $(160 + 32) = 192$; here, 32 bits are of salt value in addition to a certificate Cer_A, which is of 128 bits.

- **Miner Node (C)**: The miner node computes H_{result} in order to match with the received PoW. The communication bits incurred during the computation of H_{result} is 480 bits. In addition, the miner node returns

a decision for validation process, either as valid (1) or invalid (0). Thus, the decision process consumes only 1 bit to send the acknowledgment to entity A.

In summary, the overall communication costs incurred during block creation and validation process is (192 + 160 + 128 + 192 + 160 + 128 + 1) = 961 bits.

4.2. Computation time

The computation time is calculated based on the operations performed in the blockchain such as addition, one-way hashing function (SHA-1) and append operations. The average time taken by these operations are as follows. The addition operation takes 1 milliseconds (ms), SHA-1 takes 2.7 ms to process each block and the append operation takes 0.3 ms. Using these values, the computation time for each entity is computed as below.

- The computation time taken at entity A is given as below:
  $T_A = [(2 \text{ append}) + (1 \text{ hashing} + 2 \text{ append}) + (4 \text{ append}) + (7 \text{ addition} + 1 \text{ hashing}) + (4 \text{ append})] = [2 \times 0.30 + 1 \times 2.7 + 2 \times 0.3 + 4 \times 0.3 + 7 \times 1 + 1 \times 2.7 + 4 \times 0.3]$ ms = 16 ms.

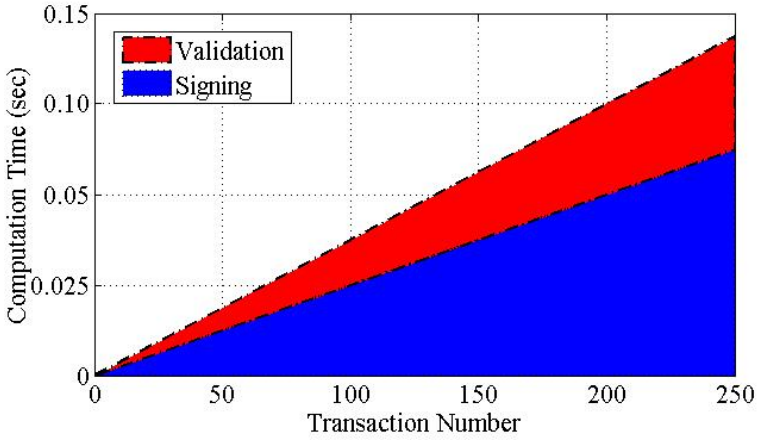
- At B, the computation time taken is shown as below:
  $T_B = (1 \text{ hash} + 1 \text{ append}) = (1 \times 2.7 + 1 \times 0.3) = 3$ ms.

- At the Miner node C, the validation process is similar to the validation process of A, hence the computation time is given as below.
  $T_C = 16$ ms.

Summing up all the above, the total computation time taken for processing is computed as below.

$$T_{Total} = (T_A + T_B + T_C) = (16 + 3 + 16)ms = 35ms.$$

Now, the variation of key transfer time with respect to an increase in the number of transactions is analyzed. For this purpose, the computation time for signing and validation processes is required. Fig. 7 depicts the computation time taken for the signing process with respect to an increase in the transaction number. Fig. 7 shows the computation time for the validation process with respect to an increase in the number. The result depicts a linear growth in signing and validation times with an increase in the transaction number. Finally, the key transfer time for the proposed scheme is computed.



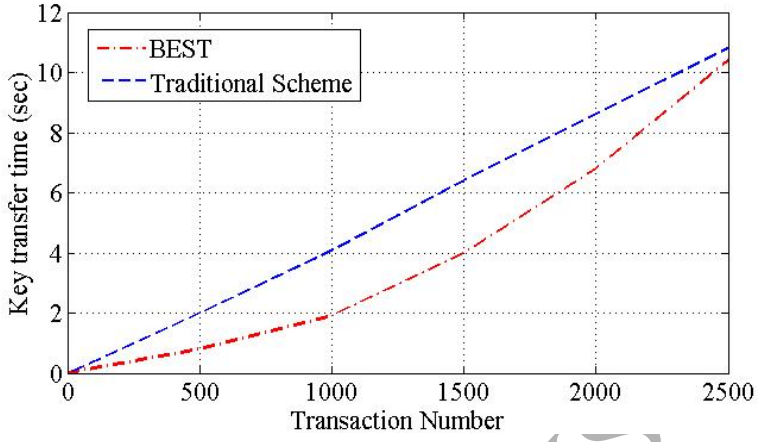
(a)

Figure 7: Computation time

Fig. 8 shows the variation of key transfer time with respect to an increase in the transaction number. It is evident from the figure that the traditional scheme takes more time for key transfer as compared to the proposed scheme. Initially, the key transfer time taken by both schemes is equal. However, the variation between them reaches the maximum value of 2.5 s for transaction range between 1000 to 1500. After this transaction range, the gap in the key transfer time for both schemes decreases slowly.

4.3. A case study

We use the following case study to explain how our proposed approach can be used in practice. We consider a small city-wide intelligent transportation scenario, which conservatively consists of 200 EVs, 10 CSs and 1 TSC. The EVs and CSs are placed at random locations in the city-block architecture. The initial SoC levels of EVs and CSs are depicted in Figs. 9 and 10, respectively. For simplicity, the threshold SoC level of both the EVs and CSs is considered to be 50% (this value can vary in practice). Based on the SoC requirements, CSs broadcast the price to all participating EVs in the vicinity. The EVs agree to the prices, which would be lowest to them depending on their own SoC requirements. To choose the miner nodes out of all the EVs, M_I is computed on the basis of their time of stay and connectivity index, and miner nodes are selected using Algorithm 1. Once the miner nodes are



(a)

Figure 8: Key transfer time

selected, the secure transactions for energy trading are processed as shown in Figs. 4 and 5.

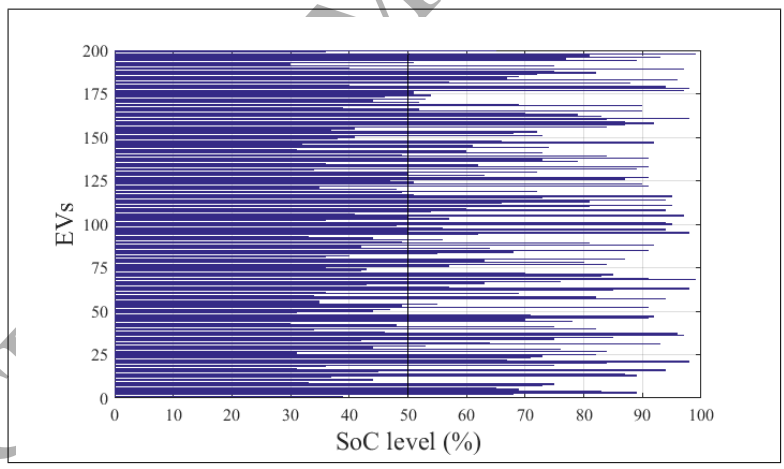


Figure 9: SoC level of EVs.

4.4. Comparative analysis

A comparative analysis of *BEST* with several other competing approaches is given in Table 1.

Table 1: Comparative analysis of *BEST* with several other competing approaches

References	**Techniques**	**F1**	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**
[37]	Blockchain	TCP/IP Networking	Voting System	Echo Announcement protocol	✓	CreditCoin	×	174.1 ms	Smart Transportation
[38]	Blockchain	TCP/IP Networking	×	Auction Mechanism, Reward Function	✓	*PoW*	×	×	Smart Transportation
[39]	Blockchain	TCP/IP Networking	×	Gamification	×	Shamir Secret Sharing (SSS)	2048 bits	×	Smart Grid
[40]	Blockchain	TCP/IP Networking	Power Capacity	Merkle Hash Tree	×	*PoW*	576 bits	33 ms	Smart Grid
[41]	Bilateral Contracts	TCP/IP Networking	×	Game Theory, Price Adjustment	×	×	×	×	Smart Grid
[42]	Coordinated Bidding Strategy	TCP/IP Networking	×	Dynamic Pricing	×	×	×	190 s	Smart Grid
BEST Scheme	Blockchain	SDN	TOS, C_I	Dynamic Pricing, available energy, distance	✓	*PoW*	961 bits	35 ms	Smart Transportation

Note- F1: Underlying Network Architecture, F2: Miner Node Selection, F3: Energy Trading, F4: Cryptocurrency Wallet, F5: Consensus Algorithm, F6: Communication Cost, F7: Computation Time, F8: Application Domain

Notation- ✓: considered, and ×: not-considered

ACCEPTED MANUSCRIPT

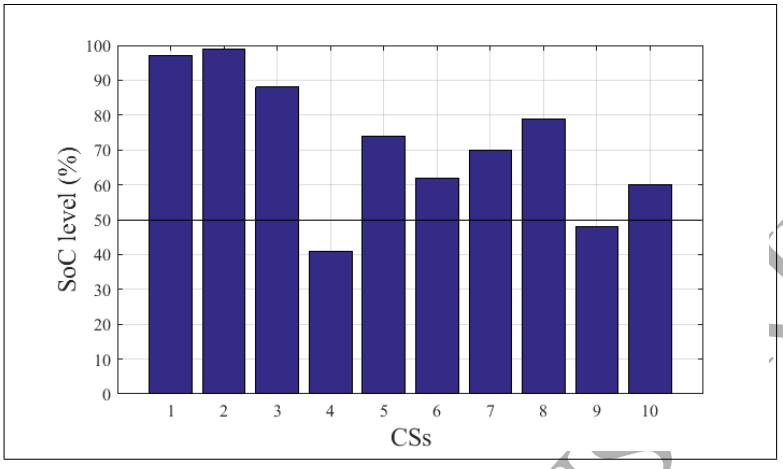


Figure 10: SoC level of CSs.

5. Conclusion

In this paper, we presented *BEST*, a blockchain-based energy trading scheme for secure energy trading in ITS. Specifically, the scheme uses SDN as the underlying architecture. In our scheme, energy coins are used for energy trading transactions in the blockchain consortium. The miner nodes responsible for validating all the network transactions are selected on the basis of various factors, such as energy requirements, pricing, and TOS. This increases the overall security of the system as it compounds the challenge for an attacker to influence or modify the node selection process. The proof of work (PoW) for validating the transactions in energy trading was also explained. The performance analysis indicates that the proposed scheme is lightweight and imposes minimal communication and computation requirements on the network resources. The results also suggests that the SDN architecture complements the blockchain by increasing the network QoS.

In the future, the flow control mechanism in SDN would be explored in our attempts to improve the network throughput. We also plan to collaborate with a city or smart grid / utility operator to implement and evaluate the prototype of our proposed approach. This will allow us to more accurately evaluate its real-world utility and scalability.

References

[1] A. Goel, M. A. R. Shuman, B. Gupta, A. Aggarwal, S. Sharma, Collaborative intelligence and decision-making in an iot device group, US Patent 9,292,832 (Mar. 22 2016).

[2] G. S. Aujla, A. Jindal, N. Kumar, Evaas: Electric vehicle-as-a-service for energy trading in sdn-enabled smart transportation system, Computer Networks 143 (2018) 247 – 262.

[3] G. S. Aujla, N. Kumar, Mensus: An efficient scheme for energy management with sustainability of cloud data centers in edgecloud environment, Future Generation Computer Systems 86 (2018) 1279 – 1300.

[4] C. C. Onn, N. S. Mohd, C. W. Yuen, S. C. Loo, S. Koting, A. F. A. Rashid, M. R. Karim, S. Yusoff, Greenhouse gas emissions associated with electric vehicle charging: The impact of electricity generation mix in a developing country, Transportation Research Part D: Transport and Environment.

[5] Global EV Outlook 2016, Available:`https://www.iea.org/publications/freepublications/publication/Global_EV_Outlook_2016.pdf`, [Accessed: Mar. 2018].

[6] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, J. J. P. C. Rodrigues, Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2629–2640. doi:10.1109/TII.2018.2789442.

[7] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, J. J. P. C. Rodrigues, Secsva: Secure storage, verification, and auditing of big data in the cloud environment, IEEE Communications Magazine 56 (1) (2018) 78–85. doi:10.1109/MCOM.2018.1700379.

[8] C. Esposito, A. D. Santis, G. Tortora, H. Chang, K. R. Choo, Blockchain: A panacea for healthcare cloud-based data security and privacy?, IEEE Cloud Computing 5 (1) (2018) 31–37.

[9] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications 126 (2019) 45 – 58.

doi:https://doi.org/10.1016/j.jnca.2018.10.020.
URL http://www.sciencedirect.com/science/article/pii/S1084804518303485

[10] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications 116 (2018) 42–52.

[11] K. Gai, K. R. Choo, L. Zhu, Blockchain-enabled reengineering of cloud datacenters, IEEE Cloud Computing 5 (6) (2018) 21–25.

[12] T. McGhin, K.-K. R. Choo, C. Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications 135 (2019) 62–75.

[13] L. Zhang, M. Luo, J. Li, M. H. Au, K. R. Choo, T. Chen, S. Tian, Blockchain based secure data sharing system for internet of vehicles: A position paper, Vehicular Communications 16 (2019) 85–93.

[14] C. Lin, D. He, X. Huang, X. Xie, K. R. Choo, Blockchain-based system for secure outsourcing of bilinear pairings, Information Sciences.

[15] G. S. Aujla, R. Chaudhary, N. Kumar, J. J. Rodrigues, A. Vinel, Data offloading in 5g-enabled software-defined vehicular networks: A stackelberg-game-based approach, IEEE Communications Magazine 55 (8) (2017) 100–108.

[16] B. Roberts, K. Akkaya, E. Bulut, M. Kisacikoglu, An authentication framework for electric vehicle-to-electric vehicle charging applications, in: IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017, pp. 565–569.

[17] J. Shen, T. Zhou, F. Wei, X. Sun, Y. Xiang, Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things, IEEE Internet of Things Journal.

[18] W. Han, Y. Xiao, Privacy preservation for v2g networks in smart grid: A survey, Computer Communications 91 (2016) 17–28.

[19] N. Saxena, S. Grijalva, V. Chukwuka, A. V. Vasilakos, Network security and privacy challenges in smart vehicle-to-grid, IEEE Wireless Communications 24 (4) (2017) 88–98.

[20] T. Volety, S. Saini, T. McGhin, C. Z. Liu, K.-K. R. Choo, Cracking bitcoin wallets: I want what you have in the wallets, Future Generation Computer Systems 91 (2019) 136–143.

[21] M. Banerjee, J. Lee, K.-K. R. Choo, A blockchain future for internet of things security: a position paper, Digital Communications and Networks 4 (3) (2018) 149–160.

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

[23] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fairaccess: a new blockchain-based access control framework for the internet of things, Security and Communication Networks 9 (18) (2016) 5943–5964.

[24] L. Zhu, Y. Wu, K. Gai, K.-K. R. Choo, Controllable and trustworthy blockchain-based cloud data management, Future Generation Computer Systems 91 (2019) 527–535.

[25] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, K. R. Choo, Blockchain-based system for secure outsourcing of bilinear pairings, Digital Communications and Networks.

[26] M. Mylrea, S. N. G. Gourisetti, Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security, in: Resilience Week (RWS), 2017, pp. 18–23.

[27] J. Sun, J. Yan, K. Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Financial Innovation 2 (1) (2016) 26.

[28] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine 55 (12) (2017) 119–125.

[29] Y. Yuan, F.-Y. Wang, Towards blockchain-based intelligent transportation systems, in: IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016, pp. 2663–2668.

[30] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet of Things Journal 4 (6) (2017) 1832–1843.

[31] P. K. Sharma, N. Kumar, J. H. Park, Blockchain-based distributed framework for automotive industry in a smart city, IEEE Transactions on Industrial Informatics (2018) 1–1doi:10.1109/TII.2018.2887101.

[32] A. Jindal, G. S. Aujla, N. Kumar, Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment, Computer Networks 153 (2019) 36 – 48.

[33] G. S. Aujla, R. Chaudhary, K. Kaur, S. Garg, N. Kumar, R. Ranjan, Safe: Sdn-assisted framework for edge-cloud interplay in secure healthcare ecosystem, IEEE Transactions on Industrial Informatics 15 (1) (2019) 469–480. doi:10.1109/TII.2018.2866917.

[34] R. Chaudhary, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, Optimized big data management across multi-cloud data centers: Software-defined-network-based analysis, IEEE Communications Magazine 56 (2) (2018) 118–126. doi:10.1109/MCOM.2018.1700211.

[35] G. S. S. Aujla, N. Kumar, S. Garg, K. Kaur, R. Ranjan, Edcsus: Sustainable edge data centers as a service in sdn-enabled vehicular environment, IEEE Transactions on Sustainable Computing (2019) 1–1doi:10.1109/TSUSC.2019.2907110.

[36] A. Jindal, G. S. Aujla, N. Kumar, R. Chaudhary, M. S. Obaidat, I. You, Sedative: Sdn-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems, IEEE Network 32 (6) (2018) 66–73. doi:10.1109/MNET.2018.1800101.

[37] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles.

[38] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3154–3164.

[39] C. Rottondi, G. Verticale, et al., A privacy-friendly gaming framework in smart electricity and water grids, IEEE Access 5 (2017) 14221–14233.

[40] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, N. Kumar, Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem, in: Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities, ACM, 2018, p. 1.

[41] T. Morstyn, A. Teytelboym, M. D. McCulloch, Bilateral contract networks for peer-to-peer energy trading, IEEE Transactions on Smart Grid.

[42] A. T. Al-Awami, E. Sortomme, Coordinating vehicle-to-grid services with energy trading, IEEE Transactions on smart grid 3 (1) (2012) 453–462.

Biography

Rajat Chaudhary is pursuing Ph.D. from Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India. He received the B.Tech degree in Computer Science and Engineering from Uttar Pradesh Technical University, Lucknow, India, in 2010, and the M.Tech degree from Uttarakhand Technical University, Dehradun, India, in 2012. He is currently working as a Junior Research fellow in Indo-Poland Joint Research Project. He has many research interests in the area of computer networking, network security, cryptography, software-defined networks, Internet of things, fog computing, and information security. He is student member of the IEEE and IEEE ComSoc.

Anish Jindal received his Bachelor of Technology degree from Punjab Technical University, India in 2012 and Master of Engineering degree from University Institute of Engineering and Technology, Panjab University, Chandigarh, India in 2014, both in Computer Science and Engineering. He received his Ph.D. degree in Computer Science and Engineering Department from Thapar University, Patiala (Punjab), India in 2018. He is working as a Senior Research Associate in the School of Computing and Communications, Lancaster University, UK. Prior to this, he was a Senior Research fellow of Council of Scientific and Industrial Research, India. He is member of the IEEE, ACM, and IAENG.

Gagangeet Singh Aujla is working as an Associate Professor in Computer Science and Engineering Department, Chandigarh University, Mohali, Punjab, India. He received the B.Tech degree and the M.Tech degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2003 and 2013, respectively. He received his Ph.D. in Computer Science and Engineering from Thapar Institute of Engineering and Technology, Patiala, Punjab, India in 2018. He received IEEE TCSC Outstanding Ph.D. Dissertation Award at Guangzhou, China in 2018. He has many research contributions in the area of smart grid, cloud computing, software defined networks, and security. He is member of the IEEE, and ACM.

Neeraj Kumar received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra (J & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as an Associate Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala (Punjab), India. He has published

more than 200 technical research papers in leading journals and conferences. He is an Associate Technical Editor of IEEE Communication Magazine and an Associate Editor of IJCS, Wiley, JNCA, Elsevier, and Security & Communication, Wiley. He is senior member of the IEEE.

Kim-Kwang Raymond Choo currently holds the Cloud Technology Endowed Professorship at the University of Texas at SanAntonio (UTSA), and has a courtesy appointment at the University of South Australia. He is the recipient of various awards including ESORICS2015 Best Research Paper Award,Winning Team of Germanys Universityof Erlangen-Nuremberg Digital Forensics Research Challenge2015, 2014 Australia New Zealand Policing Advisory Agencys HighlyCommended Award, 2010 Australian Capital-Territory Pearcey Award,Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion,and British Computer SocietysWilkes Award. He is an IEEE Senior Member, and an Australian Computer Society Fellow.