Blockchain Based Security for Vehicular Ad hoc Networks

by Nisha Malik

A dissertation submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy
in
Computer Systems

Under the supervision of
Dr. Priyadarsi Nanda

University of Technology Sydney
Faculty of Engineering and Information Technology

August 2020

Certificate of Original Authorship

I, *Nisha Malik* declare that this thesis is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy*, in the *School of Electrical and Data Engineering, Faculty of Engineering and Technology* at the *University of Technology Sydney, Australia*.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.

Signature of Student:

Date: 31/08/2020

Place: Sydney, Australia

Dedicated To

My Loving Parents and Parent- In- Laws

My extremely supportive husband Deepak

My loving daughter Laavanya

My Crazy brother Sumit

My Motivating Teachers and Mentors

My Amazingly Creative and Crazy Friends

And to Everyone Who Reads This

Acknowledgements

Foremost I would like to thank and express my sincere gratitude to Almighty God, the sustainer, who kept me going through the highs and lows of this journey and made it achievable for me. He undoubtly is the source of light for me in every aspect of life.

I would like to express my deepest gratitude to my supervisor, Dr. Priyadarsi Nanda for accepting me into the Ph.D. program and guiding me all the way through in this journey of becoming a successful researcher. Dr. Nanda's guidance, patience, and continuous support were essential to the completion of this thesis. His unmatched knowledge and invaluable feedback immensely helped me go forward in my research. I am greatly indebted to him for helping me get through the difficult times I had during my research. I feel very lucky to have worked with Dr. Nanda without whom this thesis would have only been a dream. I would like to thank my Co-supervisor Professor Xiangjian He, who always provided his valuable and expert feedback on my work. His support, co-operation, and generosity throughout the research tenure is truly undeniable. Further, I would like to express my deepest gratitude to Professor Ren Ping Liu, who guided through the NSW Cyber Security Project, which forms an essential part of this research work.

I also wish to thank all of my colleagues and friends from the School of Electrical and Data Engineering at the University of Technology Sydney. Specifically, I would like to thank Dr. Deepak Puthal, Ambar, Ashish, Upasana, Annie, and Amjad for creating a friendly atmosphere in the group and assisting me in whatever manner possible. Many thanks to all the administrative staff at the School of Electrical and Data Engineering, especially Thomas, Eryani and Aprillia who helped me with administrative issues.

I am eternally grateful to my loving and supportive husband Deepak Malik, lovely daughter Laavanya, beloved parents Ashok Kumar Saroha and Krishna Saroha and parents in law Dharampal Malik and Sudesh Malik, my brother Sumit Saroha for their sacrifices, prayers, encouragements, and endless love. Without their everyday support, I would have not been able to reach this stage. I sincerely dedicate this thesis to them. Words cannot express my gratitude and appreciation for their unwavering support and kindness throughout this journey.

Abstract

The speedy aggrandizement in Wireless communication technologies concurrently with immediate measure requisites to improve road safety have expedited a considerable development in the Intelligent Transportation Systems (ITS). ITS came into existence with a strong perspective to provide end-to-end, better, worthier, safer, efficient and much more improved transport services, both on-road and off-road. Intelligent communication technologies such as trip guiding smart phone applications (that direct you how much to walk before you take the next bus or train, where to get down, etc.), the latest safety oriented in vehicle systems (such as Anti-Lock Braking systems, air bags, Navigation systems, etc.), are all part of the ITS.

Therefore, ITS is not just about modifying or repairing the age-old infrastructures of roads, highways, stations, or bus stops, but persuading security and safety of transport to all the people and goods travelling on roads.

With increasing congestion increased the accidents, which made the government authorities, and the automobile manufacturers realize the need and embryonic benefits that can be exploited by means of wireless communications merged with in-vehicular capabilities, consequently, resulting in the formation of Vehicular communication networks termed as ***'Vehicular Ad hoc Networks'*** *(VANETS).*

VANETS are therefore, an emerging promising technology of the ITS due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. Vehicle-to-Vehicle (V2V) communications rely on what is called as the DSRC (Dedicated Short-Range Communications). A vehicle periodically broadcasts its position, speed, ID/Pseudo-ID, direction, etc. to other neighboring vehicles at 1-10Hz. These messages are called as Cooperative safety messages or beacon messages. The aim for all these vehicular applications is the ultimate driver assistance and safety to avoid any discomfort and mis happenings. Therefore, to ensure that only accurate alerts, warnings, or messages reach the drivers, without any false data injections or message alterations, security implementations are essential. If attackers send any false warning alerts, say for e.g. Impersonating an authorized user attacker broadcasts an accident alert in his area, it can cause unnecessary havoc among the road users and route diversions which were not required. Also, the authentication of the network users along with privacy perseverance is the most important security consideration. Therefore, security implementation is the foremost necessity in VANETs.

In VANETS, information is widely available across multiple systems and is accessible with appropriate authentication and access rights. But, to have access, users need to connect in the wireless environment, which poses various security *challenges. This thesis investigates the security challenges and limitations to secure VANET and how the existing solutions can be improved upon. Blockchain has emerged as the solution to securing identity and authentication along with access control among the network entities.*

This thesis is a work to secure the VANET network, by authenticating, revocating, and establishing trust among the users using the shared Blockchain Ledger, to enable them to get emergency updates and transmit only if they are authorized users, while they travel on road. This work identifies the trustworthy nodes using blockchain and smart contracts and store their reputation in the Inter Planetary File System (IPFS) storage in a transparent manner, so the reputation score is available to all the nodes without relying on the centralized infrastructure for computation or storage. The thesis provides a detailed review of existing trust and privacy works and merges the neural networks with blockchain to provide the classification of trustworthy nodes as well as providing privacy to the data, by sanitizing the data prior to transmission. The thesis is a work to secure communication in the network to provide end-end security. The proposed model guarantees privacy and security to the information transmitted and multi-level trust evaluation of the nodes before sharing any information. The thesis is divided in three phases of research with blockchain and smart contracts finally demonstrating that our solutions not only strengthen and secure the dynamic VANET, but also significantly improve the performance and efficiency as compared to existing approaches.

Author’s Publications

1. **Nisha Malik**, Deepak Puthal, and Priyadarsi Nanda, "An overview of security challenges in vehicular ad-hoc networks," in *2017 International Conference on Information Technology (ICIT)*, 2017: IEEE, pp. 208-213.

2. **Nisha Malik**, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 674-679.

3. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, "Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019: IEEE, pp. 34-41.

4. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, "Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology," *Wireless Networks,* pp. 1-20, 2020.

5. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu “A Systematic Analysis of Security and Trust Management in Vehicular Networks” (Submitted to Computer Networks).

6. Deepak Puthal, **Nisha Malik**, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine,* vol. 7, no. 2, pp. 18-21, 2018.

7. Deepak Puthal, **Nisha Malik**, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine,* vol. 7, no. 4, pp. 6-14, 2018.

Table of Contents

List of Figures

List of Tables