International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

WIRELESS DISTRIBUTED CONSENSUS IN VEHICLE -TO-VEHICLE NETWORKS FOR AUTONOMOUS DRIVING

R.Saritha, Professor, Department Of CS SICET, Hyderabad
Seliveru Pavani,Thota Abhinash,Vudarapu Nutan Nivas Kiriti,Rapolu Akhileshwar Reddy
UG Student, Department Of CS, SICET, Hyderabad

Abstract—
The importance of selmanagement in society and the business world increases with communi cation aimed at collaboration to achieve important tasks. However, as the trust and confidenc e in these autonomous networks continues to increase, the limits of the centralized communic ation and decisionmaking processes used today are being pushed. This paper focuses on routi ng illicit traffic and reporting efficient and reliable methods based on wireless consensus, eve n when communication may not be reliable and there may be incorrect local sensor readings/ decisions. To achieve this goal, a new threestage approval mechanism based on Byzantine Fa ult Tolerance (PBFT) is proposed, designed so that the veto and comment stage are carried ou t according to the strict and difficult rules of car maneuvers. Scheduling tree synthesis has als o been proposed to achieve agreement across multiple decision points while serving to identif y network members' preferences. Detailed methods include consensus decision making, tree s ynthesis planning, dynamic grouping, etc. takes place. Simulation results show that when ther e is poor wireless communication and false traffic with false readings, consensus can be reach ed and propagated through the network. The results can be extended to other autonomous syst ems to improve safety in critical industries

Introduction

In important applications such as industrial areas and intelligent transportation systems (ITS), the use of IoT devices is increasing to facilitate the process of making important flightrelated decisions[1]. For example, a car today has approximately 60 to 100 sensors, including an ine rtial measurement unit (IMU), radar, and lidar. These sensors collect data and help control the machine's decisions on its own [2]. This type of selfcontained autonomous driving has attract ed extensive research attention. In recent years, technology companies have introduced their own driverless cars, including Uber, Tesla, Waymo, and BaiduAn alternative control method is decentralized, based on a decentralized consensus protocol (also known as an agreement al gorithm) in which vehicles share information with each other and then decide the decision tog ether rather than relying on a central authority. We also present this ethical framework as the Perception-Agency-
ConsensusAction (PICA) scheme. In PICA, nodes make the initial decision based on local kn owledge and calculations, and then consensus is reached through the nodes' consensus proces s before the operation. Compared with the centralized system, the network in the distributed P ICA scheme is based on point-to-
point communication and is usually organized in a distributed manner with short paths and lo

w costs [13]. Moreover, central servers have been replaced by decentralized databases that ar e not under the control of any party.

vehicle explains its plan. The car approved by the joint approval network 1 will be operated. I t is also worth noting that the mentioned process can be used not only in the vehicular networ k, but also in other cases where there are multiple parties, robotic and integrated drone contro l by many agents for data updates in the cluster server and application blockchains. Since the application of connected vehicles has emerged and cooperation in V2V networks is an examp le of the cooperation of many agencies, in this article we will mainly focus on the use of vehi cles. -

Incorrect decisions of nodes based on sensor error or Byzantine error. Since the tool applicati on must be reliable in terms of security, we divide the proposals with different certificates int o three types, which will be shown in Section IVA. Vehicle maneuvering can be viewed as a combination of many requests of different types, as discussed in Section IIIC, and are comple ted by sequential agreement by the network. We also evaluated the actual situation of oing th e agreement by a single vote and requested the written veto phase before the scheduled time. The formula is f = ≤ (N ≤ 1) / 3. In general, the threshold is the smallest T that satisfies the in equality 2T - N - f -
1. However, if the network is large or the failure rate is high, the transition threshold to the n ext level can be calculated using the method in Section V-
A. We show a successful V2V network handshake in Figure 2 below.

complete V2V network consensus process in Fig. 2 below.

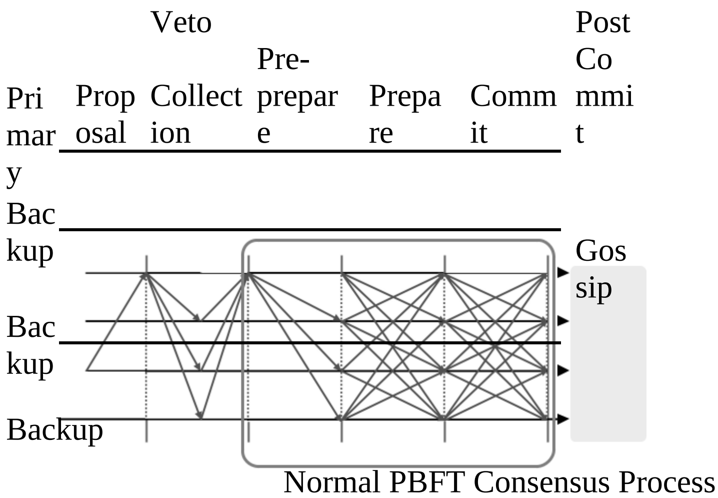

Fig. 2. Full PBFT consensus protocol with veto collection and gossip.

Below, we focus on the details of the process, including the operation of each phase, the three sub-

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

protocols (see migration, integration, and tree planning), and proof of security and livelihood.

A. Customer Proposal

will be made based on priority. The preferences and opinions of other members for specific re asons are taken into account in the approval process through the unification and optimization of wood preparation. However, the specific optimization depends on the specific application s cenario and will not be discussed in this article. Proof of security and stabilitThe security of t he system guarantees the approval of all illegal vehicles based on the number of local request s. In a system where at most f nodes fail out of 3f+1, the threshol/cluster size is set to 2f+1. Si nce there are the most faulty nodes, there must be at least one nonfaulty node at this intersecti on. This ensures security. In case of using the dynamic initialization mentioned in VA below, the algorithm also guarantees that there is at least one errorfree node at the intersection. If we consider the vehicle communication failure as a Byzantine fault, the network will be seen as p art of a synchronous network, similar to the traditional PBFT algorithm. In this case, looking at changes will change the owner's inability to continue the contract, so survival is also guara nteed. Consensus Improvement

The application process is the most decisive, the three recommended protocols (75.41%, 75.0 1%) % and 58.62% (failure rate is 0.25 for consensus protocol, relay protocol, and centralized protocol, respectively). Compared to relay systems, centralized systems suffer from faster de gradation and higher failure rates. As the percentage of defective vehicles increases, violation s may occur. However, this risk is usually reduced by a violation that causes the vehicle to m alfunction by not completing the central system and accepting our procedure. For example, ca rs can be programmed to have predictive behavior. Therefore, failure to operate does not alwa ys lead to accidents. Our continuous process reduces the probability of failure by half compar ed to the centralized system (9.50% for the proposed system and 19.65% for the centralized s ystem when failure completion equals 0.4). In comparison, the relay system is more likely to malfunction. In Figure 7 we show the statistics of the group of 10 instruments that reached co nsensus at Pc = 0.9. Probability of occurrence represents the probability that some instrument s will reach agreement within the agreement period. For example, a bar of 0 cars represents th e chance that all cars will fail to pass, while a bar of 10 cars represents the chance that the ent ire group of 10 cars will pass. The results showed that verbal complaints supported successful agreement reaching (in this case, agreement was achieved across all 10 instruments). As sho wn in Figure 7, when gossip is taken into account, all cars have a high probability of approval (88.5%), while in the absence of gossip, only 16.6% of cars can reach agreement.

Conclusion

In this article, we presented a proposal as a decisionmaking solution for wireless V2V networ ks for vehicle tooling management. The new carpooling decision was approved upon request from PBFT. Simulation results show that the proposed method can detect and stop violations in the presence of faulty vehicles. Additionally, the reliability of communication is greatly inc

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

reased thanks to the Bagua algorithm required to reach consensus. Results comparing effectiv e agreement with and without negative speech showed that the failure rate dropped from arou nd 103 to less than 106, and the reliability of communication was 103. Experiments on the bi nary tree scenario also show that the system is able to select the best solution from many cand idates obtained by planning the synthesis tree, since the binary tree is the building block of all wood working plans

REFERENCES

[1]. "Machine Learning Techniques in Cybersecurity." Encyclopedia. Retrieved from https://encyclopedia.pub/entry/25675.

[2]. Abdullah, A. H., Ahmed, M. H., & Wahab, M. H. A. (2021). A Comparative Study of Network Intrusion Detection Techniques Using NSL-KDD Dataset. IEEE Access, 9, 91924-91942.

[3]. Akhtar, S., Faisal, M., Ahmad, S., & Rho, S. (2020). Machine learning-based ransomware detection: State-of-the-art and future research directions. Journal of Network and Computer Applications, 153, 102539.

[4]. Akinyele, J. R., Gao, K., & Zhu, S. (2015). Insider threat detection using log analysis and machine learning. International Journal of Information Security, 14(5), 403-415.

[5]. Alawami, A. K., Khan, M. K., & Kiong, T. E. (2020). Insider threat detection: A review and research directions. Journal of Network and Computer Applications, 153, 102531.

[6]. Alazab, M., Hobbs, M., & Abawajy, J. (2018). A survey of botnet detection techniques. Journal of Network and Computer Applications, 110, 60-71.

[7]. Alzahrani, B., Zulkernine, M., & Alazab, M. (2020). Machine learning-based intrusion detection techniques for securing industrial control systems: A review. Computers & Security, 88, 101628.

[8]. Bhattacharya, S., Gupta, P., & Chatterjee, J. (2021). A comparative study of machine learning algorithms for malware detection. Multimedia Tools and Applications, 80(10), 14935-14957.

[9]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.

[10]. Chiong, R., Lee, V. C., & Zhou, L. (2017). Anomaly detection in cyber security: A machine learning approach. In Machine learning paradigms: Advances in data analytics (pp. 81-112). Springer, Cham.

[11]. Demertzis, K., & Karampelas, P. (2020). A review of anomaly detection techniques in financial markets: An application to emerging markets. Expert Systems with Applications, 146, 113172.

[12]. Dhamecha, T. I., & Thakkar, P. (2020). A Comprehensive Review on Anomaly Detection Techniques using Machine Learning. International Journal of Advanced Research in Computer Science, 11(4), 44-51.

[13]. Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., & Muller, P. A. (2018). Data augmentation using synthetic data for time series classification with deep residual networks. arXiv preprint arXiv:1808.08467.