A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety

Gopi Krishnan Rajbahadur[1], Andrew J. Malton[2], Andrew Walenstein[2] and Ahmed E. Hassan[1]

***Abstract*— Anomaly detection techniques have been applied to the challenging problem of ensuring both cybersecurity and safety of connected vehicles. We propose a taxonomy of prior research in this domain. Our proposed taxonomy has 3 overarching dimensions subsuming 9 categories and 38 subcategories. Key observations emerging from the survey are: Real-world datasets are seldom used, but instead, most results are derived from simulations; V2V/V2I communications and in-vehicle communication are not considered together; proposed techniques are seldom evaluated against a baseline; safety of the vehicles does not attract as much attention as cybersecurity.**

I. INTRODUCTION

Velosa *et al.* [1] predicted that there will be a quarter of a billion connected vehicles on the road by 2020. A connected vehicle is one that is capable of connecting to a network, i.e., it can be used to communicate with other vehicles (V2V) or the infrastructure (V2I) for purposes ranging from increased infotainment capabilities to sophisticated applications like collision and congestion avoidance [2]. In the case of V2V, frequently vehicles are proposed to form a Vehicular Ad-hoc Network (VANET).

While connected vehicles increase convenience and safety of the passengers, they also present a greatly expanded attack surface that could be exploited [3]. Some research [4], [5], [6] already demonstrates exploitable vulnerabilities in ordinary vehicles. The increased number of connections of the connected vehicles only stand to increase the impact and prevalence of such vulnerabilities. Furthermore, ensuring the safety and security of connected vehicles become paramount with increased efforts by governments to enable functional VANETs [7].

In this paper, we survey and analyze the research since early 2000's, that are applying anomaly detection to the problems of safety and cybersecurity of connected vehicles. Anomaly detection is the process of identifying data points or events which do not follow an expected pattern [8]. To the best of our knowledge, this is the first study to survey the use of anomaly detection in this context. We propose a taxonomy based on 3 overarching categories and 9 sub-categories. We further have 38 dimensions into which we categorize all the surveyed papers.

Our survey and analysis lead to the following inferences:

1) Most of the research (37 out of the 65 surveyed papers) has been carried out on simulated datasets (Only 19 out of the 65 surveyed papers used real-world datasets).
2) V2X and in-vehicle communications are largely not explored together (except for 1 out of the 65 surveyed papers), making the research fragmented.
3) The safety of connected vehicles is less well studied (only 21 out of the 65 surveyed papers) than their cybersecurity.
4) Newly proposed approaches that employ anomaly detection techniques are seldom (only 4 out of the 65 surveyed papers) compared to a baseline, leading to poor quantification of the effectiveness of the proposed approaches.

Therefore, we propose that greater attention could be spent to establish benchmarks and baseline techniques against which new techniques could be evaluated. Furthermore, we also advocate for the increased utilization of real-world data instead of simulated data.

The remainder of the paper is organized as follows. We explore the related work and our survey methods in Sections II and III, and propose our taxonomy in Section IV. Finally we discuss our inferences in Section V, and conclude the paper in Section VI.

II. RELATED WORK

Unlike the present survey, the prior surveys, since early 2000's, consider VANET and in-vehicle networks separately. For instance, Erritali *et al.* [9] surveyed a variety of intrusion detection methods proposed in VANETs, and Sakiz *et al.* [10] comprehensively surveyed all the possible attacks and proposed detection mechanisms pertaining to VANETs. Neither of the studies considers possible in-vehicle network based cybersecurity or safety issues. Few of the research surveyed the possible threats and countermeasures in in-vehicle networks. For instance Liu *et al.*, McCune *et al.* and Kelberger *et al.* [11], [12], [13] present the various threats and possible countermeasures for in-vehicle (Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay etc.,) cybersecurity issues (VANET based issue are not considered). Our present survey is the first to review anomaly detection techniques in general, in the context of connected vehicles.

[1]Gopi Krishnan Rajbahadur and Ahmed E. Hassan are with School of Computing in Queen's University, Canada krishnan@cs.queensu.ca, ahmed@cs.queensu.ca

[2]Andrew J. Malton and Andrew Walenstein are with BlackBerry amalton@blackberry.com, awalenstein@blackberry.com

III. Survey Method

To ensure reproducibility, our survey follows Wholin's snowballing method [14] as follows.

Scope definition: Following Chandola *et al.* [8] we define anomaly detection as "finding patterns in data that do not conform to expected behavior." A model is formed or learned and then data are monitored for conformance.

Collecting initial set of studies: We identified an initial set of papers by keyword search in Google scholar. We did so to avoid publisher bias. The keywords used were: "Anomaly detection", "Connected vehicles", "VANET", "V2I", "V2V", "Intrusion detection", "Misbehavior detection", "CAN bus", "In-Vehicle", "safety", "Security".

Snowballing: The initial set collected through keyword search might not be exhaustive. Therefore, we performed backward and forward snowballing to collect all the references that are cited by the initial set. Papers were then included or excluded by reading the abstract followed by a thorough reading with the scope in mind (thereby, eliminating papers that are out of our scope). This snowballing process was iterated until no new relevant papers that were added. There are 65 papers finally in our study.

Although Wholin [14] recommends contacting the prominent researchers in the field for more relevant literature, we omitted this step as we could not conclusively establish the most important researchers, given the diversity of the field.

Data extraction and taxonomy development: Once all the relevant papers were collected exhaustively through Wholin's survey methodology [14], we noted down the key elements of each paper. We employed an open card sort technique [15] with the collected key points to arrive at the dimensions of our proposed taxonomy. The open card sorting technique is the process of organizing key elements into conceptual groups by consensus among the participants in the process. We used this technique to arrive at our 38 dimensions (bottom-level). We then used a bottom-up approach and grouped these dimensions into 9 sub-categories (middle-level) which we later subsumed into 3 overarching categories (top-level) based on multiple iterations of the sorting. We carried out the process of open card sorting only among the authors of this study, even though the process typically involves a larger group [15]. Finally, we assigned each of the collected papers into our taxonomy, by labeling each with every assigned dimension it occupies.

IV. Taxonomy

The process above yielded a taxonomy (see Figure 1) with 3 top-level categories, 9 sub-categories, and 38 dimensions. The categories represent the higher level traits of the research area. Our aim was to identify the addressed **threat, solution, and the research characteristics** of each paper. Especially, the captured the research characteristics, shine light on the type and rigor of the conducted experiments.

Each of the proposed categories, in turn, comprises of several sub-categories. The Threat Characteristics has 2 sub-categories, Solution Characteristics has 4, and research characteristics has 3 each, that better capture the traits of each category. The sub-categories further have dimensions as illustrated in Figure 1, which capture and highlight the technical differences that distinguish each sub-category, as follows.

A. *Threat Characteristics*

This category concerns the threat addressed by each surveyed paper. We divide it into two orthogonal sub-categories as follows.

1) Attack surface: Attack surface identifies the potential points of vulnerability in a connected vehicle. For instance, a paper might be addressing CAN bus (Other Buses not considered due to lack of sufficient literature) based attacks whereas some other papers focus exclusively on attacks that counterfeit a vehicle's ECU (Electronic Control Unit) output.

2) Attack method: A paper may address more than one attack method. We specifically call attention to the Black/Grey/Worm hole attacks dimension in this sub-category. These are routing based attacks that involve either dropping, selectively forwarding or malicious rerouting of communication packets in a VANET [16].

B. *Solution Characteristics*

This category represents the nature of the solution proposed to counter the threat.

1) Motivation: Whether an anomaly detection technique is used to detect a threat or to also provide a response to the threat.

2) Deployment point: Which part of the connected vehicle is the proposed solution deployed to. For instance, a solution might be deployed in the ECU of a vehicle, or in the Central Authority (CA) or the Road Side Unit (RSU) of a VANET.

3) Security goal: Whether the information security (integrity, confidentiality, availability) [17] and/or safety of a connected vehicle is safeguarded. Physical security is out of the scope of this work.

4) Anomaly detection method: Anomalies may be detected in multiple ways. The taxonomy distinguishes the anomaly detection method used. We draw attention to the rule-based methods dimension here, which, represents only research which infers rules automatically from vehicles operation, rather than those eliciting rules from the experts.

C. *Research Characteristics*

While the above-mentioned categories distinguished prior research based on the addressed threats and the solutions by identified dimensions, this category addresses the research methods and the data.

1) Scientific character: This sub-category records whether a paper is a theoretical, experimental, empirical or survey paper. A paper may be a combination of types.

2) Data source: This sub-category records if paper uses authentic (real data) or simulated data.

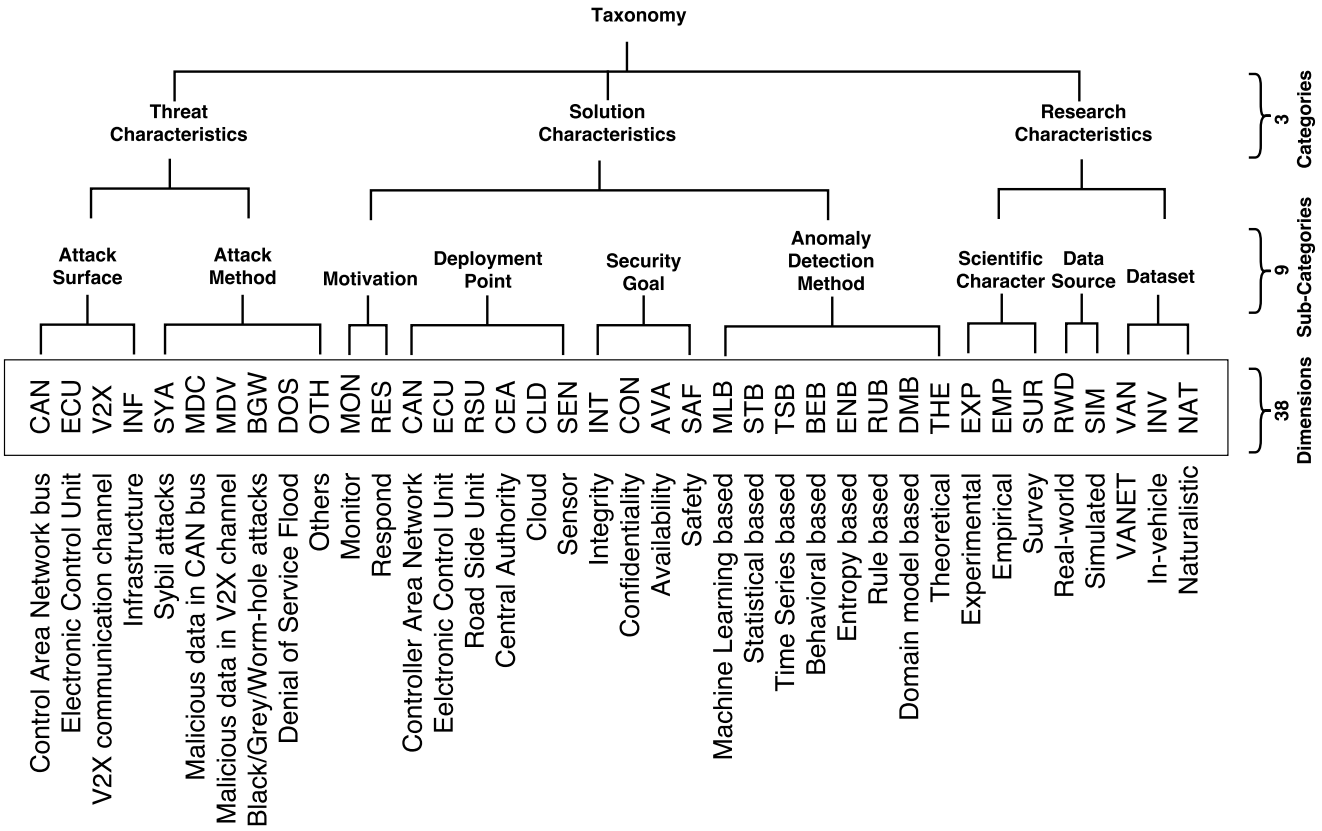

Fig. 1. Taxonomy structure depicting all the dimensions, categories, sub-categories. Dimension acronyms in the box are the column headings of Table I

3) Dataset: This sub-category records whether the paper uses VANET or In-Vehicle (CAN Bus etc.,) or naturalistic data [18]. A paper is considered to use naturalistic data if it observes the connected vehicle in operation and observes the data, as such, in its natural operating environment without any artificial data introduced (e.g., for attacks).

V. Inferences Derived from the Taxonomy

Table I presents our categorization of the papers collected in Section III according to the taxonomy described in Section IV. The main purpose of presenting the paper classifications in this way is to draw inferences and insights from it, and in this paper we draw inferences focused on analyzing the current state of research. Each paper in Table I is denoted in column "PAP" by the first and last letters of the first author's last name followed by the year of the publication.

A. Concerns

Two concerns emerge from our analysis of the survey.

None of the papers researching on VANETs use real-world data. From all the papers that we surveyed and taxonomized not even one paper (out of the 35/65 papers that study VANET data) in the VANET uses real data (all the research is conducted on simulated datasets (37/65 papers)). We can see this from Table I by observing that there is no paper with a marking on both VANET and Real-world dimension in the research characteristic category. Overall out of the 65 surveyed papers, only 28 of them use real-world datasets (mostly in in-vehicle networks research).

The proposed anomaly detection-based solutions are seldom evaluated against a baseline. As we can see from the empirical dimension (EMP) in Table I, only 4 of the surveyed papers (4 out of 65 surveyed papers) evaluated the proposed solution against a baseline. We expect that establishing a baseline to quantify improvement would be a welcome sign of maturity in a field [79].

B. Gaps

Three clear gaps remain to be filled in this research area.

With an exception of 1 paper (Levi *et al.* [47]) out of the 65 surveyed papers, no other paper considers safeguarding the connected vehicle by analyzing both In-Vehicle and VANET data together: even though faulty/malicious communications from either VANETs or in-vehicle networks could affect the safety and security of a connected vehicle. For instance, if the in-vehicle network of a connected vehicle is compromised, it might start sending faulty data on to the VANET which, in turn, may compromise the other vehicles.

Safety receives less attention than ensuring cybersecurity. In many instances, a safety breach could compromise the security of a connected vehicle and vice versa. Therefore, ensuring the safety of a connected vehicle even when there is no security concern is important.

Only a small number of surveyed papers (13 out of the 65 surveyed papers) also consider responding to

TABLE I

MATRIX SHOWING PAPER ASSIGNMENTS TO CATEGORIES.

PAP	CAN	ECU	V2X	INF	SYA	MDC	MDV	BGW	DOS	OTH	MON	RES	CAN	ECU	RSU	CEA	CLD	SEN	INT	CON	AVA	SAF	MLB	STB	TSB	BEB	ENB	RUB	DMB	THE	EXP	EMP	SUR	RWD	SIM	VAN	INV	NAT
AI13 [19]			●				●	●			●			●					●		●		●								●				●	●		
AI15 [20]				●					●	●	●							●			●		●		●						●				●	●		
AI15 [21]				●				●	●		●				●						●		●						●	●	●				●	●		
AI15 [22]			●					●	●		●			●					●		●		●								●				●	●		
AI16 [23]				●	●	●	●	●	●		●				●						●		●						●	●	●				●	●		
AI16 [24]			●		●		●				●							●	●		●		●								●				●	●		
AI16 [25]			●		●		●		●		●							●	●		●		●								●				●	●		
AI16 [26]			●				●	●		●	●			●					●		●		●								●				●	●		
AI17 [27]		●								●	●							●	●		●		●								●				●		●	
AI17 [28]			●				●	●			●			●					●		●			●							●				●	●		
AM14 [29]				●	●						●							●	●	●	●					●			●	●	●				●	●		
AM16 [12]	●					●					●	●	●						●		●					●		●	●		●		●	●		●		
AZ14 [30]			●				●				●	●			●	●		●	●		●			●							●				●	●		
BN16 [31]	●		●			●	●				●			●			●		●	●	●		●	●				●		●				●		●	
BN16 [32]										●	●							●				●								●	●						●
BR14 [33]			●		●					●	●			●					●		●									●	●				●	●		
DA13 [34]			●		●						●					●			●		●	●	●		●					●	●				●	●		
DL14 [35]			●				●				●			●					●		●							●		●	●				●	●		
EI13 [9]			●				●	●	●	●	●	●							●		●			●					●				●		●	●		
GE04 [36]			●		●		●	●	●	●	●							●	●	●	●							●	●	●	●				●	●		
GH10 [37]			●				●				●	●		●					●			●							●		●				●	●		
GN16 [38]	●	●				●			●		●		●	●					●		●	●			●						●				●		●	
GN17 [39]	●					●					●			●					●			●		●					●		●	●		●			●	
HE09 [40]	●	●				●			●	●	●	●	●	●					●			●						●	●		●			●			●	
HS17 [41]			●		●		●	●	●		●			●					●		●		●							●			●		●	●		
KG16 [42]	●					●			●		●		●						●				●								●			●			●	
KI11 [43]										●	●							●	●		●			●							●				●	●		
KR11 [13]	●					●			●	●									●		●												●					
KR14 [44]			●							●	●	●						●	●		●	●		●				●	●		●				●	●		
LG12 [45]	●	●				●					●		●	●					●									●			●			●			●	
LI09 [46]				●						●	●						●				●	●															●	
LI17 [47]	●		●		●	●	●	●	●	●	●			●		●			●		●	●	●	●	●				●					●	●	●	
LR04 [48]			●				●				●			●					●			●				●		●	●	●				●	●		
LR07 [49]																						●										●			●		
LU17 [11]	●												●						●													●					
MI16 [50]	●					●					●		●						●		●						●				●			●			●	
MI17 [51]	●					●					●			●					●									●	●		●	●		●			●	
MI17 [52]	●					●			●		●		●						●		●	●	●								●			●			●	
MR10 [53]	●	●				●				●	●		●	●					●		●							●		●				●			●	
MR11 [54]	●					●			●	●	●		●						●								●				●			●			●	
MS15 [55]			●	●			●		●	●	●	●	●	●	●	●			●	●	●		●								●				●	●		
MZ17 [56]	●					●					●			●				●	●		●									●				●			●	
NN15 [57]	●					●				●	●							●	●		●	●		●							●			●			●	
PA13 [58]			●							●	●	●				●					●							●			●				●	●		
PK14 [59]			●					●			●			●							●	●							●		●				●	●		
RA07 [60]			●		●			●		●	●	●		●		●			●		●						●				●				●	●		●
RE17 [61]	●									●	●		●					●	●					●					●		●			●			●	
RI11 [62]																																						
SG16 [63]	●					●					●		●						●		●	●			●						●			●			●	
SI14 [64]			●	●						●	●	●			●				●		●	●		●		●				●				●	●		
SL14 [65]				●				●	●		●							●	●		●					●			●	●				●	●		
SZ17 [10]	●				●		●	●	●	●	●	●		●	●	●			●	●	●		●	●	●	●	●	●	●				●				
TN10 [66]			●		●		●	●	●		●							●	●		●		●					●			●				●	●		
TR14 [67]	●									●	●		●						●			●	●		●					●	●	●		●			●	
TR15 [68]	●						●		●		●		●						●		●		●		●					●			●			●	
TR16 [69]	●					●					●		●						●		●		●		●					●	●		●			●	
TR17 [70]		●									●			●							●	●	●	●						●					●		●	
VA17 [71]	●					●			●		●		●						●		●			●	●					●				●			●	
WB16 [72]				●				●		●	●							●	●		●																
XO06 [73]			●		●						●			●	●				●	●	●			●							●				●	●		
YG16 [74]			●				●			●	●	●		●					●		●	●	●								●				●	●		●
YU13 [75]			●		●						●			●	●				●	●	●			●							●				●	●		
ZG11 [76]				●						●								●			●							●		●	●				●	●		
ZG17 [77]		●								●	●	●		●								●				●				●	●							●
ZI16 [78]			●		●		●				●							●	●		●	●		●						●	●				●	●		

countermand the detected threats. Most of the papers (59 of the 65 surveyed papers) are aimed only at monitoring for threats with the help of anomaly detection.

VI. Conclusion

Anomaly detection for enhancing the safety and security of a connected vehicle is commonly studied. The varied use and scattered publication of anomaly detection research has given rise to a sprawling literature with many gaps and concerns. To identify those gaps and concerns, and to develop a comprehensive understanding of the research area, we performed a survey of 65 relevant papers, developed a novel taxonomy during the survey, and categorized the papers surveyed against the taxonomy to identify the gaps.

The survey reveled that: much of the research is performed on simulated data (37 out of the 65 surveyed papers); in-vehicle network data and VANET data are seldom considered together to safeguard the connected vehicles (except for 1 out of the 65 surveyed papers); Connected vehicles safety research does not get the same amount of attention as cybersecurity research (only 13 out of the 65 surveyed papers); and, much of the research does not evaluate the newly proposed techniques against a baseline (only 4 out of the 65 surveyed papers do so), which may lead to results that are difficult to quantify. Therefore we urge researchers to address these identified shortcomings and periodically analyze the research with our proposed taxonomy to understand the state of the research and its evolution.

References

[1] A. Velosa, J. Hines, H. LeHong, and E. Perkins, "Predicts 2015: The Internet of Things," *Gartner: Stamford, CT, USA*, 2014.

[2] C. Evans-Pughe, "The connected car," *IEE Review*, vol. 51, no. 1, pp. 42–46, 2005.

[3] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, 2008.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*. San Francisco, 2011.

[5] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *DEF CON*, vol. 21, pp. 260–264, 2013.

[6] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington DC*, 2010, pp. 11–13.

[7] U. DoT, "Connected vehicle pilot deployment program," 2016. [Online]. Available: https://www.its.dot.gov/pilots/index.htm

[8] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[9] M. Erritali and B. E. Ouahidi, "A review and classification of various VANET intrusion detection systems," in *2013 National Security Days (JNS3)*, 2013, pp. 1–6.

[10] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[11] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: challenges and future directions," *IEEE Network*, vol. 31, no. 5, pp. 50–58, 2017.

[12] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network CAN bus," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, 2016, pp. 1–8.

[13] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *2011 IEEE Intelligent Vehicles Symposium (IV)*, 2011, pp. 528–533.

[14] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Intl. Conf. on Evaluation and Assessment in Software Engineering*, 2014, p. 38.

[15] M. Soegaard and R. F. Dam, *The encyclopedia of human-computer interaction*. The Interaction Design Foundation, 2012, ch. 2.2: Card Sorting.

[16] V. S. Abel, "Survey of attacks on mobile adhoc wireless networks," *International Journal on Computer Science and Engineering*, vol. 3, no. 2, pp. 826–829, 2011.

[17] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.

[18] T. A. Dingus, S. G. Klauer, V. L. Neale, A. Petersen, S. E. Lee, J. Sudweeks, M. Perez, J. Hankey, D. Ramsey, S. Gupta *et al.*, "The 100-car naturalistic driving study, phase II-results of the 100-car field experiment," U.S DoT, Tech. Rep., 2006.

[19] K. M. Alheeti, L. Al-Jobouri, and K. McDonald-Maier, "Increasing the rate of intrusion detection based on a hybrid technique," in *2013 5th Computer Science and Electronic Engineering Conference (CEEC)*. IEEE, 2013, pp. 179–182.

[20] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," in *2015 12th Annual IEEE Consumer Communications and Networking Conf. (CCNC)*, 2015, pp. 916–921.

[21] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," in *2015 7th Computer Science and Electronic Engineering Conference (CEEC)*. IEEE, 2015, pp. 231–236.

[22] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "An intrusion detection system against black hole attacks on the communication network of self-driving cars," in *2015 6th International Conference on Emerging Security Technologies (EST)*. IEEE, 2015, pp. 86–91.

[23] K. M. Alheeti and K. McDonald-Maier, "Hybrid intrusion detection in connected self-driving vehicles," in *22nd IEEE International Conference on Automation and Computing (ICAC)*, 2016, pp. 456–461.

[24] K. M. Alheeti and K. McDonald-Maier, "An intelligent intrusion detection scheme for self-driving vehicles based on magnetometer sensors," in *2016 International Conference for Students on Applied Engineering (ICSAE)*. IEEE, 2016, pp. 75–78.

[25] K. M. Alheeti, A. Gruebler, K. McDonald-Maier, and A. Fernando, "Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy Petri net model," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 2016, pp. 502–503.

[26] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks," *Computers*, vol. 5, no. 3, p. 16, 2016.

[27] K. M. Alheeti, R. Al-Zaidi, J. Woods, and K. McDonald-Maier, "An intrusion detection scheme for driverless vehicles based gyroscope sensor profiling," in *2017 IEEE International Conference on Consumer Electronics (ICCE)*, 2017, pp. 448–449.

[28] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," *Digital Communications and Networks*, vol. 3, no. 3, pp. 180–187, 2017.

[29] M. Al-Mutaz, L. Malott, and S. Chellappan, "Detecting Sybil attacks in vehicular networks," *Journal of Trust Management*, vol. 1, p. 4, 2014.

[30] K. C. Abdelaziz, N. Lagraa, and A. Lakas, "Trust model with delayed verification for message relay in VANETs," in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2014, pp. 700–705.

[31] O. Berlin, A. Held, M. Matousek, and F. Kargl, "POSTER: Anomaly-based misbehaviour detection in connected car backends," in *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, pp. 1–2.

[32] A. R. Beukman, G. P. Hancke, and B. J. Silva, "A multi-sensor system for detection of driver fatigue," in *14th International Conference on Industrial Informatics (INDIN)*. IEEE, 2016, pp. 870–873.

[33] N. Bissmeyer, "Misbehavior detection and attacker identification in vehicular ad-hoc networks," PhD Thesis, TU Berlin, 2014.

[34] N. Dutta and S. Chellappan, "A time-series clustering approach for Sybil attack detection in vehicular ad hoc networks," in *Proc. Intl. Conf. on Advances in Vehicular Systems, Technologies, and Applications*, Nice, 2013, pp. 21–26.

[35] S. Dietzel, R. van der Heijden, H. Decke, and F. Kargl, "A flexible, subjective logic-based framework for misbehavior detection in V2V networks," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, 2014, pp. 1–6.

[36] 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, pp. 29–37.

[37] 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.

[38] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. IEEE, 2016, pp. 176–180.

[39] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," SAE, Tech. Rep. 2017-01-1654, 2017.

[40] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying intrusion detection to automotive it-early insights and remaining challenges," vol. 4, pp. 226–235, Jan. 2009.

[41] R. E. Haas, D. P. F. Mller, P. Bansal, R. Ghosh, and S. S. Bhat, "Intrusion detection in connected cars," in *2017 IEEE Intl. Conf. on Electro Information Technology (EIT)*, 2017, pp. 516–519.

[42] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, 2016.

[43] B. Khorashadi, F. Liu, D. Ghosal, M. Zhang, and C. N. Chuah, "Distributed automated incident detection with VGRID," *IEEE Wireless Communications*, vol. 18, no. 1, pp. 64–73, 2011.

[44] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.

[45] C. Ling and D. Feng, "An algorithm for detection of malicious messages on CAN buses," in *2012 National Conference on Information Technology and Computer Science. Atlantis Press*, 2012.

[46] X. Li, Z. Li, J. Han, and J. G. Lee, "Temporal outlier detection in vehicle traffic data," in *2009 IEEE 25th International Conference on Data Engineering*, 2009, pp. 1319–1322.

[47] M. Levi, Y. Allouche, and A. Kontorovich, "Advanced analytics for connected cars cyber security," *arXiv:1711.01939 [cs]*, 2017.

[48] T. Leinmüller, A. Held, G. Schäfer, and A. Wolisz, "Intrusion detection in VANETs," in *In Proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session*, 2004.

[49] T. Leinmüller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *4th IEEE Conf. on Wireless on Demand Network Systems and Services*, 2007, pp. 84–91.

[50] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI)*, 2016, pp. 1–6.

[51] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *Intelligent Vehicles Symposium (IV), 2017 IEEE*. IEEE, 2017, pp. 1577–1583.

[52] F. Martinelli, F. Mercaldo, V. Nardone, and A. Santone, "Car hacking identification through fuzzy logic algorithms," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2017, pp. 1–7.

[53] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *2010 6th International Conference on Information Assurance and Security*, 2010, pp. 92–98.

[54] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *2011 IEEE Intelligent Vehicles Symposium (IV)*, 2011, pp. 1110–1115.

[55] L. Maglaras, "A novel distributed intrusion detection system for vehicular ad hoc networks," *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 6, 2015.

[56] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Vehicular Communications*, vol. 9, pp. 43–52, 2017.

[57] S. N. Narayanan, S. Mittal, and A. Joshi, "Using data analytics to detect anomalous states in vehicles," *arXiv:1512.08048 [cs]*, 2015.

[58] V. L. Praba and A. Ranichitra, "Detecting malicious vehicles and regulating traffic in VANET using RAODV protocol," *International Journal of Computer Applications*, vol. 84, no. 1, 2013.

[59] O. Pattnaik and B. K. Pattanayak, "Security in vehicular ad hoc network based on intrusion detection system," *American Journal of Applied Sciences*, vol. 11, no. 2, pp. 337–346, 2014.

[60] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. p Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[61] R. Rieke, M. Seidemann, E. K. Talla, D. Zelle, and B. Seeger, "Behavior analysis for safety and security in automotive systems," in *2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 2017, pp. 381–385.

[62] 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*, 2011, pp. 827–834.

[63] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *2016 International Conference on Information Networking (ICOIN)*. IEEE, 2016, pp. 63–68.

[64] H. Sedjelmaci, T. Bouali, and S. M. Senouci, "Detection and prevention from misbehaving intruders in vehicular networks," in *2014 IEEE Global Communications Conference*, 2014, pp. 39–44.

[65] H. Sedjelmaci and S. M. Senouci, "A new intrusion detection framework for vehicular networks," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 538–543.

[66] D. Tian, Y. Wang, G. Lu, and G. Yu, "A vehicular ad hoc networks intrusion detection system based on BUSNet," in *2010 2nd International Conference on Future Computer and Communication*, vol. 1. IEEE, 2010, pp. V1–225–V1–229.

[67] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," *Big data and applications*, p. 23, 2014.

[68] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," in *2015 IEEE World Congress on Industrial Control Systems Security (WCICSS)*, 2015, pp. 45–49.

[69] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 2016, pp. 130–139.

[70] A. Theissler, "Detecting known and unknown faults in automotive systems using ensemble-based anomaly detection," *Knowledge-Based Systems*, vol. 123, pp. 163–173, 2017.

[71] D. K. Vasistha, "Detecting anomalies in controller area network for automobiles," Ph.D. dissertation, Texas A&M University, 2017.

[72] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Expert Systems with Applications*, vol. 50, pp. 40–54, 2016.

[73] B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil nodes in VANETs," in *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*. ACM, 2006, pp. 1–8.

[74] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for Internet of Vehicles: A trust management scheme with affinity propagation," *Mobile Information Systems*, vol. 2016, pp. 1–10, 2016.

[75] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[76] Y. Zhang and G. Cao, "V-PADA: Vehicle-platoon-aware data access in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 5, pp. 2326–2339, 2011.

[77] M. Zhang, C. Chen, T. Wo, T. Xie, M. Z. A. Bhuiyan, and X. Lin, "SafeDrive: online driving anomaly detection from large-scale vehicle data," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 2087–2096, 2017.

[78] 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 Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, 2016.

[79] S. Lessmann, B. Baesens, C. Mues, and S. Pietsch, "Benchmarking classification models for software defect prediction: A proposed framework and novel findings," *IEEE Transactions on Software Engineering*, vol. 34, no. 4, pp. 485–496, 2008.