A Blockchain-based Privacy Preserving Scheme for Vehicular Trust Management Systems

Yuli Yao, Wendong Chen, Xiao Chen, Jie Ding and Senshan Pan

School of Computer Science, Jiangsu University & University of Edinburgh & Shanghai Maritime University

三等奖

Abstract

The Internet of Vehicles (IoV) trust management systems usually aims to provide a security guarantee for the interaction between vehicles, which has attracted many researchers' attention. However, most studies rarely consider data security and identity privacy protection issues brought about by trust management systems. Due to the untrusted environment, data dissemination among vehicles is easy to falsify. Meanwhile, the true identity information of vehicles may be exposed to message transmission and evaluation. To address these issues, this paper applies consortium blockchain to build a two-layer vehicular network architecture, and based on it, homomorphic encryption and pseudonym technology are introduced to protect data security while simultaneously preserving identity privacy of vehicles. For performance analysis, a novel compositional approach, named Performance Evaluation Process Algebra (PEPA), is applied to model the scheme.

Scheme

1. Architecture

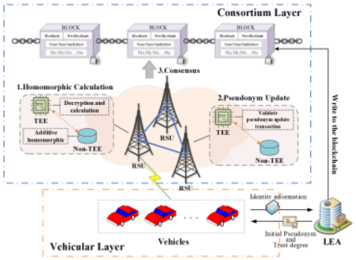

Fig 1: Two-layer consortium blockchain-based vehicular network architecture

The consortium layer includes a set of road-side units (RSUs), which serve as consortium members to maintain the consortium blockchain. The RSU consists of two parts: Trusted Execution Environment (TEE) and Non-TEE. The Non-TEE part collects and preprocesses messages from vehicles, while the TEE part performs the final trust calculation and pseudonym update verification. Additionally, the consortium layer is responsible for managing related operations regarding homomorphic computation, pseudonym updates, and consensus processes.

The vehicular layer is composed of a large number of vehicles that need to submit identity information to LEA for registration authentication before entering the system. Moreover, the vehicles can behave as message senders, trust evaluators, or validators depending on their participant activities in the system. The vehicular layer is the bottom layer of such a two-layer structure, and all vehicles here need to be under the administration of the consortium layer.

2. Implementation

Initialization Phase

1) A vehicle V_i first establishes a secure channel from it to LEA. Then it will send a registration request containing its true identity information to LEA through this channel.
2) When LEA receives the request from V_i, LEA invokes function to verify the true identity of V_i.
3) If identity is valid, LEA will initialize the pseudonym and trust degree of V_i and generate a public-private key pair for TEE.

Homomorphic Encryption Phase

1) Upon reception of the message from V_i, evaluator invokes function to evaluate message and get the rating value.
2) Then rating value is encrypted with TEE's public key as part of the evaluation result.
3) The evaluation result is sent to the RSU, completing the trust evaluation.
4) The non-TEE part of RSU sorts evaluation results and complete the addition homomorphism.
5) TEE calculates the final trust degree.

Pseudonym Update Phase

1) V_i submits a pseudonym update request to RSU in the form $< P_{V_i}, P_{V_i}^{new}, T_{V_i} >$, where P_{V_i}, $P_{V_i}^{new}$, T_{V_i} represent the current pseudonym, the pseudonym requested to be updated, and the trust degree, respectively.
2) Upon reception, the TEE generates a transaction for the request and broadcasts it to all validators.
3) Then validators invoke function to verify the transaction. The transaction is considered valid if and only if P_{V_i} & $P_{V_i}^{new}$ & T_{V_i}=true.
4) If valid, TEE will package transaction into a block, and write it to the blockchain.

3. Algorithm

Algorithm 1 Predefined Functionality

function $Init\_identity(V_i, VID_i)$
  for each VID_i **do**
    if verify VID_i = true **then**
      $V_i \leftarrow (P_{V_i}^c, T_{V_i}^c); R_k \leftarrow (PK_{T_k}; SK_{T_k})$;
    else
      return(invalid VID_i);
function $Evaluate\_trust(m_{i,j,k})$
  for each $< V_z, m_{i,j,k} >$ **do**
    $d_{z,i}^j \leftarrow evaluate(m_{i,j,k})$;
    $[d_{z,i}^j]_{PK_{T_k}} \leftarrow encrypt(d_{z\rightarrow i}^j)$;
  return($m_{i,j,k}, e_{j,i,k}^z$);
function $Compute\_trust(e_{j,i,k}^z)$
  compute $Sum_{V_i}^j \leftarrow \prod_{z=1}^{w} [d_{z,i}^j]_{PK_{T_k}}$;
  $NSum_{V_i}^j \leftarrow decryption(Sum_{V_i}^j)$;
  compute $T_{V_i} \leftarrow \frac{\sum_{j=1}^{p} NSum_{V_i}^j w}{p}$;
  return (T_{V_i});
function $Update\_pseudonym(Psdreq)$
  for each pseudonym update request **do**
    if verify P_{V_i} & $P_{V_i}^{new}$ & T_{V_i}= true **then**
      return(valid);
    else
      return(invalid $request$);

Algorithm 2 Normal Case Operations

upon reception of VID_i from V_i, LEA **do:**
▷ invoke $Init\_identity(V_i, VID_i)$ to verify V_i;
▷ generate $< P_{V_i}^c, T_{V_i}^c >$ for V_i and write it to blockchain;
▷ generate $< PK_{T_k}, SK_{T_k} >$ for T_k and broadcast PK_{T_k};
upon reception of $m_{i,j,k}$ from V_i, evaluator **do:**
▷ invoke $Evaluate\_trust(m_{i,j,k})$ to evaluate $m_{i,j,k}$;
▷ upload the transaction of $< m_{i,j,k}, e_{j,i,k}^z >$ to R_k;
upon reception of transaction from evaluator, R_k **do:**
▷ sort transactions with vehicle identification attributes;
▷ invoke $Compute\_trust(e_{j,i,k}^z)$ to compute T_{V_i};
▷ generate the transaction of $< P_{V_i}, T_{V_i}^{new} >$ and write it to blockchain;
upon reception of $pseudonym\ update\ request$ from V_i, TEE **do:**
▷ generate the transaction of $request$ and broadcast it to all validators;
upon reception of transaction from TEE, V_x **do:**
▷ invoke $Update\_pseudonym(Psdreq)$ to verify transaction;
upon reception of valid verification from V_x, TEE **do:**
▷ package $< P_{V_i}^{new}, T_{V_i} >$ transaction and write it to blockchain;

Performance evaluation

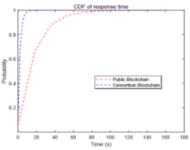

Fig 2: CDF of response time vs different blockchain

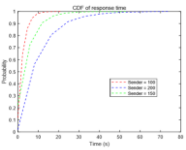

Fig 3: CDF of response time vs number of Senders

Figure 2 (left) shows that response time of our scheme in consortium blockchain is much lower than in public blockchain. Therefore, the vehicle network architecture based on consortium blockchain can reduce the overhead of trust computing.

Figure 3 (right) shows that with an increment in the number of Senders, the probability of the system is lower. It means that Senders should spend more time receiving a response from the system.

Conclusions

This paper mainly considers the data security and identity privacy preservation of vehicles in vehicular trust management systems. Firstly, we designed a two-layer vehicular network architecture based on a consortium blockchain. Secondly, according to the architecture, homomorphic encryption and pseudonym technology are introduced to protect data security and identity privacy, respectively. Finally, a novel compositional approach——PEPA, is employed to model our scheme and implement performance analysis. In the future, we will focus on the protection of data and identity information when RSU is threatened. Furthermore, reducing overhead as much as possible while protecting security is also a problem we should consider.

References

[1] Z. Lu, Q. Wang, G. Qu, H. Zhang and Z. Liu, "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2792-2801, Dec. 2019.

[2] H. Khelifi, S. Luo, B. Nour, H. Moungla and S. Hassan Ahmed, "Reputation-Based Blockchain for Secure NDN Caching in Vehicular Networks," 2018 IEEE Conference on Standards for Communications and Networking (CSCN), Paris, 2018, pp. 1-6.

[3] X. Chen, J. Ding and Z. Lu, "A Decentralized Trust Management System for Intelligent Transportation Environments," IEEE Transactions on Intelligent Transportation Systems.

[4] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 184-193.

[5] J. Ding, R. Wang and X. Chen, "Performance modeling and evaluation of real-time traffic status query for intelligent traffic systems," 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, 2016, pp. 238-242.

[6] X. Chen and L. Wang, "A Cloud-Based Trust Management Framework for Vehicular Social Networks," IEEE Access, vol. 5, pp. 2967-2980, 2017.

[7] Y. Bensitel and R. Romadi, "Secure data storage in the cloud with homomorphic encryption," 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), Marrakech, 2016, pp. 1-6.

[8] Y. Wang, F. Luo, Z. Dong, Z. Tong and Y. Qiao, "Distributed meter data aggregation framework based on Blockchain and homomorphic encryption," IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 1, pp. 30-37, 2019.

[9] L. Benarous and B. Kadri, "Privacy Preserving Scheme for Pseudonym Refilling in VANET," 2018 International Conference on Smart CommunicationsinNetworkTechnologies(SaCoNeT),ElOued,2018,pp.114-119.

[10] S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun and M. Huth, "Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems," IEEE Access, vol. 7, pp. 80390-80403, 2019.

[11] J. Hillston, "A compositional approach to performance modelling," Cambridge University Press, 1996.

[12] J. Hillston, "Fluid flow approximation of PEPA models," Second International Conference on the Quantitative Evaluation of Systems (QEST'05), Torino, 2005, pp. 33-42.

For further information

Linkman：Yuli Yao
Phone：18252580306
Email：Yuli.Yao@foxmail.com