CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Trust models in vehicular ad-hoc networks: Towards an evaluation and comparison

Master's thesis in Software Engineering

MICHAELA FRITIOFSSON

PATRIK OLSSON

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2017

Master's thesis 2017

Trust models in vehicular ad-hoc networks: Towards an evaluation and comparison

MICHAELA FRITIOFSSON
PATRIK OLSSON

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2017

Trust models in vehicular ad-hoc networks: Towards an evaluation and comparison
MICHAELA FRITIOFSSON
PATRIK OLSSON

Supervisor: Christian Berger, Department of Computer Science and Engineering
Examiner: Jan-Philipp Steghöfer, Department of Computer Science and Engineering

Master's Thesis 2017
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Typeset in LaTeX
Gothenburg, Sweden 2017

Acknowledgements

We would like to thank Christian Berger, our supervisor, for tirelessly providing valuable feedback throughout the thesis process. We also would like to thank Niklas Lundin at AstaZero for helping us shape our thesis in the early phase of the thesis project. Finally, we would like to thank our friend, Sam Halali, for providing support and many laughs throughout the entire project.

Michaela Fritiofsson & Patrik Olsson, Gothenburg, December 2017

Trust models in vehicular ad-hoc networks: Towards an evaluation and comparison
MICHAELA FRITIOFSSON, PATRIK OLSSON
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

As traffic systems are becoming autonomous, communication between vehicles, and between vehicles and other entities, are becoming a vital part of the systems. One type of technology used in this area is vehicular ad-hoc networks (VANETs). VANETs have shown promising results in numerous areas, such as dynamic routing and safety applications. However, this technology comes with several security threats, since erroneous data might lead to travel inconveniences and possibly even car accidents. By using trust models, these risks can be mitigated. Even though there exist many trust models, there is a lack of comparable evaluations, which in turn makes it difficult to determine which is the most suitable model. The goal of this thesis is to provide a foundation for future evaluations and comparisons of VANET trust models. This has been done by both finding existing trust models, and also deriving appropriate settings for evaluating trust models in the VANET domain. The methodologies that were used were a systematic mapping study and interviews with both industrial and academic representatives. 48 trust models in the domain have been found and categorized. A simulative evaluation has been shown to be the most appropriate evaluation type, and platooning was found as the most valuable application. The results can be used by future researchers that aim to either evaluate their own trust model, or ultimately evaluate other researchers' trust models.

Keywords: Trust models, VANETs, vehicular ad-hoc networks, evaluation, comparison, criteria

Contents

List of Figures

List of Tables

1

Introduction

As traffic systems are becoming autonomous, communication between vehicles, and between vehicles and other entities are becoming a vital part of the systems. One type of technology used in this area is vehicular ad-hoc networks (VANETs). This is an ad-hoc network environment that can be used to send kinematic data such as speed and direction, as well as real-time traffic information (Eze *et al.* [1]). This information sharing can be used for numerous applications, ranging from dynamic routing to preventing car crashes and other accidents (Sommer and Dressler [2]).

Although this information transferring comes with several security threats. For instance, if the idea is to send the speed of the vehicles and information about various obstacles along the road, then this information has to be valid in order to avoid traffic accidents. Thus, protecting the entities (i.e. vehicles) from acting based on erroneous information is of high importance.

As mentioned earlier, security is one of the main issues in VANETs, and as said by Soleymani *et al.* [3], trust is a key element of security, hence trust models can play a vital role in solving previously mentioned problems. Liao *et al.* [4] also state that ensuring trustworthiness in VANETs is essential. Trust in the notion of VANETs corresponds to the set of relations among the participants, or entities, in the network (Theodorakopoulos and Baras [5]). Previous interactions between the participants affect the relations in the network. Although, exactly how the trust is computed varies between application and trust model.

1.1 Problem domain & motivation

While there are a lot of benefits with VANETs, the benefits cannot be fully realized unless the system can protect itself from nodes sending false information, either willingly (a malicious node) or unwillingly (a dysfunctional node) (Liao *et al.* [4]). The presence of these nodes will be inevitable in such an open environment that VANETs require. The malicious nodes, also termed attackers, may send false information for various reasons; to benefit themselves, cause inconveniences, or even cause harm. Hence, ensuring trustworthiness in VANETs is essential (Liao *et al.* [4]).

There are numerous trust models available that address this issue (Soleymani *et al.* [3] and Kerrache *et al.* [6]). However, there is a lack of studies and reviews on existing trust models, making it hard to compare those models (Soleymani *et al.* [3]). There is a couple of simple comparative qualitative studies, e.g. Soleymani *et al.* [3], Alriyami *et al.* [7], and Zhang [8], although the findings by Kerrache *et al.* [6] indicate that simulation is the most suitable evaluation form. This is also something that Zhang [8] recommends, and furthermore states that many of the trust models are only tested in their own simulation frameworks. Thus, there is a need for a comprehensive simulation framework, in order to make the evaluations comparable (Zhang [8]).

There are many trust models available in other domains as well, which have been evaluated and can therefore be compared (Jelenc *et al.* [9]). Although, VANETs is such a specific domain that many of those models cannot be applied in this domain. Some of the reasons are because of its ephemeral nature, its dynamic topology with a possible large number of peers, as well as the ever-changing nature of traffic; a road that is reported as congested might not be congested after 5 minutes (Zhang [8]).

Following the statements above, the conclusion is that there is a need for objectively evaluating VANET trust models in order to make them comparable.

1.2 Background

VANET is the application of self-configuring wireless networks in the vehicular domain (Sommer and Dressler [2]). Its general implementation is to let each participating vehicle act as a router, and forward all messages it receives to its neighbours, which allows information to propagate through the network (Zhang [8]).

Whenever a computing entity gets in contact with a potentially unknown entity there is an inherent element of risk. One way to mitigate this risk is by introducing trustworthiness in the system, which has shown promising results in many domains (Jelenc *et al.* [9]). A trust-based decision is a domain-specific multi-stage process. First the collection of trust evidence is done in order to conduct a trust computation that produces trust values, i.e. the estimation of trustworthiness of an entity (Longo *et al.* [10]).

Which trust evidence to use, and how to do the subsequent trust computation, are decided by the trust model. Hence, the decision mechanism is not part of the trust model. It is this definition of a trust model this thesis uses.

1.3 Research goal & research questions

Following the conclusion that VANET trust models need to be evaluated in a comparable way, this thesis aims to help contribute to that goal. Therefore, the goal of this thesis project is to provide a foundation for evaluating and comparing trust models in the VANET environment. To reach this goal, two research questions have been derived.

In order to evaluate the trust building models it has to be clear which models exist and are relevant to the VANET environment. This leads to the first research question:

RQ1. Which models for ensuring trust in a VANET environment exist?

When the models have been found, it has to be clear what evaluations that are most suitable for the specific domain. Hence the second research question:

RQ2. What are relevant criteria for industrial settings to evaluate trust models in the VANET environment?

The answers to these two questions will be used to fulfill the goal by deriving guidelines for future work that aim to conduct said evaluation and comparison.

1.4 Contributions

The purpose of this study is to provide a foundation for conducting evaluations upon trust building models within the VANET domain. By providing this foundation, future research can get a good starting point by knowing what to focus on in potential evaluations. In turn, these preferably objective evaluations of trust models will allow transparency in the domain, making it possible for different VANET trust models to be compared to each other.

Concretely, this foundation consists of two parts, derived from the research questions previously defined. The answer to RQ1 provides an easily overviewed map of the existing trust models in the VANET environment. It can give any researcher or industry representative a good comprehension of what models that exist today, as well as how they are categorized.

The results from RQ2 gives a good starting point for any future evaluation of VANET trust models, either for researchers that want to compare their own models to existing models, or ultimately researchers that want to make an objective evaluation of others' trust models. The result will help identifying the most relevant evaluation type, evaluation metric, simulation dynamics and environment, and also a preferable VANET application.

In turn, a publicly available comparison of VANET trust models could help both academia and the industry to find, implement, and further develop the best trust models for their particular application.

1.5 Scope & limitations

In order to in the end get an evaluation that is as accurate as possible, this thesis focuses only on the foundation itself, to be used for future evaluations. Hence the evaluation per se is not included in the scope of this thesis.

1.6 Structure of the article

Chapter 2 introduces relevant background information that can be necessary to understand the rest of the thesis. It describes the VANET domain, how computational trust works, as well as how trust works in the VANET domain.

Chapter 3 introduces related work that have similarities with this thesis' problem domain and goal. It introduces literature in the VANET domain, the existing VANET trust model comparisons, and trust model evaluations in a general domain.

Chapter 4 describes how the research goal and the subsequent research questions were approached; the mapping study and the interviews.

Chapter 5 describes the key findings from the conducted mapping study and the interviews.

Chapter 6 compares and analyzes the results in relation to existing literature and other authors' findings. The chapter ends with a discussion of the threats to validity of the thesis.

Chapter 7 presents the conclusion of the thesis together with suggestions for future research.

2

Background

This chapter is divided into three sections. First, in Section 2.1 the VANET domain is explained, together with its possibilities and challenges. After that, in Section 2.2, trust in the context of information security is explained. Finally, trust in the notion of VANETs is explained in Section 2.3.

2.1 VANETs

As traffic systems are becoming autonomous, the vehicles will have to be able to make decisions on their own. This will in turn require communication between vehicles (V2V), and between vehicles and other entities (V2I). One type of technology used in this area is VANETs which are, according to Yang *et al.* [11], a particularly challenging class of mobile ad-hoc networks (MANETs), as they are characterized by high mobility and dynamic network topology (Liang *et al.* [12]).

VANETs are self-configuring wireless networks that are established when a number of vehicles approach each other. The vehicles can then enter or leave the network, hence the dynamic topology. The general implementation of VANETs is to let each participating vehicle act as a router, and forward all messages it receives to its neighbours. This allows information to propagate through the network, reaching receivers that the sender directly could not communicate with (Zhang [8]). VANETs can be used to send kinematic data such as speed and direction, as well as real time traffic information, as described by Eze *et al.* [1], which helps prevent car crashes and other accidents.

Sommer and Dressler [2] recognize multiple application areas for VANETs, for instance:

- **Traffic information systems**
  To be able to share and receive traffic information, for instance in order to dynamically update the route depending on the current road traffic situation. The type of information could be icy roads or traffic jams.

- **Intersection collision warning systems**

To be able to warn peers about a possible forthcoming collision. A possible implementation would be to allow nodes with full vision of an intersection to warn peers that in some way have an obstructed view, and cannot see approaching vehicles. Hence the vehicles would be able to brake in time, and possibly prevent collisions.

- **Platooning**
  Sommer and Dressler describe platooning, or cooperative cruise-control, as one of the most demanded applications. This is the case of several vehicles, usually trucks, driving together on the road with a common destination. The implementation of vehicular communication allows vehicles to drive closer to each other, which will reduce fuel consumption and emissions, which in turn reduce costs.

- **Traffic-light information and control**
  Sommer and Dressler describe this as three different applications, with the goal to optimize the traffic flow and increase the safety. The applications are: data flow about the upcoming state change, adaptive traffic lights for emergency vehicles, and virtual traffic lights.

- **Entertainment applications**
  To be able to share content and information between vehicles that are not necessarily connected to the driving of the vehicle, for instance video streaming and multiplayer games.

While there are a lot of benefits with VANETs, the benefits cannot be fully realized unless the system can protect itself from nodes sending false information, either willingly (a malicious node) or unwillingly (a dysfunctional node) (Liao *et al.* [4]). The presence of these nodes will be inevitable in an open environment, that VANETs require. The malicious nodes, also termed attackers, may send false information for various reasons; to benefit themselves, cause inconveniences, or even cause harm.

In order to send information from the source node to the destination node correctly, a routing protocol is used, as an instruction on how the communication shall propagate through the network (Sommer and Dressler [2]). There is a large number of protocols available, each optimized to a specific application.

2.2 Computational trust

The fact that the computing environment has changed during the previous decades, from centralized stationary computers to distributed systems, has had implications for security models and mechanisms (Seigneur [13]). Whenever a computing entity gets in contact with a potentially unknown entity there is an inherent element of risk. One way to mitigate this risk is by introducing trustworthiness in the system, i.e. allowing the local entity to assess the trustworthiness of the other entity. Using

trust models have shown promising results in many domains (Jelenc *et al.* [9]).

Gambetta [14] defines trust as:

> Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.

Longo *et al.* [10] defines the trust-based decision as a domain-specific multi-stage process. The first step is to gather the appropriate input data, also called the *trust evidence*. The second step would be to conduct a *trust computation* based on these trust evidence, which in turn produces *trust values*, i.e. the estimation of trustworthiness of each of the entities.

The trust values are usually defined on the interval, or normalized to the interval [-1, 1] (Trček [15]), where "-1" denotes untrusted, "0" not decided and "1" trusted. These values can be either discrete or continuous.

Which trust evidence to use, and how to do the subsequent trust computation, are decided by the specific *trust model*. Finally, the actual decision is taken by combining the previously calculated trust values with other exogenous factors, such as risk assessments.

Hence, by using this definition, the trust model only includes the selection of trust evidence, the trust computation, and the allocation of trust values, excluding the decision mechanism. It is also this definition of a trust model this thesis uses.

2.3 Trust in the VANET domain

Soleymani *et al.* [3] states that trust is a key element of security. This implies that trust models can play a vital role in solving the previously mentioned issue of protecting VANETs from malicious nodes and other types of security threats. Liao *et al.* [4] also state that ensuring trustworthiness in VANETs is essential.

Trust in the notion of VANETs corresponds to the set of relations among the participants, or nodes, in the network (Theodorakopoulos and Baras [5]). The evidence based on previous interactions among the participants affect the relations in the network. Although, exactly how the trust is computed varies between application and trust model.

There are many trust models in other domains as well, which have also been evaluated (Jelenc *et al.* [9]). Although, VANETs is such a specific domain that many of those models cannot be applied. Some of the reasons are because of its ephemeral

nature, its dynamic topology with a possible large number of peers, as well as the ever-changing nature of traffic; a road that is reported as congested might not be congested in 5 minutes, making the detection of malicious information hard (Zhang [8]). These characteristics makes building trust within the network a complex task.

Trust models in VANETs are usually classified into three categories based on what the main object of consideration is when computing the trust (Soleymani *et al.* [3] and Alriyami *et al.* [7]). The categories are: *Entity-based trust models* where the vehicles sending information is evaluated, *Data-based trust models* where the actual data that is being sent is evaluated, and *Combined trust models* which evaluates both the entity and the data. As they also mention, the models in each category have different ways of approaching the trust issue in VANETs. They have different characteristics and are therefore suitable in different situations and VANET applications. For instance, entity-based models can handle sparse traffic better than data-based models (Minhas *et al.* [16]), although it can be difficult to make a trust evaluation based on interactions, since there is a low probability for two vehicles to meet again (Wu *et al.* [17]). Data-based models on the other hand can be more accurate, although would not perform well with sparse traffic, and might experience high latency with high traffic density (Soleymani *et al.* [3]).

3

Related work

This chapter aims to present previous work that relate to the research goal of this thesis. Articles regarding the domain of trust models in VANETs, and specifically comparisons between them, were searched for in academic databases, using keywords such as "VANET trust models" and "VANET trust model evaluation". The articles references were searched through, using the snowball sampling technique described in Marshall [18], resulting in very few articles. The results were cross-checked with the subsequently conducted mapping study, which is outlined in Section 4.1, that did not unveil further works except for the work of Ahmed and Tepe [19]. The chapter starts from the vehicular network domain with a study that surveys simulation approaches for VANETs. After that, an adversary-oriented overview is presented, followed by the objective qualitative comparisons of trust models in VANETs that could be found. This is followed by a simulative comparison of two models. Finally, this chapter mentions another evaluation conducted on trust models, but in a different domain than VANETs.

In the book Vehicular Networking, Sommer and Dressler [2] give both an in-depth view as well as an overview of the topic of vehicular networking, including VANETs. In the chapter *Performance evaluation*, they survey the different simulation dynamics and environments used in inter-vehicular communication studies, i.e. which type of simulation tools they use, and if the simulations take place in an urban or highway environment. This survey is done on inter-vehicular communication simulations in general, and not on the simulation of trust models in particular, which this thesis aims to provide a foundation for. They only survey studies from 2009 to 2011, and they find that the usage of network simulators is a bit more common than the use of road traffic simulators, and that modelling the simulations in an urban environment is a bit more common than in a highway environment.

Kerrache *et al.* [6] survey available trust models in VANET and their usual evaluation methods, including both their simulation dynamics and their performance evaluation metrics. This is closely related to RQ2 in this thesis. They also show possible critical scenarios that existing trust models cannot handle. They do not conduct an extensive evaluation, but only discuss which models address which scenarios. When talking about the different simulation techniques, they mention that there is a need for testing existing trust models. They find that simulative evaluations are the most frequent evaluation type, and they suggest the deployment of testbeds in the domain.

They end up in the conclusion that there is great importance in combining trust models with a cryptography-based solution. They relate cryptography to trust-based solutions, and describe situations where one is preferred over the other, or when they must be used in conjunction. One situation when trust management must be used to complement cryptography is the case of inside attackers, for instance when an authorized and authenticated user turns malicious, or if it ends up in the control of an attacker. They end up in the conclusion that there is great importance in combining trust models with a cryptography-based solution.

Alriyami *et al.* [7] highlight the characteristics of VANETs and how they differ from conventional ad-hoc networks. They then introduce some of the available trust models grouped by their main object of consideration. Thereafter they propose a list of criteria that are desireable for trust models, and briefly discuss which models that do, or do not, fulfill each of these criteria. Their article has similarities to this thesis in their aim to make the evaluations of trust models comparable. However, their comparisons are not made in-depth and their evaluation is only done qualitatively, by discussion and reasoning. This thesis on the other hand focus on finding relevant criteria and settings for the evaluation per se.

Zhang [8] writes about the different challenges and desired properties that exist for VANET trust models and how they are connected to the characteristics of VANETs. He suggests useful solutions from other domains that could potentially address these issues. He then surveys seven different trust models and evaluates if they fulfill the desired properties. This survey can also be found in Zhang [20]. The evaluation is only done qualitatively, just as the previously discussed article, Alriyami *et al.* [7]. Zhang [8] then concludes that none of the models fulfill all properties. He then suggests the usage of simulations for VANET modelling, and to develop a comprehensive simulation framework, so that trust models' robustness can be extensively tested.

Soleymani *et al.* [3] conduct a systematic review over the trust management domain in VANETs. They originate from the same issue as this thesis; that there is a lack of comprehensive studies and reviews on existing trust models, making it hard to compare models. Although, instead of focusing on an extensive comparison, they conduct a systematic review. They do however include a qualitative comparison between ten of the found models, based on the desired properties suggested by Zhang [8]. They also land in the same conclusion as Zhang [8], that no model fulfill all desired properties.

Ahmed and Tepe [19] perform an evaluation on two similar trust models in VANET. Although as in several other evaluations, one of the models is the one presented by the same authors conducting the evaluation, making it a subjective evaluation. The evaluation is done through simulation, and the models are evaluated on their ability to distinguish true events from the false.

However, trust models do not only exist in the VANET domain. Jelenc *et al.* [9] present the same problems that are introduced in this thesis; that authors of

trust models set up experiments and present results that are difficult to compare. A solution to that problem is to introduce trust testbeds, which are easy-to-use independent platforms used to compare different trust models. The basic thought is that a subjective party can provide a tool for evaluation and comparison, using predefined scenarios and metrics. Their article aims for trust models in general, and not VANET trust models in particular, which this thesis does. Although, in the general domain there is already presence of trust model testbeds. They therefore focus on the evaluation method of the testbeds. They claim, and conclude, that including the decision making mechanism in the models does make a difference to the evaluation, despite other testbeds' assumptions of the opposite. They then evaluate and compare existing trust models. This thesis relate to their work in the way that this thesis also wants to contribute to the evaluation of trust models. However since evaluations in the VANET specific domain is not that well developed or standardized, the evaluation settings must first be derived. Hence, this is what this thesis aim to do, and these settings might then in turn be implemented in a VANET trust testbed.

4

Methodology

As stated in Section 1.3, the goal of this thesis project is to provide a foundation for evaluating and comparing trust models in the VANET environment. To reach the goal of the thesis project, two research questions were derived. These can be found in Section 1.3.

RQ1 and RQ2 were approached with a systematic mapping study. This process can be found in Section 4.1. The expected result was systematic maps that categorized existing models and evaluation processes. These maps can be found in Sections 5.1 and 5.2.

To complement the result of the mapping study for RQ2, interviews were conducted with industry and academia representatives. The interviews are described in Section 4.2.

4.1 Systematic mapping study

To be able to answer the first and second research question, a systematic mapping study was conducted. The mapping study followed the steps described by Petersen *et al.* [21] and is described in this section.

4.1.1 Define research questions

The first step of a systematic mapping study is to define the scope of the study. In this project, the scope was defined by using the research question 1 and 2, previously defined in Section 1.3.

4.1.2 Search

The second step of the mapping study was the initial search for articles. To avoid making the search too narrow, four different online libraries were used to find related

work: *ACM Digital Library* [22], *IEEE Explore* [23], *Scopus* [24] and *Springer Link* [25]. By including Scopus some results from other libraries, such as Wiley and Science Direct, were also found.

The initial thought of the mapping study was to divide it into two tracks, one per research question. Although after having read some of the articles that were found in the search for RQ1, it was found that many of these articles presenting a model also included an evaluation of that model, which made the article relevant for RQ2 as well. Hence, it was decided to use one search string for the entire mapping study, and then separate the articles relevant for each of the research questions by setting different inclusion and exclusion criteria (see Section 4.1.3). The final search string was:

```
(("Trust model") OR ("Trust management")) AND
(("Evaluation") OR ("Criteria")) AND
(("VANET") OR ("Vehicular ad-hoc network") OR
 ("V2V") OR ("V2I") OR ("V2X"))
```

The different ways of writing *ad-hoc* (*ad hoc*, *adhoc*) were tested in the different search engines. It was found that *ad-hoc* and *ad hoc* generated the same results, and *adhoc* generated results in the form of a subset of the previous forms, i.e. *adhoc* generated fewer results, which were all included in the previous forms of writing. Because of the indication that *ad-hoc* and *ad hoc* will generate the same results, and also more results than *adhoc*, the form *ad-hoc* was chosen.

Initially the terms *V2V*, *V2I* and *V2X* were not included. Although as vehicular networks were studied further, it was found that those terms were sometimes used to denote inter-vehicular communication, and they were therefore added to the search string.

This step resulted in 234 articles at the time of writing this thesis.

4.1.3 Study selection

After the initial search, inclusion and exclusion criteria were used to filter the results. The criteria are listed in Table 4.1 with respect to each of the two first research questions. The criteria were modified during the selection process. First, only articles in English were included in the data extraction. Furthermore, it was added to the inclusion criteria that the articles should propose a model *explicitly* for VANETs and not just mentioning VANETs as a possible application area. This was done to exclude general trust models that might not be suitable for the complex dynamics of VANETs. Lastly the criteria were changed to require one *single* model, since one article was found that suggested numerous models with minor differences, which could skew the result of the mapping study.

Table 4.1: Inclusion and exclusion criteria for the mapping study

	RQ1	**RQ2**
Inclusion criteria	*Both shall be fulfilled*	*Either can be fulfilled*
	The title or abstract should explicitly mention that the paper suggests one single trust model to be applied in VANET.	The same inclusion criteria used for RQ1, but also explicitly stating that the article evaluates the proposed model.
	From the abstract or title, the researcher shall be able to deduce that VANET is the main application area for the trust model.	The abstract should explicitly mention evaluation suggestions for trust models in VANET.
Exclusion criteria	Papers that are not written in English shall be excluded.	

All of the articles found in the search were filtered based on these criteria. The filtering was based solely on the articles' abstracts and titles. No sources were excluded based on the type of study, although the sources after filtering only contained scientific journal articles and conference papers.

The filtering resulted in 57 articles for RQ1 and 59 articles for RQ2. After duplicates were removed, 48 articles remained for RQ1, and 47 for RQ2. An overview of the results of these steps can be found in Table 4.2.

The two sets of articles for the two research questions had quite a large overlap. The reason for this was, as previously mentioned, that most of the available evaluations have been done in order to evaluate a presented model, usually in the same article. Some articles that were not part of the overlap, and present in the RQ1 set, are the articles that propose trust models, but do not evaluate them. The articles that were only included in the RQ2 set were on one hand those that suggested, but not conducted, evaluations, as well as one article with an evaluation of a model that was presented by the same author, but in an earlier article.

4.1.4 Keywording of abstracts

As instructed by Petersen *et al.* [21], the keywording process was done in two steps. Firstly, from the articles that were left from the previous step, all abstracts were read in order to find relevant keywords, related either to the trust model presented in the article (RQ1), or the evaluation of such models (RQ2). As the second step, the elicited keywords were then used to create a classification scheme, with relevant categories and corresponding alternatives.

Table 4.2: Number of articles found and selected in the systematic mapping study

Search engine	**Step 1 - Search**	**Step 2 - Study selection**			
		Including duplicates		Excluding duplicates	
		RQ1	RQ2	RQ1	RQ2
IEEE Explore	27	9	12		
ACM DL	3	3	1		
Scopus	69	26	30		
Springer Link	135	19	16		
Total	**234**	**57**	**59**	**48**	**47**

The full classification scheme for RQ1 can be found in Table 4.3. As seen in the table the categories are *Topology architecture*, *Main object of consideration*, and *Privacy*. The alternatives in these categories are mutually exclusive, this means that each article can only be classified into one alternative of each category.

The categories resemble the results achieved by Soleymani *et al.* [3], where they suggest that trust models can be categorized based on the main object of consideration in the model, and also mention the topology architecture, although as an evaluation metric and not as a categorization category. The topology architecture is also used in the article by Kerrache *et al.* [6], although the alternative "decentralized" is instead labeled "distributed". The privacy category can also be found in the same article.

Topology architecture is whether the model uses central infrastructure; some of the models depend on road-side units. Main object of consideration is what the model bases its trust evidence upon. This aspect was explained more thoroughly in Section 2. The privacy category is whether the model works to ensure the privacy of the drivers and passengers. Alriyami *et al.* [7] describe the privacy issue so that confidential information, such as name, address of the driver, and the location history are not exposed. They argue that a successful trust model should be able to preserve the privacy of the drivers.

The classification scheme for RQ2 can be found in Table 4.4. The alternatives in the two first categories (*Evaluation type* and *Evaluation metric*) for RQ2 are not mutually exclusive. This means that each article can be classified into several alternatives of those categories. The alternatives in the remaining categories are on the other hand mutually exclusive. The alternatives for the category *Evaluation metric* do reflect some of the metrics in the article by Soleymani *et al.* [3].

Evaluation type is how the article conduct or suggest the evaluation to be done. Evaluation metric is how the trust models are evaluated; how their success are measured, in order to be compared. The three last categories are only applied for

Table 4.3: Classification scheme for the mapping study for RQ1

Category	Alternative	Description
Topology architecture	Centralized	The model depends on a central entity to function
	Decentralized	The model can function without a central entity
Main object of consideration	Entity-centric	The trust evaluation is based on the entity from which the data
	Data-centric	The trust evaluation is based on the data and information that are being sent and received
	Combined	The trust evaluation is based on both the data and information as well as the entity from which it is sent
Privacy	Yes	In the article the authors claim that the model enables privacy
	No	In the article the authors do not claim that the model enables privacy

conducted simulative evaluations and they are: in what environment the simulation takes place, which dynamics the simulation uses in order to simulate as close to a real-life scenario as possible, and what application the VANETs are being used for in the simulations.

Regarding the classification of scenario environments in the simulations within the articles, the logic that was used is illustrated in Figure 4.1. First, the road characteristics were analyzed. If there was only a straight, one directional lane, this was classified as a highway scenario. Intersections and road grids were classified as urban scenarios. If no characteristics were found, speed was considered. Here, high speed roads (over 80km/h) were classified as highway scenarios, whereas low speed roads (below 80km/h) were classified as urban scenarios. Some of the articles used both types of scenarios in their simulations.

Table 4.4: Classification scheme for the mapping study for RQ2

Category	Alternative	Description
Evaluation type	Simulative	The evaluation is based on simulations
	Analytical	The evaluation is done by using analytical models, e.g. a Markov chain
	Qualitative	The evaluation is done by theoretical discussion and reasoning
Evaluation metric	Path time	The article evaluates how the path time is affected when using the VANET for route planning
	Accuracy	The article evaluates how well the model can distinguish true information from false
	Performance	The article evaluates efficiency connected to the computational part of the model, e.g. response time and computational efficiency
	Scalability	The article evaluates if the model can be applied in networks of a larger scale
	Privacy	The article evaluates how well the model can preserve privacy among the vehicles in the network
	Decentralization	The article evaluates whether the model needs a central unit to function
	Dynamic	The article evaluates how well the model handles changes in the network
	Cost	The article evaluates how cost efficient the model is
Simulation scenario environment	Urban	See Figure 4.1
	Highway	See Figure 4.1
	Both	The simulation uses both type of environments. See Figure 4.1
	Unknown	The scenario environment is not known by reading the article
Simulation dynamics	Network	The model is simulated using a network simulator
	Traffic	The model is simulated in a traffic simulator, or explicitly mentioned that the traffic is simulated as well

Table 4.4: Classification scheme for the mapping study for RQ2 (continued)

Category	Alternative	Description
	Both	The model is simulated with both traffic and network dynamics
	Neither	The model is not simulated using either dynamics above
Simulation VANET application	Road events	In the simulation, the VANET is used to send information about discrete, binary, road events at particular locations, such as if there is an accident at a particular location or not
	Route planning	In the simulation, the VANET is used to send information about the travel time for the different paths
	Platooning	In the simulation, the VANET is used to let the vehicles participating platoon
	Not specified	In the simulation, the VANET is not used for a particular application, or there is a missing description for the application

4.1.5 Data extraction & mapping process

The last step of the systematic mapping study is the data extraction and mapping process. The articles found earlier were mapped based on the classification scheme presented in the previous section. To answer RQ1, a single systematic map was compiled, and can be found in Figure 5.1.

For RQ2, five systematic maps were compiled. They can be found in Figures 5.2, 5.3, 5.4, 5.5, and 5.6.

4.2 Interviews

To complement the result from the mapping study, and provide further foundation for analysis when answering RQ2, interviews were conducted. The main purpose of the interviews were to get input from the automotive industry of what their view on VANETs and the corresponding trust models is. Both the potential and most valuable applications of VANETs were approached, as well as the value of implementing

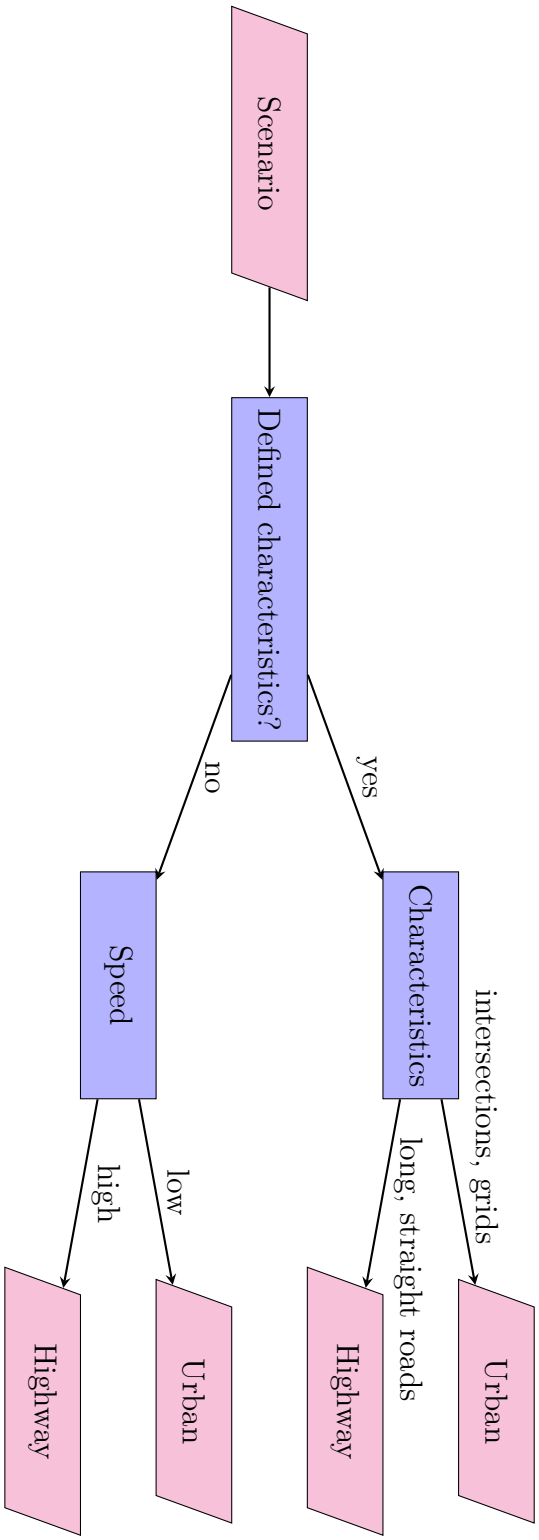

Figure 4.1: Visualization of reasoning for classification of simulation scenarios.

trust models in relation to existing cryptography solutions. The interviews were of semi-structured character and the interview subjects included representatives from both industry and academia.

As described by Longhurst [26], semi-structured interviews are suitable in qualitative studies where the researcher aims to elicit information from a person by asking questions, in a conversational manner. It is also stated in Longhurst [26] that the interviewer should prepare questions before the interview, but can choose which of them to actually include and in which order, as the interview proceeds.

The interview subjects were selected by focusing on interviewees with experience mainly in the automotive domain, but most preferably also with experience of trust models. Potential subjects were selected by targeting relevant companies in the industry as well as researchers received by recommendations. Additional subjects were received by asking for other potential contacts from the interviewees.

The interviews in this thesis project were some conducted in person, at the office where the interview subject was located, or via phone calls, since some of the subjects were located outside of Sweden. The meetings always started out with an introduction of the project and an explanation of the purpose of the interview. The exact introduction and the questions that were prepared for the interviews are presented in Appendix A. For all of the interviews, the first question was the same.

5

Results

This chapter aims to present the results for the research questions in consecutive order. It is divided into three sections where Section 5.1 presents the result for RQ1 and Section 5.2 and 5.3 present the result for RQ2.

5.1 Mapping of existing models

In this section, the result of the mapping study that aimed to answer the first research question (*Which models for ensuring trust in a VANET environment exist?*) is presented. The result is displayed as a single diagram in Figure 5.1. The actual articles in each category are listed in Table 5.1. Since the categories were mutually exclusive the result could be presented in one single diagram. The diagram has the *main object of consideration* on the y-axis and the *topology architecture* on the x-axis. It is divided into two facets representing the *privacy* category.

As noted in the figure, there is currently a total of 48 models available, where 36 models do not address the privacy issue. The distribution in main object of consideration is very close to being perfectly evenly spread out, with 17, 15, and 16 models for Entity, Data, and Combined respectively.

Decentralized topology architecture is also clearly the most common topology architecture, with 35 models. This difference is visible in all of the categories on the y-axis, except the entity-based models, where centralized topology architecture is slightly more common than decentralized topology architecture. Entity-based models also have a slightly larger representation among the privacy-models. There is no large difference between data-based and combined models in terms of their topology architecture or their way of addressing the privacy issue.

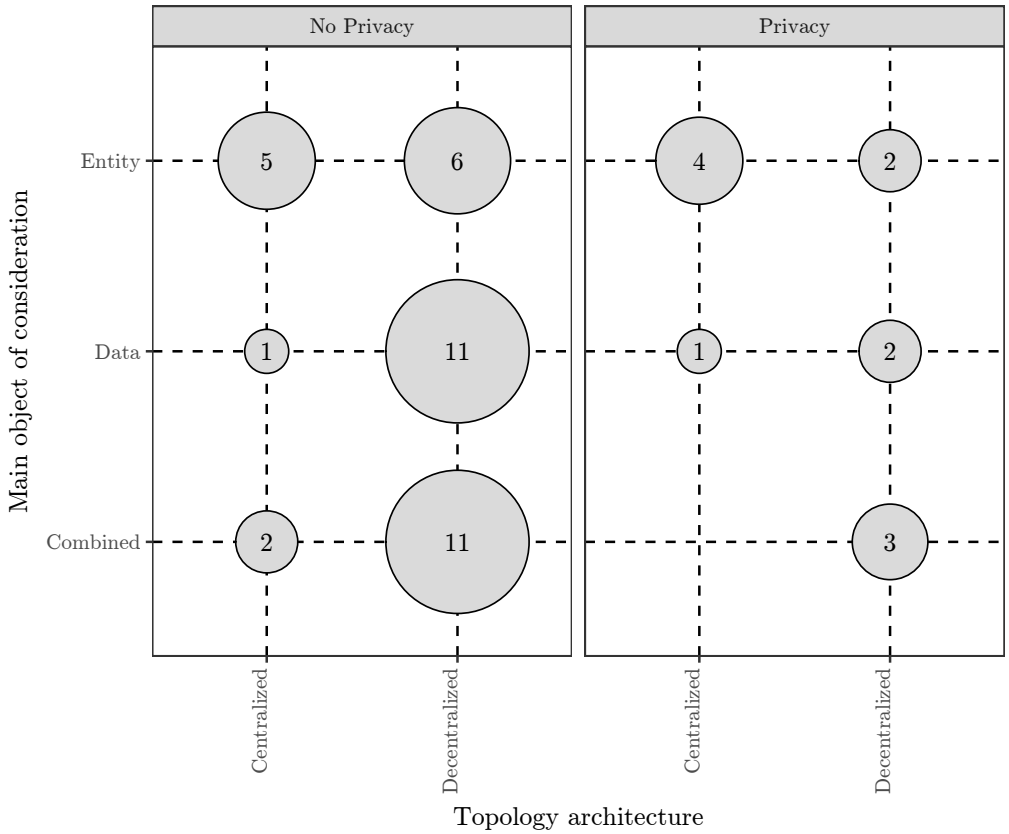

Figure 5.1: Systematic map from the mapping study for RQ1

Table 5.1: The underlying data for the systematic mapping for RQ1

Model	**Topology architecture**	**Major object of consideration**	**Privacy**
Anyigor Ogah *et al.* [27]	Centralized	Entity	No Privacy
Gai *et al.* [28]	Centralized	Entity	No Privacy
Machado and Venkatasubramanian [29]	Centralized	Entity	No Privacy
Hu *et al.* [30]	Centralized	Entity	No Privacy
Sugumar [31]	Centralized	Entity	No Privacy
Bamberger *et al.* [32]	Decentralized	Entity	No Privacy
Sengathir *et al.* [33]	Decentralized	Entity	No Privacy
Wang and Chigan [34]	Decentralized	Entity	No Privacy
Minhas *et al.* [16]	Decentralized	Entity	No Privacy
Bhargava *et al.* [35]	Decentralized	Entity	No Privacy
Abdelaziz *et al.* [36]	Decentralized	Entity	No Privacy
Kothari *et al.* [37]	Centralized	Data	No Privacy
Wu *et al.* [17]	Decentralized	Data	No Privacy
Gazdar *et al.* [38]	Decentralized	Data	No Privacy
Mehdi *et al.* [39]	Decentralized	Data	No Privacy
Wang and Wu [40]	Decentralized	Data	No Privacy
Shrivastava *et al.* [41]	Decentralized	Data	No Privacy
Gurung *et al.* [42]	Decentralized	Data	No Privacy
Ding *et al.* [43]	Decentralized	Data	No Privacy
Basheer *et al.* [44]	Decentralized	Data	No Privacy
Abumansoor and Boukerche [45]	Decentralized	Data	No Privacy
Koster *et al.* [46]	Decentralized	Data	No Privacy
Rehman *et al.* [47]	Decentralized	Data	No Privacy
Huang *et al.* [48]	Centralized	Combined	No Privacy
Liao *et al.* [4]	Centralized	Combined	No Privacy
Ltifi *et al.* [49]	Decentralized	Combined	No Privacy
Finnson *et al.* [50]	Decentralized	Combined	No Privacy
Haddadou *et al.* [51]	Decentralized	Combined	No Privacy
Primiero *et al.* [52]	Decentralized	Combined	No Privacy
Soleymani *et al.* [53]	Decentralized	Combined	No Privacy
Cohen *et al.* [54]	Decentralized	Combined	No Privacy

Table 5.1: The underlying data for the systematic mapping for RQ1 (continued)

Model	Topology architecture	Major object of consideration	Privacy
Saraswat and Chaurasia [55]	Decentralized	Combined	No Privacy
Sargunavathi and Martin L. M. [56]	Decentralized	Combined	No Privacy
Haddadou and Rachedi [57]	Decentralized	Combined	No Privacy
Liu *et al.* [58]	Decentralized	Combined	No Privacy
Haddadou *et al.* [59]	Decentralized	Combined	No Privacy
Monir *et al.* [60]	Centralized	Entity	Privacy
Kim and Bae [61]	Centralized	Entity	Privacy
Gao *et al.* [62]	Centralized	Entity	Privacy
Hu *et al.* [63]	Centralized	Entity	Privacy
Wei *et al.* [64]	Decentralized	Entity	Privacy
Hasrouny *et al.* [65]	Decentralized	Entity	Privacy
Wei and Chen [66]	Centralized	Data	Privacy
Shaikh and Alzahrani [67]	Decentralized	Data	Privacy
Mazilu *et al.* [68]	Decentralized	Data	Privacy
Tajeddine *et al.* [69]	Decentralized	Combined	Privacy
Choi *et al.* [70]	Decentralized	Combined	Privacy
Wei and Chen [71]	Decentralized	Combined	Privacy

5.2 Mapping of evaluation settings

In this section, the results of the mapping study that aimed to answer the second research question (*What are relevant criteria for industrial settings to evaluate trust models in the VANET environment?*) are presented. The result is displayed in multiple bar charts, one per category, which makes potential correlations between the different categories impossible to extract. The underlying data can be found in Appendix B. The diagrams are presented consecutively, ending with a summary.

The first diagram, Figure 5.2, displays the *Type of evaluation*. A single article may have conducted or suggested multiple types of evaluations. The simulative evaluation method is clearly the most popular. 42 articles conduct or suggest simulative evaluations, while analytical and qualitative evaluations are only suggested or conducted 8 and 9 times respectively.

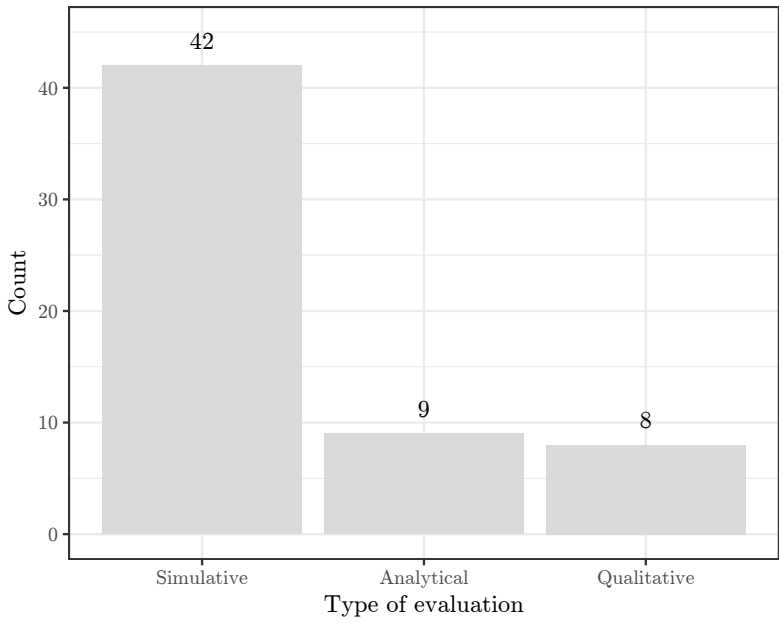

Figure 5.2: Systematic map from the mapping study for RQ2: Type of evaluation conducted, or suggested, in each article

The second diagram, Figure 5.3, displays the *Type of evaluation metric*. A single article may have used or suggested multiple metrics. The clearly most popular evaluation metric is the accuracy metric, with 33 articles, followed by the performance metric, with 17 articles. The other metrics all have about the same frequency, with 5 or 6 articles, except the cost metric, which was only used or suggested once.

The last three diagrams only include the articles that actually conduct a simulative evaluation, which is a total of 41 articles.

The first of the simulation diagrams, Figure 5.4, displays the *Simulation scenario environment*. About one fourth, 10 models, did not present in what environment the simulation was conducted in. Only 6 models were simulated in both environments. The urban environment was almost twice as common as the highway environment, with a total of 24 articles versus 13 articles.

The second of the simulation diagrams, Figure 5.5, displays the *Simulation dynamics*. A clear majority, 29 articles, use both network and traffic dynamics in their simulations. Only seven articles do not use either dynamics. There is no big difference in the usage of network or traffic dynamics.

The last one of the simulation diagrams, Figure 5.6, displays the *Simulation VANET application*. A clear majority, 26 articles, do not simulate using a specific VANET application. 8 of the articles simulate VANET for road events messaging, 6 for route planning and only one single article simulate platooning.

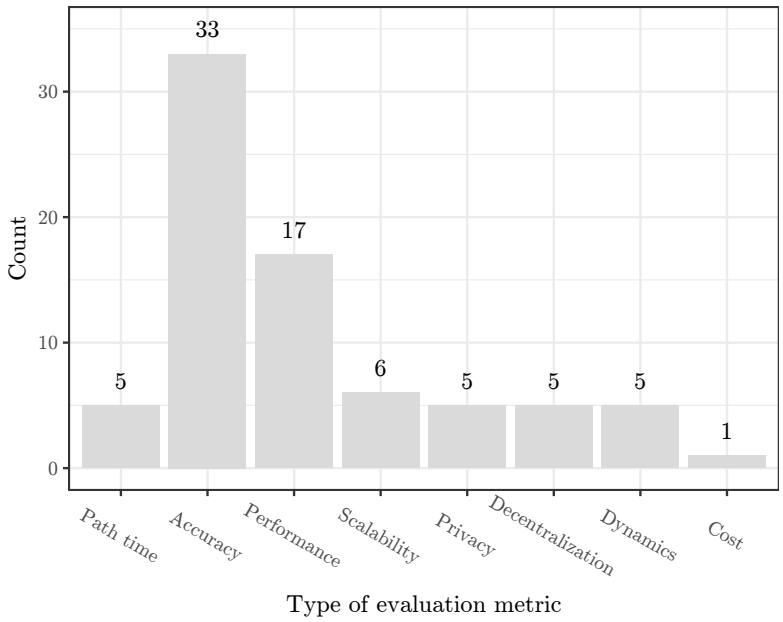

Figure 5.3: Systematic map from the mapping study for RQ2: Type of metric used or suggested in the articles

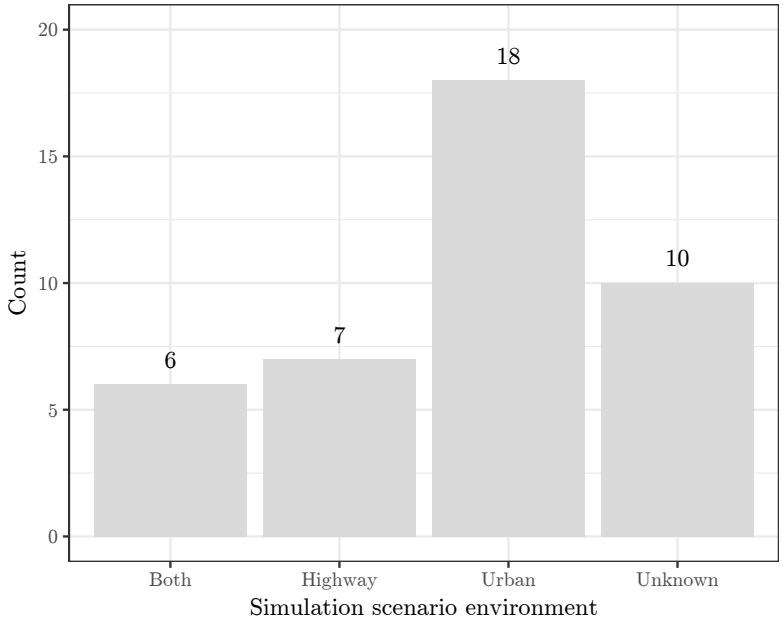

Figure 5.4: Systematic map from the mapping study for RQ2: Type of simulation scenario environment in each article

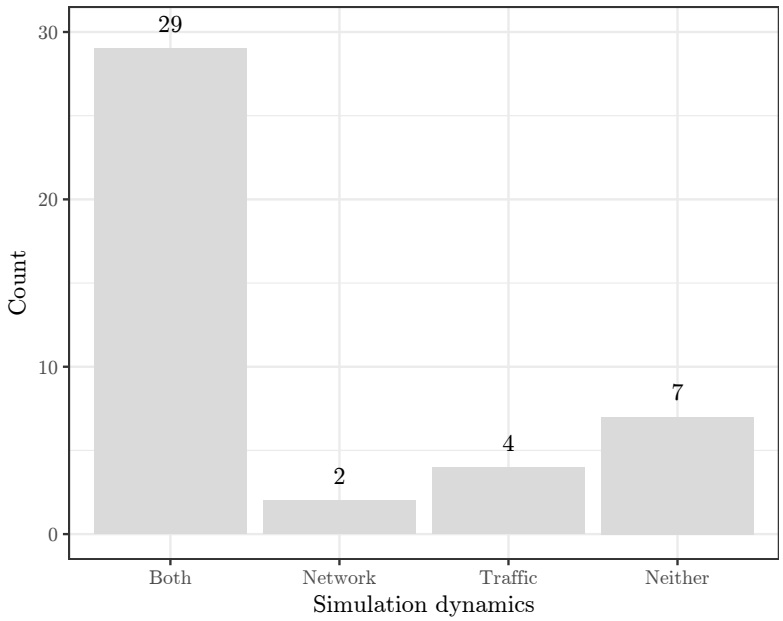

Figure 5.5: Systematic map from the mapping study for RQ2: Type of dynamics included in each simulation

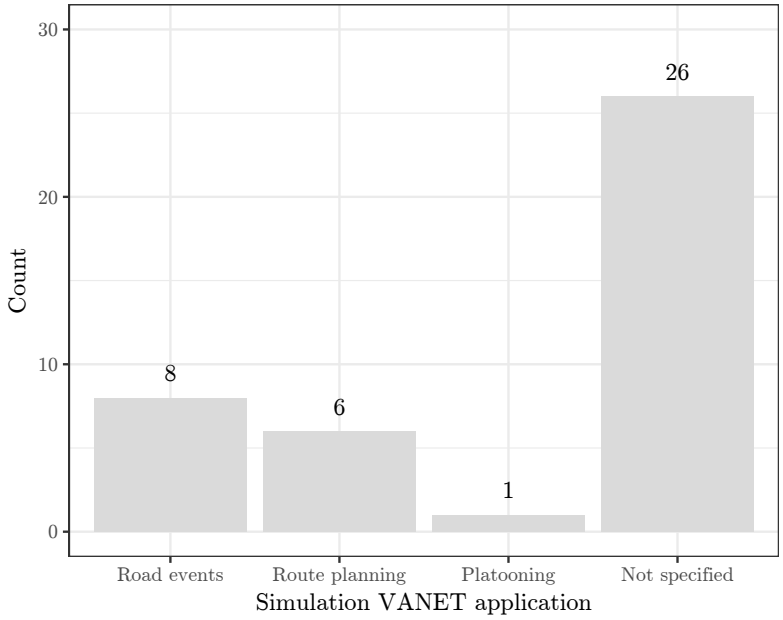

Figure 5.6: Systematic map from the mapping study for RQ2: Type of VANET application used in the simulations

5.3 Interview results for VANET applications

The results from the interviews are presented below, divided per interview question. These results complement the mapping study for RQ2 by showing what view the industry and academia has on the topic of VANET and corresponding trust models, in contrast to what theory showed in the articles that were analyzed in the mapping study.

5.3.1 Relevant application areas for VANETs

Out of the six people that were interviewed, four mentioned platooning for trucks as the most relevant VANET application area. Other application areas included communication between vehicles as well as road side units such as traffic lights. The information being sent in this type of application could be, according to our interview subjects, regarding road conditions as well as potential traffic congestions. It is also mentioned that VANET could be used to schedule traffic.

5.3.2 Challenges of implementing VANET applications

One of the challenges of implementing these different VANET applications, was said in the interviews to be to reach the critical mass. This means that enough vehicles would have the same VANET technology implemented in order to create enough value of implementing the technology for additional vehicles. Connected to this, one of the interview subjects mentioned the challenge of standardization, and how to make every vehicle using VANET interpret information and parameters the same way. Another challenge that was explained by one of the interview subjects is the issue of responsibility. If one vehicle sends information to another that causes an accident – is the sending vehicle or the receiving vehicle responsible for the accident? This is a question that the same interview subject said is hard to answer but still necessary to answer if the goal is to send information between vehicles.

5.3.3 Trust model in relation to cryptography

By multiple interview subjects, it was mentioned that trust models should be developed and presented as a complement to cryptography. One reason for this was said to be that no matter how advanced and secure a cryptography solutions is, it will only be a matter of time until there is an attack that can break the cryptography. It was further mentioned that errors such as dysfunctional sensors cannot be handled by cryptography, but can theoretically be handled by a trust model.

5.3.4 Valuable VANET applications for the industry

Connected to the issue previously mentioned regarding reaching a critical mass of VANET users, the VANET application that is closest to hand for the industry is said by the majority of the interview subjects to be platooning for trucks. The reason for this was since it only requires very few vehicles, the participating vehicles in the platoon, to implement VANET technology. Further on, platooning was described as a clear business case for the automotive industry, with measurable benefits such as decreased fuel consumption and thus lower costs. It was also mentioned that shipping firms that will use platooning, will most probably require that trucks of multiple brands can be included in one platoon.

5.3.5 Potential attack scenarios

The attack scenarios that were mentioned in the conducted interviews were hijacking attacks. The result of these attacks was said to be that the hijacking agents might take over the control of the vehicles and hence cause a collision. It could also result in the hijacker sending false information in order to stop or misdirect traffic.

6

Discussion

In this chapter the results of the study are analyzed and discussed. The answers to the research questions are presented in Section 6.1. This is followed by Section 6.2 which discusses potential threats to the validity of the study.

6.1 Analysis

This section is divided into two subsections discussing the results related to each respective research question, and how those results relate to the goal.

6.1.1 Classification of existing trust models

In the classification of existing trust models, the first category is topology architecture, where the majority of the models were classified as decentralized. This is coherent with the general recommendation for trust models in VANETs; to prefer decentralization over centralization (Alriyami *et al.* [7]). This also suggests that most authors are aware of the preferred topology architecture.

In terms of the second classification category, main objective of consideration, the models were almost evenly distributed over the alternatives entity-based, data-based and combined. This is probably an effect of the fact that the different categories have both advantages and disadvantages, and are suitable in different situations and applications, as mentioned by Alriyami *et al.* [7]. Hence, it might be necessary in the future to use several trust models in vehicles to be able to handle a large variety of threats.

The third and last category of the classification was whether or not the model addressed the privacy issue. Out of the 48 models that were classified in the mapping study, only 12 were said to approach the issue of retaining the privacy of the vehicles in the VANETs. This is in itself an issue since, as previously mentioned according to Alriyami *et al.* [7], privacy of the vehicles is an important dilemma, not least in order for VANET technologies to be attractive within the industry. It is however

a complex issue, which might be the reason why most models do not address the privacy issue yet. Regarding correlation between the categories, the largest amount of models that approach the privacy issue (9 out of 12), are entity-based or combined. This correlation is expected since the entities themselves are being evaluated, and hence, the privacy of the entities, i.e. the vehicles, is exposed.

It should also be noticed that some of the models might not be realizable. As stated by Alriyami *et al.* [7], some of the models make assumption that are not feasible or realistic. For instance, they find that one model assumes global knowledge of the network. One reason for this might be that many models are fairly old and not fully developed, or that there are no established ways for how to test the models. This indicates that some sort of filtering, or guidelines for how to quickly assess a found model, should be done in future work, in order to make sure that only realistic models are evaluated.

The derived systematic map can be used for different purposes when conducting a future evaluation. The most evident one is to get an overview of what type of models exist today and what characterizes them. Another benefit of the systematic map is that it will be possible to quickly find several models with similar characteristics, or models with a specific set of characteristics, by using the systematic map together with its data.

6.1.2 Industrial settings for evaluation of trust models

As stated in the results section, the simulative evaluations were by far the most popular evaluation type. This is similar to the findings in Kerrache *et al.* [6], and also follows the recommendations by Zhang [8]. Hence, the way current evaluations are done do not contradict the suggested methodology, however, just like the findings in Zhang [8], the current simulations may not be done as comprehensively as suggested by Kerrache *et al.* [6] and Zhang [8], who suggest to use testbeds and comprehensive simulation software. It is also suggested that evaluations should be done in real-life, although this lowers the reproducibility of the evaluation, and obviously the feasibility (Sommer and Dressler [2]). An impact in feasibility might limit the number of evaluations, since only researchers with a large amount of resources will be able to conduct the evaluations. A lowered reproducibility will also make it hard to validate any empirical studies, both by the conducting researchers as well as other researchers. Consequently, the transparency that was desired among the evaluations might not be reached using real-life evaluations. The high frequency of simulative evaluations confirms that simulations are an appropriate evaluation method for VANET trust models.

Among the evaluation metrics, the accuracy metric was the most popular, followed by the performance metric. This thesis' definition of the accuracy metric is mainly based on if the model produces trust values that reflect reality. For instance, a malicious node receives lower trust than trustworthy nodes. An example of such a

measure is the F-measure. The performance metric is mainly based on the load the model make on the system, for instance computational efficiency, network overhead or response time. The other metrics' definitions can be found in Section 4. Accuracy is one of the key metrics in the testbed developed by Jelenc *et al.* [9], and is the only used metric when choosing not to include a decision mechanism in the evaluation. Thus, they suggest that the accuracy metric is the most important metric, which the results in this thesis also indicate. Hence, it is highly recommended to use accuracy as one of the metrics when evaluating trust models.

The performance metric resembles the *Opinion cost* metric in the testbed by Jelenc *et al.* [9] since both are a measure of the amount of work conducted, although the metrics are measured in completely different ways. The performance metric is usually a measure of load on the on-board computational unit when doing calculations, while the opinion cost metric is more related to how many other agents the model asks for opinion. The performance metric might be popular in VANETs because it is such a unique domain, where the trust computation usually takes place on a device with limited computational power, and particularly in the evaluation of data-centric trust models which usually require processing of larger amount of data. Although, since computers get more and more efficient, equipped with more computational power, this metric might become less relevant, and is therefore not as important to include as the accuracy metric.

The last metric that Jelenc *et al.* [9] include is the *Utility* metric, which combines the trust model with a decision mechanism, and evaluates the quality of the decision taken. Although, in the articles found, there is seldom a decision mechanism included. The only metric that is found to evaluate the decision is the path time metric, although it is very specific to the route planning application. Hence, in general, a utility metric, or evaluation of decision, is not included in the mapped evaluations. According to Jelenc *et al.* [9], one should be careful in the choice of decision mechanism, since it will impact the evaluation results. They give the options to evaluate with multiple decision mechanisms, but also stress that the evaluation can be conducted solely without the decision mechanism. Hence, it is not a priority to include the quality of the decision taken, as a metric.

Among the simulation environments, the urban environment was much more common than the highway environment. This is similar to the findings by Sommer and Dressler [2], which indicates that VANET trust model simulations do not differ that much from VANET simulations in general. The choice of urban environment is however in contrast with the fact that VANETs are particularly useful in rural areas, where there might be a lack of fixed communication infrastructure (Zhang and Wolff [72]). Although, the models might be evaluated as often in urban environments due to their requirement of high network density. Also, the choice of environment is depending on application, for instance routing application might be more relevant in urban areas, and platooning in highway environment. Hence, even though the findings show that simulations can be conducted in both types of environments, the choice of environment will be connected to the choice of application.

The usage of both network and traffic dynamics in the simulations have high frequency, and is coherent with the general recommendations in Sommer and Dressler [2] and Grzybek *et al.* [73]. The finding that most of the evaluations use both dynamics is similar to the findings of the mapping of general VANET simulations in Sommer and Dressler [2]. This confirmation that trust models can be evaluated with both dynamics, together with the general recommendations to use both dynamics for VANET simulations, entails that when simulating in the future, using both dynamics in combination is highly recommended.

The high frequency of simulations that did not specify application might have multiple explanations, for instance that the authors aimed to make a model that can be generally applied since it is still not clear which application that is most relevant for VANETs. The interview results showed something entirely different, since a majority of the interview objects agreed on platooning being the most relevant VANET application. The mapping study results also contradict the recommendation by Zhang [8], which emphasizes the need to simulate as close to real-life scenarios as possible.

The high frequency of simulations that did not specify application might also indicate that the models themselves are general, and that the choice of application does not affect the evaluation. However, this hypothesis is easily tested, by evaluating the models with different applications. Hence, for a future simulation, an evaluation with several application areas is desirable.

The road events application might be most common because it is easy to simulate and implement, with discrete binary events that could easily be confirmed or disproved by the entities. Hence, for a first simple simulation this application could be a good starting point.

The low frequency of simulating platooning might indicate that trust models will not really contribute to that particular application, and that cryptography might be a sufficient security solution. However, in the interviews, it was pointed out that shipping firms require their fleet to contain trucks from multiple brands, hence pushing towards an open VANET environment for platooning as well, which requires the cryptography to be completed with trust models. Sommer and Dressler [2] also recognize platooning as one of the most demanded applications. Because of the value platooning will provide, and the indication that trust models is required for it to work, platooning is a very relevant application to evaluate with.

A very important part in the simulation of VANETs is the routing protocol (Sommer and Dressler [2]). Although this was not a part of the mapping study, and hence not of the result either. One possible explanation is given by the very methodology that was used, the systematic mapping, in conjunction with what Kerrache *et al.* [6] write. The mapping study is dependent on what is written in the subject that are studied; if a particular subject is never mentioned, it will not be included in the mapping, which points towards that routing protocols are not mentioned in the articles. This is confirmed by Kerrache *et al.* [6], which mention that none of the

models they study mention which routing protocol they use in their simulations. The most common routing protocol is therefore something that is unknown and cannot be given a recommendation about. Although, the routing protocol is usually related to the application (Sommer and Dressler [2]), and the best recommendation that can be given is that future researchers explicitly state all assumptions, including which routing protocol that is used, in order to provide more transparency.

To summarize; simulative evaluations are preferred over analytical or qualitative evaluations. When evaluating the models, they should preferably be evaluated with regards to their accuracy. Both simulation dynamics, networks and traffic, should be included in the simulations. It is highly recommended to use a VANET application in the simulations, and to choose an appropriate environment in order to simulate a close to real-life scenario as possible. Choosing platooning as application is preferred, although for a more simpler simulation, the road events application can suffice.

6.2 Threats to validity

The threats to validity of this thesis are presented in this section, and are divided by the two research methods that were used in this thesis.

6.2.1 Systematic mapping study

The threats to validity of the systematic mapping study were divided into construct validity, reliability, internal validity and external validity.

Construct validity in the context of a mapping study is about whether what was studied actually was coherent with the goal of the mapping study (Engström and Runeson [74]). One factor that might have had an impact on this is the terms used in the initial search. For instance, the term *Inter Vehicular Communication* is a term that could be a synonym to VANET and using that term in the search might have given a more extensive result. Although, many other synonyms were used to denote such communication, which in turn minimizes this risk. Another possible factor is that not all relevant articles matching the string were found. By choosing four well known databases, and not excluding any result based on type, the authors believe that this validity threat is fairly mitigated.

Reliability of a mapping study is according to Engström and Runeson [74] a measure of whether the study is repeatable. To increase the reliability of the mapping study in this thesis, the execution is described thoroughly in Section 4.1, with defined search strings, inclusion and exclusion criteria and classification schemes. One factor that might have decreased the reliability is the fact that the two authors of this thesis divided the articles between them, both when it came to applying the inclusion and exclusion criteria, as well as to classifying the selected articles. The

risk was mitigated by the authors working in close collaboration, raising any issues and uncertainties, and then iterating over the criteria or classification scheme if necessary. At the same time, some of the articles were classified by both authors who then compared the result, in order to ensure that both authors interpreted the criteria and classification scheme the same way.

Internal validity is regarding the analysis of the study and whether the conclusions drawn are reasonable (Engström and Runeson [74]). The area of trust models in VANETs is rather unexplored, making it hard to validate any analysis of results. However, by carefully comparing the analysis of the result to the related work that is available in the domain, the risks to internal validity could be somewhat mitigated.

Finally, the external validity determines the generalizability of the result (Engström and Runeson [74]). It is related to if experiments conducted can be generalized to other parts of the domain or to completely different domains. Since the mapping study is conducted over the entire domain of VANETs, the threats to the external validity are minimal, however to generalize the results to another domain might not be possible because of the unique nature of VANETs.

6.2.2 Interviews

The main threat to validity of the interviews in this thesis is the possibility of convenience sampling. Convenience sampling exist when data is collected from objects that are conveniently available when conducting the study (Dudovskiy [75]). Since this thesis was written in Gothenburg, some of the interview subjects came from the many organizations working in the automotive industry in Gothenburg. Although to avoid convenience sampling to some extent, 3 people outside of Gothenburg were contacted and interviewed, including 2 from outside of Sweden.

The sample size of the interview subjects, i.e. the number of people that were interviewed, might also be a threat to validity. As the interviews subjects were chosen for this thesis, it was taken into consideration to include representatives from both industry and academia, as well as from different geographical position. By doing this, the authors believe that the resulting sample size is large enough to include relevant aspects.

7

Conclusion & future work

The purpose of this study was to provide a foundation for evaluating and comparing trust models in the VANET environment. To reach the goal, existing trust models in the VANET environment have been mapped, and possible evaluation settings for such models have been derived. It has been done through a systematic mapping study and through interviews. 48 trust models have been found, and subsequently categorized by their topology architecture, their main object of consideration as well as if they address the privacy issue. Five aspects regarding evaluation have been considered; evaluation type, evaluation metric, simulation dynamics, simulation environment and VANET application in simulations. Guidelines for future research; how to choose a model to evaluate as well as how to choose appropriate evaluation settings have also been derived and presented.

Regarding future work, as stated previously, the mapped trust models have not been systematically evaluated so far, and other research suggests that trust models in the VANET domain have varying quality, with for instance unrealistic assumptions. Hence, an initial qualitative filtering, or guidelines for how to quickly assess a found model, would provide value for future researchers trying to select models to implement or evaluate. In addition, the foundation provided in this thesis does not offer any concrete information about routing protocols, even though they make up a central part in VANETs. Hence, any research towards adding information about routing protocols to the foundation is desirable.

As this thesis purpose is to contribute to future evaluations of trust models, future research conducting objective simulative evaluations would greatly contribute to the research area. In order to conduct an evaluation, a choice of models must be made. The choice of models can be supported by the systematic map of the trust models provided earlier. The evaluation settings must also be specified, and can be supported by the earlier provided arguments, with regards to evaluation metric, simulation dynamics, simulation environment, and VANET application. Even though there are preferred settings in which simulations should be conducted, there are still no, to the best of the authors' knowledge, objective simulative evaluations available in this domain. Hence, any simulative evaluation and comparison will still be a contribution.

Bibliography

[1] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward", in *ICAC 2014 - Proceedings of the 20th International Conference on Automation and Computing: Future Automation, Computing and Manufacturing*, 2014, ISBN: 9781909522022. DOI: 10.1109/IConAC.2014.6935482.

[2] C. Sommer and F. Dressler, *Vehicular Networking*. Cambridge: Cambridge University Press, 2015. DOI: 10.1017/CBO9781107110649.

[3] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee, and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review", *EURASIP Journal on Wireless Communications and Networking*, 2015, ISSN: 1687-1499. DOI: 10.1186/s13638-015-0353-y.

[4] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", in *2013 IEEE 5th International Symposium on Wireless Vehicular Communications, WiVeC 2013 - Proceedings*, 2013, ISBN: 9781467363396. DOI: 10.1109/wivec.2013.6698224.

[5] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks", *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 24, no. 2, 2006. DOI: 10.1109/JSAC.2005.861390.

[6] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, *Trust Management for Vehicular Networks: An Adversary-Oriented Overview*, 2016. DOI: 10.1109/ACCESS.2016.2645452.

[7] Q. Alriyami, A. Adnane, and A. K. Smith, "Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs)", in *2014 International Conference on Connected Vehicles and Expo, ICCVE 2014 - Proceedings*, 2014, ISBN: 9781479967292. DOI: 10.1109/ICCVE.2014.7297525.

[8] J. Zhang, "Trust Management for VANETs: Challenges, Desired Properties and Future Directions", *International Journal of Distributed Systems and Technologies*, pp. 48–62, 2012. DOI: 10.4018/jdst.2012010104.

[9] D. Jelenc, R. Hermoso, J. Sabater-Mir, and D. Trček, "Decision making matters: A better way to evaluate trust models", *Knowledge-Based Systems*, 2013, ISSN: 09507051. DOI: 10.1016/j.knosys.2013.07.016.

[10] L. Longo, P. Dondio, and S. Barrett, "Temporal factors to evaluate trustworthiness of virtual identities", in *Proceedings of the 3rd International Con-*

ference on Security and Privacy in Communication Networks, SecureComm, 2007, ISBN: 1424409756. DOI: 10.1109/SECCOM.2007.4550300.

[11] Y. Yang, J. Xu, D. Cheng, L. H. Wu, P. J. Tan, and L. T. Yang, "VANET link characteristics and analysis in urban and suburban scenarios", in *2008 International Conference on Communications, Circuits and Systems Proceedings, ICCCAS 2008*, 2008, ISBN: 9781424420636. DOI: 10.1109/ICCCAS.2008.4657733.

[12] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, *Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends*, 2015. DOI: 10.1155/2015/745303.

[13] J.-M. Seigneur, "Trust, Security and Privacy in Global Computing", 2005.

[14] D. Gambetta, "Can We Trust Trust?", vol. 13, pp. 213–237, 2000.

[15] D. Trček, "Towards trust management standardization", *Computer Standards and Interfaces*, 2004, ISSN: 09205489. DOI: 10.1016/j.csi.2004.03.007.

[16] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty", in *Proceedings - 2010 IEEE/WIC/ACM International Conference on Intelligent Agent Technology, IAT 2010*, 2010, ISBN: 9780769541914. DOI: 10.1109/WI-IAT.2010.66.

[17] Y. Wu, F. Meng, G. Wang, and P. Yi, "A Dempster-Shafer Theory Based Traffic Information Trust Model in Vehicular Ad Hoc Networks", in *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, 2015, pp. 1–7.

[18] M. N. Marshall, "Sampling for qualitative research", *Family Practice © Oxford University Press*, vol. 13, no. 6, 1996.

[19] S. Ahmed and K. Tepe, "Evaluating Trust Models for Improved Event Learning in VANETs", in *IEEE 30th Canadian Conference on Electrical and Computer Engineering*, Windsor, 2017.

[20] J. Zhang, "A survey on trust management for VANETs", in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2011, ISBN: 9780769543376. DOI: 10.1109/AINA.2011.86.

[21] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update", in *Information and Software Technology*, 2015, ISBN: 0360-1315. DOI: 10.1016/j.infsof.2015.03.007.

[22] *ACM Digital Library*, 2017. [Online]. Available: http://dl.acm.org/.

[23] *IEEE Explore*, 2017. [Online]. Available: http://ieeexplore.ieee.org/Xplore/home.jsp.

[24] *Scopus*, 2017. [Online]. Available: https://www.scopus.com/search/form.uri?display=basic.

[25] *Springer Link*, 2017. [Online]. Available: https://link.springer.com/.

[26] R. Longhurst, *Key Methods in Geography*, Third, N. Clifford, M. Cope, T. Gillespie, and S. French, Eds. London: SAGE Publications Ltd, 2016, pp. 143–156.

[27] C. P. Anyigor Ogah, H. Cruickshank, P. M. Asuquo, A. Lei, and Z. Sun, "Delay Tolerant Revocation Scheme for Delay Tolerant VANETs (DTRvS)", 2017. DOI: 10.1007/978-3-319-67639-5.

[28] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Ratee-Based Trust Management System for Internet of Vehicles", 2017. DOI: 10.1007/978-3-319-60033-8.

[29] R. G. Machado and K. Venkatasubramanian, "Short paper: Establishing trust in a vehicular network", in *IEEE Vehicular Networking Conference, VNC*, 2013, ISBN: 9781479926879. DOI: 10.1109/VNC.2013.6737611.

[30] H. Hu, R. Lu, and Z. Zhang, "TPSQ: Trust-based platoon service query via vehicular communications", *Peer-to-Peer Networking and Applications*, 2017, ISSN: 19366450. DOI: 10.1007/s12083-015-0425-0.

[31] R. Sugumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)", *Wireless Networks*, 2016. DOI: 10.1007/s11276-016-1336-6.

[32] W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory", in *Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust*, 2010, ISBN: 9780769542119. DOI: 10.1109/SocialCom.2010.20.

[33] J. Sengathir, @. R. Manoharan, and R. Manoharan, "Co-operation Enforcing Reputation-Based Detection Techniques and Frameworks for Handling Selfish Node Behaviour in MANETs: A Review", *Wireless Personal Communications*, vol. 97, pp. 3427–3447, 2017. DOI: 10.1007/s11277-017-4677-2.

[34] Z. Wang and C. Chigan, "Cooperation enhancement for message transmission in VANETs", *Wireless Personal Communications*, 2007, ISSN: 09296212. DOI: 10.1007/s11277-006-9235-2.

[35] A. Bhargava, S. Verma, and B. K. Chaurasia, "Kalman filter for trust estimation in VANETs", in *2015 IEEE UP Section Conference on Electrical Computer and Electronics, UPCON 2015*, 2016, ISBN: 9781467385077. DOI: 10.1109/UPCON.2015.7456757.

[36] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs", in *IWCMC 2014 - 10th International Wireless Communications and Mobile Computing Conference*, 2014, ISBN: 9781479909599. DOI: 10.1109/IWCMC.2014.6906441.

[37] A. Kothari, P. Shukla, and R. Pandey, "Trust Centric Approach Based on Similarity in VANET", *International conference on Signal Processing, Communication, Power and Embedded System*, 2016.

[38] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs", in *GLOBECOM - IEEE Global Telecommunications Conference*, 2012, ISBN: 9781467309219. DOI: 10.1109/GLOCOM.2012.6503113.

[39] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular Ad hoc Networks (VANETs)", *Computer Networks*, 2017, ISSN: 13891286. DOI: 10.1016/j.comnet.2017.04.024.

[40] G. Wang and Y. Wu, "BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks", *IEEE 13th International Con-*

ference on Trust, Security and Privacy in Computing and Communications, 2014. DOI: 10.1109/TrustCom.2014.137.

[41] A. Shrivastava, K. Sharma, and B. K. Chaurasia, "HMM for Reputation Computation in VANET", *International Conference on Computing, Communication and Automation (ICCCA2016)*, pp. 667–670, 2016.

[42] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks", in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, ISBN: 9783642386305. DOI: 10.1007/978-3-642-38631-2{_}8.

[43] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based Trust Model in Vehicular Ad Hoc Networks", in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, 2010.

[44] H. S. Basheer, C. Bassil, and B. Chebaro, "Toward using data trust model in VANETs", in *2015 1st International Conference on Applied Research in Computer Science and Engineering, ICAR 2015*, 2015, ISBN: 9781467385428. DOI: 10.1109/ARCSE.2015.7338136.

[45] O. Abumansoor and A. Boukerche, "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services", in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, 2011, ISBN: 978-1-4244-9268-8. DOI: 10.1109/GLOCOM.2011.6134243.

[46] A. Koster, A. Tettamanzi, A. L. C. Bazzan, and C. Da Costa Pereira, "Using trust and possibilistic reasoning to deal with untrustworthy communication in VANETs", in *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2013, ISBN: 9781479929146. DOI: 10.1109/ITSC.2013.6728579.

[47] A. Rehman, A. Ali, R. Ul Amin, and A. Shah, "VANET thread based message trust model", in *8th International Conference on Digital Information Management, ICDIM 2013*, 2013, ISBN: 9781479906130. DOI: 10.1109/ICDIM.2013.6693972.

[48] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs", *Peer-to-Peer Networking and Applications*, 2014, ISSN: 19366450. DOI: 10.1007/s12083-012-0136-8.

[49] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "A Cooperation Based Scheme for Managing Alert Propagation in VANET", *Wireless Personal Communications*, 2015, ISSN: 1572834X. DOI: 10.1007/s11277-015-2900-6.

[50] J. Finnson, J. Zhang, T. Tran, U. F. Minhas, and R. Cohen, "A framework for modeling trustworthiness of users in mobile vehicular ad-hoc networks and its validation through simulated traffic flow", in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, ISBN: 9783642314537. DOI: 10.1007/978-3-642-31454-4{_}7.

[51] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, 2015, ISSN: 00189545. DOI: 10.1109/TVT.2014.2360883.

[52] G. Primiero, F. Raimondi, T. Chen, and R. Nagarajan, "A proof-theoretic trust and reputation model for VANET", in *Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017*, 2017, ISBN: 9780769561073. DOI: 10.1109/EuroSPW.2017.64.

[53] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing", 2017. DOI: 10.1109/ACCESS.2017.2733225.

[54] R. Cohen, J. Zhang, J. Finnson, T. Tran, and U. F. Minhas, "A trust-based framework for vehicular travel with non-binary reports and its validation via an extensive simulation testbed", *Journal of Trust Management*, vol. 1, no. 10, 2014. [Online]. Available: http://www.journaloftrustmanagement.com/content/1/1/10.

[55] D. Saraswat and B. K. Chaurasia, "AHP based trust model in VANETs", in *Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013*, 2013, ISBN: 9780768550695. DOI: 10.1109/CICN.2013.86.

[56] S. Sargunavathi and J. Martin L. M., "Design and Development of CTSR with Direct & Indirect Observations of MANET Applications", *Mobile Networks and Applications*, 2017. DOI: 10.1007/s11036-017-0843-8.

[57] N. Haddadou and A. Rachedi, "DTMˆ2: Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad Hoc Networks", *IEEE ICC 2013 - Ad-hoc and Sensor Networking Symposium*, 2013.

[58] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs", *Mobile Information Systems*, 2016, ISSN: 1875905X. DOI: 10.1155/2016/7628231.

[59] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in Vehicular Ad Hoc Networks: An economic incentive model based approach", in *2013 Computing, Communications and IT Applications Conference, ComComAp 2013*, 2013, ISBN: 9781467360432. DOI: 10.1109/ComComAp.2013.6533601.

[60] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A Categorized Trust-Based Message Reporting Scheme for VANETs", in *Communications in Computer and Information Science*, 2013, ISBN: 9783642405969. DOI: 10.1007/978-3-642-40597-6{_}6.

[61] C. H. Kim and I. H. Bae, "A misbehavior-based reputation management system for VANETs", in *Lecture Notes in Electrical Engineering*, 2012, ISBN: 9789400750753. DOI: 10.1007/978-94-007-5076-0{_}54.

[62] T. Gao, Y. Li, and N. Guo, "An Anonymous Access Authentication Scheme for VANETs Based on ISGS", in *Innovative Mobile and Internet Services in Ubiquitous Computing : Proceedings of the 11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2017)*, L. Barolli and T. Enokido, Eds., Cham: Springer International Publishing, 2018, pp. 310–320, ISBN: 978-3-319-61542-4. DOI: 10.1007/978-3-319-61542-4{_}29. [Online]. Available: https://doi.org/10.1007/978-3-319-61542-4_29.

[63] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: A privacy-preserving trust-based relay selection scheme in VANETs", *Peer-to-Peer Networking and Applications*, 2017, ISSN: 19366450. DOI: 10.1007/s12083-016-0473-0.

[64] Y. C. Wei, Y. M. Chen, and H. L. Shan, "Beacon-based trust management for location privacy enhancement VANETs", in *APNOMS 2011 - 13th Asia-Pacific Network Operations and Management Symposium: Managing Clouds, Smart Networks and Services, Final Program*, 2011, ISBN: 9781457716706. DOI: 10.1109/APNOMS.2011.6077002.

[65] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, *Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET*. 2017, pp. 71–83. DOI: 10.1007/978-981-10-3503-6{_}6.

[66] Y. C. Wei and Y. M. Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012, ISBN: 9780769547459. DOI: 10.1109/TrustCom.2012.79.

[67] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks", *Networks*, vol. 7, pp. 1652–1669, 2014. DOI: 10.1002/sec.862.

[68] S. Mazilu, M. Teler, and C. Dobre, "Securing vehicular networks based on data-trust computation", in *Proceedings - 2011 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2011*, 2011, ISBN: 9780769545318. DOI: 10.1109/3PGCIC.2011.18.

[69] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for VANETs", in *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, 2010, ISBN: 9780769541082. DOI: 10.1109/CIT.2010.157.

[70] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks", in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, ACM, 2005, pp. 79–87, ISBN: 1-59593-241-0.

[71] Y.-C. Wei and Y.-M. Chen, "Efficient Self-organized Trust Management in Location Privacy Enhanced VANETs", in *Information Security Applications: 13th International Workshop, WISA 2012, Jeju Island, Korea, August 16-18, 2012, Revised Selected Papers*, 2012.

[72] M. Zhang and R. S. Wolff, "Routing Protocols for Vehicle Ad Hoc Networks in Rural Areas", *IEEE Communications Magazine*, 2008.

[73] A. Grzybek, M. Seredynski, G. Danoy, and P. Bouvry, "Aspects and trends in realistic VANET simulations", in *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings*, 2012, ISBN: 9781467312394. DOI: 10.1109/WoWMoM.2012.6263793.

[74] E. Engström and P. Runeson, "Software product line testing - a systematic mapping study", *Information and Software Technology*, vol. 53, no. 1, pp. 2–13, 2011, ISSN: 0950-5849. DOI: 10.1016/j.infsof.2010.05.011.

[75] J. Dudovskiy, *Research Methodology*, 2017. [Online]. Available: https://research-methodology.net/sampling-in-primary-data-collection/convenience-sampling/.

[76] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs", *EURASIP Journal on Wireless Communications and Networking*, 2011. DOI: 10.1186/s13638-015-0257-x.

[77] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of Ad-Hoc Networks", *IEEE Transactions on Vehicular Technology*, 2016, ISSN: 00189545. DOI: 10.1109/TVT.2015.2495325.

[78] P. T. N. Diep and C. K. Yeo, "A trust-privacy framework in vehicular ad hoc networks (VANET)", in *Wireless Telecommunications Symposium*, 2016, ISBN: 9781509003143. DOI: 10.1109/WTS.2016.7482038.

[79] S. Heibati and N. Movahedinia, "Decreasing of trust-based routing delay in vehicular ad hoc networks", in *2016 8th International Conference on Information and Knowledge Technology, IKT 2016*, 2016, ISBN: 9781509043354. DOI: 10.1109/IKT.2016.7777759.

[80] Y. C. Wei and Y. M. Chen, "Evaluation of collusion resistance on trust management systems for VANETs", in *2012 12th International Conference on ITS Telecommunications, ITST 2012*, 2012, ISBN: 9781467330701. DOI: 10.1109/ITST.2012.6425197.

[81] ——, *Reliability and efficiency improvement for trust management model in VANETs*. 2012, ISBN: 9789400750852. DOI: 10.1007/978-94-007-5086-9{_}14.

[82] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based Trust Model in Vehicular Ad Hoc Networks", *7th COST-273 Meeting and Workshop Paris 2003*, 2003.

[83] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs", *International Journal of Distributed Sensor Networks*, 2016, ISSN: 15501477. DOI: 10.1155/2016/6138251.

[84] R. A. Shaikh and A. S. Alzahrani, "Trust Management Method for Vehicular Ad Hoc Networks", 2013.

[85] J. Zhang, C. Chen, and R. Cohen, "Trust modeling for message relay control and local action decision making in VANETs", *Security and Communication Networks*, 2013, ISSN: 19390122. DOI: 10.1002/sec.519.

A

Interview template

The interviews started by the authors introducing the thesis, see Section A.1. Then the questions in Section A.2 were asked.

A.1 Introduction

We are two software engineering students from Chalmers in Gothenburg. When we studied the research field of VANET trust models, we saw that there was a lack of comparable evaluations, and the evaluations we did find were evaluations often made by the same authors proposing the model, hence they are not objective. So we thought we wanted to contribute to making the models comparable.

We derived two main research questions:

- What trust models exist?
- How are they evaluated?

After having started our study, we decided that we want to investigate the possibility to evaluate the models through simulation. Here, we found different areas that needs to be investigated:

- What trust models shall we compare?
- What tools shall we use?
- What specific model of VANET shall we use? I.e. routing protocol, multihop etc.
- For what VANET application shall we compare?
  Usually these models are general, and not specific to a certain application area. If they are to be simulated, an application area must be specified.

A.2 Questions

1. What do you see as the most relevant application area for VANETs?
2. What are the challenges of implementing this VANET application?
3. Is there a value of implementing a trust model in this application, in relation to cryptography?
4. What VANET application would be most valuable for the industry to compare the models in?
5. What are potential attack scenarios in the mentioned VANET application?

B

The articles and their classification

Table B.1: The classified articles with regards to evaluation type

Model	Simulative	Analytical	Qualitative
Monir *et al.* [60]		x	x
Ltifi *et al.* [49]	x		
Wu *et al.* [17]	x		
Gazdar *et al.* [38]	x	x	
Finnson *et al.* [50]	x		
Mehdi *et al.* [39]	x		
Haddadou *et al.* [51]	x	x	
Tajeddine *et al.* [69]	x		
Zhou *et al.* [76]	x		
Huang *et al.* [48]	x		
Tan *et al.* [77]	x		
Liao *et al.* [4]	x		
Cohen *et al.* [54]	x		x
Diep and Yeo [78]	x		
Saraswat and Chaurasia [55]	x		
Gao *et al.* [62]		x	
Wei and Chen [66]	x		
Wei *et al.* [64]	x		
Wang and Wu [40]	x		
Heibati and Movahedinia [79]	x		
Haddadou and Rachedi [57]	x		
Wei and Chen [71]	x		
Ahmed and Tepe [19]	x		
Alriyami *et al.* [7]	x	x	x

Table B.1: The classified articles with regards to evaluation type (continued)

Model	**Simulative**	**Analytical**	**Qualitative**
Wei and Chen [80]	x		
Shrivastava *et al.* [41]	x		
Gurung *et al.* [42]	x		
Minhas *et al.* [16]	x		
Shaikh and Alzahrani [67]	x	x	x
Bhargava *et al.* [35]	x		
Liu *et al.* [58]	x		x
Hu *et al.* [63]	x		
Gai *et al.* [28]	x		
Wei and Chen [81]	x		
Ding *et al.* [82]	x		
Wang *et al.* [83]	x		
Mazilu *et al.* [68]	x		
Hasrouny *et al.* [65]		x	
Machado and Venkatasubramanian [29]	x		
Abumansoor and Boukerche [45]	x		x
Hu *et al.* [30]	x	x	x
Kothari *et al.* [37]	x		
Sugumar [31]	x		
Zhang [8]			x
Shaikh and Alzahrani [84]		x	
Abdelaziz *et al.* [36]	x		
Zhang *et al.* [85]	x		

Table B.2: The classified articles with regards to evaluation metric

Model	**Pt**	**A**	**Pe**	**Sc**	**Pr**	**De**	**Dy**	**C**
Monir *et al.* [60]		x		x	x	x	x	
Ltifi *et al.* [49]			x					
Wu *et al.* [17]	x	x						
Gazdar *et al.* [38]								
Finnson *et al.* [50]	x							
Mehdi *et al.* [39]			x					
Haddadou *et al.* [51]		x						
Tajeddine *et al.* [69]		x						
Zhou *et al.* [76]								
Huang *et al.* [48]			x					
Tan *et al.* [77]			x					
Liao *et al.* [4]		x						
Cohen *et al.* [54]	x							
Diep and Yeo [78]		x						
Saraswat and Chaurasia [55]			x					
Gao *et al.* [62]			x					
Wei and Chen [66]		x	x					
Wei *et al.* [64]		x			x			
Wang and Wu [40]	x	x						
Heibati and Movahedinia [79]			x					
Haddadou and Rachedi [57]		x	x					
Hasrouny *et al.* [65]		x	x					
Ahmed and Tepe [19]		x						
Alriyami *et al.* [7]			x	x	x	x	x	
Wei and Chen [80]		x	x					
Shrivastava *et al.* [41]		x						
Gurung *et al.* [42]			x					
Minhas *et al.* [16]	x	x						
Shaikh and Alzahrani [67]		x		x	x	x	x	
Bhargava *et al.* [35]		x						
Liu *et al.* [58]		x				x	x	x
Hu *et al.* [63]		x						
Gai *et al.* [28]		x						

Table B.2: The classified articles with regards to evaluation metric (continued)

Model	**Pt**	**A**	**Pe**	**Sc**	**Pr**	**De**	**Dy**	**C**
Wei and Chen [81]		x						
Ding *et al.* [82]		x						
Wang *et al.* [83]		x						
Mazilu *et al.* [68]		x						
Hasrouny *et al.* [65]								
Machado and Venkatasubramanian [29]		x						
Abumansoor and Boukerche [45]		x		x				
Hu *et al.* [30]		x	x					
Kothari *et al.* [37]		x						
Sugumar [31]		x	x					
Zhang [8]		x	x	x	x	x	x	
Shaikh and Alzahrani [84]		x	x					
Abdelaziz *et al.* [36]		x						
Zhang *et al.* [85]		x		x				

Notes: Pt = Path time, A = Accuracy, Pe = Performance, Sc = Scalability, Pr = Privacy, De = Decentralization, Dy = Dynamic, C = Cost

Table B.3: The classified simulations with regards to simulation environment

Model	Both	Urban	Highway	Unknown
Ltifi *et al.* [49]			x	
Wu *et al.* [17]		x		
Gazdar *et al.* [38]	x			
Finnson *et al.* [50]	x			
Mehdi *et al.* [39]	x			
Haddadou *et al.* [51]	x			
Tajeddine *et al.* [69]		x		
Zhou *et al.* [76]				x
Huang *et al.* [48]		x		
Tan *et al.* [77]				x
Liao *et al.* [4]		x		
Cohen *et al.* [54]				x
Diep and Yeo [78]				x
Saraswat and Chaurasia [55]	x			
Wei and Chen [66]	x			
Wei *et al.* [64]		x		
Wang and Wu [40]		x		
Heibati and Movahedinia [79]				x
Haddadou and Rachedi [57]		x		
Wei and Chen [71]		x		
Ahmed and Tepe [19]			x	
Wei and Chen [80]		x		
Shrivastava *et al.* [41]				x
Gurung *et al.* [42]				x
Minhas *et al.* [16]		x		
Shaikh and Alzahrani [67]		x		
Bhargava *et al.* [35]				x
Liu *et al.* [58]				x
Hu *et al.* [63]		x		
Gai *et al.* [28]		x		
Wei and Chen [81]		x		
Ding *et al.* [82]		x		
Wang *et al.* [83]		x		

Table B.3: The classified simulations with regards to simulation environment (continued)

Model	**Both**	**Urban**	**Highway**	**Unknown**
Mazilu *et al.* [68]		x		
Machado and Venkatasubramanian [29]			x	
Abumansoor and Boukerche [45]			x	
Hu *et al.* [30]				x
Kothari *et al.* [37]			x	
Sugumar [31]			x	
Abdelaziz *et al.* [36]			x	
Zhang *et al.* [85]		x		

Table B.4: The classified simulations with regards to simulation dynamics

Model	Both	Network	Traffic	Neither
Ltifi *et al.* [49]	x			
Wu *et al.* [17]	x			
Gazdar *et al.* [38]	x			
Finnson *et al.* [50]	x			
Mehdi *et al.* [39]	x			
Haddadou *et al.* [51]	x			
Tajeddine *et al.* [69]	x			
Zhou *et al.* [76]				x
Huang *et al.* [48]	x			
Tan *et al.* [77]		x		
Liao *et al.* [4]	x			
Cohen *et al.* [54]	x			
Diep and Yeo [78]	x			
Saraswat and Chaurasia [55]	x			
Wei and Chen [66]	x			
Wei *et al.* [64]	x			
Wang and Wu [40]	x			
Heibati and Movahedinia [79]		x		
Haddadou and Rachedi [57]	x			
Wei and Chen [71]	x			
Ahmed and Tepe [19]			x	
Wei and Chen [80]	x			
Shrivastava *et al.* [41]				x
Gurung *et al.* [42]				x
Minhas *et al.* [16]	x			
Shaikh and Alzahrani [67]	x			
Bhargava *et al.* [35]				x
Liu *et al.* [58]				x
Hu *et al.* [63]			x	
Gai *et al.* [28]	x			
Wei and Chen [81]	x			
Ding *et al.* [82]	x			
Wang *et al.* [83]	x			

Table B.4: The classified simulations with regards to simulation dynamics (continued)

Model	**Both**	**Network**	**Traffic**	**Neither**
Mazilu *et al.* [68]	x			
Machado and Venkatasubramanian [29]			x	
Abumansoor and Boukerche [45]	x			
Hu *et al.* [30]				x
Kothari *et al.* [37]	x			
Sugumar [31]	x			
Abdelaziz *et al.* [36]	x			
Zhang *et al.* [85]			x	

Table B.5: The classified simulations with regards to VANET application

Model	RE	RP	P	NS
Ltifi *et al.* [49]	x			
Wu *et al.* [17]		x		
Gazdar *et al.* [38]	x			
Finnson *et al.* [50]		x		
Mehdi *et al.* [39]				x
Haddadou *et al.* [51]	x			
Tajeddine *et al.* [69]				x
Zhou *et al.* [76]				x
Huang *et al.* [48]				x
Tan *et al.* [77]				x
Liao *et al.* [4]	x			
Cohen *et al.* [54]		x		
Diep and Yeo [78]				x
Saraswat and Chaurasia [55]				x
Wei and Chen [66]				x
Wei *et al.* [64]				x
Wang and Wu [40]		x		
Heibati and Movahedinia [79]				x
Haddadou and Rachedi [57]				x
Wei and Chen [71]				x
Ahmed and Tepe [19]	x			
Wei and Chen [80]				x
Shrivastava *et al.* [41]				x
Gurung *et al.* [42]				x
Minhas *et al.* [16]		x		
Shaikh and Alzahrani [67]				x
Bhargava *et al.* [35]				x
Liu *et al.* [58]				x
Hu *et al.* [63]				x
Gai *et al.* [28]				x
Wei and Chen [81]				x
Ding *et al.* [82]	x			
Wang *et al.* [83]		x		

Table B.5: The classified simulations with regards to VANET application (continued)

Model	**RE**	**RP**	**P**	**NS**
Mazilu *et al.* [68]	x			
Machado and Venkatasubramanian [29]				x
Abumansoor and Boukerche [45]				x
Hu *et al.* [30]			x	
Kothari *et al.* [37]				x
Sugumar [31]				x
Abdelaziz *et al.* [36]				x
Zhang *et al.* [85]	x			

Notes: RE = Road Events, RP = Route Planning, P = Platooning, NS = Not specified