FUZZY TRUST MODEL FOR TRUSTWORTHINESS OF INFORMATION IN VEHICULAR AD HOC NETWORK

SEYED AHMAD SOLEYMANI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy in (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

MAY 2019

DEDICATION

I would like to dedicate the thesis to all those who supported and encouraged me.

ACKNOWLEDGEMENT

This research is done with the help of people whose contribution in assorted ways to the research and the making of the thesis deserved special mention. It is a pleasure to convey my gratitude to them all in my humble acknowledgment.

I would like to record my gratitude to Prof Abdul Hanan Bin Abdullah for his supervision, advice, and guidance as well as providing me unflinching encouragement and support in various ways. I gratefully acknowledge Dr Mohammad Hossein Anisi for his advices and supervision during my study.

Words fail me to express my appreciation to my wife Shidrokh and my daughter Afsoon Sadat whose dedication, love and persistent confidence in me, has taken the load off my shoulder. Finally, my parents deserve special mention for their inseparable support and prayers.

ABSTRACT

Vehicular ad hoc networks (VANETs) represent a class of ad hoc networks created to enhance road safety, passenger comfort, traffic efficiency, and reduce overall traffic accidents. In this network, all applications are based on the exchange of data among vehicles, hence, the trustworthiness of data and vehicles is essential. The presence of selfish nodes, as well as obstacles, by generating inaccurate and incomplete information, has a negative impact on the trustworthiness of the vehicular environment. Therefore, the aim of this research is to propose a trust model in a vehicular environment, which results in the safety and comfort of passengers, by increasing the trustworthiness of information. For this purpose, a fuzzy trust model (F-TRUST) composed of three modules, namely, plausibility, experience, and decision-making, was proposed. To cope with the inaccurate and incomplete data, the proposed model evaluated the trust level of both data and vehicles by performing fuzzy logic in both line-of-sight (LOS) and non-line-of-sight (NLOS) conditions. The proposed model was evaluated by well-known evaluation measures such as precision, recall, F-measure, overall accuracy, and communication overhead. The results indicate that F-TRUST had better performance as compared to the weighted voting (WV) approach. In addition, the F-TRUST scheme outperformed the WV approach under various patterns of attacks such as simple attack, opinion tampering attack, and cunning attack. In conclusion, this study demonstrates that F-TRUST can improve the trustworthiness of information objectively, and in turn help vehicles to detect the selfish nodes and inaccurate data.

ABSTRAK

Rangkaian Ad hoc Kenderaan (VANETs) merangkumi rangkaian jaringan ad hoc yang dicipta untuk memantapkan keselamatan jalanraya, keselesaan penumpang, kecekapan lalu lintas, dan mengurangkan kemalangan jalanraya secara keseluruhan. Dalam jaringan ini, semua aplikasi adalah berdasarkan pertukaran data antara kenderaan, oleh itu kebolehpercayaan data dan kenderaan adalah penting. Kewujudan nod yang mementingkan diri sendiri serta halangan yang menghasilkan maklumat yang tidak tepat dan tidak lengkap, mempunyai impak negatif terhadap kebolehpercayaan suasana persekitaran kenderaan. Oleh itu, tujuan kajian ini adalah untuk mencadangkan model kepercayaan dalam suasana kenderaan, yang akan memberi keselamatan dan keselesaan penumpang dengan meningkatkan kebolepercayaan maklumat. Untuk tujuan ini, model *fuzzy trust* (F-TRUST) yang terdiri dari 3 modul, iaitu kemunasabahan, pengalaman dan pembuatan keputusan, telah dicadangkan. Untuk mengendalikan data yang tidak lengkap dan tepat, model yang dicadangkan telah menilai tahap kepercayaan kedua-dua data dan kenderaan dengan melakukan logik *fuzzy* dalam keadaan *line-of-sight* (LOS) dan *non-line-of-sight* (NLOS). Model yang dicadangkan telah dinilai melalui ukuran penilaian yang terkenal seperti ketepatan, ingat semula, *F-measure*, ketepatan keseluruhan dan komunikasi overhed. Hasilnya menunjukkan bahawa F-TRUST mempunyai prestasi yang lebih baik berbanding kaedah *weighted voting* (WV). Selain itu, skema F-TRUST mempunyai prestasi lebih baik berbanding kaedah WV dalam pelbagai corak serangan seperti serangan mudah, serangan yang memodifikasikan pendapat dan serangan licik. Kesimpulannya, kajian ini menunjukkan bahawa F-TRUST boleh meningkatkan kebolehpercayaan maklumat secara objektif, dan membantu kenderaan-kenderaan untuk mengesan nod yang mementingkan diri sendiri dan data yang tidak tepat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	-	Artificial Neural Network
AODV	-	Ad hoc On-demand Distance Vector
ART	-	Attack-Resistant Trust Model
BT	-	Bayesian Theorem
BTM	-	Beacon-based Trust Management System
CAM	-	Cooperative Awareness Message
CBR	-	Constant Bit Rate
COA	-	Centre Of Area
DDoS	-	Distributed Denial-of-Service Attack
DoS	-	Denial-of-Service Attack
DST	-	Dampster Shafer Theory
EC	-	Event Confidence
EL	-	Experience Level
EO	-	Event Observer
EP	-	Event Participant
EQM	-	Extended Quality Method
EP	-	Event Participant
ER	-	Event Reporter
FANET	-	Flying Ad hoc Network
FDM	-	Fuzzy Decision-Making Module
FEM	-	Fuzzy Experience Module
FL	-	Fuzzy Logic
FLS	-	Fuzzy Logic System
FN	-	False Negative
FP	-	False Positive
FPM	-	Fuzzy Plausibility Module
GA	-	Genetic Algorithm
GPS	-	Global Positioning System
LOS	-	Line-Of-Sight
LVoD	-	Location Verification using Distance

LVoT	-	Location Verification using Time
MAC	-	Media Access Control
MLT	-	Maximum Local Trust
MoM	-	Mean of Maximum
NLOS	-	Non-Line-Of-Sight
OBU	-	On-Board Unit
OSM	-	Open Street Map
PL	-	Plausibility Level
PN	-	Plausibility Network
PVN	-	Plausibility Validation Network
RaBTM	-	RSU and Beacon based Trust Management
RATE	-	Roadside-unit Aided data centric Trust Establishment
RMCV	-	Real-time Massage Content Validation
RSSI	-	Received Signal Strength Indicator
RSU	-	Road-Side Unit
TFDD	-	Trust-based Framework for Reliable Data Delivery
TN	-	True Negative
ToV	-	Type of Vehicle
TP	-	True Positive
TRIP	-	Trust and Reputation Infrastructure-based Proposal
UAV	-	Unmanned Air Vehicle
UDP	-	User Datagram Protocol
V2V	-	Vehicle to Vehicle
V2I	-	Vehicle to Infrastructure
VANET	-	Vehicular Ad Hoc Network
WV	-	Weighted Voting

LIST OF SYMBOLS

τ	-	Type of vehicle
P	-	Precision
R	-	Recall
$PLAUS_{Level}$	-	Plausibility Level
K_M	-	Private Key for Signature
ID_k	-	Identifier f Node K
$Dist_{RSS}$	-	Distance between two Nodes using RSSI
$Dist_{GPS}$	-	Distance between two Nodes using GPS
θ	-	Angle between two Vectors
c	-	Propagation Speed
$time_{exp}$	-	Expected Time
$time_{rec}$	-	Received Time
$EXPER_{Level}$	-	Experience Level
ToV	-	Type of Vehicle
$TRuST_{level}$	-	Trust Level

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.1 Overview

Vehicular Ad hoc NETwork (VANET), as a key part of the intelligent transportation systems, is a mobile network that consists of vehicles and infrastructures. VANET is commonly obtainable through communications either between two vehicles (V2V), or between a vehicle and an infrastructure (V2I). As shown in Figure 1.1, vehicles can broadcast warning messages and traffic management instructions in the vehicular environment to raise driver's awareness of possible travel hazards. In terms of comfort and convenience of passengers, vehicles also can exchange specific information such as various media types like text, audio, video, and animation with other vehicles in the network.

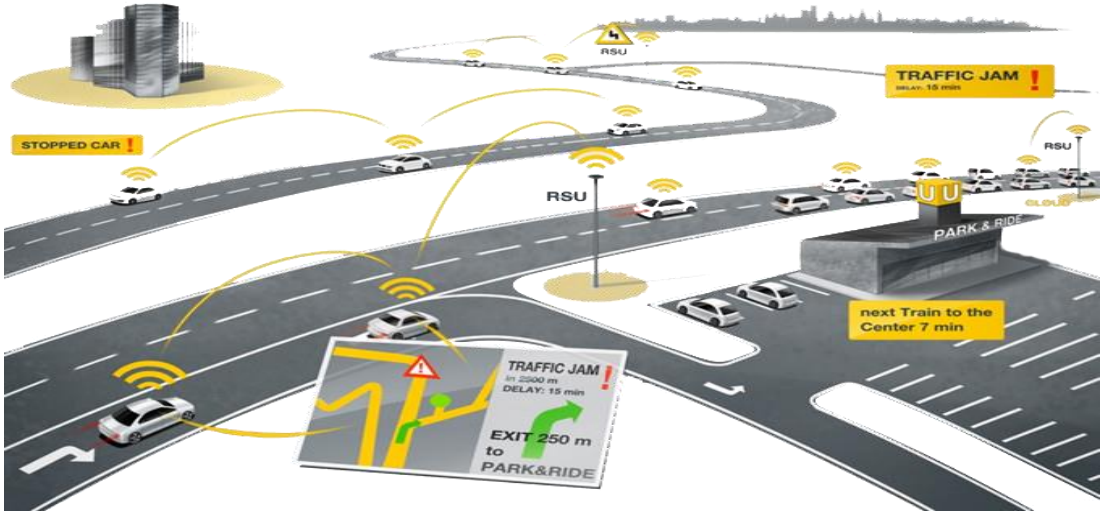

Figure 1.1 Vehicular ad hoc network scenario

Due to the increasing number of accidents, unsatisfied users and dishonest vehicles in vehicular networks; the road safety enhancement and ensure passenger comfort are the main concerns in vehicular environment. Motivated by this

observation, trust can be an efficient solution in VANET. Luo *et al.* (2009) mentioned that trust means the belief that an entity has about another entity, given past experiences, knowledge about the entity's nature and/or recommendations from trusted entities. Raya and Hubaux (2007) mentioned that trust as a key element in security systems, has the vital role to safety enhancement in the vehicular environment. Since unreliable data/vehicles have negative impact on network performance, trustworthy of data and in addition trustworthiness among vehicles are solutions to improve safety.

In VANET, vehicles might misbehave due to selfish reasons and might not send correct information all the time. Attackers may tamper the vehicles by changing the content of messages. Attackers also may create a bogus traffic warning messages to flood communication channel for causing collisions. Hence, it is important to know which data/vehicle is trustable.

During the past decade, many solutions have been introduced to detect correctness and accuracy of data in VANET using concept of trust. Trust model ensures the security of vehicular ad-hoc networks and the outcome of the trust establishment is the reliability between vehicles. Gomez and Martinez (2011) stated that trust management is an accurate alternative to deal with security threats in highly distributed and dynamic scenarios. According to (Zhang, 2012), trust models are categorized into three groups namely entity-based, data-based and hybrid trust model.

Entity-based Trust Model: The entity-based trust usually involves collecting trust information about other nodes to model the trustworthiness of vehicles with the view of evaluating their behaviour's tendency. This type of trust model is utilized to eliminate the selfish or malicious vehicles. The aim of this model is to ensure the exchange of reliable messages among vehicles (Zhang, 2012). It is very important in vehicular environment.

The entity trust is considered to be the essential measure to provide secure routing to deliver the trustworthy data in VANETs (Ya *et al.*, 2015). The existing entity-based trust method measures the level of trust typically based on the experience and the recommendation given by other nodes (Huang, 2014; Marmol and Perez,

2012). Experience is built on past knowledge of direct interaction between nodes. The recommendation depends on the opinion of one node about another node. However, due to the high dynamic nature of VANET, there is failure in collecting enough information on the neighbour nodes/sender. On the other hand, the correctness of data still remains obscure in this group of trust models. Hence, the entity-based trust model is not suitable for VANETs (Shaikh and Alzahrani, 2014).

Data-based Trust Model: The data-based trust model is always to evaluate the data trustworthiness. This model also called event-based trust model which can detect the bogus or false data in VANETs (Ahmed *et al.*, 2015). Since data has the inherent dynamic nature, the current data-based trust methods are based on the context of the event regularly. So, most of the researchers usually focus on establishing trust in data rather than in the nodes who generated them. This type of trust model usually has consideration on the number of the reports on the same event, time closeness, location closeness, in addition to the types of the events (Wu *et al.*, 2011; Zhang, 2011). However, the large number of data as well as duplicated data in heavy traffic density leads to increased latency and data lost. Also, the data-based trust model would not perform well in the sparse traffic density (Zhang, 2012).

Hybrid Trust Model: in combined trust model evaluates the trustworthiness of data by using of entity trust and sustains entity trust over time (Zhang, 2011). Since the structure of data's trust evaluation is based on entity trust, it can be accepted that a message is trusted if the message has been evaluated to be trustworthy by many other trusted peer nodes (Gurung *et al.*, 2013). Usually, there are interaction among entity trust and data trust in the current combined trust methods. Road Side Unit (RSU) and beacon-based trust management methods are the typical examples of this group, which establish entity trust by cross-checking the plausibility of event messages and beacon messages (Chen and Wei, 2013; Wei and Chen, 2012). The main goal is to propagate data opinions rapidly. Furthermore, the model can avoid internal attackers from sending or forwarding forged messages.

A review of existing trust models shows that each model used different metrics to evaluate trust value such as experience, plausibility, and type of node. In the following, some of these metrics are explained briefly:

Experience: Minhas *et al.* (2011) mentioned that the experience of direct interactions between nodes can be a factor to determine the level of trust. On the other word, the history of past interaction between nodes is effective to update one node's belief in the trustworthiness of another. It is obvious that nodes with good history of past interactions have positive impact on trust score.

Plausibility: Plausibility in vehicles includes the comparison of received information with the internal sensor data or evaluating messages from different sources about a single event and scenario. Engoulou *et al.* (2014) stated a plausibility check system is an essential module to compute trust level correctly. Bißmeyer *et al.* (2012) also stated that plausibility check is a way to detect inconsistencies in mobility data.

Type of Node (Role): Based on the level of authority, nodes in vehicular environment can be classify into different groups (Yao *et al.*, 2017). It is clear that, each group has different role to evaluate trust level of data/entity. In other words, nodes with high level of authority are more trustable than other nodes and lower authority nodes are less valuable in evaluating the amount of trust.

Mainly because of the unique features of VANET environment such as high mobility, various traffic densities, rapidly data changes and Line-Of-Sight (LOS) obstruction by obstacles; a trust model applied in this environment not only should be able to evaluate trust level of data/entity correctly, but also it has to tackle these challenges. However, the existing trust models are still at the preliminary stage and they cannot entirely conform to the characteristics of VANETs. This is because most of the proposed trust models only focus on accuracy of the model on special scenario. There are few models that consider for example obstacles as a feature in vehicular environment. They did not consider real scenario and different conditions to evaluate the performance of trust model.

1.2 Background and Motivation

Recently, many studies have paid more attention to improve passenger's safety in VANET. To deals with problems caused by the attacks in the vehicular network trustworthiness of information is an important issue for safety engineers. Trust models, as a security mechanism, try to prepare the network to be protected against different types of attacks by increasing trustworthy and reliability of data/vehicles.

Raya *et al.* (2008) mentioned that vehicles can become faulty or compromised by attackers and hence need to be revoked. To this end, they proposed a framework for trust establishment based on data. In this framework, trust value is computed for each received single message. Based on a single message it can be hard to decide whether the reported event took place, hence they defined the collection of multiple reports related to the same event. At the end, the reports along with their weights are passed to a decision logic module.

To address and tackle false messages, Gurung *et al.* (2013) proposed an infrastructure-less trust model based on data called Real-time Message Content Validation (RMCV). This model evaluates trust score of event message based on content similarity, content conflict and routing path similarity.

Selfish vehicles, as security threats in vehicular environment, try to maximize car owner's utility by sending out false information. To deal with these vehicles, Minhas *et al.* (2011) developed an entity-based trust model using role and experience. In this model vehicles which send event message will be prioritized based on experience-based and role-based trust value.

An infrastructure-based trust model is proposed to accurately distinguish malicious and selfish nodes spreading false or bogus messages by Gomez and Martinez (2012). This model computes trust score based on recommendation given by other vehicles and RSUs. In this model, the decision-making module is based on in fuzzy logic and probability.

Chen and Wei (2013) proposed a Beacon-based Trust Management (BTM) system. It aims to thwart internal attackers from sending false messages in privacy-enhanced VANET. The proposed model is a hybrid trust management mechanism which computes entity and data trust. The beacon message is utilized to measure entity trust and data trust is computed by cross-checking the plausibility of event and beacon messages. They mentioned that an event message is more trustable when the message and related beacon message be plausible. Engoulou *et al.* (2014) mentioned that the plausibility check is used to verify the information contained in the event message and thus data trustworthiness.

Shaikh and Alzahrani (2014) proposed an intrusion-aware trust model to detect malicious nodes which send fake location and timing values. In this model, a confidence value is measured for message coming from a unique sender of message. In addition, a trust value is calculated using the confidence value of all messages related to a same event. Finally, an event message is accepted/rejected based on the trust value. Although the accuracy of this model is high, however, because of the high delay, it is not suitable for safety applications in VANET.

Liu *et al.* (2016) proposed a self-organized trust model which contains trust certificate-based and recommendation-based trust evaluations. Certificate-based trust model is to cope with the collusion attack and make the evaluation result more accurate. In order to evaluate trust based on recommending a Maximum Local Trust (MLT) algorithm is presented to identify trustworthy recommenders.

An attack-resistant trust management scheme is proposed for VANETs by Li and Song (2016). It is able to cope with malicious attacks. To this end, it evaluates the trustworthiness of both data and mobile nodes in VANETs. In this scheme, data trust is specifically evaluated based on the data sensed and collected from multiple vehicles. In addition, node trust is assessed in two dimensions including functional trust and recommendation trust. Functional trust indicates how likely a node can fulfil its functionality; whereas recommendation trust demonstrates the trustworthy of recommendations from a node for other nodes.

Hu *et al.* (2017) proposed a recommendation scheme for user vehicles to select platoon head vehicle before joining a platoon namely REPLACE. Considering the uncertainties of human behaviours, the scheme is reputation based using the weighted majority method by adding up all of the historical feedback from the user vehicles together. It is well perceived that the feedback from the user vehicles could be also untrusted. To be concrete, a trust system is established to evaluate the reliability of user vehicles to deal with the uncertainties of user vehicles feedback and then to estimate their future behaviours.

Boeira *et al.* (2018) mentioned that incorrect position information can cause problems such as increased fuel consumption, reduced passenger comfort, and in some cases even accidents. Therefore, they designed a secure proof-of-location scheme tailored for VANETs called Vouch. The scheme leverages the node positioning capability of 5G wireless network roadside units. The key idea of Vouch is to disseminate periodic proofs of location, combined with plausibility checking of movement between proofs.

Based on available knowledge, few models of trust have focused on the impact of obstacles on trustworthiness of data. Both static and moving obstacles are an inseparable part of the urban vehicular network. Static obstacles on the sides of the road (e.g. buildings) and moving obstructions (e.g. trucks) interfere with radio signals and prevent a desirable communication. There are two types of conditions in vehicular enviornment includes Line-Of-Sight (LOS) and None-Line-Of-Sight (NLOS) conditions. In the LOS status there is a direct communication between vehicles; whereas in the NLOS condition, direct communication between two nodes restricts by obstacles. Obviously, these restrictions can influence the integrity, reliability, and availability of the event message. Despite the existing trust models in the literature, there is lack of a trust model that works correctly in both LOS and NLOS cases.

Moreover, because of the incomplete, inaccurate and imprecise data known by vehicles as well as uncertainty because of the conflicting information in the vehicular environment, evaluation of data/entity trust cannot be completely precise and accurate.

There is lack of proper trust model that not only evaluate the trustworthiness of data/entity correctly but also overcome uncertainty and imprecision of data.

1.3 Problem Statement

The data generated by malicious nodes, selfish node, and obstacles are intentionally or inadvertently. Generally, inaccurate information is generated by malicious nodes, deliberately. Whereas, high mobility and the presence of obstacles create incorrect data, inadvertently. Obstacle such as buildings and trucks can create a state of NLOS between two vehicles. It restricts direct communication even when corresponding vehicles exist within each other's physical communication range. Hence, obstacles have the negative impact on the accuracy of the created information in vehicular network, inadvertently. Obstacle can influence localization service integrity, reliability, and availability which result in untrustworthy in vehicular environment.

One of the other problems in the vehicular network is the presence of selfish nodes as an attacker. Some of the existing attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. On the other hand, some other attackers such as selfish nodes want to have the most benefits of the network for personal use only. The selfish vehicles are considered as a serious security threat by creation and dissemination of the incorrect information in the network. To this end, these nodes build up trust first and then deceive. Selfish nodes try to achieve the most benefit of the network using change behavior over time. This behaviour from nodes will lead to a reduction of trust among vehicles.

Inaccurate, incomplete, and imprecise of network information known by each node is also an issue in VANET. This is mainly because of the high mobility, vehicle density and fading condition. Since uncertainty and imprecision of data has negative impact on drivers' behaviour, hence it threatens the trustworthiness of VANET as well.

1.4 Research Goal

The main goal of this research is to propose a trust model in vehicular environment which result in the road safety enhancement and ensure passenger comfort by increasing trust and reliability among vehicles. The proposed trust model is composed of three modules plausibility, experience, and decision making to evaluate trust level of data and vehicles to tackle the inaccurate data and misbehaving nodes in VANET by performing fuzzy logic in both LOS and NLOS conditions.

1.5 Research Objectives

According to the problem statement the objectives of this research are as follows:

(a) To design a fuzzy algorithm to measure plausibility level of vehicle by detecting inconsistencies to deal with inaccurate information relevant to an event message in both LOS and NLOS states.

(b) To develop a fuzzy algorithm that measure the level of experience of sender of event message to cope with selfish vehicles who changes behaviour over time.

(c) To develop a fuzzy decision-making algorithm based on plausibility, experience and type of vehicle to evaluate trust level to deal with inaccurate, incomplete, uncertainty of data and misbehaving nodes in vehicular environment in both LOS and NLOS.

1.6 Contributions of Research

In this study, a trust model is proposed to deal with malicious attackers. This model evaluates the trustworthiness of data as well as nodes by integration of the fuzzy

logic under both LOS and NLOS situation. The proposed model evaluates the trustworthiness of data and node as two separate metrics, namely data trust and entity trust, respectively. In particular, data trust is used to assess level of trust of received event message by checking the plausibility whereas entity trust is utilized to evaluate trust level of entity using past direct interaction. To this purpose, two modules called plausibility module and experience module are developed. The plausibility module is used to evaluate the integrity and trustworthiness of event message using inconsistencies detection. This module is based on location verification using both distance and time. It is used to cope with inaccurate data propagated by malicious and or faulty nodes. The experience module is utilized to assess trust level of sender of the message. This module is based on history and direct interaction between vehicles. It is used to deal with vehicles who try to build up trust and then deceive. In this study, based on the authority level, vehicles are also categorized into three groups. This is because the event messages propagated by nodes in the high level of authentication are more accurate and trustable than other nodes. Moreover, a decision-making module is also proposed to combine data and entity trust. This module decides on the received event message using plausibility level, experience level and type of vehicle which can effectively detect and cope with different types of malicious behaviours in VANETs. In this research, fuzzy logic is also utilized as the main technique in the proposed modules. This is mainly because the fuzzy logic, as an artificial intelligence model, has good performance in decision-making systems to deal with uncertainty and imprecision of the network information known by each vehicle (Wu *et al*. 2010).

1.7 Research Scope

Some scopes applied to this research are as follow:

(a) All vehicles are equipped with On-Board Units (OBUs), GPS and wireless interfaces.

(b) OBUs are able to collect event messages.

(c) All the vehicles have the same transmission range.

(d) Each vehicle has a cache integrated in the on-board unit to record received event messages and history of last direct communication.

(e) Each vehicle has a list of neighbour nodes who exist within its transmission range.

(f) This research focuses on the MAC layer parameters of IEEE 802.11p.

1.8 Thesis Organization

This thesis is organized in six chapters. Chapter 1 provides the introduction of the thesis by identifying the research problem and objectives. Chapter 2 contains comprehensive literature review about classification and trust models on VANET. Chapter 3 presents the framework of research methodology. Chapter 4 describes in detail all phases of the trust model including plausibility and experience algorithms. Chapter 5 provides the performance evaluation for the proposed trust model. Finally, Chapter 6 is the conclusion of the thesis with some suggestions for future works and extension the proposed algorithms.

LIST OF PUBLICATIONS

1. Goudarzi, S., Anisi, M.H., Abdullah, A.H., Lloret, J., **Soleymani, S.A**. and Hassan, W.H., **2019**. A hybrid intelligent model for network selection in the industrial Internet of Things. Applied Soft Computing, 74, pp.529-546.

2. Goudarzi, S., Hassan, W.H., Anisi, M.H., Khan, M.K. and **Soleymani, S.A.**, 2018. Intelligent Technique for Seamless Vertical Handover in Vehicular Networks. Mobile Networks and Applications, 23(6), pp.1462-1477.

3. Goudarzi, S., Kama, M., Anisi, M., **Soleymani, S.A.** and Doctor, F., 2018. Self-organizing traffic flow prediction with an optimized deep belief network for internet of vehicles. Sensors, 18(10), p.3459.

4. **Soleymani, S.A.**, Abdullah, A.H., Zareei, M., Anisi, M.H., Vargas-Rosales, C., Khan, M.K. and Goudarzi, S., 2017. A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing. IEEE Access, 5, pp.15619-15629.

5. **Soleymani, S.A.**, Abdullah, A.H., Anisi, M.H., Altameem, A., Hasan, W.H., Goudarzi, S., Mandala, S., Razak, Z.B. and Noor, N.M., 2017. BRAIN-F: Beacon Rate Adaption Based on Fuzzy Logic in Vehicular Ad Hoc Network. International Journal of Fuzzy Systems, 19(2), pp.301-315.

6. Goudarzi, S., Hassan, W.H., Anisi, M.H., **Soleymani, S.A.**, Sookhak, M., Khan, M.K., Hashim, A.H.A. and Zareei, M., 2017. ABC-PSO for vertical handover in heterogeneous wireless networks. Neurocomputing, 256, pp.63-81.

7. Goudarzi, S., Hassan, W.H., Anisi, M.H. and **Soleymani, S.A.**, 2017. MDP-based network selection scheme by genetic algorithm and simulated annealing for vertical-handover in heterogeneous wireless networks. Wireless Personal Communications, 92(2), pp.399-436.

8. Goudarzi, S., Hassan, W.H., Anisi, M.H., Khan, M.K. and **Soleymani, S.A.**, 2017. Intelligent Technique for Seamless Vertical Handover in Vehicular Networks. Mobile Networks and Applications, pp.1-16.

9. Goudarzi, S., Hassan, W.H., **Soleymani, S.A.** and Anisi, M.H., 2017. Hybridisation of genetic algorithm with simulated annealing for vertical-handover in heterogeneous wireless networks. International Journal of Ad Hoc and Ubiquitous Computing, 24(1-2), pp.4-21.

10. **Soleymani, S.A.**, Goudarzi, S., Anisi, M.H., Hassan, W.H., Idris, M.Y.I., Shamshirband, S., Noor, N.M. and Ahmedy, I., 2016. A novel method to water level prediction using RBF and FFA. Water Resources Management, 30(9), pp.3265-3283.

11. Goudarzi, S., Hassan, W.H., Hashim, A.H.A., **Soleymani, S.A.**, Anisi, M.H. and Zakaria, O.M., 2016. A novel RSSI prediction using imperialist competition algorithm (ICA), radial basis function (RBF) and firefly algorithm (FFA) in wireless networks. PloS one, 11(7), p.e0151355.

12. Goudarzi, S., Hassan, W.H., Anisi, M.H. and **Soleymani, S.A.**, 2016. Comparison between hybridized algorithm of GA–SA and ABC, GA, DE and PSO for vertical-handover in heterogeneous wireless networks. Sādhanā, 41(7), pp.727-753.

13. Goudarzi, S., Hassan, W.H., **Soleymani, S.A.**, Zakaria, O. and Jivanadham, L.B., 2016. Artificial bee colony for vertical-handover in heterogeneous wireless networks. In Advanced Computer and Communication Engineering Technology (pp. 307-322). Springer, Cham.

14. Goudarzi, S., Hassan, W.H., Baee, M.A.R. and **Soleymani, S.A.**, 2015. The Model of Customer Trust for Internet Banking Adoption. In Computational Intelligence and Efficiency in Engineering Systems (pp. 399-414). Springer, Cham.

15. Goudarzi, S., Hassan, W.H., Baee, M.A.R. and **Soleymani, S.A.**, 2015. The Model of Customer Trust for Internet Banking Adoption. In Computational Intelligence and Efficiency in Engineering Systems (pp. 399-414). Springer, Cham.

16. **Soleymani, S.A.**, Abdullah, A.H., Hassan, W.H., Anisi, M.H., Goudarzi, S., Baee, M.A.R. and Mandala, S., 2015. Trust management in vehicular ad hoc network: a systematic review. EURASIP Journal on Wireless Communications and Networking, 2015(1), p.146.

17. Goudarzi, S., Hassan, W.H., Anisi, M.H., **Soleymani, S.A.** and Shabanzadeh, P., 2015. A novel model on curve fitting and particle swarm optimization for vertical handover in heterogeneous wireless networks. Mathematical Problems in Engineering, 2015.

18. Goudarzi, S., Hassan, W.H., Anisi, M.H. and **Soleymani, S.A.**, 2015. A comparative review of vertical handover decision-making mechanisms in heterogeneous wireless networks. Indian Journal of Science and Technology, 8(23), pp.1-20.

19. Goudarzi, S., Abdullah, A.H., Mandala, S., **Soleymani, S.A.**, Baee, M.A.R., Anisi, M.H. and Aliyu, M.S., 2013, December. A systematic review of security in vehicular Ad Hoc network. In Proc. 2nd Symp. WSCN (pp. 1-10).

20. Goudarzi, S., Ahmad, M.N., **Soleymani, S.A.** and Hosseini, N.M., 2013. Impact of trust on internet banking adoption: a literature review. Australian Journal of Basic and Applied Sciences, 7(7), pp.334-347.

21. Goudarzi, S., Ahmad, M.N., Zakaria, N.H., **Soleymani, S.A.**, Asadi, S. and Mohammadhosseini, N., 2013. Development of an instrument for assessing the impact of trust on internet banking adoption. J Basic Appl Sci Res, 3(5), pp.1022-1029.

22. **Soleymani, S.A.**, Abdullah, A.H., Mandala, S., Baee, M.A.R. and Goudarzi, S., 2013. A Hierarchical Routing Protocol for Improving the Quality of Service in Wireless Sensor Network. Life Science Journal, 10(3).