IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 8, August 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208028 |

Anomaly Detection Driven Model to Secure Heterogeneous Electric Vehicle Communication Using Controller Area Networks

Dr.D.J. Samathanaidu, T .Reddy Prasanna

Principal, Annamacharya PG College of Computer Studies, Rajampet, India

MCA Student, Department of MCA, Annamacharya PG College of Computer Studies, Rajampet, India

ABSTRACT : In this paper ,Electric vehicles frequently depend heavily on in-vehicle or between-vehicle connectivity, which can have major implications for the system. This essay will focus on the cyber attack on electric vehicles and suggest a secure and trustworthy intelligent structure to prevent hackers from entering The vehicles. The suggested design is built using an enhanced based on the support vector machine model for anomaly detection bus protocol for the controller area network (CAN). As a way to enhance the models capability for quick malicious attack identification and avoidance ,Using the social spider optimaisation (SSO) algorithm, a new optimization algorithm designed that will support the offline training procedure. Also, a two-The algorithm's search ability improves and a stage modification strategy is suggested to prevent early convergence. And last but not least, strong performance is shown by the simulation results using real data sets .The proposed models dependability and security against denial-of-service hacking in electric vehicles (DoS).

I. INTRODUCTION

Technically speaking, automobiles are made up of numerous electronic control units (ECUs) that are controlled by various software programs. All of a vehicle's fitted sensors will transmit their data to the ECU, which will process it and deliver the necessary commands to the appropriate actuators. CAN, LIN, FlexRay, or MOST are a few examples of network protocols that may be used in a very sophisticated hardware-software data transfer process.The CAN bus is the most frequently utilized of these protocols, not only in automobiles but also in agricultural equipment, medical gadgets, and other applications due to its tremendous capability and promising attributes. One of the main advantages of the CAN bus standard is that it permits data transfers at up to 1Mbps, reduces the amount of wiring required in the device, saves time and money due to simple wiring, automatically transmits missing messages, and has error detection capabilities. Unfortunately, because it was created at a time when automobiles were virtually isolated, the CAN bus protocol has some security flaws in the brand-new dynamic setting of smart grids.

To prevent attacks of various denial-of-service or error flag in the vehicle types, an algorithmic approach is applied in. In order to execute an attestation process in the system, it is advised to designate one ECU as the master ECU during the vehicle's construction stage. In order to prevent cyber attack directives from reaching the CAN bus, a firewall is added for the car in to sit between the CAN bus and the communicative system. In, it is suggested to use an intrusion detection system based On the traffic entropy of the CAN bus's in-vehicle network communication system . In, an approach to anomaly detection is created that can find problems of both known and unknown types without the need to set expert parameters. In order to provide electric vehicles with a potent anomaly detection and avoidance arrangement, this work attempts to present an intelligent and extremely secure solution. To prevent any malicious behavior in the vehicle, the suggested technique is developed with support vector machines and the idea of one-class detection systems.

II. RELATED WORK

The last sections were mainly focusing on the proposed model, the theories and backgrounds. In this section, the

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208028 |

performance of the proposed model is examined using the experimental data gathered from an electric car. This paper assesses the DoS attack since it is focusing on the vehicle intra-communication within which DoS has a high significance among different attacks. In the DoS attack, the hacker attempts to prevent legitimate users (driver) from accessing the service.

Considering the fact that vehicles are mobile devices, DoS attack is so dangerous (and thus important) in vehicles since it can make severe car crash or losses. Examples of hackings achieved through the DoS attack in the vehicles are activating the brakes while the vehicle is in motion, turning the steering wheel to the left/right suddenly, turning off the engine, unlocking a door, etc. According to the analysis from the recorded CAN traffic during a normal driving time of 10-minute, each message frame with a specific ID has some unique frequencies which can be learned by the proposed anomaly detection model.

AUTHORS

George Loukas, Eirini Karapistoli, Emmanouil Panaousis, Panagiotis Sarigiannidis, Anatolij Bezemskij, and Tuan Vuong

There is an increasing demand for intrusion detection methods that can help with defense against such dangers as the threat of cyber and cyber-physical attacks on cars, drones, ships, driverless pods, and other vehicles. Vehicles typically have finite computing power and energy resources. Consequently, these restrictions must be followed by any security provision. In contrast to what is seen in traditional computing systems, attacks on automobiles are extremely infrequent, making knowledge-based intrusion detection systems less useful than those based on behaviour. Additionally , the implementation and design of a vehicle can vary greatly between different types or manufacturers, which can result in intrusion detection designs that are vehicle-specific. Furthermore, a vehicle's capacity for autonomous movement practically defines it.

III.METHODOLOGY

Describes the core components of the proposed methodology, including:

1. Problem Definition: Define the scope of the project, including the objectives of the anomaly detection model. Specify the types of anomalies you want to detect, such as unauthorized access, data manipulation, or intrusion attempts.

2. Data Collection: Collect a diverse and comprehensive dataset of CAN messages from various types of electric vehicles, including different makes, models, and communication patterns. This dataset should include both normal and anomalous (attack or fault-injected) scenarios to facilitate training and testing.

3. Feature Extraction: Extract relevant features from the CAN messages to represent the communication patterns. These features can include message IDs, timestamps, data payloads, frequency of messages, and communication intervals.

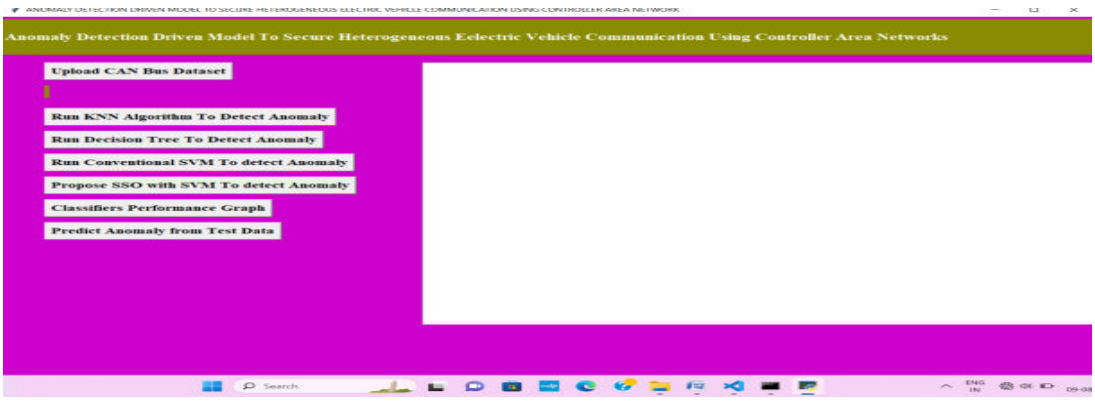
4. Data Preprocessing: Clean the dataset by handling missing values, outliers, and noise. Normalize or standardize the extracted features to ensure consistent scales for better model convergence.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

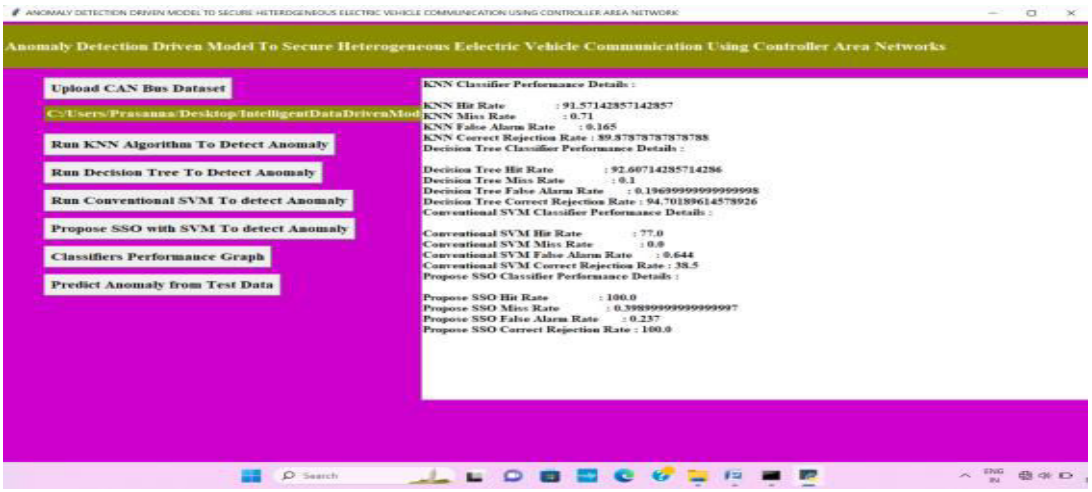
|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208028 |

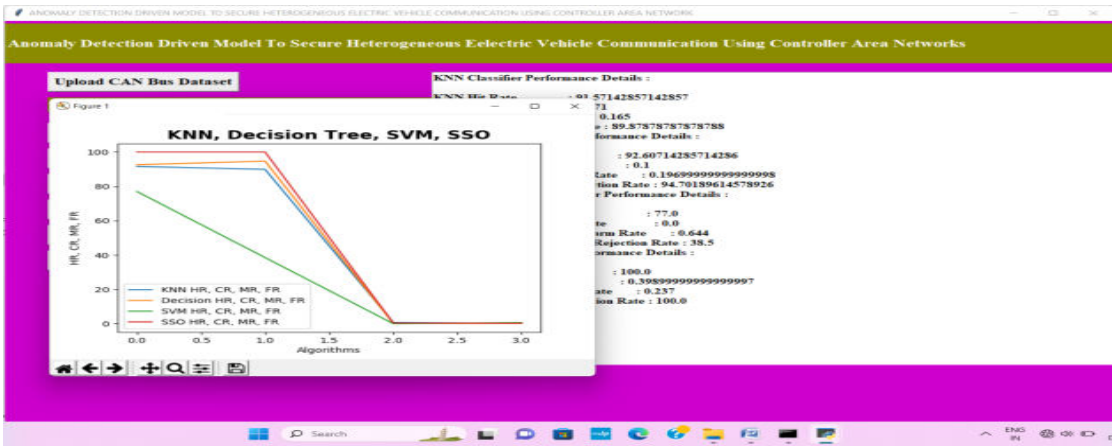
IV. EXPERIMENTALRESULTS



Screen 1: upload CAN Bus dataset



Screen 2 : SSO with SVM to detect anomaly

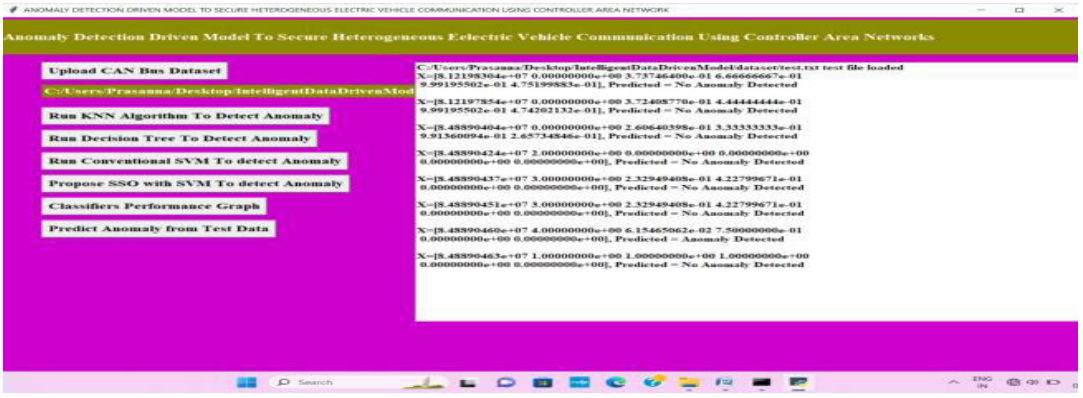


Screen 3: Graph to the Results

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208028 |



Screen 4: predict anomaly from dataset

V. CONCLUSION

This paper proposed a novel intelligent and secured anomaly detection model for cyber attack detection and avoidance in the electric vehicles. An enhanced support vector machine model reinforced by the MSSO algorithm serves as the foundation for the suggested model's construction. From a cyber security standpoint, the suggested model might effectively identify malicious actions while allowing the trustworthy message frames to be broadcast in the CAN protocol.. The high HR% and FR% indices prove the true positive and true negative decisions made by the proposed model. Regarding the MR% and CR% indices, the very low values which most of them are around the upper and lower bounds of the message frame frequency, show the highly trustable performance of this model. The authors will assess the effect of other cyber attacks on the performance of different anomaly detection models in the future works

REFERENCES

[1] A. Monot ; N. Navet ; B. Bavoux ; F. Simonot-Lion, “Multisource Software on Multicore Automotive ECUs—Combining Runnable Sequencing With Task Scheduling”, IEEE Trans. Industrial Electronics, vol. 59, no. 10. Pp. 3934-3942, 2012.

[2] T.Y. Moon; S.H. Seo; J.H. Kim; S.H. Hwang; J. Wook Jeon, “Gateway system with diagnostic function for LIN, CAN and FlexRay”, 2007 International Conference on Control, Automation and Systems, pp. 2844 – 2849, 2007.

[3] B. Groza; S. Murvay, “Efficient Protocols for Secure Broadcast in Controller Area Networks”, IEEE Trans. Industrial Informatics, vol. 9, no. 4, pp. 2034-2042, 2013.

[4] B. Mohandes, R. Al Hammadi, W. Sanusi, T. Mezher, S. El Khatib, “Advancing cyber–physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles”, International Journal of Critical Infrastructure Protection, vol. 23, pp. 33-48, 2018.

[5] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, T. Vuong, A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, Ad Hoc Networks, vol. 84, pp. 124-147, 2019.

[6] Hoppe T, Kiltz S, Dittmann J. Security threats to automotive can networks. practical examples and selected short-term countermeasures. Reliab Eng Syst Saf vol. 96, no. 1, pp. 11–25, 2011.

[7] Schulze S, Pukall M, Saake G, Hoppe T, Dittmann J. On the need of data management in automotive systems. In: BTW, vol. 144; pp. 217–26, 2009.

[8] Ling C, Feng D. An algorithm for detection of malicious messages on can buses. 2012 national conference on information technology and computer science. Atlantis Press; 2012.

[9] Oguma H, Yoshioka X, Nishikawa M, Shigetomi R, Otsuka A, Imai H. New attestation based security architecture for in-vehicle communication. In: Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE; pp. 1–6, 2008.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 8, August 2023 ||

| DOI:10.15680/IJIRSET.2023.1208028 |

[10] L. Pan, X. Zheng, H. X. Chen, T. Luan, L. Batten, "Cyber security attacks to modern vehicular systems", Journal of Information Security and Applications, vol. 36, pp. 90-100, October 2017.

[11] Kang, M. J., & Kang, J. W., "Intrusion detection system using deep neural network for in-vehicle network security", PloS one, vol. 11, no. 6, e0155781, 2016.

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

[13] F. Zhu, J. Yang, C. Gao, S. Xu, T. Yin, "A weighted oneclass support vector machine", Neurocomputing, vol. 189, pp. 1-10, 12 May 2016.

[14] Y. Zhou, Y. Zhou, Q. Luo, M. Abdel-Basset, "A simplex method-based social spider optimization algorithm for clustering analysis', Engineering Applications of Artificial Intelligence, vol. 64, pp. 67-82, 2017. [15] G. De La Torre, P.Rad, K.K.Raymond Choo, "Driverless vehicle security: Challenges and future research opportun ities", Future Generation Computer Systems, In press, corrected proof, Available online 11 January 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details