Scopus

Documents

Sharmin, S., Mansor, H., Abdul Kadir, A.F., Aziz, N.A.

Benchmarking frameworks and comparative studies of Controller Area Network (CAN) intrusion detection systems: A review
(2024) *Journal of Computer Security*, 32 (5), pp. 477-507. Cited 1 time.

DOI: 10.3233/JCS-230027

Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Selangor, Malaysia

Abstract
The development of intrusion detection systems (IDS) for the in-vehicle Controller Area Network (CAN) bus is one of the main efforts being taken to secure the in-vehicle network against various cyberattacks, which have the potential to cause vehicles to malfunction and result in dangerous accidents. These CAN IDS are evaluated in disparate experimental conditions that vary in terms of the workload used, the features used, the metrics reported, etc., which makes direct comparison difficult. Therefore, there have been several benchmarking frameworks and comparative studies designed to evaluate CAN IDS in similar experimental conditions to understand their relative performance and facilitate the selection of the best CAN IDS for implementation in automotive networks. This work provides a comprehensive survey of CAN IDS benchmarking frameworks and comparative studies in the current literature. A CAN IDS evaluation design space is also proposed in this work, which draws from the wider CAN IDS literature. This is not only expected to serve as a guide for designing CAN IDS evaluation experiments but is also used for categorising current benchmarking efforts. The surveyed works have been discussed on the basis of the five aspects in the design space - namely, IDS type, attack model, evaluation type, workload generation, and evaluation metrics - and recommendations for future work have been identified. © 2024 - IOS Press. All rights reserved.

Author Keywords
benchmarking; Controller area network; evaluation; intrusion detection

Index Keywords
Benchmarking; 'current, Comparatives studies, Controller-area network, Design spaces, Evaluation, Experimental conditions, Intrusion Detection Systems, Intrusion-Detection, Network intrusion detection systems, System evaluation; Intrusion detection

References

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

- Agbaje, P., Anjum, A., Mitra, A., Bloom, G., Olufowobi, H.
  A framework for consistent and repeatable controller area network IDS evaluation
  (2022) *NDSS Automotive and Autonomous Vehicle Security, (AutoSec) Workshop 2022*,

- Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D., Mouzakitis, A.
  Intrusion detection systems for intra-vehicle networks: A review
  (2019) *IEEE Access*, 7, pp. 21266-21289.

- Aliwa, E., Rana, O., Perera, C., Burnap, P.
  Cyberattacks and countermeasures for in-vehicle networks
  (2021) *ACM Computing Surveys*, 54 (1).

- Almomani, O., Almaiah, M.A., Alsaaidah, A., Smadi, S., Mohammad, A.H., Althunibat, A.
  Machine learning classifiers for network intrusion detection system: Comparative study
  (2021) *2021 International Conference on Information Technology (ICIT)*, pp. 440-445.

- Alshammari, A., Zohdy, M.A., Debnath, D., Corser, G.
  Classification approach for intrusion detection in vehicle systems

(2018) *Wireless Engineering and Technology*, 9 (4), pp. 79-94.

- Anyanwu, G.O., Nwakanma, C.I., Lee, J.M., Kim, D.-S.
  Countering attacks in in-vehicle network: An evaluation of machine learning algorithms
  (2021) *2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Island, Korea, Republic of*, pp. 657-660.
  ISBN 978-1-6654-2383-0

- Avatefipour, O., Saad Al-Sumaiti, A., El-Sherbeeny, A.M., Mahrous Awwad, E., Elmeligy, M.A., Mohamed, M.A., Malik, H.
  An intelligent secured framework for cyberattack detection in electric vehicles', CAN Bus Using Machine Learning
  (2019) *IEEE Access*, 7, pp. 127580-127592.

- Baldini, G.
  On the application of entropy measures with sliding window for intrusion detection in automotive in-vehicle networks
  (2020) *Entropy*, 22 (9), p. 1044.

- Barletta, V.S., Caivano, D., Nannavecchia, A., Scalera, M.
  Intrusion detection for in-vehicle communication networks: An unsupervised Kohonen SOM approach
  (2020) *Future Internet*, 12 (7), p. 119.

- Baum, L., Becker, M., Geyer, L., Molter, G.
  Mapping requirements to reusable components using design spaces
  (2000) *Proceedings Fourth International Conference on Requirements Engineering. ICRE 2000*, pp. 159-167.
  Cat. No. 98TB100219

- Berger, I., Rieke, R., Kolomeets, M., Chechulin, A., Kotenko, I.
  (2019) *Comparative study of machine learning methods for invehicle intrusion detection*, pp. 85-101.
  C. Security, S.K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, J. Mylopoulos and C. Kalloniatis, eds, Springer International Publishing, Cham, ISBN 978-3-030-12786-2

- Blevins, D.H., Moriano, P., Bridges, R.A., Verma, M.E., Iannacone, M.D., Hollifield, S.C.
  Time-based CAN intrusion detection benchmark
  (2021) *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021*, Internet Society, Virtual, ISBN 978-1-891562-68-1

- Bozdal, M., Samie, M., Jennions, I.K.
  WINDS: A wavelet-based intrusion detection system for controller area network (CAN)
  (2021) *IEEE Access*, 9, pp. 58621-58633.

- Charette, R.N.
  (2021) *How Software Is Eating the Car*,

- Chicco, D., Tötsch, N., Jurman, G.
  The Matthews Correlation Coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation
  (2021) *BioData Mining*, 14 (1), p. 13.

- Cho, K.-T., Shin, K.G.
  Fingerprinting electronic control units for vehicle intrusion detection
  (2016) *Proceedings of the 25th USENIX Conference on Security Symposium,*

SEC'16, pp. 911-927.
USENIX Association, USA, ISBN 978-1-931971-32-4

- Cho, K.-T., Shin, K.G.
Viden: Attacker identification on in-vehicle networks
(2017) *Proceedings of the 2017 ACMSIGSAC Conference on Computer and Communications Security*, pp. 1109-1123.
ACM, Dallas Texas USA, ISBN 978-1-4503-4946-8

- Choi, J., Kim, H.
On the robustness of intrusion detection systems for vehicles against adversarial attacks
(2021) *Information Security Applications*, pp. 39-50.
H. Kim, ed., Springer International Publishing, Cham, ISBN 978-3-030-89432-0

- Choi, W., Joo, K., Jo, H.J., Park, M.C., Lee, D.H.
VoltageIDS: Low-level communication characteristics for automotive intrusion detection system
(2018) *IEEE Transactions on Information Forensics and Security*, 13 (8), pp. 2114-2129.

- Corbett, C., Basic, T., Lukaseder, T., Kargl, F.
A testing framework architecture for automotive intrusion detection systems
(2017) *Automotive -Safety & Security 2017 -Sicherheit und Zuverlässigkeit für automobile Informationstechnik*, pp. 89-102.
P. Dencker, H. Klenk, H.B. Keller and E. Plödererder, eds, Gesellschaft für Informatik, Bonn

- Corrigan, S.
(2016) *Introduction to the Controller Area Network (CAN)*,
Technical Report, Texas Instruments

- Costa, T.
(2021) *Cañones, Benchmarking framework for Intrusion Detection Systems in Controller Area Networks*,
Master's thesis, Politecnico diMilano and Universitat Politecnica de Catalunya

- Desta, A.K., Ohira, S., Arai, I., Fujikawa, K.
ID sequence analysis for intrusion detection in the CAN bus using long short term memory networks
(2020) *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 1-6.
IEEE, Austin, TX, USA, ISBN 978-1-72814-716-1

- Dupont, G., Den Hartog, J., Etalle, S., Lekidis, A.
Evaluation framework for network intrusion detection systems for in-vehicle CAN
(2019) *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 1-6.
Graz, Austria, ISBN 978-1-7281-0142-2

- Dupont, G., Lekidis, A., Den Hartog, J., Etalle, S.
(2019) *Automotive Controller Area Network (CAN) bus intrusion dataset v2*,

- Fenzl, F., Rieke, R., Chevalier, Y., Dominik, A., Kotenko, I.
Continuous fields: Enhanced in-vehicle anomaly detection using machine learning models
(2020) *Simulation Modelling Practice and Theory*, 105, p. 102143.

- Foruhandeh, M., Man, Y., Gerdes, R., Li, M., Chantem, T.
SIMPLE: Single-frame based physical layer identification for intrusion detection and prevention on in-vehicle networks
(2019) *Proceedings of the 35th Annual Computer Security Applications*

Conference, pp. 229-244.
ACM, San Juan Puerto Rico, USA, ISBN 978-1-4503-7628-0

- Gadelrab, M.S., Ghorbani, A.
  A new framework for publishing and sharing network and security datasets
  (2012) *2012 SC Companion: High Performance Computing, Networking Storage and Analysis*, pp. 539-546.

- Gazdag, A., Lupták, G., Buttyán, L.
  Correlation-based anomaly detection for the CAN bus
  (2022) *Security in Computer and Information Sciences*, 1596, pp. 38-50.
  E. Gelenbe, M. Jankovic, D. Kehagias, A. Marton and A. Vilmos, eds, Communications in Computer and Information Science, Springer International Publishing, Cham, ISBN 978-3-031-09356-2 978-3-031-09357-9

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

- Hafeez, A., Rehman, K., Malik, H.
  (2020) *State of the art survey on comparison of physical fingerprinting-based intrusion detection techniques for in-vehicle security*,
  2020-01-0721

- Han, M.L., Kwak, B.I., Kim, H.K.
  Anomaly intrusion detection method for vehicular networks based on survival analysis
  (2018) *Vehicular Communications*, 14, pp. 52-63.

- Hanselmann, M., Strauss, T., Dormann, K., Ulmer, H.
  CANet: An unsupervised intrusion detection system for high dimensional CAN bus data
  (2020) *IEEE Access*, 8, pp. 58194-58205.

- Hossain, M.D., Inoue, H., Ochiai, H., Fall, D., Kadobayashi, Y.
  LSTM-based intrusion detection system for in-vehicle can bus communications
  (2020) *IEEE Access*, 8, pp. 185489-185502.

- Islam, R., Refat, R.U.D., Yerram, S.M., Malik, H.
  Graph-based intrusion detection system for controller area networks
  (2022) *IEEE Transactions on Intelligent Transportation Systems*, 23 (3), pp. 1727-1736.

- Jadidbonab, H., Tomlinson, A., Nguyen, H.N., Doan, T., Shaikh, S.A.
  A real-time in-vehicle network testbed for machine learning-based IDS training and validation
  (2021) *Workshop on Artificial Intelligence and Cyber Security (AI-CyberSec 2021), CEUR Workshop Proceedings*,

- Javed, A.R., Rehman, S.U., Khan, M.U., Alazab, M.
  CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU
  (2021) *IEEE Transactions on Network Science and Engineering*, 8 (2), pp. 1456-1466.

- Ji, H., Wang, Y., Qin, H., Wang, Y., Li, H.
  Comparative performance evaluation of intrusion detection methods for in-vehicle networks
  (2018) *IEEE Access*, 6, pp. 37523-37532.

- Kang, H., Kwak, B.I., Lee, Y.H., Lee, H., Lee, H., Kim, H.K.
  Car Hacking: Attack & Defense Challenge 2020 Dataset

(2021) *IEEE Dataport*,

- Karopoulos, G., Kambourakis, G., Chatzoglou, E., Hernández-Ramos, J.L., Kouliaridis, V.
  Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy
  (2022) *Electronics*, 11 (7), p. 1072.

- Khandelwal, S., Shreejith, S.
  A lightweight multi-attack CAN intrusion detection system on hybrid FPGAs
  (2022) *2022 32nd International Conference on Field-Programmable Logic and Applications (FPL)*, pp. 425-429.
  IEEE, Belfast, United Kingdom, ISBN 978-1-66547-390-3

- Kilincer, I.F., Ertam, F., Sengur, A.
  Machine learning methods for cyber security intrusion detection: Datasets and comparative study
  (2021) *Computer Networks*, 188, p. 107840.

- Kukkala, V.K., Thiruloga, S.V., Pasricha, S.
  INDRA: Intrusion detection using recurrent autoencoders in automotive embedded systems
  (2020) *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39 (11), pp. 3698-3710.

- Lalouani, W., Dang, Y., Younis, M.
  Mitigating voltage fingerprint spoofing attacks on the controller area network bus
  (2022) *Cluster Computing*, 26 (2), pp. 1447-1460.

- Lee, H., Jeong, S.H., Kim, H.K.
  OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame
  (2017) *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pp. 57-5709.

- Longari, S., Nova Valcarcel, D.H., Zago, M., Carminati, M., Zanero, S.
  CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network
  (2021) *IEEE Transactions on Network and Service Management*, 18 (2), pp. 1913-1924.

- Marchetti, M., Stabili, D.
  Anomaly detection of CAN bus messages through analysis of ID sequences
  (2017) *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1577-1583.

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

- Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., Payne, B.D.
  Evaluating computer intrusion detection systems: A survey of common practices
  (2015) *ACM Computing Surveys*, 48, p. 1.

- Miller, C., Valasek, C.
  (2014) *A Survey of Remote Automotive Attack Surfaces*,
  in, Black, Hat USA

- Moore, M.R., Bridges, R.A., Combs, F.L., Starr, M.S., Prowell, S.J.
  Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: A data-driven approach to in-vehicle intrusion detection
  (2017) *Proceedings of the 12th Annual Conference on Cyber and Information Security*

Research, CISRC '17,
Association for Computing Machinery, New York, NY, USA, ISBN 978-1-4503-4855-3

- Moriano, P., Bridges, R.A., Iannacone, M.D.
Detecting CAN masquerade attacks with signal clustering similarity
(2022) *Proceedings Fourth International Workshop on Automotive and Autonomous Vehicle Security*,

- Moulahi, T., Zidi, S., Alabdulatif, A., Atiquzzaman, M.
Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus
(2021) *IEEE Access*, 9, pp. 99595-99605.

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

- Nappi, F.
(2022) *A survey of intrusion detection systems for controller area networks and FPGA evaluation*,
Master's thesis, Politecnico Milano

- Nichelini, A., Pozzoli, C.A., Longari, S., Carminati, M., Zanero, S.
CANova: A hybrid intrusion detection framework based on automatic signal classification for CAN
(2023) *Computers & Security*, 128, p. 103166.

- Novikova, E., Le, V., Yutin, M., Weber, M., Anderson, C.
Autoencoder anomaly detection on large CAN bus data
(2022) *Proceedings of DLP-KDD 2020*, p. 9.
ACM, San Diego, California, ISBN 978-1-4503-9999-9

- Okokpujie, K., Kennedy, G.C., Nzanzu, V.P., Molo, M.J., Adetiba, E., Badejo, J.
Anomaly-based intrusion detection for a vehicle CAN bus: A case for hyundai avante CN7
(2021) *Journal of Southwest Jiaotong University*, 56 (5), pp. 144-156.

- Olufowobi, H., Ezeobi, U., Muhati, E., Robinson, G., Young, C., Zambreno, J., Bloom, G.
Anomaly detection approach using adaptive cumulative sum algorithm for controller area network
(2019) *Proceedings of the ACMWorkshop on Automotive Cybersecurity, AutoSec '19*, pp. 25-30.
Association for Computing Machinery, New York, NY, USA, ISBN 978-1-4503-6180-4

- Olufowobi, H., Young, C., Zambreno, J., Bloom, G.
SAIDuCANT: Specification-based automotive intrusion detection using Controller Area Network (CAN) timing
(2020) *IEEE Transactions on Vehicular Technology*, 69 (2), pp. 1484-1494.

- Panigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Jhaveri, R.H., Chowdhary, C.L.
Performance assessment of supervised classifiers for designing intrusion detection systems: A comprehensive review and recommendations for future research
(2021) *Mathematics*, 9 (6), p. 690.

- Paul, A., Islam, M.R.
An artificial neural network based anomaly detection method in CAN bus messages in vehicles
(2021) *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, pp. 1-5.

- Popa, L., Groza, B., Jichici, C., Murvay, P.-S.
  ECUPrint -physical fingerprinting electronic control units on CAN buses inside cars and SAE J1939 compliant vehicles
  (2022) *IEEE Transactions on Information Forensics and Security*, 17, pp. 1185-1200.

- Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G., Cheah, M.
  AI-based intrusion detection systems for in-vehicle networks: A survey
  (2022) *ACM Computing Surveys*, p. 3570954.

- Rathore, R.S., Hewage, C., Kaiwartya, O., Lloret, J.
  In-vehicle communication cyber security: Challenges and solutions
  (2022) *Sensors*, 22 (17), p. 6679.

- Refat, R.U.D., Elkhail, A.A., Hafeez, A., Malik, H.
  Detecting CAN bus intrusion by applying machine learning method to graph based features
  (2022) *Intelligent Systems and Applications*, 296, pp. 730-748.
  K. Arai, ed., Lecture Notes in Networks and Systems. ISBN, Springer International Publishing, Cham, ISBN 978-3-030-82198-2 978-3-030-82199-9

- Rieke, R., Seidemann, M., Talla, E.K., Zelle, D., Seeger, B.
  Behavior Analysis for Safety and Security in Automotive Systems
  (2017) *2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, pp. 381-385.

- Sami, M.
  Intrusion Detection in CAN Bus
  (2019) *IEEE Dataport*,

- Schell, O., Kneib, M.
  VALID: Voltage-based lightweight intrusion detection for the controller area network
  (2020) *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 225-232.
  IEEE, Guangzhou, China, ISBN 978-1-66540-392-4

- Seo, E., Song, H.M., Kim, H.K.
  GIDS: GAN based intrusion detection system for in-vehicle network
  (2018) *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pp. 1-6.

- Sharmin, S., Mansor, H.
  Intrusion detection on the in-vehicle network using machine learning
  (2021) *3rd International Cyber Resilience Conference (CRC)*, pp. 26-31.
  IEEE, Virtual, ISBN 978-1-66541-844-7

- Sharmin, S., Mansor, H., Kadir, A.F.A., Aziz, N.A.
  Using streaming data algorithm for intrusion detection on the vehicular controller area network
  (2022) *Ubiquitous Security*, 1557, pp. 131-144.
  G. Wang, K.-K.R. Choo, R.K.L. Ko, Y. Xu and B. Crispo, eds, Communications in Computer and Information Science. ISBN, Springer, Singapore, Singapore, ISBN 978-981-19046-7-7 978-981-19046-8-4

- Song, H., Kim, H., Kim, H.
  Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network
  (2016) *2016 International Conference on Information Networking (ICOIN)*, pp. 63-68.
  IEEE Computer Society, Los Alamitos, CA, USA

- Stabili, D., Marchetti, M.
  Detection of missing CAN messages through inter-arrival time analysis
  (2019) *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1-7.

- Stabili, D., Marchetti, M., Colajanni, M.
  Detecting attacks to internal vehicle networks through Hamming distance
  (2017) *2017 AEIT International Annual Conference*, pp. 1-6.

- Stabili, D., Pollicino, F., Rota, A.
  A benchmark framework for CAN IDS
  (2021) *Proceedings of the Italian Conference on Cybersecurity (ITASEC 2021)*,

- Stachowski, S., Gaynier, R., LeBlanc, D.J.
  (2019) *An assessment method for automotive intrusion detection system performance*, Technical Report, DOT HA 812 708, University of Michigan, Ann Arbor, Transportation Research Institute

- Stakhanova, N., Cardenas, A.A.
  Analysis of metrics for classification accuracy in intrusion detection
  (2017) *Empirical Research for Software Security*, pp. 173-199.
  CRC Press

- Studnia, I., Alata, E., Nicomette, V., Kaâniche, M., Laarouchi, Y.
  A language-based intrusion detection approach for automotive embedded networks
  (2018) *International Journal of Embedded Systems*, 10 (1).

- Sunny, J., Sankaran, S., Saraswat, V.
  A hybrid approach for fast anomaly detection in controller area networks
  (2020) *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6.

- Swessi, D., Idoudi, H.
  A comparative review of security threats datasets for vehicular networks
  (2021) *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 746-751.

- Swessi, D., Idoudi, H.
  Comparative study of ensemble learning techniques for fuzzy attack detection in in-vehicle networks
  (2022) *Advanced Information Networking and Applications*, pp. 598-610.
  L. Barolli, F. Hussain and T. Enokido, eds, Springer International Publishing, Cham, ISBN 978-3-030-99587-4

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

- Taylor, A., Leblanc, S., Japkowicz, N.
  Probing the limits of anomaly detectors for automobiles with a cyberattack framework
  (2018) *IEEE Intelligent Systems*, 33 (2), pp. 54-62.

- Thiruloga, S.V., Kukkala, V.K., Pasricha, S.
  TENET: Temporal CNN with attention for anomaly detection in automotive cyber-physical systems
  (2022) *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 326-331.

- Tomlinson, A., Bryans, J., Shaikh, S.A.
  Towards viable intrusion detection methods for the automotive controller area network
  (2018) *Proceedings of the 2nd ACM Computer Science in Cars Symposium*,
  ISBN 978-1-4503-6616-8

- Ujiie, Y., Kishikawa, T., Haga, T., Matsushima, H., Wakabayashi, T., Tanabe, M., Kitamura, Y., Anzai, J.
  A method for disabling malicious CAN messages by using a CMI-ECU
  (2016) *SAE 2016 World Congress and Exhibition*,
  ISSN 0148-7191

- Vahidi, A., Rosenstatter, T., Mowla, N.I.
  Systematic evaluation of automotive intrusion detection datasets
  (2022) *Computer Science in Cars Symposium*, pp. 1-12.
  ACM, Ingolstadt Germany, ISBN 978-1-4503-9786-5

- Verma, M.E., Iannacone, M.D., Bridges, R.A., Hollifield, S.C., Moriano, P., Kay, B., Combs, F.L.
  (2020) *Addressing the Lack of Comparability & Testing in CAN Intrusion Detection Research: A Comprehensive Guide to CAN IDS Data & Introduction of the ROAD Dataset*,
  arXiv

- Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., Li, K.
  A survey of intrusion detection for in-vehicle networks
  (2020) *IEEE Transactions on Intelligent Transportation Systems*, 21 (3), pp. 919-933.

- Xun, Y., Zhao, Y., Liu, J.
  VehicleEIDS: A novel external intrusion detection system based on vehicle voltage signals
  (2022) *IEEE Internet of Things Journal*, 9 (3), pp. 2124-2133.

- Young, C., Olufowobi, H., Bloom, G., Zambreno, J.
  Automotive intrusion detection based on constant CAN message frequencies across vehicle driving modes
  (2019) *Proceedings of the ACM Workshop on Automotive Cybersecurity, AutoSec '19*, pp. 9-14.
  Association for Computing Machinery, New York, NY, USA, ISBN 978-1-4503-6180-4

- Zago, M., Longari, S., Tricarico, A., Carminati, M., Gil Pérez, M., Martínez Pérez, G., Zanero, S.
  ReCAN -dataset for reverse engineering of controller area networks
  (2020) *Data in Brief*, 29, p. 105149.

- Zhang, J., Li, F., Zhang, H., Li, R., Li, Y.
  Intrusion detection system using deep learning for in-vehicle security
  (2019) *Ad Hoc Networks*, 95, p. 101974.

- Zhang, L., Ma, D.
  A hybrid approach toward efficient and accurate intrusion detection for in-vehicle networks
  (2022) *IEEE Access*, 10, pp. 10852-10866.

Correspondence Address
Sharmin S.; Kulliyyah of Information and Communication Technology, Selangor, Malaysia; email: shailasharmin@protonmail.com

Publisher: IOS Press BV

ISSN: 0926227X
CODEN: JCSIE
Language of Original Document: English
Abbreviated Source Title: J Computer Secur
2-s2.0-85213484640
Document Type: Article
Publication Stage: Final
Source: Scopus