**LITERATURE SURVEY**

**TITLE:**

**Credit Coin: A Privacy-Preserving Blockchain Based Incentive Announcement Network for Communications of Smart Vehicles**

**PUBLICATION: IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS**

**PUBLICATION YEAR: 2018**

**ALGORITHMS USED:**

1. **Threshold Ring Signature Algorithm:**

A ring signature is a message authentication method with the threshold 𝑡𝑡 and the member size 𝑟𝑟. It is a message-sharing protocol that a message is not valid unless at least 𝑡𝑡 participants sign it. Meanwhile, the identities of the real signers are still covered in 𝑟𝑟 people.

1. **Merkle Hash Tree:**

Merkle Hash Tree was used in the construction of cryptography in order to create the hash index of transaction records and the verification of the block’s locations on Blockchain. Merkle Hash Tree is a binary tree, and each leaf node is related to a fixed hash value calculated from a small fixed fragment.

Merkle tree serve to encode blockchain data more efficiently and securely.

1. **Byzantine fault tolerate algorithm:**

Byzantine fault tolerate algorithm is to reach agreement on the same information even when some of the vehicle in the VANET fail to respond or respond with incorrect information

The object of a BST mechanism is to safeguard against the system failure by employing collective decision making (both correct and fault information) which aims to reduce to influence of the faulty vehicles.

1. **Combined Public key Cryptosystem:**

It is used for key management and identity authentication. CPK is used to simplify certificates and reduce cryptographic time consumptions of ring signature.

1. **Sybil attack Prevention:**

To detect false identity in a VANET

The proposed algorithm includes ABC algorithm by considering two parameter as follows:

1. Closeness Centrality
2. Shapely values

ABC algorithm is used in proximity of closeness centrality to optimize route in VANET and to detect and prevent sybil attack.

Closeness centrality is used to calculate the value of each vehicular node, This value signifies the importance of each node in network and shapely value is also calculated.

1. **Man In the Middle attack prevention:**

VANET may contain dishonest vehicles such as man in the middle attackers aiming to distribute and share malicious content with the vehicle.

ARP Spoofing algorithm can be used to resolve this problem.

**TITLE:**

**A Blockchain based Incentive Provisioning Scheme for Traffic Event Validation and Information Storage in VANETs.**

**PUBLICATION: Elsevier- Information Processing and Management**

**PUBLICATION YEAR: December 30, 2020**

**ALGORITHMS:**

1. Signature verification algorithm shows the function of Certificate Authority to verify signatures of vehicles.

CA generated the List of

* Valid Signature
* Invalid Signature
* Revoked Signature

**Ring Signature Verification -Signature Verification**

function verifysignatures (signature, signaturesList, status)

for i=0: i<signaturesList.length: i++ do

if signature == signaturesList[i] and status == “Valid”

Push signaturesList[i] in validSignatures

else if signature == signaturesList[i] and status == “Invalid”

Push signaturesList[i] in invalidSignatures

else if signature == signaturesList[i] and status == “Revoked”

Push signaturesList[i] in revokedSignatures

else

return ”Invalid Signature”

end if

emit status, signature, signaturesList,

end for

end

1. The mechanism of incentivization of the witnesses that confirm the event information generated by the initiators are defined using the below algorithm.

function giveIncentives (initiatorAddress, responderAddress, amount)

Get values: initiatorBalance, responderBalance

initiatorBalance = initiatorBalance-amount

responderBalance = responderBalance+amount

emit initiatorAddress, responderAddress, amount

end

1. Reputation of an event information is computed to check the authentication of an information

function calcReputation (eventInformation, vehicleInformation)

Get values: vehicleReputation

if eventInformation == true

if vehicleReputation<60

vehicleReputation = vehicleReputation+5

else

Leave reputation value unchanged

end if

else

if vehicleReputation<20

Cancel the vehicle’s registration

else

vehicleReputation = vehicleReputation-20

end if

end if

emit vehicleInformation, vehicleReputation

end

1. Participation rate is calculated: An Incentive mechanism is to increase the participation rate

Participation Rate = (Nini / Ntot)\* 100

Nini -> number of vehicles that agree with the initiator

Ntot -> Total number of vehicles located at the event place.

1. Replay Attack Prevention:

In this attack, the hacker or any person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender. The receiver feels that it is an authenticated message but it is actually the message sent by the attacker. The main feature of the Replay Attack is that the client would receive the message twice, hence the name, Replay Attack.

PREVENTION:

Timestamp method:

Prevention from such attackers is possible, if timestamp is used along with the data. Supposedly, the timestamp on a data is more than a certain limit, it can be discarded, and sender can be asked to send the data again.

Session key method:

Another way of prevention, is by using session key. This key can be used only once (by sender and receiver) per transaction, and cannot be reused.

**TITLE:**

**Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory**

**PUBLICATION: IEEE TRANSACTIONS**

**PUBLICATION YEAR: 22 Sep 2018**

1. **Efficient Reputation Calculation Using Subjective Logic Model**

**If an information received by a vehicle from a RSU is true, vehicle give a positive opinion. A Miner candidates with more positive opinion have a secure and reliable message.**

**Some vehicles send a fake rating because of collision with malicious RSUs and selfish purpose.**

**Vehicles choose their own best miner candidates as the miner according to reputation calculation.**

**Subjective logic is utilized to formulate individual evaluation of reputation based on historical interactions and recommended opinions.**

1. **Contract Theory**

**There still exists a potential block verification collusion attack in the vehicular blockchain**

**Block Manager will offer a part of transactions**

**Reduce an impact of information that are asymmetric.**

**It provides,**

1. **Latency in Block verification**
2. **Profit of the Block Manager**
3. **Utility of Block Verifiers**