< Back to results | < Previous 8 of 39 Next >

Export Download Print E-mail Save to PDF ☆ Add to List More... >

Full Text |View at Publisher|

Document type
Conference Paper

Source type
Conference Proceedings

ISBN
978-166541844-7

DOI
10.1109/CRC50527.2021.9392627

View more

2021 3rd International Cyber Resilience Conference, CRC 2021 • 29 January 2021 • Article number 9392627 • 3rd International Cyber Resilience Conference, CRC 2021, Virtual, Langkawi Island, 29 January 2021 - 31 January 2021, 168321

Intrusion Detection on the In - Vehicle Network Using Machine Learning

Sharmin S., Mansor H.

Save all to author list

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

Abstract

Author keywords

Indexed keywords

SciVal Topics

Metrics

Funding details

Abstract

Controller Area Network (CAN) is a protocol for the in - vehicle network that connects microcontrollers called Electronic Control Units (ECUs) and other components in a vehicle so that they may communicate among themselves and control the operations of the vehicle . The CAN protocol was initially not designed with security in mind, but as modern vehicles are increasingly becoming connected to the outside world through wired and wireless interfaces, the CAN bus has become susceptible to intrusions and attacks such as message injection, replay attacks, denial of service (DoS) attacks, and eavesdropping. This paper presents an intrusion detection method based on the Isolation Forest (iForest) algorithm that detects message insertion attacks using message timing information. The resulting intrusion detection system benefits from the linear time complexity and low memory requirement of the iForest algorithm, as well as the ability to train the classifier with only a small sample of normal CAN traffic. The usage of only timing information for intrusion detection makes it a vehicle -agnostic method that does not rely on the message content, which is often proprietary and confidential information. The intrusion detection system was trained with normal CAN traffic trace and tested with two spoof attack CAN datasets. The high values obtained for the Area Under Curve (AUC) measure in the two cases, 0.966 and 0.974, indicated the effectiveness of this approach for intrusion detection . © 2021 IEEE.

Author keywords
automotive; CAN; intrusion detection ; isolation forest; message insertion

Engineering controlled terms
Control system synthesis; Controllers; Denial-of-service attack; Machine learning ; Vehicles

Engineering uncontrolled terms
Confidential information; Controller area network ; Electronic control units; In - vehicle networks; Intrusion detection method; Intrusion Detection Systems; Linear time complexity; Wired and wireless

Engineering main heading
Intrusion detection

Topic name
Connected Vehicles; CAN Bus; Electronic Control

Prominence percentile
97.726

PlumX metrics

Captures

Readers

Cited by 0 documents

Inform me when this document is cited in Scopus:

Set citation alert >

Related documents

An Enhanced Method for Reverse Engineering CAN Data Payload
Choi, W. , Lee, S. , Joo, K.
(2021) IEEE Transactions on Vehicular Technology

Detection of Injection Attacks in Compressed CAN Traffic Logs
Gazdag, A. , Neubrandt, D. , Buttyán, L.
(2019) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

Intrusion detection system for CAN using simple neural networks
Laufenberg, J. , Kropf, T. , Bringmann, O.
(2020) 30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM 2020

View all related documents based on references

Find more related documents in Scopus based on:

Authors > Keywords >

View PlumX details>

Funding sponsor	Funding number	Acronym
Ministry of Higher Education, Malaysia	RACER19-006-0006	MOHE

See opportunities by MOHE ↗

Funding text
ACKNOWLEDGMENT The work presented in this paper is supported by the Fundamental Research Grant Scheme for Research Acculturation of Early Career Researchers (FRGS-RACER) from the Ministry of Education Malaysia, no. RACER19-006-0006.

References (23)

View in search results format >

□ All | Export | Print | E-mail | Save to PDF | Create bibliography

□ 1 Young, C., Zambreno, J., Olufowobi, H., Bloom, G.
Survey of automotive controller area network intrusion detection systems (Open Access)

(2019) *IEEE Design and Test*, 36 (6), art. no. 8640808, pp. 48-55. Cited 17 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/RecentIssue.jsp?punumber=6221038
doi: 10.1109/MDAT.2019.2899062

View at Publisher

□ 2 Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., (...), Savage, S.
Experimental security analysis of a modern automobile (Open Access)

(2010) *Proceedings - IEEE Symposium on Security and Privacy*, art. no. 5504804, pp. 447-462. Cited 1014 times.
ISBN: 978-076954035-1
doi: 10.1109/SP.2010.34

View at Publisher

□ 3 Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., (...), Kohno, T.
Comprehensive experimental analyses of automotive attack surfaces

(2011) *Proceedings of the 20th USENIX Security Symposium*, pp. 77-92. Cited 802 times.
ISBN: 978-193197187-4

□ 4 Miller, C., Valasek, C.
Remote exploitation of an unaltered passenger vehicle
(2015) *White Pap. Black Hat Us Conf.*. Cited 496 times.

□ 5 Miller, C., Valasek, C.
Adventures in automotive networks and control units
(2013) *Def Con 21*, p. 99. Cited 259 times.

□ 6 Bozdal, M., Samie, M., Jennions, I.
A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions (Open Access)

(2019) *Proceedings - 2018 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2018*, art. no. 8658720, pp. 201-205. Cited 13 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/mostRecentIssue.jsp?punumber=8649565
ISBN: 978-153864904-6
doi: 10.1109/iCCECOME.2018.8658720

View at Publisher

□ 7 Avatefipour, O., Malik, H.
(2018) *State-of-the-Art Survey on In-Vehicle Network Communication (CAN-Bus) Security and Vulnerabilities*. Cited 26 times.

□ 8 Tomlinson, A., Bryans, J., Shaikh, S.A.
Towards viable intrusion detection methods for the automotive controller area network
(2018) *Proc. 2nd Acm Comput. Sci. Cars Symp.*, pp. 1-9. Cited 13 times.

□ 9 Mansor, H., Markantonakis, K., Akram, R.N., Mayes, K., Gurulian, I.
Log your car: The non-invasive vehicle forensics

(2016) *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Processing with Applications, IEEE TrustCom/BigDataSE/ISPA 2016*, art. no. 7847047, pp. 974-982. Cited 17 times.
ISBN: 978-150903205-1
doi: 10.1109/TrustCom.2016.0164

View at Publisher

□ 10 Marchetti, M., Stabili, D.
READ: Reverse engineering of automotive data frames

(2019) *IEEE Transactions on Information Forensics and Security*, 14 (4), art. no. 8466914, pp. 1083-1097. Cited 26 times.
http://www.ieee.org/products/onlinepubs/news/0705_02.html#5
doi: 10.1109/TIFS.2018.2870826

View at Publisher

□ 11 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 2016 - Proceedings*, art. no. 7952095, pp. 176-180. Cited 31 times.
ISBN: 978-150903407-9
doi: 10.1109/STA.2016.7952095

View at Publisher

□ 12 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 (Open Access)

(2017) *ACM International Conference Proceeding Series*, art. no. a11. Cited 42 times.
http://portal.acm.org.ezlib.iium.edu.my/
ISBN: 978-145034855-3
doi: 10.1145/3064814.3064816

View at Publisher

□ 13 Song, H.M., Kim, H.R., Kim, H.K.
Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network

(2016) *International Conference on Information Networking*, 2016-March, art. no. 7427089, pp. 63-68. Cited 175 times.
http://www.icoin.org/
ISBN: 978-150901724-9
doi: 10.1109/ICOIN.2016.7427089

View at Publisher

□ 14 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 (Open Access)

(2019) *AutoSec 2019 - Proceedings of the ACM Workshop on Automotive Cybersecurity, co-located with CODASPY 2019*, pp. 25-30. Cited 6 times.
http://dl.acm.org.ezlib.iium.edu.my/citation.cfm?id=3309171
ISBN: 978-145036180-4
doi: 10.1145/3309171.3309178

View at Publisher

□ 15 Marchetti, M., Stabili, D.

Anomaly detection of CAN bus messages through analysis of ID sequences (Open Access)

(2017) *IEEE Intelligent Vehicles Symposium, Proceedings*, art. no. 7995934, pp. 1577-1583. Cited 74 times.
ISBN: 978-150904804-5
doi: 10.1109/IVS.2017.7995934

View at Publisher

□ 16 Tomlinson, A., Bryans, J., Shaikh, S.A.

Using a one-class compound classifier to detect in-vehicle network attacks

(2018) *GECCO 2018 Companion - Proceedings of the 2018 Genetic and Evolutionary Computation Conference Companion*, pp. 1926-1929. Cited 8 times.
http://dl.acm.org.ezlib.iium.edu.my/citation.cfm?id=3205651
ISBN: 978-145035764-7
doi: 10.1145/3205651.3208223

View at Publisher

□ 17 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 2015*, art. no. 7420322, pp. 45-49. Cited 103 times.
ISBN: 978-190832058-2
doi: 10.1109/WCICSS.2015.7420322

View at Publisher

□ 18 Weber, M.
Hybrid anomaly detection for automotive CAN communication
(2018) *Embed. Real Time Softw. Syst. ERTS2*. Cited 13 times.

□ 19 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 (Open Access)

(2019) *IEEE Access*, 7, art. no. 2937576, pp. 127580-127592. Cited 29 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2019.2937576

View at Publisher

□ 20 Liu, F.T., Ting, K.M., Zhou, Z.-H.

Isolation forest

(2008) *Proceedings - IEEE International Conference on Data Mining, ICDM*, art. no. 4781136, pp. 413-422. Cited 1301 times.
ISBN: 978-076953502-9
doi: 10.1109/ICDM.2008.17

View at Publisher

□ 21 Seo, E., Song, H.M., Kim, H.K.

GIDS: GAN based Intrusion Detection System for In-Vehicle Network (Open Access)

(2018) *2018 16th Annual Conference on Privacy, Security and Trust, PST 2018*, art. no. 8514157. Cited 58 times.
http://ieeexplore.ieee.org.ezlib.iium.edu.my/xpl/mostRecentIssue.jsp?punumber=8498146
ISBN: 978-153867493-2
doi: 10.1109/PST.2018.8514157

View at Publisher

□ 22 Cortes, D.
(2020) *Isotree: Isolation-Based Outlier Detection.*

□ 23 Ding, Z., Fei, M.

An anomaly detection approach based on isolation forest algorithm for streaming data using sliding window

(2013) *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 3 (PART 1), pp. 12-17. Cited 84 times.
http://www.ifac-papersonline.net/browser?browse=c
ISBN: 978-390282345-8
doi: 10.3182/20130902-3-CN-3020.00044

View at Publisher

< Back to results | < Previous 8 of 39 Next >

^ Top of page

About Scopus

What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters

Language

日本語に切り替える
切换到简体中文
切換到繁體中文
Русский язык

Customer Service

Help
Contact us

ELSEVIER

Terms and conditions ↗ Privacy policy ↗

Copyright © Elsevier B.V ↗. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.
We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

RELX