HAL open science

Feasibility Study of Misbehavior Detection Mechanisms in Cooperative Intelligent Transport Systems (C-ITS)

Joseph Kamel, Arnaud Kaiser, Ines Ben Jemaa, Pierpaolo Cincilla, Pascal Urien

► To cite this version:

Joseph Kamel, Arnaud Kaiser, Ines Ben Jemaa, Pierpaolo Cincilla, Pascal Urien. Feasibility Study of Misbehavior Detection Mechanisms in Cooperative Intelligent Transport Systems (C-ITS). 2018 IEEE 87th Vehicular Technology Conference: VTC2018-Spring, Jun 2018, Porto, Portugal. hal-01779985

HAL Id: hal-01779985

https://hal.science/hal-01779985

Submitted on 27 Apr 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Feasibility Study of Misbehavior Detection Mechanisms in Cooperative Intelligent Transport Systems (C-ITS)

Joseph Kamel[1,2], Arnaud Kaiser[1], Ines Ben Jemaa[1], Pierpaolo Cincilla[1], and Pascal Urien[2]

[1]*IRT SystemX*, 8 avenue de la Vauve, 91120, Palaiseau, France. E-mail: name.surname@irt-systemx.fr
[2]*Telecom ParisTech*, 23 avenue dItalie, 75013, Paris France. E-mail: name.surname@telecom-paristech.fr

***Abstract*—Cooperative Intelligent Transport Systems (C–ITS) is an emerging technology that aims at improving road safety, traffic efficiency and drivers experience. To this end, vehicles cooperate with each others and the infrastructure by exchanging Vehicle–to–X communication (V2X) messages. In such communicating systems message authentication and privacy are of paramount importance. The commonly adopted solution to cope with these issues relies on the use of a Public Key Infrastructure (PKI) that provides digital certificates to entities of the system. Even if the use of pseudonym certificates mitigate the privacy issues, the PKI cannot address all cyber threats. That is why we need a mechanism that enable each entity of the system to detect and report misbehaving neighbors. In this paper, we provide a state-of-the-art of misbehavior detection methods. We then discuss their feasibility with respect to current standards and law compliance as well as hardware/software requirements.**

***Index Terms*—Misbehavior Detection, Cooperative ITS, Security**

I. Introduction

Cooperative Intelligent Transport Systems are based on data communication over Vehicular Ad hoc NETworks (VANETs). VANET is an open network where vehicles exchange data to ensure road safety. Safety messages exchanged over the VANETs are not encrypted. This would leave the system open to endless security threats without a PKI system that guarantees sender authentication and data integrity. However, misbehaving entities can transmits tampered data or omits data it should transmit. In this case, PKI based security would not be able to prevent such data semantic level attacks. Thus, the safety system highly requires the deployment of additional security mechanisms which are able to detect, and react to, misbehaving entities in the network.

In this paper, we assess the feasibility of existing misbehavior detection mechanisms within the current C–ITS ecosystem. We restrict our scope to the detection techniques targeted at the sybil attack and the bogus information attack as they are common and relevant attacks in C–ITS. Indeed, it was deemed that these types of attacks needed detection mechanisms specific to the VANETs as opposed to attacks such as DoS, blackhole or flooding which could inherit detection mechanisms from the Mobile Ad hoc NETworks (MANETs) or any adhoc networks. It is also worth noting that the sybil and bogus information attack are still widely untreated as opposed to other types of attacks (e.g., replay and the message alteration) which are addressed by the PKI asymmetric cryptographic mechanisms.

In this work we focus mainly on local detection in the VANETs. We contribute to the state of the art by providing a new classification and understanding of recent works on misbehavior detection in C–ITS. In our opinion, it helps to deeply analyze the feasibility of such mechanisms in the current ecosystem and discuss remaining challenges that have to be addressed by the community.

In the next section we evaluate the detection mechanisms based on their feasibility. We focus on the logic behind the detection mechanisms instead of the details of every detection method. The evaluation does not consider the performance of the detection algorithm. This is followed by a summary, a brief discussion and a conclusion.

II. Misbehavior Detection Feasibility Challenges

Feasibility is assessed on multiple levels. Currently, standardization bodies such as the European Telecommunications Standards Institute (ETSI) and Institute of Electrical and Electronics Engineers (IEEE) made significant progress in designing the C–ITS architecture. We believe that misbehavior detection mechanisms should be **in line with the current standards** to ensure a much needed fast and easy deployment. Furthermore, misbehavior detection mechanisms face challenges caused by the constant conflict between security and privacy. This conflict often appears in the form of **regulations or legal complications** (e.g. it violates the General Data Protection Regulation (GDPR) [1]) . Finally, there is feasibility challenges in term of **the required equipment** necessary for the functionality of a detection mechanism. The equipment required for a detection mechanism could be too expensive to include in each node. Additionally, the entire system could have not yet reached the maturity a mechanism requires.

In the following section we will illustrate standard incomatibilities with a circle (○), legal and regulation conflicts with a square (□) and required equipment with a triangle (△).

A. Detection of sybil attacks

With the current ETSI and IEEE C–ITS model, the PKI infrastructure provide the vehicle with multiple valid keys. The vehicle proceeds to change its identity regularly to prevent easy remote trackability. The multiple identities a vehicle uses are called pseudonyms. An attacker could take advantage of pseudonyms to launch a Sybil attack. It is worth noting that since Sybil attack is ultimately a special kind of bogus information attack, it could also be detected by some types of methods designed for bogus information detection. In particular we note physical-layer and data-centric false beacon information detection mechanisms. However, from the multiple studies that have targeted the detection and mitigation of the sybil attack, we extract three prominent methodologies used for sybil detection:

a) Path history detection mechanisms: [2], [3] and [4] propose a model where a vehicle with an On–Board Unit (OBU) collects signed time stamps from Road–Side Units (RSUs). The theory is that these stamps act as proof that a vehicle had passed a certain RSU. Each vehicle is required to broadcast collected stamps. Since a Sybil attacker can only have one physical path, a group of vehicle with a similar collection of stamps is considered a suspect of a sybil attack.

The current state of the standard requires a vehicle to change all of its identifiers when using a new certificate, in order to prevent linkability between pseudonyms [5]. However, beaconing a footprint history would negate this effect and facilitate the linkability of pseudonyms (○). Additionally, a new protocol has to be implemented to enable: the RSUs to issue signed timestamps and the OBUs to beacon these timestamps (○). Although the current ETSI Cooperative Awareness Message (CAM) messages include an optional path history field, this variable consists of a list of GPS coordinates and is not compatible with the signed timestamps proposed in this method [6]. Furthermore, it is unclear if broadcasting a type of path history is friendly to the current privacy protection laws (□). And although in [4] and [2] the privacy issue of direct traceability is addressed, however this would not negate the pseudonyms linkability problem. And finally, this approach relies on a wide coverage RSUs in the C–ITS network (△).

b) Pseudonym Linkability based mechanisms: Some studied rely on a system where in some way pseudonyms have to be linked. Linking pseudonyms would enable the detection of a sybil attacker using the certificates issued for the same vehicle. [7] introduced Privacy-Preserving Detection of Abuses of Pseudonyms (P^{2}DAP), a method which enables linkability at RSU level by using pseudonyms which hash a common value. Similarly, Detection Technique against a Sybil Attack (DTSA) [8] suggests that each vehicle verifies the identity of neighboring vehicles with the help of a VANET server, currently accessible via RSUs.

Enabling pseudonym linking at the RSU level is not compliant with the privacy requirements of C–ITS. Currently, the PKI system is designed such that not even the Authorization Authority (AA) and the Enrolment Authority (EA) are able to link pseudonyms without cooperating [9] (□). At the present time, the ETSI standard does not specify any linkage authority and the IEEE designed linkage authority is available only to the misbehavior authority [10] (○). Moreover, it is not clear how scalable is this approach when RSU has to link pseudonyms of a great number of vehicles (△).

c) Neighbor List Exchange: Studies from [11] [12], propose a protocol that relies on vehicles broadcasting a list of neighbors. The broadcasted list should include unique identifiers for neighbors such as the hash of the last beacon. Calculation then determines the legitimacy of each node according to the neighbors list and the range of each vehicle. Sybil attackers could then be reported or excluded from the network.

Exchanging the neighbor lists is a distributed and simple approach. However, its efficiency could be greatly affected by the rate of the pseudonym change [13] (○). Furthermore, data protection acts could oppose broadcasting the information about other vehicles (□).

Since Sybil attack is ultimately a special kind of bogus information attack, it could also be detected by some types of methods designed for bogus information detection. In particular we note physical-layer and data-centric false beacon information detection mechanisms. Which we address in detail in the following section.

B. Bogus information

Broadcasting bogus information on a C–ITS network could have a range of results varying from minor like deteriorating the quality of infotainment services to dramatic like causing accidents and potentially victims. Specific methods of detection have been proposed in the literature. We organize our evaluation into three sections: Detection methods for false position information (the main component of the beacon message), Detection methods for warning messages, Detection methods that evaluate a node and thus all messages it broadcasts.

1) False beacon information:

a) Physical Layer detection: Multiple studies suggest location verification using physical aspects of the signal. [14] propose a method of triangulation of a node using distributed sensors on the network, this could currently be considered RSUs. [15] and [16] propose the use of distance-bounding in vehicular networks. This method relies on the speed of light and the message timestamp to verify the distance from the source of the signal. Additionally, [12] uses the Received Signal Strength (RSS) in its location verification process.

Physical detection methods are generally compatible with the standard and the corresponding laws. However, they may require a total RSU coverage and special detection equipments (△).

b) Data-centric detection: This mechanism uses the semantics of the messages to determine the authenticity. VEhicle Behavior Analysis and Evaluation Scheme (VEBAS) [17] propose the use of multiple data-centric mechanisms such as: Acceptance Range Threshold (ART), Minimum Distance Moved (MDM), Map-Proofed Position (MPP) and Sudden Appearance Warning (SAW).The multiple methods are combined using Exponentially Weighted Moving Average (EWMA). [18] proposes a method that combines mechanism from VEBAS and a plausibility model to check intersection of multiple vehicles. [19] improves on the ART by creating enhanced Acceptance Range Threshold (eART) where the acceptance range is similar to a gaussian curve instead of a fixed threshold. The gaussian approach is better for combining eART with other mechanisms.

Generally local data-centric mechanisms don't present major feasibility issues. The presented mechanisms do not require any changes to the standard nor present legal challenges. However, according to the proposed method, they may require significant on board processing power (△).

c) Additional Information Exchange: Several of the studied proposed for local misbehavior detection use a mechanism that requires the exchange of additional information between neighboring vehicles. [20] combines the data-centric methods used in [17] and the proactive exchange of neighbor tables. [19] combines the eART and the proactive neighbor exchange using subjective logic [21]. [22] proposes a method that relies on statistical model where vehicles calculate and broadcast a flow parameter. The flow parameter is calculated based on the density and speed of vehicles in a fixed range and thus the flow for neighboring vehicles has to be within a certain threshold.

For this mechanism to work, a new protocol for exchanging additional information between neighbors has to be standardized and implemented [6] (○). Additionally, the legality of sharing certain additional data between neighbors has to be investigated (□).

2) False warning messages:

a) Data-centric detection: [23] and [16] rely on the assumption that a vehicle emitting a warning event should behave accordingly. For example, a vehicle issuing a blocked road warning needs to be on a proximity of the event and needs to change its path accordingly to avoid the obstacle. A vehicle issuing a warning event is thus monitored by receiving vehicles to determine the message authenticity.

A block of the pseudonym change after generating a warning message is currently planned to be included in the standard [24]. Thus this method is compatible with the standard, presents no legal challenges, and does not require any special equipment. However, it is worth noting that this approach assumes that the malicious vehicle is only deceptive about the warning messages. Otherwise beacons its correct location information. Therefore, this method has to be bundled with a position verification technique.

b) Voting-based detection: Some studies have proposed voting or cooperative validation of an event to insure integrity. This mechanism proved effective in a densely populated network with an honest majority. [25] proposes the validation of an event based on signatures, the signatures are collected and distributed using growth code. [26] proposes a method with a Certainty of Event (CoE) curve. The CoE is calculated using a combination of mechanisms, one of which is the reports from other vehicles. [27] considers a system where an event becomes valid if the number of witnesses exceeds a certain threshold, then proceeds to evaluate multiple threshold-based event validation algorithms.

Similarly to other mechanisms, voting schemes requires a new protocol and messages architecture [6] [28] (○). Nevertheless, this protocol could be more challenging to integrate due to the effect of pseudonymity on voting integrity (○). This effect is amplified with a high frequency of pseudonym change [13].

3) Node trust evaluation: In this section we evaluate detection methods that instead of estimating the correctness of messages separately, estimate trust in the vehicle. Therefore all messages from a corresponding node will be evaluated according to its trust level.

It is worth noting that all methods that evaluate node trust are eventually affected by pseudonym change. This issue could be more or less severe depending on the change frequency of the pseudonyms. (○)

a) Reputation-based methods: Reputation is the trust built by in a vehicle over time. The CoE [26] is calculated by combining from multiple sources one of which is a sender reputation mechanism to evaluate the integrity of an event. A vehicle's trust increases if it reports a true alert and decreases otherwise. It is worth noting that although the combination of different mechanisms increases the efficiency of the method, however it inherits all the feasibility challenges.

Reputation mechanisms are inherently incompatible with pseudonymity, therefore on conflict with privacy protection (□)(○). Furthermore, the protocol for the reputation system has to be put in place and added to the standard [6] [28](○).

b) Cooperative trust establishment: The two main methods to cooperative trust are voting and consensus mechanisms. Multiple voting mechanisms exists such as Local Eviction of Attackers by Voting Evaluators (LEAVE) [29], Suicide-based Local Eviction Protocol (SLEP) and Permanent Revocation Protocol (PRP) [30]. Consensus mechanisms have also been studied. [31] proposes a method that builds trust using data-centric mechanisms (like the MDM) then broadcast the results for neighbors to incorporate in their total trust. [32] introduce a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS (T-VNets), a method that proposes a building trust on using a combination of different mechanisms: data-centric, event-based, watchdog, RSU-based trust. The trust level is shared between nodes using CAMs and regularly updated.

Similarly to all node-centric approaches, compatibility with pseudonyms is always a challenge (○). Additionally, cooperative trust establishment requires the modification of the current communications architecture whether to include voting or for consensus mechanisms [6] [28] (○). And last, revocation of a node from the network entails a denial of security application to the node. Legally it is unclear if nodes of the same clearance level could deny other nodes from accessing the network (□).

c) Data-centric trust evaluation: Data-centric methods evaluate trust without using cooperation between vehicles. This approach would reduce the risk of a sybil attack. [33] proposes a method that evaluate trust based on: the type of

TABLE I
SUMMARY OF THE FEASIBILITY CHALLENGES.
✔: COMPATIBLE, ✚: REQUIRES ADJUSMENT/STUDY, ✖: INCOMPATIBLE

	Detection Method	**Current feasibility**		
		Standard ○	Legal □	Equipment △
Sybil	Path History [2] [3] [4]	✖	✖	✚
	RSU linkability [7] [8]	✚	✚	✚
	Neighbor List [11] [12]	✚	✚	✔
Sybil & Bogus Info	***Beacon Messages***			
	RSU triangulation [14]	✔	✔	✚
	Signal Properties [12] [15] [16]	✔	✔	✔
	Data-Centric [17] [18] [19]	✔	✔	✚
	Info Exchange [19] [20] [22]	✚	✚	✔
Bogus Info	***Warning Messages***			
	Data-Centric [23] [16]	✔	✔	✔
	Voting-Based [25] [26] [27]	✚	✔	✔
	Node-Trust			
	Reputation-Based [26]	✖	✖	✔
	Cooperative [29] [30] [31] [32]	✖	✚	✔
	Data-Centric [33]	✖	✔	✔
	Pseudonym Linking [34] [35]	✔	✖	✔

the vehicle (police vehicle, emergency vehicle, ...), the event-specific trustworthiness (trust based on the relation of the event to the emitting vehicle), the dynamic trustworthiness (based on the revocation status) and the time and location indicators such as the proximity to the event.

Data-centric methods are generally compatible with the laws and the standard. However, the node-centric approach also adopted by these methods may have a conflict with the pseudonymity ensured in the standard (○).

d) Pseudonym linking: In order to circumvent the issue of pseudonymity for the trust establishing mechanisms, some methods propose solution to achieve an implicit linkability between pseudonyms. The main idea is to analyze the beacon messages to estimate the trajectory of a vehicle. [34] proposes a method that uses Kalman filters for trajectory prediction and vehicle tracking. Therefore implicitly linking the pseudonyms. [35] Discuss the opportunities of wireless fingerprinting for node identification. The result of the simulations claims a high success rate in the detection of sybil attacks. Both those methods could be used with any node-based detector to increase the integrity of honest nodes.

Although the implicit linking of pseudonyms benefits greatly all node-based mechanisms, privacy protection regulations may oppose to these types of methods to ensure that linkability is only feasible by a trusted authority. Otherwise, the whole concept of pseudonyms may as well be questioned (□).

III. DISCUSSION

Table **??** summarizes the feasibility evaluation of Section II. The first observation is that mechanisms designed to detect false beacon messages or warning messages separately, are globally feasible. Interestingly, these methods could be combined to form a global misbehavior detection framework. On the other hand, mechanisms based on node-trust face more feasibility challenges. However, the feasibility is not the only factor to consider. The performance of a mechanism should also be evaluated [36]. Some problems could be overcome if there is a big enough incentive. A system that requires changes in the regulations, in existing standards, or requires specific equipment should justify a clear major benefit to have a chance to be adopted.

A system with incompatibilities with the standard could be considered if the advantages it presents are significant. For example, several solutions [11], [12], [18]–[20] are based on a neighbor's information sharing mechanism. In simulation, this mechanism shows promising results [19] and does not imply major changes in standardized protocols to add the relevant fields on exchanged messages. For these reasons, we classify this methods among those that have a good balance between ”costs” and benefits. On the other hand, reputation-based mechanisms that requires the C–ITS to have a stable identity, are harder to integrate. Requiring a stable vehicle identity would directly oppose the pseudonymity both practically and in principle. Therefore, the addition of a reputation protocol requires rethinking major parts of the current system and is unlikely to be adopted.

Systems that present legal issues are difficult to adopt, because they need a change in the regulations. Legal issues (usually privacy violations) itself can prevent system deployment despite the advantages it presents. For instance, detection methods that rely on broadcasting a path history present major legal concerns related to privacy. Similarly, methods that are based on the implicit local linkability of pseudonym explicitly oppose the mechanisms put in place for privacy protection. In our humble opinion, in practice privacy threatening methods such as those that rely on path history broadcasting and local pseudonym linking are unlikely to be deployed, especially in the presence of alternative methods more privacy friendly.

Lastly, methods that require specific equipment face the simple trade off of cost and benefits. For a method to be eligible for deployment, in some way the benefits have to outweigh the costs. With this in mind, we take the example of the RSU triangulation technique for location verification. Currently, RSU coverage is limited and thus the cost of a total RSU coverage is high compared to the benefits. Moreover, other less demanding methods exist. However, in a later stage of the connected C–ITS network, with a wider and more secure RSU coverage, the triangulation check could be easier to be justified and subsequently integrated.

In essence, this study aims not to evaluate the detection methods based on their current compatibility status. Instead, the goal is to evaluate the compatibility status itself. The C–ITS systems are reaching the deployment stages. A misbehavior detection system, based on the current state of the art needs to be implemented and deployed in parallel with the deployment of C–ITS systems. The need for a robust and seamlessly compatible detection method is imminent. Moving forward, the gap between the regulations and the scientific methods needs to be bridged. The regulations need to be adapted to accommodate for some detection mechanisms. Correspondingly, studies need to consider the feasibility challenges while innovating new misbehavior detection mechanisms.

IV. Conclusion

In this paper we present an overview on the misbehavior detection techniques common to multiple studies. We reflect on the feasibility of the presented techniques. We discuss our point of view on which propositions are eligible for a real deployment and which requires major revisions. We also conclude that more research should target the legal aspect of the security mechanisms present in the literature. This work will be useful to the community to have an understanding of the state of the art with respect to technical, legal and standardization constraints.

Acknowledgments

This research work has been carried out in the framework of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program *Investissements d'avenir*.

References

[1] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L119, pp. 1–88, May 2016.

[2] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," *IEEE TPDS*, vol. 23, no. 6, pp. 1103–1114, June 2012.

[3] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban vanets," in *2009 29th IEEE ICDCSW*, June 2009, pp. 270–276.

[4] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, Oct 2009, pp. 1–7.

[5] "ETSI TS 102 940 v1.2.1: Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management," *ETSI WG5 Technical Specification*, pp. 1–38, November 2016.

[6] "ETSI EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," *ETSI WG5 Technical Specification*, pp. 1–44, November 2014.

[7] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," in *2007 MobiQuitous*, Aug 2007, pp. 1–8.

[8] I. J. ByungKwan Lee, EunHee Jeong, "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET," *IJSIA*, vol. 7, pp. 1–10, 2013.

[9] "ETSI TS 102 941 V1.1.15: Intelligent Transport Systems (ITS);Security;Trust and Privacy Management," *ETSI WG5 Technical Specification*, pp. 1–65, August 2017.

[10] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *2013 IEEE VNC*, Dec 2013, pp. 1–8.

[11] Y. Hao, J. Tang, and Y. Cheng, "Cooperative sybil attack detection for position based applications in privacy preserved vanets," in *IEEE - GLOBECOM 2011*, Dec 2011, pp. 1–5.

[12] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *DIWANS 2006*, 2006, pp. 1–8.

[13] "ETSI TR 103 415 V0.1.9: Intelligent Transport Systems (ITS); Security; Pre-standardisation study on pseudonym change management ," *ETSI WG5 Technical Specification*, pp. 1–31, November 2017.

[14] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE TDSC*, vol. 3, no. 4, pp. 377–385, Oct 2006.

[15] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May 2004.

[16] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in vanets," in *2011 IEEE VTC Fall*, Sept 2011, pp. 1–5.

[17] R. K. Schmidt, T. Leinmller, E. Schoch, A. Held, , and G. Schaefer, "Vehicle behavior analysis to enhance security in vanets," in *V2VCOM 2008*, 2008, pp. 1–8.

[18] N. Bimeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in vanets through verification of vehicle movement data," in *2010 IEEE VNC*, Dec 2010, pp. 166–173.

[19] R. W. van der Heijden, A. Al-Momani, F. Kargl, and O. M. F. Abu-Sharkh, "Enhanced position verification for vanets using subjective logic," in *2016 IEEE VTC-Fall*, Sept 2016, pp. 1–7.

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

[21] A. Jøsang, "A logic for uncertain probabilities," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 9, no. 3, pp. 279–311, Jun. 2001.

[22] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for vanets: A statistical approach to rogue node detection," *IEEE TVT*, vol. 65, no. 8, pp. 6703–6714, Aug 2016.

[23] 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, 2010.

[24] "ETSI TS 101 539-1 V1.1.1: Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification ," *ETSI WG5 Technical Specification*, August 2013.

[25] Z. Cao, J. Kong, U. Lee, M. Gerla, and Z. Chen, "Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks," in *IEEE INFOCOM Workshops 2008*, April 2008, pp. 1–6.

[26] T. H.-J. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Vanet alert endorsement using multi-source filters," in *Proceedings of the Seventh ACM International Workshop on VehicularAr InterNETworking*, ser. VANET '10, 2010, pp. 51–60.

[27] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for vanets," in *ACM WiSec 2011*, 2011, pp. 163–174.

[28] "ETSI EN 302 637-3 V1.2.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service ," *ETSI WG5 Technical Specification*, pp. 1–73, September 2014.

[29] 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.

[30] X. Zhuo, J. Hao, D. Liu, and Y. Dai, "Removal of misbehaving insiders in anonymous vanets," in *ACM MSWiM*, 2009, pp. 106–115.

[31] T. Leinmüller, R. K. Schmidt, and A. Held, "Cooperative position verification - defending against roadside attackers 2.0," in *Proceedings of 17th ITS World Congress*, 2010.

[32] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-vnets: a novel trust architecture for vehicular networks using the standardized messaging services of etsi its," *Comput. Commun.*, vol. 93, no. C, pp. 68–83, Nov. 2016.

[33] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008*, April 2008.

[34] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 1, pp. 11–21, Jan 2012.

[35] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surv. Tutor*, vol. 18, no. 1, pp. 94–104, Firstquarter 2016.

[36] R. W. V. D. Heijden and F. Kargl, "Evaluating Misbehavior Detection for Vehicular Networks," in *FG-IVC 2017*, no. June, 2017.