ENHANCED BLOCKCHAIN CONSENSUS TECHNIQUE FOR TRUST MODEL IN VEHICULAR AD HOC NETWORK

MUHAMMAD SULKHAN NURFATIH

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

SEPTEMBER 2021

DEDICATION

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Prof. Madya. Dr. Mohd Yazid bin Idris, for encouragement, guidance, critique and friendship. I am also very thankful to my co-supervisor Assoc. Prof. Deris Stiawan. Ph.D for their guidance, advice and motivation. Without their continued support and interest, this thesis would not have been the same as presented here.

I am also indebted to Universiti Teknologi Malaysia (UTM) for funding my Master study and the librarians at UTM for their assistance in supplying the relevant literatures.

My fellow postgraduate students should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members.

ABSTRACT

The Vehicular Ad-hoc Network (VANET) provides smart network services across vehicles that are capable of sharing data. However, during an accident there are network security issues encountered, such as in the trustworthiness of vehicle information which is an important aspect of security in VANET. Therefore, the trust model has become an essential element in overcoming this problem. Various trust models at the time of a vehicle accident have been suggested in literatures, including the use of blockchain consensus algorithms. Proof of Event (PoE) consensus has been suggested to improve the trustworthiness of information within VANET, even though, PoE does not guarantee the trustworthiness of accident location data. As such, the aim of this research was to improve the blockchain consensus technique in improving the VANET trust model through the PoE consensus process and Proof of Location (PoL) consensus by generating Proof of Event and Location (PoEL) consensus. The PoEL consensus was used to obtain reliable location data from the vehicle, and to guarantee the authenticity of the event. Experiments were performed to see the level of trust of the information generated by the PoEL consensus. The results showed that the PoEL consensus gave a better level of information trust than the previous consensus. The average value of the information trust level based on the experiments conducted by PoEL consensus was 57.6%, compared to the PoW consensus of 38.2%, and PoE consensus of 49.4%. These increments occurred due to additional parameters to raise the level of trust in the information, namely confirmation of the event and the location of the accident. This study has proven that the use of PoEL consensus in VANET has succeeded in increasing the trust of vehicle information during accidents.

ABSTRAK

Rangkaian Kenderaan secara *Ad-hoc* (VANET) menyediakan perkhidmatan rangkaian pintar merentasi kenderaan yang mampu berkongsi data. Walau bagaimanapun, semasa kemalangan terdapat masalah keselamatan rangkaian yang dihadapi, seperti kesahihan maklumat kenderaan yang merupakan aspek penting dalam keselamatan VANET. Oleh itu, model kesahihan telah menjadi elemen penting dalam mengatasi masalah ini. Pelbagai model kesahihan pada waktu kenderaan menghadapi kemalangan telah dinyatakan dalam kajian lepas, termasuk penggunaan algoritma konsensus rantaian blok. Konsensus Bukti Peristiwa (PoE) telah dicadangkan untuk meningkatkan kesahihan maklumat dalam VANET, walaupun, PoE tidak menjamin kesahihan data lokasi kemalangan. Oleh yang demikian, tujuan penyelidikan ini untuk adalah meningkatkan teknik konsensus rantaian blok dalam meningkatkan model kepercayaan VANET melalui proses konsensus PoE dan konsensus Bukti Lokasi (PoL) dengan menghasilkan konsensus Bukti Peristiwa dan Lokasi (PoEL). Konsensus PoEL digunakan untuk mendapatkan data lokasi yang boleh dipercayai dari kenderaan, dan menjamin kesahihan peristiwa tersebut. Eksperimen telah dilakukan untuk melihat tahap kesahihan maklumat yang dihasilkan oleh konsensus PoEL. Hasil kajian menunjukkan bahawa konsensus PoEL memberikan tahap kesahihan maklumat yang lebih baik daripada konsensus sebelumnya. Nilai purata tahap kepercayaan maklumat berdasarkan eksperimen yang dilakukan oleh konsensus PoEL adalah 57.6%, berbanding dengan konsensus PoW sebanyak 38.2%, dan konsensus PoE sebanyak 49.4%. Peningkatan ini berlaku kerana terdapat parameter tambahan untuk meningkatkan tahap kepercayaan terhadap maklumat, iaitu pengesahan peristiwa dan lokasi kemalangan. Kajian ini telah membuktikan bahawa penggunaan konsensus PoEL dalam VANET telah berjaya meningkatkan kesahihan maklumat kenderaan semasa berlakunya kemalangan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BARS	-	Blockchain-based anonymous reputation system
BTEV	-	Blockchain-based Traffic Event Validation
CAM	-	Cooperative Awareness Messages
CerBC	-	Blockchain for Certificates
DEMN	-	Decentralized Environmental Notification Message
DPoS	-	Delegated Proof of Stake
EDR	-	Event Data Recorder
ITS	-	Intelligent Transportation System
MANET	-	Mobile Ad Hoc Network
MesBC	-	Blockchain for Messages
NS-3	-	Network Simulator 3
GPS	-	Global Positioning System
OBUs	-	On-Board Units
P2P	-	Peer to Peer
PBFT	-	Practical Byzantine Fault Tolerance
PoW	-	Proof of Work
PoS	-	Proof of Stake
PoE	-	Proof of Event
PoL	-	Proof of Location
RevBC	-	Blockchain for Revoked Public Keys
RSU	-	Road-Side Units
SUMO	-	Simulation of Urban Mobility
TDCS	-	Traffic Data Collection System
UNL	-	Unique Node List
V2I	-	Vehicles to Infrastructure
V2V	-	Vehicle to Vehicle
V2X	-	Vehicle to Everything

LIST OF SYMBOLS

a_1, a_2	-	*accident*
B	-	*block*
E	-	*event*
$Ei_1, Ei_2, \ldots, Ei_n$	-	*event ID*
$L_1, L_2, \ldots, L_n$	-	*location Vw*
pv, pr	-	*periode time*
r	-	*range*
Rv	-	*RSU validation*
St	-	*time synchronization*
t	-	*time*
TL	-	*trust level*
Tx	-	*message transactions*
τv	-	*threshold*
V	-	*speed*
Va	-	*vehicle accident*
Vv	-	*vehicle validation*
Vw	-	*vehicle witness*
$W_1, W_2, W_{\|s\|}$	-	*warning*

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

An ad hoc network is a network that is composed of individual devices communicating with each other directly. Mobile Ad Hoc Network (MANET) and Vehicular Ad Hoc Network (VANET) are popular ad hoc networks. MANET is a mobile device wireless network that can configure itself. Meanwhile, VANET refers to a network created in an ad hoc manner where different moving vehicles and other connecting devices come in contact over a wireless medium and exchange useful information to one another (Tomar *et al.*, 2017). VANET works as a safety warning on the road, to warn of hazards such as collisions and road congestion. The warnings are sent using communication between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) (Soleymani *et al.*, 2015). The V2V procedure is a vehicle to send and receive messages from each other. The messages contain warnings about accidents, road congestion, and other traffic information. On the other hand, V2I works between infrastructure and vehicles that send and receive messages from one another. The messages contain information such as location of gas stations and traffic light alerts. An On-Board Unit (OBU) is installed in each vehicle in order for interaction to occur between vehicles (Mokhtar and Azab, 2015). OBU is a transmitter that communicates between the vehicle and the Road-Side Units (RSU).

VANET will improve traffic flow by promoting intelligent transport and providing efficient information facilities. The purpose of VANET is to provide smart transportation that is capable of processing data and can manage itself for each vehicle. Then, it provides an application facility such as driving assistance and safety warning (Eze *et al.*, 2014). However, there are network security issues encountered, such as the trust of vehicle information during an accident. Thus, the VANET trust model becomes an important element.

The research conducted by Lu and Wang (2018) uses a blockchain-based anonymous reputation for the VANET trust model. Blockchain is a decentralized distributed database that creates data blocks in sequential series and integrates them within different data structures into a chain. Cryptography is used on blockchains to ensure that the data is tamper-proof and can be used for distributed networks and data storage in nodes (Zhang and Chen, 2019). The theory behind the blockchain originates from the simple essay entitled "Bitcoin: a peer-to-peer online cash network". written by Satoshi Nakamoto (2008). In the context of digital currency, the consensus is an important element for every blockchain network since the consensus is reliable for the stability of the distributed network and protecting integrity. The consensus for a digital currency that was first developed was proof-of-work and introduced in Bitcoin. The consensus processes may be classified as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) and Ripple (Mingxiao *et al.*, 2017). On VANET, a blockchain is used to verify the truth of information from vehicles because the vehicle can basically access the event information history on the blockchain.

1.2 Problem Background

The trustworthiness of information is a parameter used to measure the validity of information. This is important aspect of security at VANET Xiaonan *et al.*, (2007), because data reliability in VANET affects the quality of safe or non-safe systems, and the trustworthiness of information has an important role in the security and efficiency of vehicle networks (Hutchison and Mitchell, 2013). Therefore, VANET focuses on the security of data exchange between vehicles. In addition, data communication between trusted vehicles can affect security. Thus, a comprehensive study of the trust model is required (Soleymani *et al.*, 2015). Academics have recently conducted research on a blockchain that has great potential in various areas like the trust model needed at VANET.

Lu, *et al.* (2018) proposed a blockchain-based anonymous reputation system (BARS) to establish a privacy-preserving trust model for VANETs. This system is

used to prevent the distribution of false messages from internal vehicles while maintaining vehicle privacy. Two blockchains are used, namely Blockchain for Certificates (CerBC) and Blockchain for Revoked Public Keys (RevBC). All entities in VANET get transparent authority activities. In the communication for V2I and V2V, the public key acts as a pseudonym. In addition, Blockchain for Messages (MesBC) is used to record all the messages that are broadcasted and as proof to evaluate the reputation of each vehicle. Thus, the distribution of fake messages and bad behavior from evil vehicles can be overcome by reputation evaluation. In this research, the PoW consensus is adopted and the vehicles act as miners. However, the consensus is not the main focus of this research.

A decentralized trust management system in vehicular networks based on blockchain techniques was proposed by Yang *et al.* (2019). In this system, the Bayesian Inference Model is used by vehicles to validate the messages received from neighboring vehicles. The result of validation is that each vehicle's source message will get a rating from other vehicles. The roadside unit (RSU) will use the rating of the vehicle to calculate the trust value of the vehicle involved and package this data into blocks. Then, each RSU will try to add their block to the trust blockchain managed by all RSUs. This research uses the consensus of PoW and PoS together. Thus, the greater the total offset (stake) value in the block, the easier the RSU can find the value for the hash function. During the rating generation, the distance between the message sender and event location are considered as the indicators of message credibility. However, there is no guarantee for the correctness of the location.

Additionally, there is a new type of blockchain to resolve critical message dissemination issues in the VANET. As proposed by Shrestha *et al.* (2019), a local blockchain is created for real-world event message exchange among vehicles within the boundary of a country, which is a new type of blockchain suitable for the VANET. In this scheme, event messages are used as transactions instead of cryptocurrency. This research adopts the PoW consensus mechanism. A consensus of all mining vehicles in the blockchain network can be established to generate a new block that can be used as ground truth for the next block. The Proof of Location (PoL) consensus is used to obtain trusted locations from vehicles that broadcast information about events on the

network. PoL provides certificates of the original location. RSU validates the delivery event information by vehicle. According to Tippenhauer *et al.* (2011), GPS use is ineffective because it can easily be faked. PoL is safe because the location certificate can only be created with a valid RSU signature. Therefore, the vehicles cannot produce fake certificates. However, message trust is not guaranteed from the usage of only PoL. A blockchain mechanism that can make the messages more reliable is proposed to overcome this problem (Shrestha *et al.*, 2019).

In another scenario, Yao-Tsung *et al.* (2019) proposed a Blockchain-based Traffic Event Validation (BTEV) using a proof-of-event (PoE) consensus mechanism. RSU is used to collect traffic data and verification of the data is conducted by the vehicle upon receiving notification of the event. This research has a two threshold-based and two-phase consecutive transaction-based event validation mechanism on the blockchain in order to identify the truth of events and speed up the delivery of transactions to the blockchain. The local-chain is circulated only for RSUs in the same region. Thus, vehicles can access traffic information efficiently when it comes to an area. The producer is chosen based on the timestamp of the event confirmation and each producer is qualified with proof of his own event. Thus, this can save power consumption costs compared to the PoW approach. Besides that, in this study other nodes can be used to verify block producers through proof of description of traffic events. This research focuses on the part that can be verified through vehicles and RSUs. However, verification of the incident and vehicle location is not discussed. The vehicle has information such as speed, direction, and location, which is packaged in the Cooperative Awareness Messages (CAM) (ETSI, 2014).

There are five main requirements that must be met in order to have information security and privacy in VANET. First, authentication is when the identity of each vehicle can be guaranteed and verified. Second, non-repudiation is a data operation that cannot be rejected by the sender. Third, privacy must be maintained where the true identity is well protected from any malicious threats. Fourth, efficiency is a real-time guarantee that must be achieved under certain conditions and good power consumption. Fifth, data integrity and correctness are guaranteed in the transmission

process and must not be modified so that the sender's geographical data is accurate to avoid the recipient being blamed.

1.3 Problem Statement

Previous research describes some of the problems of blockchain implementation in VANET. First, a study conducted by Shrestha *et al.* (2019) which adopted the PoW consensus. In the PoW consensus, all mining nodes on the blockchain network can generate new blocks which can be used as the ground truth for the next block. However, large power consumption becomes a problem. Vehicles usually have limited power, and have difficulties in producing the power needed. Second, research conducted by Yao-Tsung *et al.* (2019) proposes a new consensus called Proof of Event (PoE) to validate traffic events and perform as a trust verification mechanism based on the decentralized nature of blockchain. This consensus is unlike the previous consensus which requires large computing power to solve difficult hash problems while this consensus only uses computing power for event validation.

However, there is a gap in this PoE consensus. PoE consensus uses a period of time to verify an event. So, the accuracy of the data will be questioned when two types of events occur at the same time. In the research, data such as destination, speed, and location are packaged in CAM. Should there be false data, CAM will give a value of 0 which indicates that the data is false. However, the is no further explanation given to why the data is false. Next, the vehicle is used to verify the proof of an event. However, the selection of verifiers is chosen randomly. This will affect the trustworthiness of information if there are any malicious vehicles. Several proposals have been made to overcome the problem. A proposal by Shrestha *et al.* (2019) uses an identity that is categorized based on the type of event. In addition to the problem where parameters are not elaborated in cases where data used in CAM is false. This can be overcome by proposing a Proof of Location (PoL) consensus that is used to provide evidence about the location of the vehicle at a certain time. A consensus proposed by Dasu *et al* (2018) produces a location certificate.

The location certificate is digital proof that the vehicle is in a certain place. All vehicle locations must have a location certificate to prove their position at a certain time. This certificate is provided by a valid RSU. PoL is safe because the vehicle cannot produce fake location certificates without a valid RSU signature. The aim of this research is to hybridize a model of PoE consensus that uses little computing power with PoL consensus that provides evidence of vehicle location at a given time to improve security, information trust, and efficiency in the VANET trust model.

1.4 Research Goal

The main objective of this research is to enhance the blockchain consensus technique for information trustworthiness in the VANET trust model.

1.4.1 Research Objectives

The following issues need to be thoroughly investigated and analyzed in order to achieve the research goal:

(a) To hybrid PoE consensus with PoL consensus into Proof of Event and Location (PoEL) consensus for the VANET trust model.

(b) To develop a PoEL consensus to increase the trust level of information in the VANET trust model.

1.5 Research Scopes

To achieve the objectives, the scope of the research is restricted to the following conditions:

(a) This study only compares the blockchain consensus technique used for VANET based on previous research.

(b) The results of this research are to increase the trust level of information in the VANET trust model with accurate event and location information

(c) The traffic data used in this study uses data based on previous research.

1.6 Significance of the Study

The expected outcome of this research is to increase the trust level of information in the VANET trust model with the proposed PoEL consensus. Thus, ensuring reliable information exchange in the VANET environment and guaranteeing the accuracy of the information. Research related to a hybrid consensus model between PoE and PoL is new. The use of the PoL consensus is expected to make the performance of PoE better. Thus, increasing the safety and security of the driver. This model is intended to be used by manufacturers and vehicle authorities in dealing with traffic problems and vehicle safety to protect human life and existing infrastructure. Thus, it can assist drivers to be more careful in driving a vehicle.

1.7 Organization of the Thesis

The following is an organization of the thesis:

(a) **Chapter 1** explains the introduction of the research which consists of background problems and statements. The purpose of the research and research scope is discussed. Finally, the organization of the thesis is presented in the research.

(b) **Chapter 2** explains the VANET literature review, overview of blockchain, blockchain consensus, previous research on blockchain in relation to VANET, and the VANET trust model with blockchain.

(c) **Chapter 3** explains the research methodology which consists of a research operational framework, a research conceptual framework, a software simulator in research, and evaluation parameters.

(d) **Chapter 4** explains the design and implementation of the research. Which consists of VANET and blockchain scenarios, proposed blockchain consensus, and environment scenarios.

(e) **Chapter 5** explains the experiment and the results of the analysis of the research. Which consists of scenario simulation, simulation results and analysis, and evaluation of experimental results.

(f) **Chapter 6** explains research contributions to knowledge and future works.

REFERENCES

Ahmad, F., Adnane, A., Franqueira, V. N. L., Kurugollu, F. and Liu, L. (2018) 'Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks : Evaluating the Impact of Attackers ' Strategies, *Sensors*, 18(11), 1–19.

Ahmad, F., Adnane, A., Kurugollu, F. and Hussain, R. (2019) 'A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks', *Wireless Days (WD)*, 1–8.

Ahmed, S. and Tepe, K. (2016) 'Using logistic trust for event learning and misbehaviour detection', *IEEE Vehicular Technology Conference*, 1–5.

Amoretti, M., Brambilla, G., Medioli, F. and Zanichelli, F. (2018) 'Blockchain-Based Proof of Location', *IEEE 18th International Conference on Software Quality, Reliability, and Security Companion,* 146–153.

Bai, X., Gong, M., Gao, Z. and Li, S. (2012) 'Reliable and efficient data dissemination protocol in VANETs', *IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, 1–4.

Casino, F., Dasaklis, T. K. and Patsakis, C. (2019) 'Telematics and Informatics A systematic literature review of blockchain-based applications : Current status , classification and open issues', *Telematics and Informatics. Elsevier 3*6, 55-81.

Castro, M. (2001) 'Practical Byzantine Fault Tolerance'. *ACM Transactions on Computer Systems Volume* 20(4) 398–461

Chen, Y. M. and Wei, Y. C. (2013) 'A beacon-based trust management system for enhancing user centric location privacy in VANETs', *Journal of Communications and Networks*. JCN, 15(2), 153–163.

Conti, M., Member, S., Kumar, E. S. and Lal, C. (2018) 'A Survey on Security and Privacy Issues of Bitcoin', *IEEE Commun. Surv. Tutor. 2018*. IEEE, 20(4), 3416–3452.

Dasu T, Kanza Y, Srivastava D. (2018) 'Unchain Your Blockchain', *in: Proc. Symposium on Foundations and Applications of Blockchain 2018*, 1623.

Dhurandher, S. K., Obaidat, M. S., Jaiswal, A., Tiwari, A. and Tyagi, A. (2014) 'Vehicular security through reputation and plausibility checks', *IEEE Systems Journal*. IEEE, 8(2), 384–394.

Douceur, J. R. (2002) 'The Sybil Attack', *In Proceedings of the International Workshop on Peer-to-Peer Systems*, 1–6.

ETSI (2014) 'Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service', *ETSI*, 55(2), 306–315.

Eze, E. C., Zhang, S. and Liu, E. (2014) 'Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward', *Proceedings of the 20th ICAC*, 176–181.

Gazdar, T., Belghith, A. and Abutair, H. (2017) 'An Enhanced Distributed Trust Computing Protocol for VANETs', *IEEE Access*, 6,. 380–392.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Čapkun, S. (2016) 'On the security and performance of Proof of Work blockchains', *Proceedings of the ACM Conference on Computer and Communications Security*,. 3–16.

Gustavo J. A. M. Carneiro, (2010) NS-3: Network Simulator 3. *E-book library* [online]. Available at: https://www.nsnam.org (Accessed: 23 September 2020).

Huh, J. and Kim, S. (2019) 'The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies' *Sustainability*, 11(11), 3184

Hutchison, D. and Mitchell, J. C. (2013) 'Network and System Security', *Network*, 6(1), 1061–1067.

J. Wang and M. Hwang, (2017) 'A novel approach to extract significant time intervals of vehicles from superhighway Gantry Timestamp sequences', *International Conference on Applied System Innovation* ,. 1679-1682

Javaid, U., Aman, M. N. and Sikdar, B. (2019) 'DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart contracts', *IEEE Vehicular Technology Conference,* 1–5.

Kchaou, A., Abassi, R. and Guemara, S. (2018) 'Toward a distributed trust management scheme for VANET', *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 1-6.

Kerrache, C. A., Calafate, C. T., Lagraa, N., Cano, J. C. and Manzoni, P. (2017) 'Trust-Aware Opportunistic Dissemination Scheme for VANET Safety Applications', *Proceedings 13th IEEE International Conference on Ubiquitous Intelligence and Computing*, 153–160.

Khan, A. S., Balan, K., Javed, Y., Abdullah, J. and Tarmizi, S. (2019) 'Secure trust-based blockchain architecture to prevent attacks in VANET', *Sensors*, 19(22) 4954.

Khan, U., Agrawal, S. and Silakari, S. (2015) 'Detection of Malicious Nodes (DMN) in vehicular ad-hoc networks', *Procedia Computer Science. Elsevier Masson SAS* 46, 965–972.

King, S. and Nadal, S. (2012) 'PPCoin : Peer-to-Peer Crypto-Currency with Proof-of-Stake'.

Komalavalli, C., Saxena, D. and Laroiya, C. (2020) *Overview of Blockchain Technology Concepts*, *Handbook of Research on Blockchain Technology*, Elsevier Inc:Academic Press.

Kroll, J. A., Davey, I. C. and Felten, E. W. (2013) 'The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries', *In Proceedings of the Twelfth Workshop on the Economics of Information Security*,. 1–21.

Kwon, J. (2014) 'Tendermint : Consensus without Mining', 6, 1–11.

Leiding, B., Memarmoshrefi, P. and Hogrefe, D. (2016) 'Self-managed and blockchain-based vehicular ad-hoc networks', *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 137–140.

Lin, K. and Gannon, J. D. (1985) 'Atomic Remote Procedure Call', IEEE Transactions on Software Engineeri 11 (10), 1126-1135.

Lu, Z., Liu, W., Wang, Q., Qu, G. and Liu, Z. (2018) 'A privacy-preserving trust model based on blockchain for VANETs', *IEEE Access* 6, 45655–45664.

Lu, Z., Wang, Q., Qu, G. and Liu, Z. (2018) 'BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs', *IEEE International Conference on Trustcom/BigDataSE*, 6, 98–103.

Lu, Z., Wang, Q., Qu, G., Zhang, H. and Liu, Z. (2019) 'A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs', *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 1–10.

M. Haklay and P. Weber, (2008), 'OpenStreetMap: User-Generated Street Maps,' *IEEE Pervasive Computing*, 7(4), 12-18

Malhi, A. K., Batra, S. and Pannu, H. S. (2020) 'Computers & Security Security of vehicular ad-hoc networks : A comprehensive survey'. *Computers & Security* 89(1):101664.

Malik, R. F. and Nurfatih, M. S. (2017) 'Evaluation of Greedy Perimeter Stateless Routing Protocol On Vehicular Ad Hoc Network in Palembang City', *International Conference on Data and Software Engineering*.

Marmol et al. (2012) 'TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks', *Journal of Network and Computer Applications*, 35(3), 934–941.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. and Qijun, C. (2017) 'A Review on Consensus Algorithm of Blockchain', *IEEE International Conference on Systems, Man and Cybernetics (SMC)*, 2567–2572.

Minhas, U. F., Zhang, J., Tran, T. and Cohen, R. (2011) 'A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks', *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, 41(3), 407–420.

Mokhtar, B. and Azab, M. (2015) 'Survey on Security Issues in Vehicular Ad Hoc Networks', *Alexandria Engineering Journal*, 54(4), 1115–1126.

Nguyen, G. and Kim, K. (2018) 'A Survey about Consensus Algorithms Used in Blockchain', *Journal of Information Processing Systems* 14(1), 101–128.

Ongaro, D., Ousterhout, J., Ongaro, D. and Ousterhout, J. (2014) 'In Search of an Understandable Consensus Algorithm In Search of an Understandable Consensus Algorithm' *Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference*, 305-320.

P. Pablo Garrido Abenza, Manuel P. Malumbres, P. P. P. (2017) Towards Simulation for Autonomous Mobility, *SUMO 2017 Towards Simulation of Autonomous Mobility*, 31.

Raya, M., Papadimitratos, P., Gligor, V. D. and Hubaux, J. P. (2008) 'On data-centric trust establishment in ephemeral ad hoc networks', *Proceedings IEEE INFOCOM*, 1912–1920.

Satoshi Nakamoto (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', *E-book library* [Online]. Available: https://bitcoin.org/bitcoin.pdf (Accessed: 10 March 2020).

Schrijvers, O, Bonneau, J., Boneh, D. and Roughgarden, T. (2016) 'Incentive Compatibility of Bitcoin Mining Pool Reward Functions', *Conference: International Conference on Financial Cryptography and Data Security*, 477-498.

Schwartz, David Noah Youngs, A. B. (2018) 'The Ripple Protocol Consensus Algorithm David', *E-book library* [Online]. Available: https://ripple.com Accessed: 10 March 2020)

Sheikh, M. S. and Liang, J. (2019) 'A Comprehensive Survey on VANET Security Services in Traffic Management System', *Wireless Communications and Mobile Computing*, 2019(1), 1–23.

Shrestha, R., Bajracharya, R., Shrestha, A. P. and Yeob, S. (2019) 'A new type of blockchain for secure message exchange in VANET', *Digital Communications and Networks*.6(2), 177-186.

Shrestha, R. and Nam, S. Y. (2017) 'Trustworthy event-information dissemination in vehicular Ad Hoc networks', *Mobile Information Systems*, 2017(2) 1-16.

Soleymani, S. A., Abdullah, A. H., Hassan, W. H., Anisi, M. H., Goudarzi, S., Rezazadeh Baee, M. A. and Mandala, S. (2015) 'Trust management in vehicular ad hoc network: a systematic review', *Eurasip Journal on Wireless Communications and Networking*, 2015(1), 1–22.

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B. and Čapkun, S. (2011) 'On the requirements for successful GPS spoofing attacks', in *Proceedings of the ACM Conference on Computer and Communications Security*, 75–85.

Tomar, R., Prateek, M., Sastry, G. H.,Vehicular Adhoc Network (VANET)-An Introduction, *Control theory applications*, 9(18), 8883–8888.

Vukolić, M., Quest, T., Fabric, B. and Bft, P. (2017) 'The Quest for Scalable Blockchain Fabric : Proof-of-Work vs . BFT Replication, *iNetSec 2015: Open Problems in Network Security*, 112-125:

WHO (2018) Global Status Report on Road Safety. *E-book library* [Online]. Available:https://www.who.int/publications/i/item/9789241565684 (Accessed: 13 February 2020).

Wu, A., Ma, J. and Zhang, S. (2011) 'RATE: A RSU-aided scheme for data-centric trust establishment in VANETs', *7th International Conference on Wireless Communications, Networking and Mobile Computing,* 1–6.

Xiaonan, L., Zhiyi, F. and Lijun, S. (2007) 'Securing vehicular ad hoc networks', *2007 2nd International Conference on Pervasive Computing and Applications,* 15(1), 424–429.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N. and Member, S. (2019) 'Delegated Proof of Stake with Downgrade : A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism', *IEEE Access*, 7, 118541-118555.

Yang, N. (2013) 'A Similarity based Trust and Reputation Management Framework for VANETs', *International Journal of Future Generation Communication and Networking*, 6(2), 25–34.

Yang, Z., Yang, K., Lei, L., Zheng, K. and Leung, V. C. M. (2019) 'Blockchain-based decentralized trust management in vehicular networks', *IEEE Internet of Things Journal*. IEEE, 6(2), 1495–1505.

Yao-Tsung, Y., Li-Der, C., Chia-Wei, T., Fan-Hsun., T. and Chien-Chang., L. (2019) 'Blockchain-Based Traffic Event Validation and Trust Verification for VANETs', *IEEE Access*. IEEE, 7, 30868–30877.

Yuan, Y. and Wang, F. Y. (2016) 'Towards blockchain-based intelligent transportation systems', *IEEE International Conference on Intelligent Transportation Systems,* 2663–2668.

Zhang, S. and Lee, J. (2019) 'Analysis of the main consensus protocols of blockchain', *ICT Express*. 6(2), 93-97.

Zhang, X. and Chen, X. (2019) 'Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network', *IEEE Access*, 7, 58241–58254.

LIST OF PUBLICATIONS

Indexed Conference Proceedings

1. Malik, R. F. and **Nurfatih, M. S**. (2017) 'Evaluation of Greedy Perimeter Stateless Routing Protocol On Vehicular Ad Hoc Network in Palembang City', *International Conference on Data and Software Engineering (ICoDSE) Evaluation*.

2. **Nurfatih, S**., Yazid, M., Stiawan, D. and Winanto, E. A. (2020) 'Enhancing Trust Model of Information Vehicular Ad-Hoc Networks Through Blockchain Consensus Algorithm', *International Conference on Information and Communications Technology 2020*, 483–488.