BLOCKCHAIN-ENABLED SECURITY IN ELECTRIC VEHICLES CLOUD AND EDGE COMPUTING

Seminar Report

Submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

In

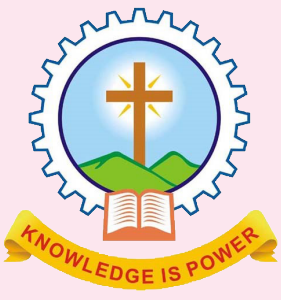
COMPUTER SCIENCE AND ENGINEERING

of

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Submitted By

MIDHUN S



Department of Computer Science & Engineering
Mar Athanasius College Of Engineering
Kothamangalam

BLOCKCHAIN-ENABLED SECURITY IN ELECTRIC VEHICLES CLOUD AND EDGE COMPUTING

Seminar Report

Submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

In

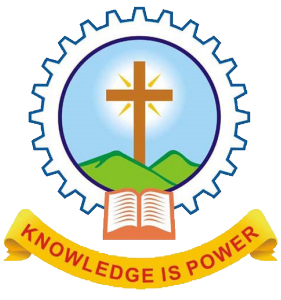
COMPUTER SCIENCE AND ENGINEERING

of

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

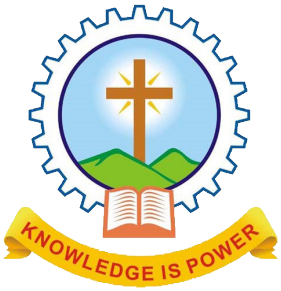
Submitted By

MIDHUN S



Department of Computer Science & Engineering
Mar Athanasius College Of Engineering
Kothamangalam

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
MAR ATHANASIUS COLLEGE OF ENGINEERING
KOTHAMANGALAM



CERTIFICATE

This is to certify that the report entitled **Blockchain - Enabled Security In Electric Vehicles Cloud and Edge Computing** *submitted by* **Mr. MIDHUN S**, *Reg. No.* **MAC15CS039** *towards partial fulfillment of the requirement for the award of Degree of Bachelor of Technology in Computer science and Engineering from APJ Abdul Kalam Technological University for December 2018 is a bonafide record of the seminar carried out by him under our supervision and guidance.*

.....	.....	.....
Prof. Joby George	**Prof. Neethu Subash**	**Dr. Surekha Mariam Varghese**
Faculty Guide	***Faculty Guide***	***Head Of Department***

Date:

Dept. Seal

Acknowledgement

First and foremost, I sincerely thank the 'God Almighty' for his grace for the successful and timely completion of the seminar.

I express my sincere gratitude and thanks to Dr. Solly George, Principal and Dr. Surekha Mariam Varghese, Head Of the Department for providing the necessary facilities and their encouragement and support.

I owe special thanks to the staff-in-charge Prof. Joby george, Prof. Neethu Subash and Prof. Joby Anu Mathew for their corrections, suggestions and sincere efforts to co-ordinate the seminar under a tight schedule.

I express my sincere thanks to staff members in the Department of Computer Science and Engineering who have taken sincere efforts in helping me to conduct this seminar.

Finally, I would like to acknowledge the heartfelt efforts, comments, criticisms, co-operation and tremendous support given to me by my dear friends during the preparation of the seminar and also during the presentation without whose support this work would have been all the more difficult to accomplish.

Abstract

Electric Vehicles Cloud and Edge (EVCE) computing is a network paradigm involvingseamless connections among heterogeneous vehicular contexts. It will be a trend along withElectric Vehicles (EV) becoming popular in Vehicle to Everything communication. The EVsact as potential resource infrastructures referring to both information and energy interactionsand there are serious security challenges for such hybrid cloud and edge computing. Contextaware vehicular applications are identified according to the perspectives of information andenergy interactions. Blockchain inspired data coins and energy coins are proposed based ondistributed consensus, in which data contribution frequency and energy contribution amountare applied to achieve the proof of work. Security solutions are presented for securing vehicularinteractions in EVCE computing

Contents

List of Figures

List of Abbreviations

EV	Electric Vehicle
POW	Proof of Work
POS	Fully Proof of Stack
HMAC	Hash Machine Authentication Code
ECDSA	Elliptic Curve Digital Signature Algorithm

Introduction

Electric vehicles cloud and edge (EVCE) computing is an attractive network paradigm involving seamless connections in heterogeneous vehicular contexts to aggregate distributed electric vehicles (EVs) into a common resource pool, and to invoke the EVs for locally flexible usage [1]. In EVCE computing, information flow and energy flow are dynamically exchanged during the vehicle to anything communications, including vehicle to grid (V2G), vehicle to infrastructure (V2I), and vehicle to vehicle (V2V), to achieve collaborative data sensing, information analyzing, and energy sharing. Due to the data sensitivity and context complexity, vehicular applications confront serious security issues.

The emergence of autonomous vehicles promotes the popularity of the combination of distributed vehicular resources. EVs constitute a noteworthy portion of connected services with energy, communication, and computation resources to perform processing at the network edge. Meanwhile, EVs' idle resources may be aggregated to establish a mobile resource pool for collaborative utilization [2]. Thus, a vehicular ecosystem will be established based on the distributed and aggregated EVs through their activity cycles, in which information and energy interactions are achieved among EVs, sensors, roadside units (RSUs), and local aggregators (LAGs) for interactive applications.

The coexistence of hybrid cloud computing and edge computing is becoming the trend of future vehicular applications, which have the following three characteristics

Centerless Trust: There is no center node in peer-to-peer communications, in which data exchange is performed without pre-assigned trust relationships.

Collaborative Intelligence: An EV makes a limited contribution to specific processing, the coordinated EVs will jointly address problem solving for crowd intelligence.

Spatio-Temporal Sensitivity: An EV's exchanged information and energy are sensitive data with obvious spatio-temporal attributes for the data provenance requirement.

Unlike traditional system infrastructures, the EVCE confronts serious security challenges due to the legal entities and attackers being equipotent participants owning equal privi-

lege. For instance, an EV provides dynamic traffic information and idle energy as distributed resources. An attacker could receive omni-bearing messages via open interfaces and wireless communication channels. In order to address the security issues, blockchain is introduced as a potential solution with two main features. Decentralization means that the data accounting, storage, maintenance, and transmission are performed based on distributed computing capabilities, and there is no core node for centralized management; Co-participation means that all the participants will join in block transactions based on consensus algorithms.

Toward the blockchain, cryptographic algorithms are applied to establish mutual or multi-party trust relationships. Mass collaboration is performed by collective self-interests, and the possible data uncertainty is regarded as a marginal element. Any block records and stores a receipt to a link with the previous block, and a new block is attached to the ledger only if the corresponding messages pass authentication by the majority of participants [3]. This special data structure provides better robustness under a single point of failure, and avoids tampering attack with data traceability. Currently, blockchain based key management [4], anonymous multi-signatures [5], and secure software defined network architecture [6] have been proposed and leveraged to enhance security. In this article, the blockchain is applied during information and energy interactions to achieve enhanced security protection.

The remainder of this work is organized as follows. The next section introduces the network architecture and context-aware vehicular applications. Following that, we present security requirements and distributed consensus. Then we present the security solutions for both information and energy interactions. The final section draws a conclusion.

Existing System

2.1 Network Architecture and Context-Aware Application

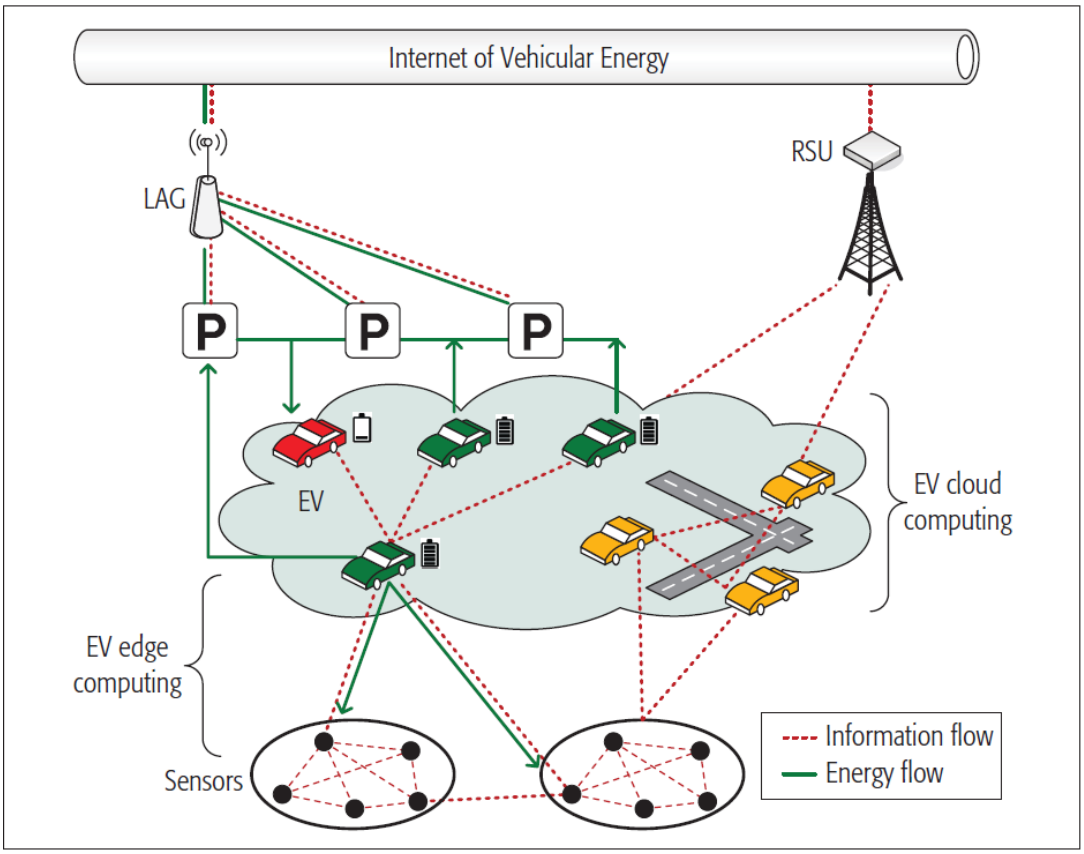


Figure 2.1: Network Architecture

2.1.1 EV Cloud Computing

The EVs' idle energy, computation, and communication resources can be aggregated into a common pool. The EVs are regarded as mobile cloudlets based on vehicular ad hoc networks (VANETs) and other networks. The connected EVs are gathered for providing cooperative services while moving round different areas or spending hours in parking lots. The cloud

computing mode highlights extending traditional cloud infrastructures into flexible connected EVs to establish interactions with RSUs, LAGs, and other entities [7, 8].

2.1.2 EV Edge Computing

The EVs act as distributed units to perform a substantial amount of data processing and analysis during collaborative operations, in which sensors are geographically dispersed to establish interactions [9]. Flexible computing is achieved instead of establishing direct communications with the remote cloud. This edge computing mode provides higher accuracy on measurement, and emphasizes the proximity to sensors, dense geographical distribution, latency reduction, and support for mobility to enhance the quality of services [10, 11]. The moving EVs could enhance the network connectivity and capability with high-speed data transmission and low communication latency.

This hybrid network architecture is fundamentally different from that of the traditional system paradigm. It is established based on distributed vehicular cloudlets and units, and highlights the performance of local information and energy processing with the collaboration of nearby vehicular resources.

2.2 Vehicular Information and Energy Interaction

2.2.1 Vehicular Information Interactions

During information interactions, an EV establishes wireless communications with multiple sensors for distributed perception and cooperative processing, including traffic updates monitoring and road environment detection. The sensing data is gathered by EVs for satisfying diverse functional requirements. Much vehicular data temporarily exists or entirely remains on the EVs, while some may be transmitted to and from other entities. [2].

The EVs are distributed computing nodes to aggregate data together, and the associated data is applied for cooperative services, including traffic query, driving assistance, and entertainment sharing. The EVs realize resource reallocation to satisfy specific individual demands. Here , information interactions are generally based on V2I and V2V communications.

For instance, an EV communicates with fixed surrounding infrastructures, communicates with parking lots to provide assistant information servers, and exchanges messages with a LAG during V2G communications.

2.2.2 Vehicular Energy Interaction

During energy interactions, an EV performs changing and discharging operations during V2G communications with the roles of energy demand, energy storage, and energy supply. A LAG acts as an agent between the power grid and the gathered EVs for aggregating distributed batteries.

The EVs own potentially available batteries to interact with a LAG for energy exchanging. The aggregated EVs jointly establish a large and flexible energy pool, and the size of the energy pool continually varies according to EVs' arrivals and departures within an area [12, 13]. Meanwhile, an EV interacts with multiple sensors, and also supplies redundant energy to surrounding and dispersed sensors based on the emerging wireless charging technology for creating a perpetual energy source to provide power over distance, one-to-many charging, and controllable wireless power. Considering an EV's activity cycle perspective, it moves around different area networks along with distributed energy support.

Note that 4G LTE cellular telecommunication, WiFi, and IEEE 802.11p/wireless access for vehicular environments (WAVE) are available broadband wireless communication technologies for vehicular data transmission [7]. Both in-band spectrum and the 5.9 GHz dedicated short-range communications (DSRC) spectrum are popular for ubiquitous vehicular applications. The International Standards Organization/International Electrotechnical Commission (ISO/IEC) 15118 standard is particularly designed to support V2G communication interfaces.

2.3 Context Aware Vehicular Applications

Figure illustrates context-aware vehicular applications, in which there are four scenarios referring to information and energy interactions. The first two scenarios (shown by the red areas) refer to information interactions, which consider the moving EVs as infrastructures to

enhance computation capability for the vehicular cloud and edge. The other two scenarios (shown by the green areas) refer to energy interactions.

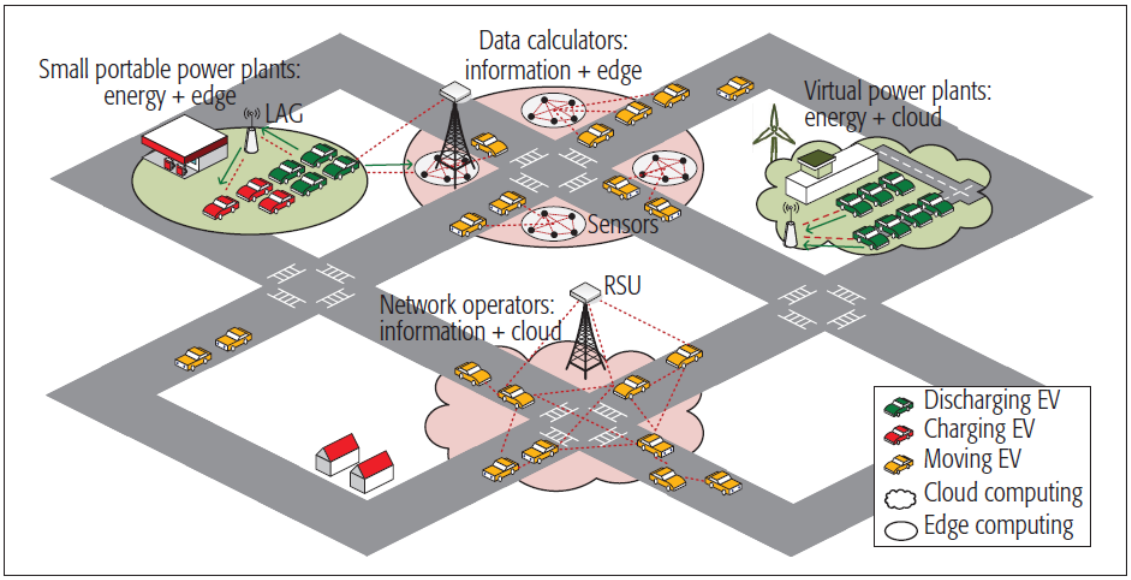


Figure 2.2: Context Aware Vehicular Application Based on the Information and Energy Interactions

2.3.1 Spontaneous Network Operators

During the cloud-computing-based information interactions, slowly moving EVs act as spontaneous network operators to perform a substantial amount of communications with neighboring EVs and RSUs for establishing robust connectivity [4]. The vehicular networking forms a core component by carrying and forwarding data packets to other EVs, and is achieved through the combination of V2I and V2V communications. The EVs establish interactions with the RSUs to exchange information by monitoring roadside infrastructures, and also interacts with other EVs within a certain range. Data-driven interactions provide network connectivity for enabling data transmission. Collaborative networking is achieved considering high mobility and localized scattering from the neighboring EVs and RSUs.

2.3.2 Mobile Data Calculators

During the edge-computing- based information interactions, the EVs act as mobile data calculators to provide local data processing by integrating various sensing data to extract available information for transportation management. The moving EVs are traffic probes, integrated with private sector probe data for directly linking roadside sensors to physical surroundings. For instance, road detection and traffic optimization of automated vehicles are performed based on the cooperation of proper sensors. The EVs approach network boundaries with dense geographical distribution and collaborative computing capability.

2.3.3 Virtual Power Plants

During the cloud-computing based energy interactions, the EVs act as virtual power plants to provide flexible energy aggregation with a cluster of scattered energy. Assume that there are many fully charged EVs during a long period of working time and nighttime, and the EVs are potentially available to feed energy back into the power grid or other neighboring entities. Moreover, an EV may play the role of mobile energy transporter to balance energy pools among different areas.

2.3.4 Small Portable Power Plants

During the edge-computing-based energy interactions, the EVs act as small portable power plants to share energy with roadside infrastructures (e.g., sensors and RSUs). Energy consumption of sensors and RSUs is one of the most important constraints; it will influence the network reliability and lifetime. Energy connectivity is crucial for enabling energy flow among different entities. The EVs are expected to be applied for wireless discharging to transmit idle energy to nearby sensors along with the development of wireless charging technology. Long-staying EVs become abundant and convenient power plants for energy sharing.

Proposed System

3.1 Security Requirements and Distributed Consensus

3.1.1 Security Requirements

Traditional security requirements including the data confidentiality, integrity, and availability (CIA triad), authentication, authorization, and accounting (AAA), privacy preservation (e.g., location, charge status, and identity) should also be addressed. Due to the limitations of wireless communication channels, data tampering, identity impersonation, and privacy violation related security issues become severe in EVCE computing.

Considering the characteristics of centerless trust, collaborative intelligence, and spatio-temporal sensitivity, traceability and transparency should be highlighted.

Traceability

Traceability refers to data provenance to identify data lineage tracing for collaborative EVs and other entities. It is required that the origins and intermediate flow of information and energy be traced during interactions. Due to attackers and legal entities being equally privileged and equipotent participants, the interactive data may be maliciously utilized or tampering.

Transparency

Transparency refers to an entity (e.g., an EV) knowing which other entity (e.g., a LAG) obtains its related data, when and where the entity has used the data, and how the entity realizes a specific function. Transparency has limited visibility during interactions based on the software defined security model (e.g., zero-trust model), and private data should be confused by scrambling mechanisms to avoid the data being resolved by irrelevant entities.

Towards EV Cloud Computing

EVs establish information interactions along with computation resource sharing, and it is challenging to achieve data access control and traceability during dynamic participation. EVs establish energy interactions with energy resource sharing, and it is challenging to achieve aggregated energy transmission with identity privacy preservation.

Towards EV Edge Computing

EVs communicate with neighboring sensors, and it is challenging to achieve anonymous data transmission and batch authentication. EVs and LAGs establish direct energy interactions, EVs and sensors establish indirect energy interactions via RSUs, and it is challenging to achieve centralized and distributed energy allocation with energy status privacy preservation.

3.1.2 Distributed Consensus

EVCE computing has similar features (e.g., centerless trust and collaborative intelligence) as the blockchain, in which all the participants collectively validate new blocks for collaborative management [8]. Blockchain establishes distributed consensus before transaction records are written into a digital ledger. It is executed by the collaborative participants based on timestamps and Merkle hash tree algorithms. The proof of work (PoW) and proof of stake (PoS) are two typical consensus algorithms. The PoW is absolutely dependent on the computing power, and the participants compete to obtain correct data writing with relatively random and low probability. The PoS is based on a deterministic approach and probability, and an account is chosen depending on its total stakes.

Figure below shows the structure of a consortium blockchain, and each block contains a cryptographic hash value to the prior block. The traditional PoW in Bitcoin is available for the distributed consensus, which is achieved based on data contribution frequency and energy contribution amount.

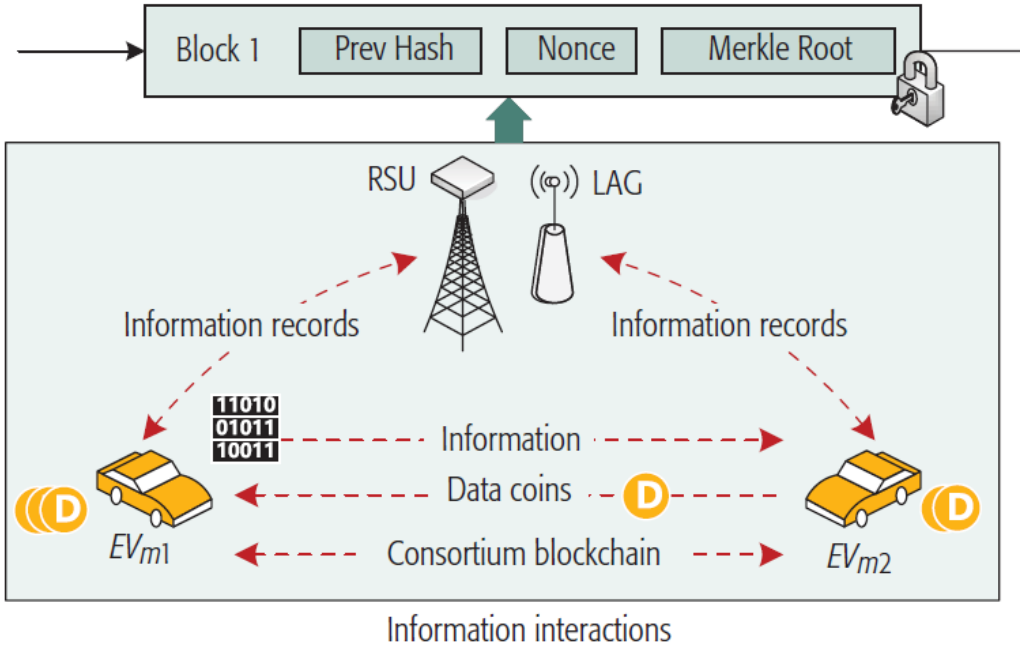


Figure 3.1: Information Interaction

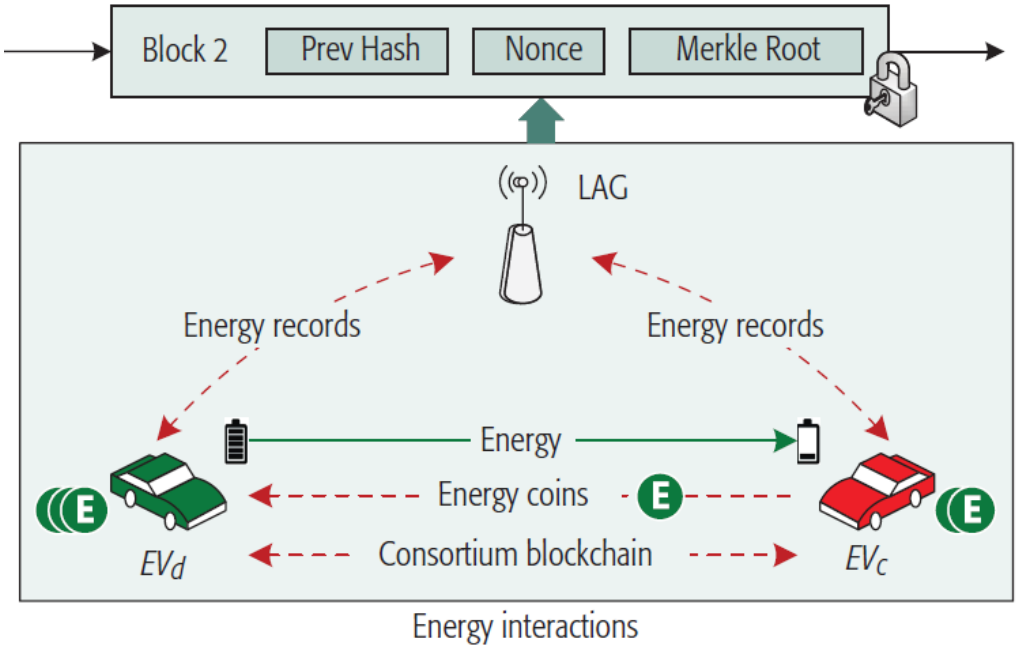


Figure 3.2: Energy Interaction

Datacoin

Datacoin is a reliable, censorship-free currency that can be used for transactions and data storage within its sophisticated blockchain.

Figure 3.3: Datacoin

Data is stored in the blockchain forever and can be retrieved using a transaction hash as an identifier. Datacoin is a platform that can be used by applications such as torrent trackers, encrypted messaging services, and can be used to store other kinds of small data all censorship-free!

Developers can store torrent files, certificates, and with future development, HTML pages and other kinds of meta-information in the Datacoin blockchain. These are also very recoverable in case of data loss.

Energycoin

EnergyCoin is a Peer to Peer cryptocurrency based on the disruptive Bitcoin technology. Transactions in EnergyCoin run on the Proof of Stake protocol. The choice was a conscious one for a sustainable aware vision of our future. Staking is more energy efficient compared to mining and for now, sit the principles of the EnergyCoin platform better than other protocols

Figure 3.4: Energycoin

Proof of Data Contribution Frequency

During information interactions, data coins are defined based on the proof of EVs' data contribution frequency. A consensus process is performed by authorized RSUs or LAGs for audit, and a new block will be formed for verification during a consensus process. If the EV has the highest data contribution frequency in a certain period, it will be rewarded by data coins as incentive to encourage other EVs to contribute information.

Proof of Energy Contribution Amount

During energy interactions, energy coins are defined based on the proof of EVs' energy contribution amount, which is directly related to the periodic energy interactions. A consensus process is performed by the authorized LAGs, and the amount of discharged energy is measured by smart meters. If an EV has the most energy contributions in a certain period, it will be rewarded by energy coins for encouraging other available EVs to participate in the discharging operations.

The data coins and energy coins are only exchanged among EVs, and are allowed to be circulated and traded. During the information interactions, the sensors will not obtain data

coins due to their inherent functions for data distribution. During the energy interactions, the sensors and RSUs will not obtain any energy coins since they have no redundant energy to perform discharging operations.

The proof of data contribution frequency and the proof of energy contribution are defined for determining representation in majority decision making. The established data coins and energy coins can be applied for vehicular resources allocation. If an EV contributes more frequently for collaborative intelligence, it will obtain more data coins. It will be assigned higher priority to access the resource pool, and its data may be assigned higher credibility for decision assistance. If an EV feeds more energy back into the grid or other entities, it will own more energy coins, and will be assigned with higher

3.2 Security Solutions for Electric Vehicles Cloud and Edge Computing

In EVCE computing, there are moving EVs (i.e., EVm), discharging EVs (i.e., EVd), charging EVs (i.e., EVc), RSU, LAG, and multiple sensors. The data coins and energy coins are considered during the EVs' interactions; anonymous data transmission and aggregated energy transmission are achieved during heterogeneous interactions.

3.2.1 Security Interaction in Cloud Computing

Figure 3.5 shows secure interactions in cloud computing, involving EVs (i.e., EVm and EVd), an RSU, and a LAG, and the distributed EVs' resources are aggregated for more flexible allocation and usage.

Information-Driven Security Scheme

The moving EVs act as network operators to establish V2V communications. EVm interacts with its neighboring EVs EVm1, EVm2, . . . , EVmi for collaborative operations. These moving EVs jointly perform cooperations in which data-coinbased anonymous data confirmation and access control should be particularly considered for data exchanging and sharing.

In the initialization, the moving EVs perform key agreement and distribution based on

the peer-to-peer networks; temporary session keys could be established based on lightweight symmetric encryption. The shortest path tree routing and multi-path key mode could be applied for group key agreement. Thereafter, the moving EVs and the RSU establish interactions via access challenges and responses. Here, the moving EVs jointly complete cooperation for data exchanging, the signed data could be broadcast to neighboring EVs, and mutual authentication could be established based on homomorphic encryption and secure multi-party computation.

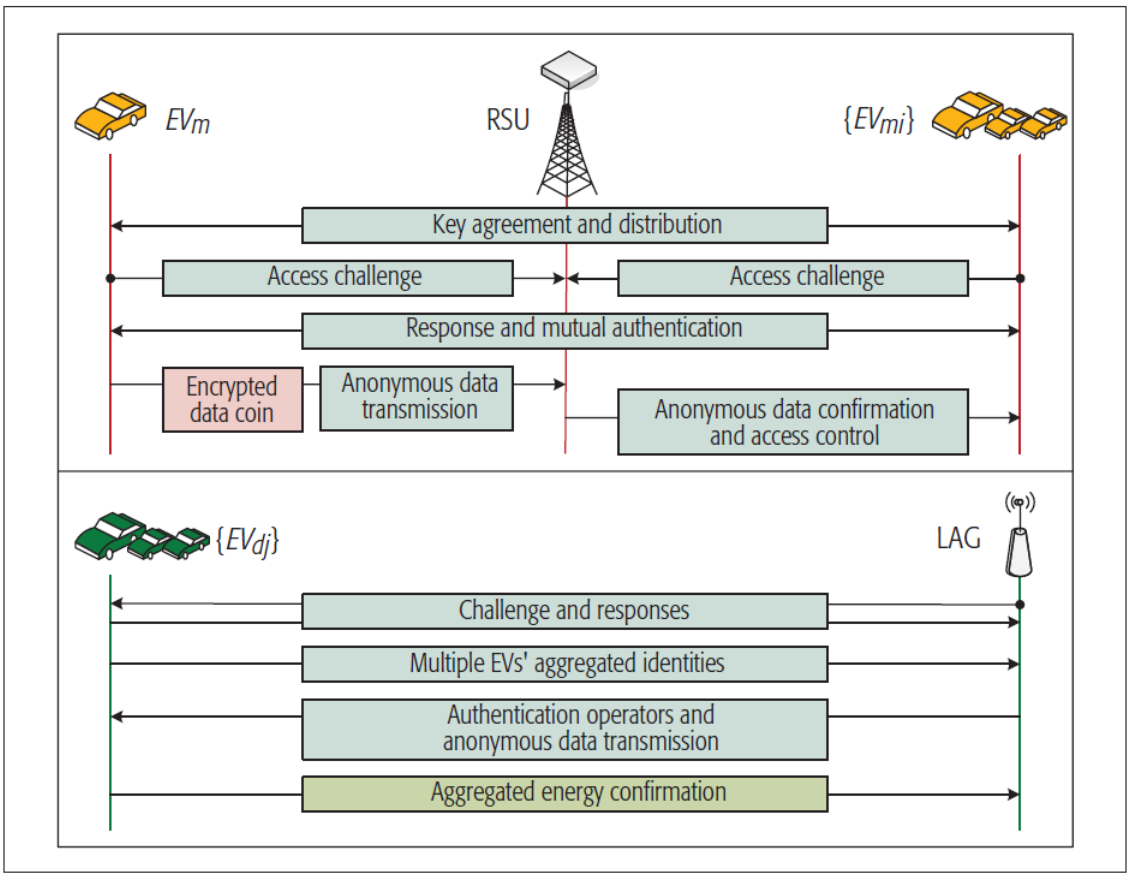


Figure 3.5: Secure Scheme in Electric Vehicle Cloud Computing

The encrypted data coins directly influence resource allocation among different moving EVs. Moreover, spatio-temporal attributes could be applied for access control, and conditional proxy re-encryption could be used to address data sharing and data hiding issues among different EVs. [1].

Energy Driven Security Scheme

The multiple discharging EVs EVd1, EVd2, . . . , EVdj (j N*) act as virtual power plants to establish an aggregated energy resource pool via the LAG. These discharging EVs' energy should be aggregated during transmission with privacy considerations.EVd1, EVd2, . . . , EVdj generate pseudo random numbers as access challenges to be transmitted to the LAG for launching a session. When the EVs and LAG establish interactions, the EVs' aggregated identifiers are transmitted to the LAG for mutual authentication. The LAG extracts its local values to compute authentication operators based on lightweight cryptographic primitives for identification and authentication. Here, elliptic curve digital signature algorithm (ECDSA)-based signature (e.g., ring, group, and blind signatures) could be applied for anonymous data transmission.

ECDSA

Elliptic Curve Digital Signature Algorithm or ECDSA is a cryptographic algorithm used by Bitcoin to ensure that funds can only be spent by their rightful owners.

A few concepts related to ECDSA:

Private key: A secret number, known only to the person that generated it. A private key is essentially a randomly generated number. In Bitcoin, someone with the private key that corresponds to funds on the public ledger can spend the funds. In Bitcoin, a private key is a single unsigned 256 bit integer (32 bytes).

Public key: A number that corresponds to a private key, but does not need to be kept secret. A public key can be calculated from a private key, but not vice versa. A public key can be used to determine if a signature is genuine (in other words, produced with the proper key) without requiring the private key to be divulged. In Bitcoin, public keys are either compressed or uncompressed. Compressed public keys are 33 bytes, consisting of a prefix either 0x02 or 0x03, and a 256-bit integer called x. The older uncompressed keys are 65 bytes, consisting of constant prefix (0x04), followed by two 256-bit integers called x and y (2 * 32 bytes). The prefix of a compressed key allows for the y value to be derived from the x value.

Signature: A number that proves that a signing operation took place. A signature is

mathematically generated from a hash of something to be signed, plus a private key. The signature itself is two numbers known as r and s. With the public key, a mathematical algorithm can be used on the signature to determine that it was originally produced from the hash and the private key, without needing to know the private key. Signatures are either 73, 72, or 71 bytes long, with probabilities approximately 25percent, 50percent and 25percent respectively, although sizes even smaller than that are possible with exponentially decreasing probability.

The EVs have diverse energy preferences for the discharging request. An EV supplies its idle energy back into the power grid for aggregating distributed energy. During energy interactions, the energy is regarded as a non-differential resource for reallocation. The discharging EVs jointly establish a flexible energy pool, which can be shared by the EVs around the same LAG. The Merklehash- tree-based selective disclosure mechanism could be applied for protecting the sensitive data fields. Such data structure avoids storing all the data fields to realize efficient and secure verification of a large data structure.

3.2.2 Securing Interaction in Edge Computing

Figure 5 shows secure interactions in edge computing, involving the EVs (i.e., EVm, EVd, EVc), an RSU, a LAG, and sensors, and the distributed EVs' resources are applied for local computing and processing.

Information-Driven Security Scheme

Information-Driven Security Scheme: The moving EVm acts as a mobile data calculator during information interactions in edge computing. Batch authentication should be established by ultra-lightweight algorithms.

The sensors constantly broadcast omni-bearing queries, and EVm gives a response upon receiving a periodic query. Thereafter, a key agreement and distribution scheme could be established to support dynamic participation and authentication. EVm and sensors perform mutual authentication based on the permutation, symmetric encryption, or hash/hash-based message authentication code (HMAC). The multicast message authentication and batch authentication become efficient for secure interactions among multiple sensors.

HMAC

In cryptography, an HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message, as with any MAC. Any cryptographic hash function, such as SHA256 or SHA-3, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-X, where X is the hash function used (e.g. HMAC-SHA256 or HMAC-SHA3). The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and the size and quality of the key.

HMAC uses two passes of hash computation. The secret key is first used to derive two keys – inner and outer. The first pass of the algorithm produces an internal hash derived from the message and the inner key. The second pass produces the final HMAC code derived from the inner hash result and the outer key. Thus the algorithm provides better immunity against length extension attacks.

HMAC does not encrypt the message. Instead, the message (encrypted or not) must be sent alongside the HMAC hash. Parties with the secret key will hash the message again themselves, and if it is authentic, the received and computed hashes will match. Here, EVmfirst obtains the raw sensing data Data0, and further performs processing and computing to obtain the advanced data Data'0. Thereafter, EVm transmits Data'0 to an RSU for data integration. Other neighboring EVs also perform similar authentication operations, and further transmit Data'1, Data'2, ..., Data'x to the RSU. Based on the distributed consensus, Data'* will be written into the digital ledger, and data coin will be assigned to the appropriate EV.

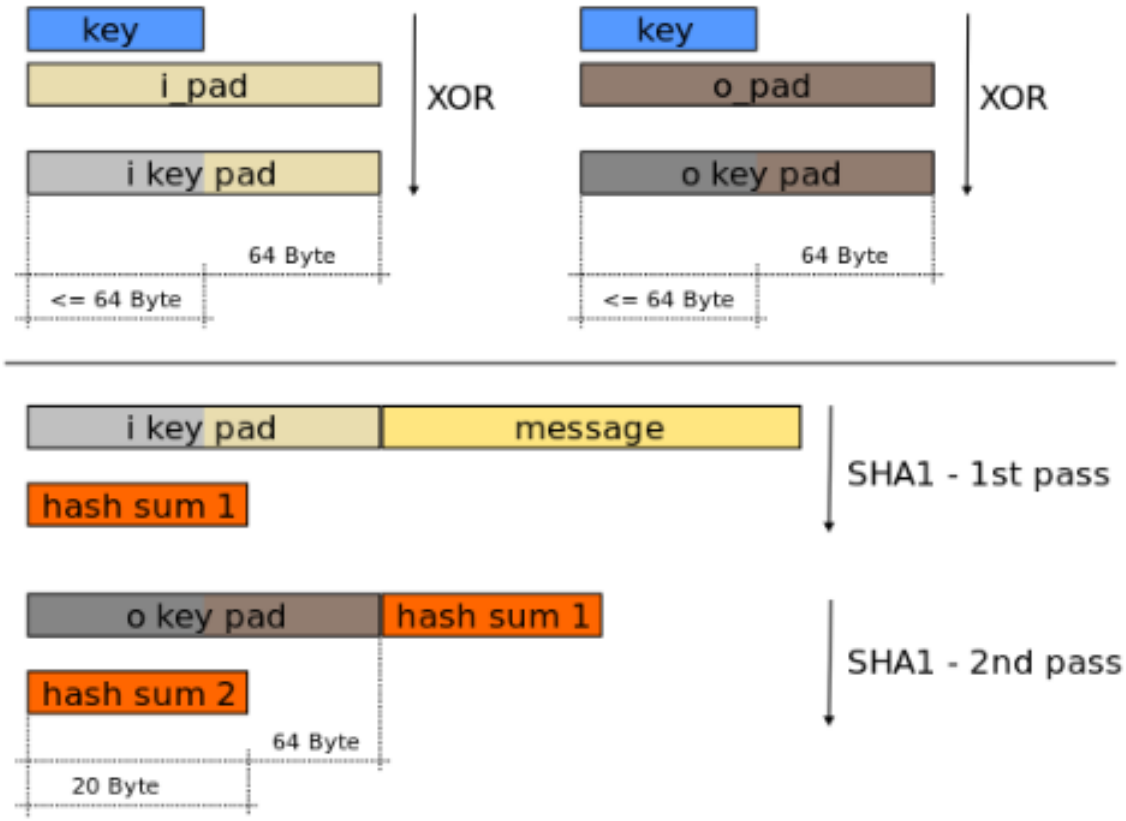


Figure 3.6: Hash Machine Authentication Code

Here, EVm first obtains the raw sensing data Data0, and further performs processing and computing to obtain the advanced data Data'0. Thereafter, EVm transmits Data'0 to an RSU for data integration. Other neighboring EVs also perform similar authentication operations, and further transmit Data'1, Data'2, ..., Data'x to the RSU. Based on the distributed consensus, Data'* will be written into the digital ledger, and data coin will be assigned to the appropriate EV.

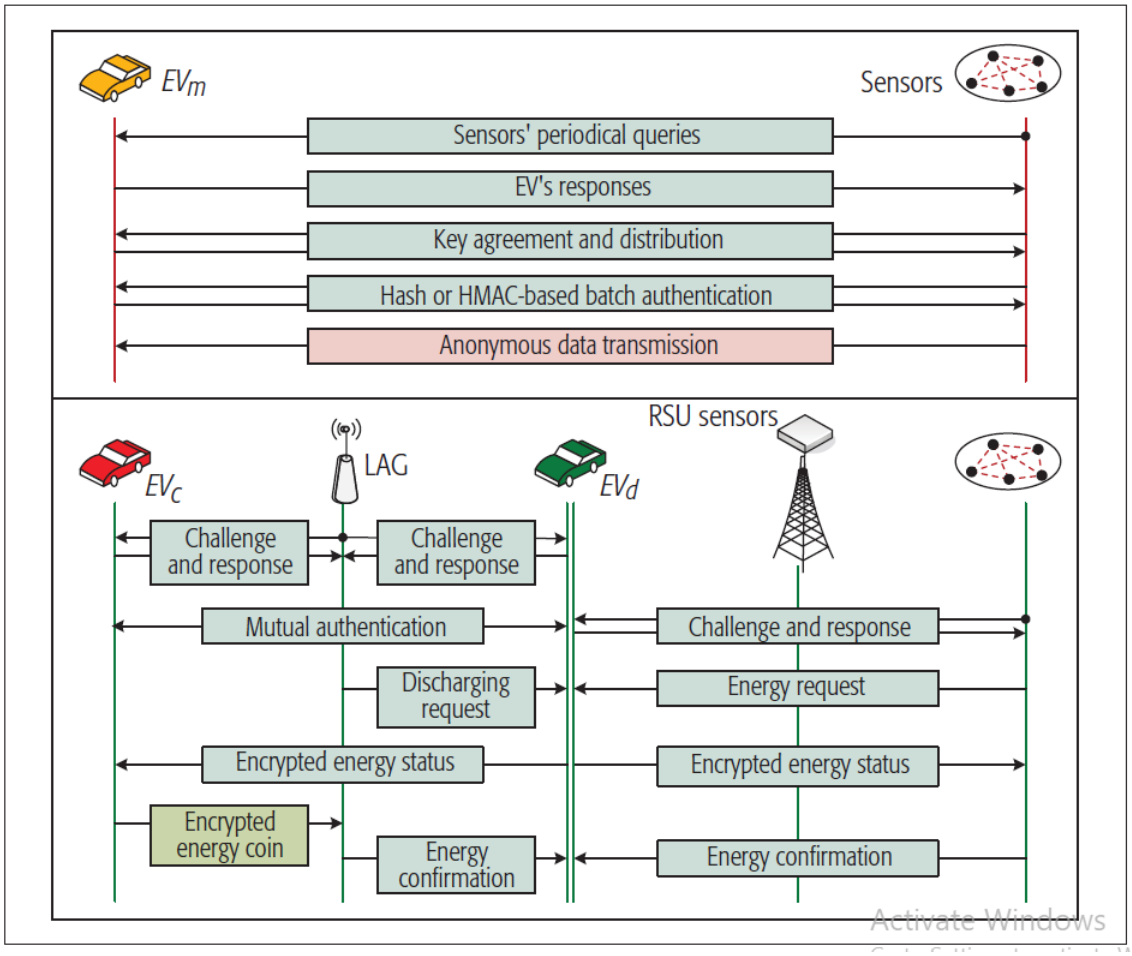


Figure 3.7: Security Scheme in EV Edge Computing

Energy Driven Security Scheme

The discharging EVd acts as a small portable plant to establish communications with EVc, LAG, RSU, and sensors during energy interactions in the edge computing. For one aspect, the LAG generates pseudo- random numbers as access challenges, and respectively transmits them to surrounding EVc and EVd. After the LAG and EVs establish mutual authentication, EVd is requested to perform discharging operation to feed a local vehicle EVc. Upon EVd receiving the discharging request, it could wrap its energy status into ciphertexts and transmit the encrypted energy status to EVc. The delivery of energy coins is performed based on pseudonym, avoiding sensitive privacy disclosure. For the other aspect, the sensors

perform similar operations, and establish challenges and responses with EVd. The sensors transmit energy requests to EVd via an RSU for local energy access. EVd's energy status will be transmitted to the sensors for energy confirmation. EVc and sensors will be charged by the wired and wireless charging technology, and energy coins are exchanged between EVd and EVc based on the distributed consensus. The concealed data aggregation can be applied for privacy preservation, and hierarchical data access control can be applied intra-network (e.g., V2G communications) and inter-networks (e.g., V2G and V2I communications).

Conclusion

This study focuses on security issues for both information and energy interactions in EVCE computing. The context-aware vehicular applications are presented according to the EVs' different roles, blockchain-inspired data coins and energy coins are defined to achieve distributed consensus; and data contribution frequency and energy contribution amounts are applied for proof determination. Security schemes are proposed for cloud and edge computing to launch perspectives on vehicular applications.

References

[1] S. K. Datta et al., "Vehicles as Connected Resources: Opportunities and Challenges for the Future", *IEEE Computer*, vol. 12, no. 2, 2017, pp. 26–35.

[2] H. Li et al.,"Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP,"]*IEEE Wireless Commun.,* vol. 22, no. 4, Aug. 2015, pp. 74–80.

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

[4] A. Lei et al., "Blockchain-Based Dynamic Key Management for HeterogeneousIntelligent Transportation Systems," *IEEE Internet of Things J.,* 2017.

[5] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and AnonymousMessaging Streams, " *IEEE Trans. Dependable and Secure Computing,* 2017.

[6] P. K. Sharma et al., "DistBlockNet: A Distributed Blockchains- Based Secure SDN Architecture for IoT Networks, " *IEEE Commun. Mag.,* vol. 55, no. 9, Sept. 2017, pp. 78–85.

[7] K. Zhang et al., "Mobile Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Offloading, "*IEEE Vehic. Tech. Mag.,* vol.12, no. 2, 2017, pp. 36–44.

[8] Z. Zhou et al., "Software Defined Machine-to-Machine Communication for Smart Energy Management, " *IEEE Commun. Mag.,*vol. 55, no. 10, Oct. 2017, pp. 52–60.

[9] X. He et al., "A Novel Load Balancing Strategy of Software- Defined Cloud/Fog Networking in the Internet of Vehicles, " *China Commun.,* vol. 13, Supplement 2, 2016, pp. 140–49.

[10] K. Sasaki et al., "Vehicle Control System Coordinated Between Cloud and Mobile Edge Computing, " *Proc. 55th Annual Conf. Society of Instrument and Control Engineers of Japan,* 2016, pp. 1122–27.