A Flexible, Subjective Logic-based Framework for Misbehavior Detection in V2V Networks

Stefan Dietzel, Rens van der Heijden
Institute of Distributed Systems
University of Ulm
89081 Germany
Email: stefan.dietzel@uni-ulm.de
rens.vanderheijden@uni-ulm.de

Hendrik Decke
Konzernforschung
Volkswagen AG
38436 Wolfsburg, Germany
Email: hendrik.decke@volkswagen.de

Frank Kargl
Institute of Distributed Systems
University of Ulm
89081 Germany
Email: frank.kargl@uni-ulm.de

***Abstract*—Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication aims to increase safety, efficiency, and comfort of drivers. Vehicles periodically broadcast their current status, such as position, velocity, and other information. Received information is stored in a local knowledge base, often called world model, and used for application decisions. Because of the potential impact, V2V communication is an interesting target for malicious attackers. Message integrity protection using cryptographic signatures only protects against outsider attackers. In addition to signatures, misbehavior detection mechanisms comparable to intrusion detection systems (IDS) are needed to detect insider attackers. Given the complexity and large number of foreseen V2V and V2I applications, misbehavior detection cannot be a one-size-fits-all solution. In this paper, we present a flexible framework that can combine a range of different misbehavior detection mechanisms by modeling their outputs using subjective logic. We demonstrate the feasibility of our framework by using a combination of existing detection mechanisms to increase their misbehavior detection results.**

I. Introduction

Throughout the past decade, vehicle to vehicle and vehicle to infrastructure communication (V2X) has attracted significant attention in the network research community. This also includes aspects of security and privacy protection (cf. [1, Ch. 9]). As a result of this research, emerging standards both in the U.S. [2] and Europe [3] include the deployment of security mechanisms that aim to ensure authenticity, integrity of messages, and privacy protection of drivers. In both standards, this is done by means of ECDSA digital signatures on messages and cryptographic certificates issued to vehicles by a certification authority. In addition, to protect privacy, vehicles will have multiple pseudonymous and renewable certificates at their disposal so that they are not directly identifiable and can change pseudonyms over time to provide unlinkability. It is generally agreed that these mechanisms will provide a solid protection against external attackers. Casual road-side attackers equipped with a laptop and an IEEE 802.11p radio will not be able to inject spoofed or altered messages into the communication system.

However, V2X attacker models (e.g., as defined by ETSI [4]), also include insider attackers that control necessary credentials to create signed messages with a correct and valid certificate. Such an attacker will be able to disseminate incorrect information via perfectly valid messages, for example, wrong position claims or warning about inexistent road obstacles. Depending on specific implementations, this can lead to incorrect warnings signaled to drivers or even incorrect automatic reactions of vehicles, like automatic emergency braking. The potentially life-threatening consequences of such attacks are obvious.

The risk of insider attacks can be reduced by carefully safeguarding the cryptographic key material in hardware security modules (HSM) [5]. Attackers will then not be able to extract and use secret keys. In addition, efficient and fast revocation mechanisms can be used to invalidate cryptographic keys in case an abuse is detected [6]. However, relying on the security of an HSM alone is not sufficient, as an attacker may be able to bypass the protection or just use a valid HSM but feed it with incorrect input data. And revocation is only effective after an abuse is detected. So this leads us to the critical question: how can we detect entities in a V2X system that misbehave in the sense that they disseminate incorrect and potentially malign information to other vehicles or road-side entities?

While this is closely related to (anomaly-based) Intrusion Detection Systems (IDS), we refer to such mechanisms as misbehavior detection, because they also catch other forms of misbehavior, such as that caused by malfunctioning sensors in vehicles. In addition, IDS normally only deal with abstractions of data, while V2X mechanisms are closely related to the real-world semantics of the data being processed, such as location or road condition information. We define the term misbehavior detection in the context of V2X communication as the detection of incorrect information in communicated data where incorrect refers to an abnormal deviation from the actual information that is being sensed by vehicles and other entities in the system.

While a wide range of solutions for misbehavior detection in specific applications exists (cf. Section II), we argue that the field of V2X communication is too diverse and detection mechanisms need to be too application-specific for a single solution to address all requirements. Rather than presenting a new misbehavior detection mechanism, our contribution in this paper is, therefore, to propose a flexible framework that can accommodate existing as well as new mechanisms. Detection results can be combined and related to each other to support a wide range of applications.

In the following, we first review existing work on misbehavior detection (Section II). Section III introduces our

misbehavior detection framework, and we discuss its utility in Section IV. We conclude with a discussion of other misbehavior detection frameworks and other application of subjective logic in Section V and an outlook on open issues in Section VI.

II. Misbehavior Detection

Misbehavior detection is about detection of incorrect information transmitted in the network. Causes for incorrect information are malicious intent, as well as malfunctioning sensors. Both can lead to unclear situations if they are not filtered out. We argue that vehicles should not rely on other vehicles to behave correctly. Rather, they should implement misbehavior detection to detect such erroneous and malicious messages. Because attackers are typically considered more challenging by the literature, as evidenced by the large body of work concerning them [7]–[14], we focus on their detection in this work.

In previous work, we have illustrated that misbehavior detection can be divided into two categories: node-centric and data-centric misbehavior detection [7]. Node-centric mechanisms focus specifically on the use of identities to detect attackers, while data-centric misbehavior detection covers mechanisms that use semantics associated with the exchanged packets to detect attackers. Both types of mechanisms are complementary, which we exploit in our framework. We will illustrate both types with an example from the state of the art.

An example for a node-centric misbehavior detection mechanism is the trust framework developed by Raya et al. [8], which discusses how a vehicle can draw conclusions about messages for certain events based on the trust it has in the senders associated with the event and the contents of these messages. We focus on the node-centric aspect of their work. Based on the type of event and the type of sending vehicle, a vehicle will assign different trust levels to those senders. A police vehicle may be given authority for specific event types, such as accident situations. On the other hand, a vehicle's distance to the reported event can be used to assign a different trust value. For example, a vehicle very close to the event can have verified its occurrence and should be given higher trust.

Previous work by Leinmüller et al. [9] contains several examples of data-centric misbehavior detection. These mechanisms provide simple and efficient checks using the data contained in messages by directly analyzing their content and the associated semantics. For example, the authors define an acceptance range threshold, which exploits that transmission range in wireless networks is limited by the channel. One-hop beacon messages that contain a location much further away than the maximum transmission range can be regarded as untrustworthy. Similarly, the mobility grade threshold defines a maximum speed for a given road (greater than the speed limit), which can be compared to an estimate of reported speeds. If a vehicle exceeds the threshold, its messages are untrustworthy. In addition, the maximum density threshold defines the maximum amount of vehicles that can be driving in a particular region, which is a rough metric for detecting Sybil attacks. The authors have also defined several mechanisms for cooperative detection between vehicles, which we do not discuss here.

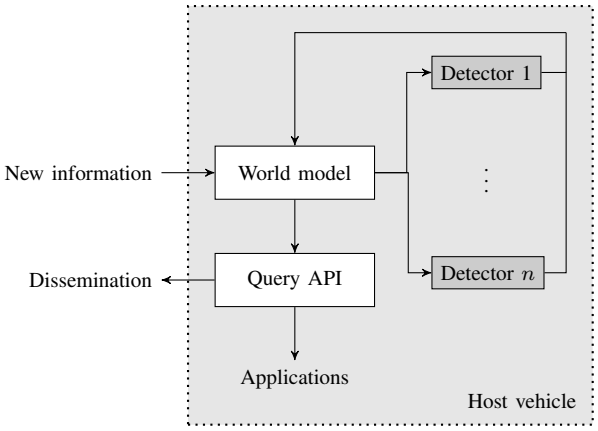

Fig. 1: Conceptual overview of our misbehavior detection framework.

Although both works discuss very useful mechanisms that can detect attacks, they have only very simplistic mechanisms to combine information from multiple sources, such as the vehicle's sensors, and messages from many distinct vehicles. The approaches basically use weighted averages with static and manually determined weights. With this work we propose a much more flexible framework to integrate arbitrary types of detection mechanisms in order to enhance detection accuracy and limit the type of misbehavior that may go undetected.

III. Detection with Subjective Logic

A. Overview

Our goal is to create a flexible framework for misbehavior detection that allows to combine a number of different misbehavior detection mechanisms. Figure 1 shows a conceptual overview of the information flow. Vehicles receive new information from other vehicles or own sensor readings. All information known is stored in a *world model,* also called local dynamic map (LDM) in current standardization [15]. Based on the world model, information is possibly disseminated to other vehicles, and local safety and traffic efficiency applications use the world model contents as information base. In this paper we focus on how the world model can be represented so that a number of misbehavior detection mechanisms can analyze and evaluate the contents. We show how their detection results can be represented alongside the information, and how detection results can be merged and used to filter the information that is send to applications and other vehicles.

B. Requirements

Our proposal aims to support a large number of different detection mechanisms to detect a wide range of possible attacks. On the other hand, the world model is a central component that should support a number of different applications. Therefore, we discuss two main categories of requirements: security requirements and application requirements.

From a *security perspective,* our framework must be able to flexibly support various different detection mechanisms, including node-centric and data-centric mechanisms. Therefore, the framework should model known other vehicles, as well

as known information items. Also, the connection between vehicles and information should be modeled. If vehicles are marked as likely attackers by node-centric mechanisms, the information received from them should be rated accordingly. Some detection mechanisms reward positive behavior of vehicles while others penalize bad behavior, and both need to be represented in our model. In addition, some mechanisms will be more certain about their results than others. Therefore, our framework should support uncertainty. In addition, uncertainty allows different weights for mechanisms in certain situations. Given that we aim to combine a number of different detection mechanisms, it is likely that multiple statements about the same information item or vehicle will be the norm rather than the exception. Such different statements need to be merged by our framework to come to a conclusive statement about information items and vehicles. Besides such multiple statements about the *same* item, our framework should support statements about different items that are *related* to each other. For instance, our framework should support transitivity of statements where applicable.

As discussed above, the number of security mechanisms used in our framework will result in a large number of statements about information items and vehicles. *Applications* need a way of accessing information in the world model that takes into account these statements in a way that is useful for the application. For example, safety relevant applications have strict requirements about the trustworthiness of information they operate on. Other applications may support differing levels of information trustworthiness. In all cases, our framework needs to resolve transitivity and conflicts of statements before returning information to applications.

C. World model graph representation

In our framework, we require a representation that allows us to represent both node-centric and data-centric mechanisms and their results in a consistent way. We now introduce a graph representation for the world model, as illustrated in Figure 2. The directed graph represents the entire world view of the vehicle v_{me}, including knowledge about other vehicles (v_4 and v_5) and data that was received (d_3 and d_5), which is indicated by the edges. We annotate these edges with evaluations that represent trust (in vehicles) and confidence (in information). Besides edges from v_{me} to information, there are also edges from vehicles v_i to some information. These represent knowledge about the confidence in data from other nodes. For example, we assume that other vehicles only disseminate information if they have some confidence it is correct. Therefore, we model this default sender confidence in our world model. Similar to this, vehicles can express trust in other vehicles. v_5 has expressed its trust in v_4, which is represented by edge o_4.

D. Subjective logic detection representation

All statements of misbehavior detection mechanisms are represented by annotations of edges in the world model graph (see Section III-C). We use subjective logic, introduced by Adun Jøsang [16], to represent the detection mechanisms' statements. Subjective logic is especially suitable for our use case, because it allows to model uncertainty, models possible and negative statements, and offers a wide range of logical operators to combine and relate different opinions, thereby addressing all our requirements discussed in Section III-B.

The main construct of subjective logic is an *opinion,* which is represented as follows:[1]

$$o := (b, d, u). \tag{1}$$

Opinions represent both trust in other vehicles and confidence in data. Opinions annotate each edge in the world model graph and have an opinion holder h and a subject s:

$$h \xrightarrow{o} s. \tag{2}$$

The opinion holder h and subject s are both nodes in the graph representation, as shown in Figure 2. As explained in Section III-C, opinion holders are the own or the other vehicles and subjects are other vehicles or data. Each opinion is expressed as a triple of

- belief $b \in [0, 1]$, meaning that a mechanism thinks a vehicle is honest or data is correct;
- disbelief $d \in [0, 1]$, meaning that a vehicle is considered an attacker or data is incorrect; and
- uncertainty $u \in [0, 1]$, representing the extent to which a mechanism is unsure about its result.

In subjective logic, belief, disbelief and uncertainty are mutually exclusive. This is represented by requiring $b+d+u = 1$.

Subjective logic opinions address all the security requirements we discussed in Section III-B. Namely, opinions allow for explicit modeling of positive statements, negative statements, and uncertainty. In addition, we discussed a number of requirements that relate to merging of different opinions, which are supported by subjective logic, as well. To perform calculations on opinions, subjective logic defines a number of operators, which extend classical logic operators, such as boolean `AND` or `OR`. The full list of subjective logic operators is discussed in [18]. The two most applicable to our framework are *consensus* and *transitivity.*

- *Consensus* is used to merge several opinions of the same holder about the same subject (for example, the outputs of two mechanisms). Given $h \xrightarrow{o_1} s$ and $h \xrightarrow{o_2} s$, we denote the consensus as $o_3 = o_1 \oplus o_2$, such that $h \xrightarrow{o_3} s$. Let $o_1 = (b_1, d_1, u_1)$ and $o_2 = (b_2, d_2, u_2)$. Then $o_1 \oplus o_2 = ((b_1u_2 + b_2u_1)/\kappa, (d_1u_2 + d_2u_1)/\kappa, (u_1u_2)/\kappa)$ where $\kappa = u_1 + u_2 - u_1u_2$.
- *Transitivity* is used to combine related opinions. Given $h \xrightarrow{o_1} s$ and $s \xrightarrow{o_2} t$, we denote the transitive opinion as $o_3 = o_1 \otimes o_2$, such that $h \xrightarrow{o_3} t$.
  Let $o_1 = (b_1, d_1, u_1)$ and $o_2 = (b_2, d_2, u_2)$. Then $o_1 \otimes o_2 = (b_1b_2, b_1d_2, d_1 + u_1 + b_1u_2)$. Complete trust is modeled as $o_1 = (1, 0, 0)$: then, $o_3 = o_2$.

In combination, these operators can be used to evaluate information in the world model graph. Whenever an application requests information from the world model, we follow a path from the own vehicle v_{me} to the information as shown in Figure 2. Consider, for instance, d_3 is requested by an application. There are two paths from v_{me} to d_3 in the graph:

[1] In later papers, e.g., [17], an additional value a, representing an opinion's atomicity, is added; however, we keep the original opinion format.

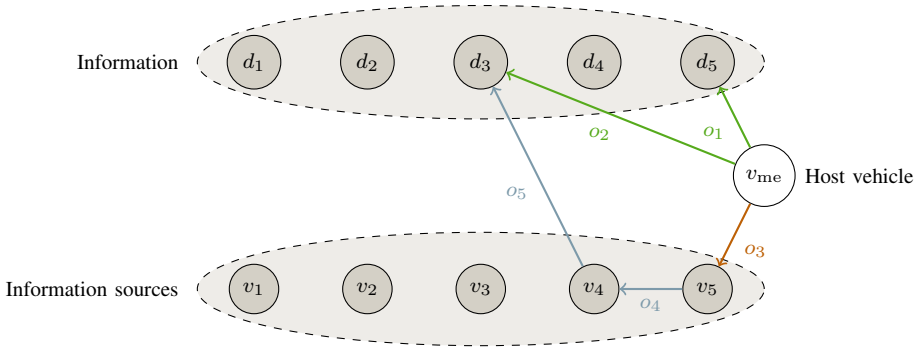

Fig. 2: This figure shows our graph representation of the world, and the possible relations in it. v_{me} is the vehicle storing this data, v_i are other vehicles, d_i are data items.

1) $v_{\text{me}} \xrightarrow{o_3} v_5 \xrightarrow{o_4} v_4 \xrightarrow{o_5} d_3$ and
2) $v_{\text{me}} \xrightarrow{o_2} d_3$.

To acquire a merged opinion about d_3, consensus and transitivity can be combined. The first path is merged using the transitivity operator; the result is then merged with the second path using consensus:

$$o_{\text{result}} = ((o_3 \otimes o_4) \otimes o_5) \oplus o_2. \tag{3}$$

As can be seen, subjective logic opinions and operators allow for a very flexible annotation of a vehicle's world model that supports both security and application requirements. Detectors of all sorts can be used in this framework to contribute their opinions on trustworthiness of data and vehicles. In the next section, we discuss applications for specific detection mechanisms in more detail using some examples.

IV. Discussion

In Section II, we introduced two types of misbehavior detection mechanisms. One type operates on the assumption that certain nodes are more trustworthy than others, and the other verifies common behavior by analyzing beaconing data. We will use such detectors to show how our framework can improve misbehavior detection by mechanism combination in an example scenario: vehicles are driving in a dense city road network. The speed limit is 50 km/h. Traffic flows freely, and some drivers speed slightly, up to 60 km/h. At the same time, an ambulance vehicle rushes towards an accident scene. Using its special right of way, the ambulance speeds and takes shortcuts to arrive at the scene as fast as possible.

Data-centric detector: As data-centric detector, we take the mobility grade threshold (MGT) from [19]. The detector continuously examines received beacon messages, calculates the estimated vehicle speed from relative location distance, and determines speed plausibility. In the city scenario, the detector considers all speeds up to 60 km/h as plausible and higher speeds increasingly unlikely.

Node-centric detector: As node-centric detector, we take the default vehicle trustworthiness discussed in [8]. Each vehicle is assigned a default trust value, which is higher if the vehicle is assumed to be better protected against attacks. We assume that the ambulance car in our scenario has a higher trust rating than regular vehicles.

Intuitively, the data-centric detector will detect movement of regular vehicles correctly. However, the ambulance movement will likely be interpreted as an attack for two reasons. First, the ambulance has special rights of way and will move with much higher speeds than regular vehicles. Second, the ambulance is not bound to adhere to road markings, such as specific lanes to take turns on intersections, and so forth. As a result, the ambulance car's movement pattern will in general be less predictable than that of a regular car and can easily be mistaken for an attack. If the data-centric detector would be adapted to accept higher speeds and unpredictable movements, attackers might not be detected.

What is therefore needed is a combination of the data-centric detector with the node-centric detector such that all regular vehicles that move implausibly fast are detected as attackers with the exception of special cars, such as ambulances. While this detection rule could be hard-coded for this simple example scenario and two detectors, managing specific exceptions will quickly become too complex in different scenarios and with different combinations of detectors. In our framework, we introduce subjective logic and its operators as an abstraction step that facilitates easy and flexible combination of mechanisms for all kinds of scenarios. For the example scenario, the detectors can be integrated as follows.

First, mechanism output needs to be modeled as subjective logic opinions. For the data centric detector, we use the following mapping:

$$o_{\text{data}} = (0, d, 1-d), \tag{4}$$

$$d = \min\left(\frac{\max(V-60,0)}{80}, 0.5\right), \tag{5}$$

where V is the speed calculated using two consecutive beacon messages. Essentially, all speeds below 60 km/h result in an indifferent opinion, modeled by complete uncertainty, $o = (0, 0, 1)$. Speeds above 60 km/h will lead to increasingly distrusting opinions; the maximum disbelief $o = (0, 0.5, 0.5)$ is reached at 100 km/h. However, the mechanism never results in disbelief values higher than 0.5, because some uncertainty about the result always remains.

The node-centric detector mapping is slightly simpler. We use two fixed opinions for regular vehicles and ambulance cars:

$$o_{\text{regular}} = (0, 0, 1), \tag{6}$$

$$o_{\text{ambulance}} = (0.5, 0, 0.5). \tag{7}$$

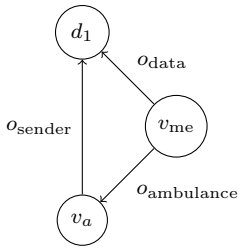

Fig. 3: Example world model graph for data-centric and node-centric detector.

Finally, we model receiving a message from another vehicle with an edge that is associated with a default opinion, namely:

$$o_{\text{sender}} = (1, 0, 0). \tag{8}$$

The reason is that we assume that each vehicle that sends a message has a certain default confidence in the contained data, otherwise the vehicle should discard the message and not transmit it. In more complex settings, the default sender opinion could be replaced by the actual misbehavior detection results of the other vehicle, but for this example we will use the simpler default opinion.

Having received several beacon messages from the ambulance (v_a), the complete world model graph looks as shown in Figure 3. We assume the ambulance moves with 80 km/h, therefore $o_{\text{data}} = (0, 0.25, 0.75)$, that is, the ambulance would be considered an attacker using the data-centric detector alone (regardless of how uncertainty is treated, which may be application-dependent if the application can cope with this).

To get the merged confidence in the ambulance's beacon messages, we combine the data-centric, node-centric, and default sender opinions using subjective logic consensus and transitivity:

$$\begin{aligned} o &= o_{\text{data}} \oplus \big(o_{\text{ambulance}} \otimes o_{\text{sender}}\big), \\ &= (0, 0.25, 0.75) \oplus \big((0.5, 0, 0.5) \otimes (1, 0, 0)\big) \\ &= (0, 0.25, 0.75) \oplus (0.5, 0, 0.5) \\ &\approx (0.43, 0.14, 0.43). \end{aligned} \tag{9}$$

Looking at the merged opinion $o \approx (0.43, 0.14, 0.43)$, we can see that the ambulance's beacon message is more likely to be correct ($b = 0.43$) than it is likely to be false ($d = 0.14$), with some uncertainty remaining ($u = 0.43$). To further reduce uncertainty, more node- and data-centric mechanisms can be added to the framework. Still, for this example scenario the two detection mechanisms proved to be sufficient for correctly detecting attackers that try to send beacons with implausible speed values while still correctly distinguishing messages from ambulance cars and other vehicles with higher default trustworthiness.

V. Related Work

Misbehavior detection and ways to combine output of several mechanisms have been an ongoing effort in V2X research. Golle et al. [10] have developed one of the earliest data-centric misbehavior detection mechanisms for V2X. Specifically, they introduce an abstract framework that allows each vehicle to tag observed events with positive or negative hypotheses on the basis of a particular model of the system. The observed events include input from the vehicle's sensors, as well as received messages from other vehicles. At any point in time, the vehicle can evaluate the different hypotheses against the received events and determine the most likely explanation. However, the authors use some simplifying assumptions about the exchange of messages between vehicles. Fundamentally, our approach is similar to theirs, because we also use data-centric misbehavior detection mechanisms that essentially test information contained in messages against existing models. However, we use subjective logic to better cope with contradictory information and we represent individual vehicles as well as data in our model, allowing vehicles to exchange reproducible results.

Rezgui & Cherkaoi [11] describe the use of data mining to analyze patterns of messages received by a vehicle. The goal of their analysis is to detect misbehavior in the sense of inconsistent messages by extracting rules from messages that are received over time. The principle idea behind their work is that data mining can identify patterns in data without requiring an underlying model that explains them. Hence, the approach can detect inconsistencies that are not detected by manually designed mechanisms. However, it is difficult to determine whether a message that is inconsistent with previous messages is false, or simply indicates a change in the real world (e.g., relatively rare occurrences like crashes). Also, the authors' work did not analyze the usefulness of the rules, and the authors have only tested their mechanism for a small scenario (68 vehicles).

Stübing et al. [12] describe a model focused on maintaining an accurate world model in the presence of regularly changing pseudonyms. To this end, the authors have used a Kalman filter to perform position estimation, which is updated according to newly received beacon messages. Their approach effectively revokes pseudonyms in the direct vicinity of the vehicle with high probability, which is useful for both attack detection, as well as collision avoidance applications.

Ghosh et al. [13] have developed a data-centric misbehavior detection mechanism that performs a root-cause analysis on the available information regarding a specific event. The authors determine the trajectory driven by a driver between the reception of the event and its reported location. This is compared against two different trajectories: a free-flow and a crash notification trajectory. The mechanism avoids marking messages as malicious that are related to a crash, because the underlying model changes to accommodate the case of a legitimate alert. However, this work only provides a mechanism to establish after-the-fact that misbehavior has occurred. This means the mechanism must be combined with others in order to be effective. Our framework can be used to allow vehicles to store trajectories and transmit them to each other or a back-end authority, providing solid evidence for revocation.

Raya et al. [8] describes the establishment of trust in nodes based on the data they transmit. Specifically, the authors propose ways to evaluate the trust a vehicle should have based on its history and several parameters, which then allow the dynamic establishment of trust between vehicles. The authors

describe several decision logics, including Bayesian inference and the Dempster-Shafer Theory of evidence. Our work instead uses subjective logic, which allows a more intuitive representation, higher expressiveness, and more resilience. This resilience is especially important for short-term decisions, because many important events may consist of anomalous data, for instance, an accident has unusual speeds for a given scenario.

Bamberger et al. [14] discuss the use of subjective logic for V2X. Similar to our work, they incorporate opinions from other vehicles and the evaluation of the own vehicle, represented using subjective logic. However, their work focuses on node-centric detection, neglecting data-centric detection mechanisms. In our work, we use subjective logic to represent both trust in vehicles as well as confidence in information, allowing us to model data-centric detection with subjective logic and combining it with node-centric mechanisms.

Gomez et al. [20] have discussed the use of subjective logic to represent the trustworthiness of data transmitted by sensors in a wireless sensor network for monitoring cows. The authors have used subjective logic to represent deteriorating sensor accuracy during battery depletion. Although the authors acknowledge the need for attack detection, they do not specifically address this issue. However, they implemented subjective logic as part of a real-world system and have shown that its use has led to a significant overall improvement of the assessed system.

VI. Conclusion

In this paper, we raise the issue of misbehavior detection in vehicular networks and highlight its importance for gaining trustworthy vehicular communication systems. As we have discussed, single detection mechanisms are insufficient and need to be combined in a flexible framework in order to enhance accuracy and allow easy interaction with applications.

The framework we propose is based on subjective logic which suits very well the requirements of a misbehavior detection frameworks in V2X communication. All data known to a vehicle can be captured in a world-model and can then be annotated by detection mechanisms with opinions. Such opinions can not only express belief or disbelief in a stated fact or data source, but also model uncertainty. Using logic operators such as consensus or transitivity, we have shown examples how a combination of mechanisms becomes easily possible.

In our on-going work, we are currently implementing our framework to allow more detailed evaluation. While our examples have shown the general applicability of our approach, this of course opens a lot of questions related to scalability, overhead, and feasibility in more complex situations with more and more complex detection mechanisms.

If those can be addressed successfully, a subjective-logic-based detection framework should be incorporated into future V2X systems to enhance robustness and security. As the set of detection mechanisms is not fixed and can easily be extended during operation time, our framework would also allow to react to future attacks by designing and deploying appropriate detectors into vehicles.

Acknowledgment

This work was funded within the project CONVERGE by the German Federal Ministries of Education and Research as well as Economics and Technology. The authors would like to thank Henning Kopp for his insightful comments.

References

[1] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*. Wiley, 2010.

[2] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, 2013.

[3] ETSI, "Intelligent Transport Systems (ITS); Security; Security header and certificate formats, TS 103 097," Tech. Rep., 2013.

[4] ——, "Intelligent Transport Systems (ITS); Security; Threats, Vulnerability and Risk Analysis (TVRA), TR 102 893," Tech. Rep., 2011.

[5] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Information Security and Cryptology - ICISC 2011*, ser. LNCS, H. Kim, Ed. Springer Berlin Heidelberg, Jan. 2012, no. 7259, pp. 302–318.

[6] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[7] R. W. van der Heijden, S. Dietzel, and F. Kargl, "Misbehavior detection in vehicular ad-hoc networks," Proceedings of the 1st GI/ITG KuVS Fachgespäch Inter-Vehicle Communication, Innsbruck, Austria, Tech. Rep. CCS-2013-01, Feb. 2013.

[8] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE 27th Conference on Computer Communications*, 2008, pp. 1238–1246.

[9] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, vol. 3, no. 4, pp. 289–302, 2010.

[10] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, p. 29–37.

[11] J. Rezgui and S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining," in *2011 IEEE 36th Conference on Local Computer Networks (LCN)*, 2011, p. 827–834.

[12] H. Stübing, J. Firl, and S. A. Huss, "A two-stage verification process for car-to-x mobility data based on path prediction and probabilistic maneuver recognition," in *Vehicular Networking Conference*. IEEE, 2011, pp. 17–24.

[13] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," *Ad Hoc Networks*, vol. 8, no. 7, pp. 778–790, Sep. 2010.

[14] W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory," in *IEEE Second International Conference on Social Computing*, 2010, pp. 73–80.

[15] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization, TR 102 863," Tech. Rep., 2011.

[16] A. Jøsang, "Artificial reasoning with subjective logic," in *Proceedings of the Second Australian Workshop on Commonsense Reasoning*, 1997.

[17] A. Jøsang, S. O'Hara, and K. O'Grady, "Base rates for belief functions," in *Workshop on the Theory on Belief Functions (Belief 2010)*, 2010.

[18] A. Jøsang, *Subjective Logic (draft book)*, 2013, http://folk.uio.no/josang/papers/subjective_logic.pdf.

[19] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. New York, New York, USA: ACM Press, 2006, pp. 57–66.

[20] L. Gomez, X. Gentile, and M. Riveill, "A framework for trust assessment of sensor data," in *4th Joint IFIP Wireless and Mobile Networking Conference*, 2011, pp. 1–7.