ACM International Conference Proceeding Series • Pages 218 - 226 • 23 February 2023 • 12th International Conference on Software and Computer Applications, ICSCA 2023 • Kuantan • 23 February 2023through 25 February 2023 • Code 189662

Document type
Conference Paper

Source type
Conference Proceedings

ISBN
978-145039858-9

DOI
10.1145/3587828.3587861

Publisher
Association for Computing Machinery

Original language
English

View less

Comparative Evaluation of Anomaly-Based Controller Area Network IDS

Sharmin, Shaila ; Mansor, Hafizah ; Kadir, Andi Fitriah Abdul ; Aziz, Normaziah A.

Save all to author list

[a] Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Selangor, Malaysia

Full text options Export

Abstract

Author keywords

Indexed keywords

SciVal Topics

Abstract

The vulnerability of in-vehicle networks, particularly those based on the Controller Area Network (CAN) protocol, has prompted the development of numerous techniques for intrusion detection on the CAN bus. However, these CAN IDS are often evaluated in disparate experimental settings, with different datasets and evaluation metrics, which hinder direct comparison. This has given rise to efforts at benchmarking and comparative evaluation of CAN IDS under similar experimental conditions to provide an understanding of the relative performance of these CAN IDS. This work contributes to these efforts by reporting results of the comparative evaluation of four statistical and two machine learning-based CAN intrusion detection algorithm, against the Real ORNL Automotive Dynamometer (ROAD) CAN intrusion dataset. The ROAD dataset differs from datasets used in previous work in that it includes the stealthiest possible version of targeted ID fabrication attacks which are more difficult to detect. It also consists of masquerade attacks, which have not been commonly used in comparative evaluation studies. Furthermore, in addition to metrics such as accuracy, precision, recall, and F1-score, we report balanced accuracy, informedness, markedness, and Matthews correlation coefficient, which place equal important on positive and negative classes and are better measures of detection capability,

especially for imbalanced datasets. We also report training and testing times for each CAN IDS as an indicator of real-time intrusion detection performance. Results of experiments were found to be generally concordant with previous work, in terms of accuracy, precision, recall, and F1-score. Entropy- and frequency-based CAN IDS were found to be relatively better at detecting attacks, particularly fabrication attacks; while other algorithms did not perform well, as indicated by low MCC scores.

Author keywords

Automotive; Comparative evaluation; Controller area network; Intrusion detection

Indexed keywords

SciVal Topics

References (28)

View in search results format >

All

Export Print E-mail Save to PDF Create bibliography

1 Agbaje, P., Anjum, A., Mitra, A., Bloom, G., Olufowobi, H.
(2022) *A Framework for Consistent and Repeatable Controller Area Network IDS Evaluation*

2 Aliwa, E., Rana, O., Perera, C., Burnap, P.
Cyberattacks and Countermeasures for In-Vehicle Networks
(2021) *ACM Computing Surveys*, 54 (1), art. no. 21. Cited 46 times.
http://dl.acm.org/citation.cfm?id=J204

3 Berger, I., Rieke, R., Kolomeets, M., Chechulin, A., Kotenko, I.
Comparative study of machine learning methods for in-vehicle intrusion detection
(2019) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11387 LNCS, pp. 85-101. Cited 20 times.
https://www.springer.com/series/558
ISBN: 978-303012785-5
doi: 10.1007/978-3-030-12786-2_6

View at Publisher

4 Blevins, D.H., Moriano, P., Bridges, R.A., Verma, M.E., Iannacone, M.D., Hollifield, S.C.
Time-Based CAN Intrusion Detection Benchmark
(2021) *Proceedings Third International Workshop on Automotive and Autonomous Vehicle Security*. Cited 2 times.
Internet Society, Virtual
https://doi.org/10.14722/autosec.2021.23013

5 Charette, R.N.
(2021) *How Software Is Eating the Car*. Cited 9 times.
https://spectrum.ieee.org/software-eating-carSection:Transportation

6 Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., (...), Kohno, T.
(2011) *Comprehensive Experimental Analyses of Automotive Attack Surfaces (SEC'11)*, p. 6. Cited 72 times.
USENIX Association, USA

7 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, art. no. 13, pp. 1-22. Cited 246 times.
http://www.biodatamining.org/
doi: 10.1186/s13040-021-00244-z

View at Publisher

8 Cho, K.-T., Shin, K.G.
Fingerprinting electronic control units for vehicle intrusion detection

(2016) *Proceedings of the 25th USENIX Security Symposium*, pp. 911-927. Cited 353 times.
ISBN: 978-193197132-4

9 Corrigan, S.
(2016) *Introduction to the Controller Area Network (CAN)*. Cited 188 times.
Technical Report. Texas Instruments. May
www.ti.com

10 Cañones, T.C.
(2021) *Benchmarking framework for Intrusion Detection Systems in Controller Area Networks*
Ph. D. Dissertation. Politecnico di Milano and Universitat Politecnica de Catalunya
https://www.politesi.polimi.it/handle/10589/176269

11 Dupont, G., Den Hartog, J., Etalle, S., Lekidis, A.
Evaluation framework for network intrusion detection systems for in-vehicle CAN

(2019) *2019 8th IEEE International Conference on Connected Vehicles and Expo, ICCVE 2019 - Proceedings*, art. no. 8965028. Cited 8 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8952572
ISBN: 978-172810142-2
doi: 10.1109/ICCVE45908.2019.8965028

View at Publisher

12 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. Cited 32 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2018.2848106

View at Publisher

13 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 (Switzerland)*, 11 (7), art. no. 1072. Cited 12 times.
https://www.mdpi.com/2079-9292/11/7/1072/pdf
doi: 10.3390/electronics11071072

View at Publisher

14 Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., (...), Savage, S.

Experimental security analysis of a modern automobile

(2010) *Proceedings - IEEE Symposium on Security and Privacy*, art. no. 5504804, pp. 447-462. Cited 1312 times.
ISBN: 978-076954035-1
doi: 10.1109/SP.2010.34

View at Publisher

15 Marchetti, M., Stabili, D.

Anomaly detection of CAN bus messages through analysis of ID sequences

(2017) *IEEE Intelligent Vehicles Symposium, Proceedings*, art. no. 7995934, pp. 1577-1583. Cited 144 times.
ISBN: 978-150904804-5
doi: 10.1109/IVS.2017.7995934

View at Publisher

16 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 2016*, art. no. 7740627. Cited 107 times.
ISBN: 978-150901131-5
doi: 10.1109/RTSI.2016.7740627

View at Publisher

17 Miller, C., Valasek, C.
Remote Exploitation of an Unaltered Passenger Vehicle
(2015) *Black Hat USA*. Cited 775 times.
Las Vegas

18 Müter, M., Asaj, N.

Entropy-based anomaly detection for in-vehicle networks

(2011) *IEEE Intelligent Vehicles Symposium, Proceedings*, art. no. 5940552, pp. 1110-1115. Cited 244 times.
ISBN: 978-145770890-9
doi: 10.1109/IVS.2011.5940552

View at Publisher

19 Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., (...), Duchesnay, É.

Scikit-learn: Machine learning in Python (Open Access)

(2011) *Journal of Machine Learning Research*, 12, pp. 2825-2830. Cited 45871 times.
http://jmlr.csail.mit.edu/papers/volume12/pedregosa11a/pedregosa11a.pdf

View at Publisher

20 Powers, D.M.W.
(2020) *Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation*. Cited 1294 times.
2020
https://doi.org/10.48550/ARXIV.2010.16061

21 Stabili, D., Marchetti, M., Colajanni, M.

Detecting attacks to internal vehicle networks through Hamming distance (Open Access)

(2017) *2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017*, 2017-January, pp. 1-6. Cited 72 times.
ISBN: 978-888723737-5
doi: 10.23919/AEIT.2017.8240550

View at Publisher

22 Stabili, D., Pollicino, F., Rota, A.
(2021) *A benchmark framework for CAN IDS*

23 Swessi, D., Idoudi, H.

Comparative Study of Ensemble Learning Techniques for Fuzzy Attack Detection in In-Vehicle Networks (Open Access)

(2022) *Lecture Notes in Networks and Systems*, 450 LNNS, pp. 598-610. Cited 2 times.
springer.com/series/15179
ISBN: 978-303099586-7
doi: 10.1007/978-3-030-99587-4_51

View at Publisher

24 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. Cited 21 times.
doi: 10.1109/MIS.2018.111145054

View at Publisher

25 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*. Cited 29 times.
2018. ISBN
https://doi.org/10.1145/3273946.3273950

26 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 Instrusion Detection Research: A Comprehensive Guide to CAN IDS Data & Introduction of the ROAD Dataset*. Cited 5 times.
2020
http://arxiv.org/abs/2012.14600arXiv:2012.14600

27 Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., Li, K.
A survey of intrusion detection for in-vehicle networks
(Open Access)

(2020) *IEEE Transactions on Intelligent Transportation Systems*, 21 (3), art. no. 8688625, pp. 919-933. Cited 144 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6979
doi: 10.1109/TITS.2019.2908074

View at Publisher

28 Young, C., Olufowobi, H., Bloom, G., Zambreno, J.
Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes

(2019) *AutoSec 2019 - Proceedings of the ACM Workshop on Automotive Cybersecurity, co-located with CODASPY 2019*, pp. 9-14. Cited 35 times.
http://dl.acm.org/citation.cfm?id=3309171
ISBN: 978-145036180-4
doi: 10.1145/3309171.3309179

View at Publisher

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us