INCENTIVE BASED COMMUNCATION IN VAN USING BLOCK CHAIN TECHNOLOGY

[1]Archana K V,[2]Savitha S K
[1]Student,[2]Assistant Professor
[1]Computer Science and Engineer,
[1]Bangalore Institute of Technology, Bengaluru,India

*Abstract :*From the last two-three years, the growth of smart cities has increased. As smart cities increase the problem of traffic and pollution upsurges, in order to overcome these issues, the VANET concept had introduced. VANET is one of the most promising utilities in the smart transportation system. In general, there are two major issues in VANET i.e., It is very difficult to forward a reliable announcement without revealing user identities and users have a lack of motivation to forward the announcement. So that to resolve these two issues we proposing an effective announcement network called credit coin and privacy-preserving based on the block chain. Block chain and credit coin allows the multiple users to generate or send an announcement in the non-filly trusted environment and also by offering some credit coins to the users for who is involved in the announcement of traffic information. Credit coin achieves privacy preserving by hashing all the user's information and also motivates users to forward announcement anonymously and reliably, the experiment results show the transmitting of information in an effective manner and offering credit coins.

***IndexTerms* -.VANET, Credit coin, Block chain, Incentive mechanism**

I. INTRODUCTION

VANET is used across vehicles and road safety devices for communication purposes which in turn responsible for smooth and secure vehicle behavior across the roads and also introducing the privacy-preserving incentive announcement network based on block chain named credit coins.

Block chain is introduced by Satoshi nakomota it is a decentralized distributed ledger it offers many benefits to business and it helps to develop a high degree of trust for business transactions. Block chain is mainly used for storage purposes once we store the data it is very difficult to alter the data because each node manages a copy of the whole or part of a database from the system. The block chain-based network is promising in the recording of data which is useful in vanet.

Credit coin able to build trust in the communication of smart vehicles and it motivates the users to forward announcements anonymously in a non-fully trusted environment and reliably. every user has a credit account and owns a credit coin at several addresses the account contains reputation points called coins and also it traces the malicious users and identifies in anonymous with related transaction Credit coins.

In general, there are two major issues in building an effective vehicular announcement network First, Difficult to forward reliable announcements without revealing user identities. Secondly, users usually lack the motivation to forward announcements so, to resolve these to issue we are designing an effective privacy preserving incentive announcement network based on block chain for motivating forward announcements.

II. Related Work

"A Threshold Anonymous Authentication protocol for vanets":

In this paper the author considers the threshold authentication to send the messages in reliability over the VANET and consider the multiple signatures to tackle the challenges but the solutions suffer from the heavy workload and lack of motivation to forward message. Advantages: Provides an efficient threshold anonymous authentication protocol. Disadvantages: Doesn't provide effectiveness of the batch verification in VANET.

"Efficient Secure Aggregation in Vanets":

The author addresses the trade-off between efficiency and security in VANET'S by combining the signature by providing higher level security but the performance is very low.Advantages: Provides efficiency & accuracy and Disadvantages: Performance is low.

"Aggregate Privacy- Preserving Authentication in VANET":

The author mainly concerns on increasing privacy in VANETS by using cryptographic data but several attacks occur over the like sybel attack because of this reliability decreases between the user's privacy and messages and efficiency is also very low.

Advantages: The proposed system allows aggregate privacy-preserving authenticated vehicular communications. The protocol guarantees trustworthiness of vehicle-generated messages and privacy of vehicles. The APPA protocol does not heavily rely on roadside units, which implies that the protocol can work even if the VANET infrastructure is incomplete and Disadvantages: Doesn't provide efficiency.

"Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications":

In this paper, the authors had proposed a new efficient system for balancing public safety and vehicle privacy in VANETs. Both a priori and a posteriori countermeasures have been used to thwart attackers. They had achieved this goal by drawing on the novel technology of MLGSs. They realized a context-aware threshold-authentication scheme for V2V communications in which the threshold can adaptively change in light of the context of messages, rather than having to be present during the system-design stage. Furthermore, a fast batch-verification method has been presented to speed up the validation of authenticated messages. Such a batch-verification approach is critical to make authentications implementable in VANETs, since vehicles in those networks periodically receive a large number of messages to be validated. Advantages: Propose an efficient

system for balancing public safety and vehicle privacy, Achieves a quite low latency and message loss ratio. And Disadvantages: Doesn't provide flexibility.

III. EXISTING SYSTEM

Existing work leveraged threshold authentication and group signatures to tackle the challenges of forwarding messages anonymously in VANETs. However, these solutions suffer from having a heavy workload and lack of incentives to forward messages. The existing work proposed the mechanism that works with the protocol Echo-announcement, with an objective to sencourage the users to honestly forward the true announcements. Existing work has proved this mechanism is effective in crowdsourcing tasks and ad hoc networks. However, they are not suitable for the privacy-preserving requirements of vehicular announcement networks.

Drawbacks:

Suffers from having a heavy workload and lack incentives to forward messages and Not suitable for privacy-preserving.

IV.PROPOSED SYSTEM

In the proposed system we present a Block chain-based network to build accounts and record transactions so that users' behavior is in privacy-preserving without loss of reliability. Credit Coin consists of five entities: The Trusted authority, the Trace manager, users (i.e., OBUs), RSUs, and a cloud application server. Each user is given a credit account, storing reputation points, i.e., coins. The users are encouraged to forward and receive packets with the incentive to increase their coins. In order to build an effective vehicular announcement network, there are two parts in Credit Coin. The first part is the announcement protocol, namely Echo-Announcement. This protocol provides threshold authentication and a certain privacy level to guarantee that anonymous announcements are reliable in Credit Coin. Users set their roles as follows: An Initiator invites other witnesses as Replies to agree with his/her announcement with corresponding signatures and generates an announcement with traffic information and responses signed by Repliers. Since there is a larger group of users concealing all of the participants in the protocol, the receivers of the announcement know the number of participants but cannot figure out their identities. The second part is the Block chain-based incentive mechanism that works together with Echo-Announcement. Every user in Credit Coin owns a credit account at several addresses. The account contains reputation points called the coins. Users reward traffic announcements from a certain area by paying some coins as incentives. They can also spend some coins to make an announcement for hunting others' reward missions. Thus, in Credit Coin, a user gets a small number of coins from replying to the aggregation request for an announcement of others. Meanwhile, he/she also has a chance to hunt a large number of coins by making an announcement to someone in particular, as someone else needs it. In Credit Coin, the traffic missions are managed by a cloud application server, and the transactions among users are forwarded based on Block chain. After constructing transactions, users forward the transactions to RSUs nearby, and then RSUs vote the validity of transactions. Later, the valid transactions are confirmed by the consensus server. Finally, the valid transactions are added to the blocks on the chain.

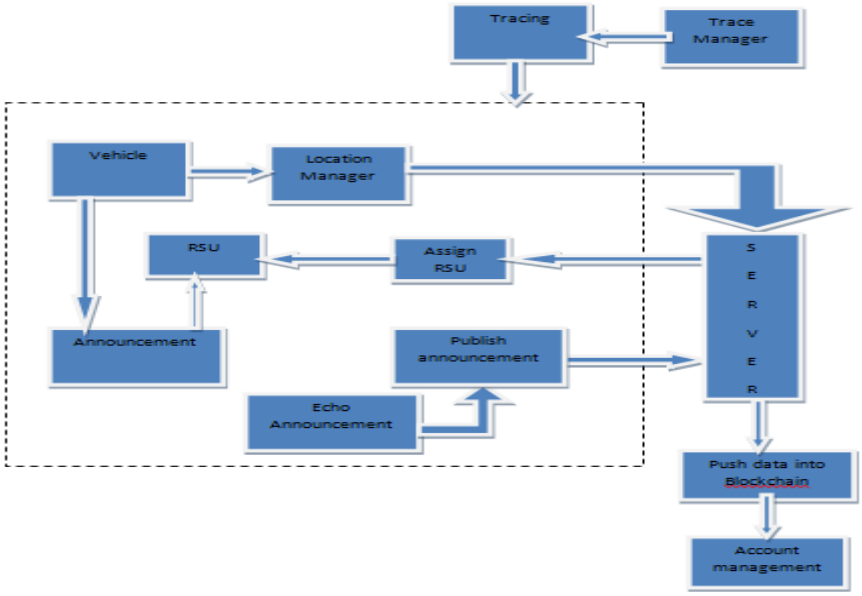

Fig.1: Architecture

Advantage: Provides an effective network for communication of smart vehicles. It is able to build trust in communications of smart vehicles, It achieves efficiency and privacy-preserving for the practical usage in forwarding announcements, Prevents many security attacks and achieves conditional privacy because Trace manager will trace malicious nodes when an unexpected event occurs, Credit Coin is efficient and practical in the simulations of smart transportation and smart vehicles.

V. METHODOLOGY

Incentive based communication can be done by using Credit coin app and block chain. Credit coin app is used to make announcement that get attached to the server and the ethereum wallet called mist.
Initially every users should register over the credit coin app while registering for each and every users obtain the private key and public key that is obtained by the trusted authority has well all registration data going to store in navicat that can access only by trusted authority.

A User1 get login over the app if its private key is correct then trace manager allow him to make announcement and that login detail get stored in navicat in login details table or else if its private key does not match then it get stored in activity table that process done by trace manager. And then User1 motivate the other users to involve in his/her announcement so User2 and User3 login over the app get the accept the announcement. And other User4 who want the information of traffic he requests and accepted based on required location.

When User1 make the announcement from his account ether (coins) is deducted and from User2 and User3 who are involved in the voting for their account ether (coins) are credited. And the User4 who accept or request for information from is account deducted and that amount is add-on to the user1.

VI. IMPLEMENTATION

The procedure of place the system in actual use is known as system implementations. System Implementation is the stage of proof when the theoretical design is turned out into working system. Therefore, this chapter gives complete details about our project implementation. The main aim is to inform the logic for the heterogeneous modules after notifying the analytical technique. This chapter appears with the implementation technicalities of the whole system and modules wise description.

Major modules

- Echo Announcement protocol
- Blockchain-based incentive mechanism

Modules Implemented

Echo Announcement protocol:

The first part is announcement protocol, namely Echo-Announcement. This protocol provides threshold authentication over non fully trusted environment. This method is used to send messages in the network to get reliability and certain privacy level to guarantee that anonymous announcements are reliable in credit coin for example. An Initiator invites other witnesses as Repliers to agree with his/her announcement with corresponding signatures and generates an announcement with traffic information and responses signed by Repliers. Since there is a larger group of users concealing all of the participants in the protocol, the receivers of the announcement knows the number of participants but cannot figure out their identities.

In threshold authentication protocols the receiver only accepts a message when the message is confirmed by the threshold number of vehicles in vanets. Although threshold authentication is a common method to send messages in the network, according, our protocol is under a non-fully-trusted environment. Thus, the signers who generate the signatures in Echo-Announcement are non-deterministic.

Echo-Announcement as the following example: Bob witnesses an accident and would like to let other drivers know by sending an announcement. To make such an announcement message trustworthy, Bob needs to cooperate with other witnesses. To do that, Bob firstly initiates a request to the surrounding witnesses for confirming his announcement message. After getting $t-1$ replies, Bob forwards the announcement with t confirmations (including himself) to other drivers heading to this place. Suppose Alice receives the announcement, who then checks its validity and re-plans the travailing route.

To accomplish Echo-Announcement, three types of packets are generated by the vehicles, depending on their roles.

- **Request Packet** (**RQP**) is a type of packets that are from an Initiator to a group of witnesses. The purpose is to ask the witnesses to agree on the announcement and sign it. In particular, RQP contains three information: the message reports, the threshold value t and the large group of r value.
- **Reply Packet** (**RPP**) is a type of packets from Repliers to the Initiator. If a witness is willing to join the announcement, the identity information for the generation of the ring will be sent back to Initiator. Particularly, if most of the RPPs are sent to one witness (Replier), the witness replies as Algorithm 1 to avoid congestion.
- **Announcements-Aggregated Packet (AGP)** is a type of packets sent from Initiator to other Verifiers. An AGP includes an announcement and a threshold ring signature of this announcement.

ECHO ANNOUNCEMENT PSEUDO CODE

PROTOCOL: PROPOSED ANNOUNCEMENT PROTOCOL

STEP1: SETUP ( )

- Trusted authority generates public parameters for all and generates the key for user registration

STEP2: REQUEST ( )

- User becomes a Initiator when he sees an accident.
- Initiator selects some parameters for announcement.
- Formulates RQP to other witness and invites them to join announcements.

Step3: Reply ( )

- Witness will forward back the RQP and becomes R by agreeing with the announcement.
- RPP includes fraction of ring signature.

Step4: Announcement ( )

- Initiator forwards the AGP to others after receving more than threshold.

Step5: Verifiers ( )

- Any user receiving the AGP can become verifiers V to verify the validity of AGP.

Block chain-based incentive mechanism

Blockchain-based incentive mechanism that works together with Echo-Announcement. Every user in Credit Coin owns a credit account at several addresses. The account contains reputation points called the coins. Users reward traffic announcements from a certain area by paying some coins as incentives. They can also spend some coins to make an announcement for hunting others' reward missions. Thus, in Credit Coin, a user gets a small amount of coins from replying to the aggregation request for an announcement of others. Meanwhile, he/she also has a chance to hunt a large amount of coins by making an announcement to someone in particular, as someone else needs it.

In Credit Coin, the traffic missions are managed by a cloud application server, and the transactions among users are forwarded based on Block chain. After constructing transactions, users forward the transactions to RSUs nearby, and then RSUs vote the validity of transactions. Later, the valid transactions are confirmed by the consensus server. Finally, the valid transactions are added to the blocks on the chain.

THERE ARE FIVE ENTITIES:

- Cloud application server: Cloud application server manages and stores non-privacy information in the VANETs, such as messageconsisting in AGPs. For security reasons, they are separated from the encrypted information to help the entire network operate safely. Application server spreads public information, such as missions and announcements. Cloud application server works as a watcher in Credit Coin.
- User (OBU): The user is an entity that trades in Credit Coin network. He/she creates or receives transactions. A user behaves in varieties of roles, such as Hunter, Replier, Initiator, and Verifier. We will elaborate these roles later in the following part.
- Public role: Public role is defined similarly to the user. However, it is more privileged than the user. It receives and sends transactions and creates coins as well.
- Trusted authority: Trusted authority takes charge of the generation and delivery of public keys. It createdaddresses for each user, and records the relationship between users and addresses.
- Trace manager: Trace manager is the role that traces malicious users. If a fraudulent transaction is reported to Trace manager, Trace manager will trace the malicious users with the help of Trusted authority and send a report to cloud application server.

VII. CONCLUSION

Here we proposed a credit coin, privacy-preserving Blockchain-based incentive announcement network with vehicle announcement protocol. Our announcement protocol maintains a reliable and efficient in the non-fully-trusted environment in vanets and offers an incentive who is involved in the announcement.

References

[1] L. Chen, S.-L.Ng, and G. Wang, "Threshold anonymous announcement in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 605–615, Mar. 2011.

[2] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[3] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 6, pp. 164–171, Jun. 2008.

[5] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc. Workshop Hot Topics Netw. (HotNets-IV), MD, USA, Nov. 2005, pp. 1–6.

[6] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in Proc. Int. Workshop Privacy Enhancing Technol., May 2005, pp. 197–209.