Poster: (SmartCoin) A Novel Incentive Mechanism for Vehicles in Intelligent Transportation System Based on Consortium Blockchain

Lokendra Vishwakarma, Debasis Das
Indian Institute of Technology Jodhpur, India
vishwakarma.3@iitj.ac.in, debasis@iitj.ac.in

Abstract

An intelligent transportation system (ITS) improves traffic safety and efficiency by enabling vehicles to generate and broadcast messages. However, it is not easy to trust the received message's credibility in an untrusted environment or untrusted network. Additionally, there is no reward mechanism for the honest message generator. Hence, to improve safety and network efficiency and encourage more vehicles to participate in network improvisation, we proposed a novel incentive mechanism for vehicles called SmartCoin based on a consortium blockchain. The proposed scheme aims to achieve social welfare, improved transportation, less traffic congestion, reduced road accidents, and a transportation network free from fraud messages. In the proposed scheme, vehicles give the rating to the message source vehicle based on the validity of the message. Some SmartCoins are credited into the vehicle's account at the blockchain according to the rating of the message. The SmartCoins could be redeemed either at the fuel station, electric charge station for electric vehicles and vehicle service station. Blockchain technology provides decentralization, immutability, transparency to the ITS. The secure storage for the SmartCoin, traffic messages and user information is achieved using blockchain. The secure hash algorithm (SHA256) and elliptic curve digital signature algorithm (ECDSA-192 bit) are used to provide secure communication, message integrity and authentication for vehicles and information. The result analysis reveals that the proposed scheme is effective, comprehensive, and feasible in collecting and storing trust values in the ITS network. The performance evaluation showed enhancement in performance as 90% less consensus delay and 70-80% less storage and communication cost compared to state-of-the-art schemes.

I. Bibliographic Reference

Lokendra Vishwakarma, Debasis Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain", Elsevier Vehicular Communications 2022,
DOI: https://doi.org/10.1016/j.vehcom.2021.100429

Poster: (SmartCoin) A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain

Lokendra Vishwakarma, Debasis Das
{vishwakarma.3, debasis }@iitj.ac.in

Problem Overview

Improved traffic safety and network efficiency can be achieved by using the Intelligent Transportation System (ITS) to create and transmit traffic-related messages such as traffic information and road accidents. However, it is difficult to trust the messages broadcasted in an untrustworthy environment. In addition, there is no incentive for honest message generators to improve network efficiency, which discourages the participation of network objects, especially vehicles. For a network like ITS, where real-time solutions are needed, state-of-the-art techniques are ineffective because of their large consensus latency, low throughput, and low involvement of network objects. We developed a new incentive system for ITS based on a consortium blockchain called SmartCoin to generate trust and offer authentication, integrity, and confidentiality.

Contribution

1. To improve the network efficiency and maximum honest public participation, a novel incentive mechanism based on consortium blockchain is proposed.
2. A new digital cryptocurrency called SmartCoin is introduced, which is used as an incentive for vehicles.
3. The performance analysis based on the propagation delay, block processing time, consensus delay, computation cost, storage cost and communication cost, reveals that the performance is enhanced as 90% less consensus delay and 70-80% less storage and communication cost.

Type of Messages

We have taken 7 type of messages into account and the corresponding value of SmartCoin, which is to be credited into the vehicle account if messages are generated by the vehicles. The messages are arranged in priority order. $M1$ has the highest priority, so the SmartCoins are, and $M7$ has the lowest priority. The priority is assigned based on the emergency to take action. The Accident is a life lost event, so it has the highest priority. Similarly, priority is assigned to other types of messages. The STC is the representation unit for SmartCoins.

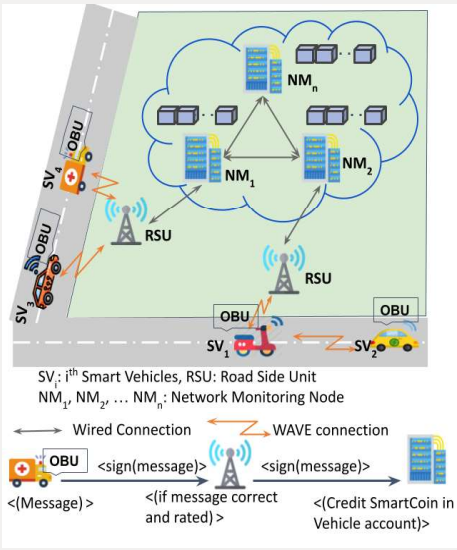
Symbol	Meaning	Credit SmartCoin
$M1$	*Accident occurred*	$\rightarrow 100STC$
M2	*Accident area*	$\rightarrow 50STC$
M3	*School Zone*	$\rightarrow 30STC$
M4	*Malicious information*	$\rightarrow 20STC$
M5	*Traffic Jam*	$\rightarrow 15STC$
M6	*Fuel station*	$\rightarrow 10STC$
M7	*Road intersection*	$\rightarrow 5STC$

Bibliographic Reference

Lokendra Vishwakarma, Debasis Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain", Elsevier Vehicular Communications 2022, DOI: https://doi.org/10.1016/j.vehcom.2021.100429

Proposed System Model and Consensus Algorithm

We have employed the consortium blockchain in the proposed scheme. Below figure illustrated the network model and consensus algorithm of the proposed scheme. It consists of three components, i.e., Vehicle (V), Roadside unit (RSU) and the network monitoring (NM) node. The vehicles are equipped with OBU, which provides the vehicles' computation, storage, and communication capacity. The RSU broadcasts the messages into the network and coordinates the vehicles to communicate with other vehicles if they are not in each other's coverage area. The type of communication in the scheme is vehicle to vehicle (V2V), vehicle to RSU or RSU to vehicle (V2R)/(R2V), RSU to NM node or NM node to RSU (R2N)/(N2R). The NM node maintains the vehicle information and network performance messages received from vehicles in a blockchain. We have employed the consortium blockchain, where vehicles and RSU are the public nodes that generate, receive and rate the messages but are not responsible for block mining. In contrast, the NM nodes make the private blockchain network, mine the blocks, and append them into the blockchain using Algorithm 1.



Algorithm 1: Consensus algorithm.

```
Input: Transaction: Tr_1, Tr_2, ...Tr_n
Result: Block
transaction_pool.append= new_transaction;
  // append all the new transactions in the transaction pool
if node == proposer then
    merkle_root = createHashTree (transaction_pool.getAllTransactions);
    Timestamp=T;
    nonce=random_number;
    previousBlockHash = getHash(previous_block);
    blockHash = getHash(merkle_root, Timestamp, previousBlockHash);
    block = createBlock(merkle_root, Timestamp, previousBlockHash,
      blockHash, nonce);
    sign_block(block);
end
if node != proposer then
    receive_block(block, nonce);
    merkle_root = createHashTree (transaction_pool.getAllTransactions);
    block*= createBlock(merkle_root, Timestamp, previousBlockHash,
      blockHash, nonce);
    if block == block* then
        block_status(valid);
    else
        block_status(not_valid),
        node.status = bad;
    end
end
if (count(block_status == valid)≥3N/4) then
    blockchain.append(block);
end
```

Security and Perform anceAnalysis

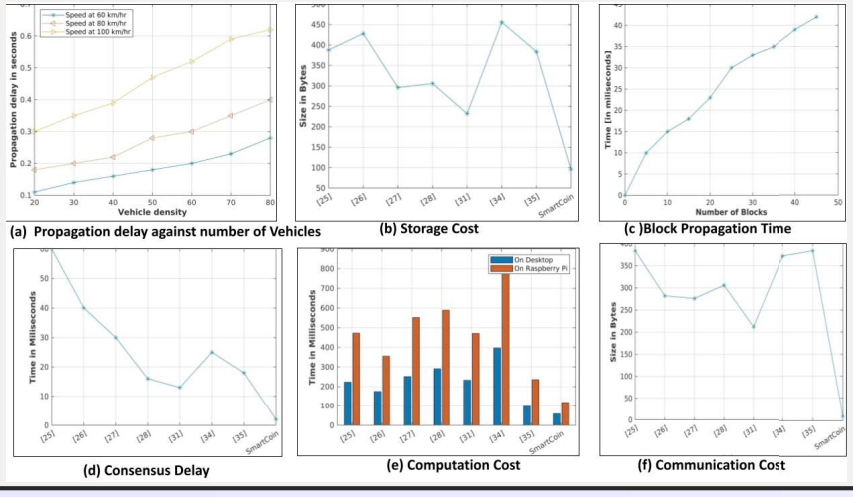
Theorem 1. *The SmartCoin supports authenticity of the data shared between OBU and NM node.*

Theorem 2. *The SmartCoin supports data integrity of the network traffic messages, user information and transactions.*

Theorem 3. *The SmartCoin supports non-repudiation of the network traffic messages, user information and transactions.*

Lemma 4. *The SmartCoin protocol is protected from double-spending attack. A double-spending attack is possible if there exist a double-spending attack time $t_{dsa} \in [0, \infty]$ such that, in this duration, the fraudulent chain length is longer than that of honest chain length.*

Lemma 5. *The SmartCoin protocol prevents fork generation. A fork in the blockchain is possible if $t_{fork} \in [0, \infty]$ such that, in this duration, the fraudulent chain length is longer than that of honest chain length.*



(a) Propagation delay against number of Vehicles (b) Storage Cost (c)Block Propagation Time

(d) Consensus Delay (e) Computation Cost (f) Communication Cost