An Intelligent Data-Driven Model to Secure Intra vehicle Communications Based on Machine Learning

Jairam sujith yarram¹, B Veerendra²
¹PG student, DEPARTMENT C.S.E, Kakinada Institute of Technology and Science, Kakinada,AP
²Associate Professor,DEPARTMENT C.S.E, Kakinada Institute of Technology and Science, Kakinada,AP

ABSTRACT

Electric vehicles' heavy reliance on in-vehicle or between-vehicle connectivity can have serious effects on the system. This study will focus on cyber attacks against electric vehicles and suggest a secure and trustworthy intelligent architecture to prevent hackers from breaking into the cars. The proposed model is built using a modified support vector machine model for detecting anomalies based on the CAN bus protocol. A novel optimization method based on the social spider (SSO) algorithm has been developed to enhance the model's capabilities for quick harmful attack identification and avoidance. This algorithm will support the offline training process. Additionally, a two-stage modification approach is suggested to improve the algorithm's search capability and untimely convergence. Last but not least, the simulation results on the actual data sets demonstrate the excellent performance, dependability, and security of the suggested model against DoS hacking in the electric vehicles.

Keywords: Electric vehicles, DoS hacking, CAN bus protocol, social spider (SSO)

1 INTRODUCTION

Technically speaking, automobiles are made up of numerous electronic control units (ECUs) that are controlled by various software programmes. Every sensor that is put in a vehicle will transmit data to the ECU, which will process the data and send the necessary commands to the appropriate actuators [1]. Through the use of several network protocols, such CAN, LIN, FlexRay, or MOST [2], such a very complex hardware-software data transfer process may take place. Due to its great capability and promising qualities, CAN bus is the most widely used of these protocols, not only in automobiles but also in agricultural equipment, medical devices, and other applications. Allowing data transfer rates of up to 1Mbps is one of the key benefits of the CAN bus standard. Because of the device's simple wiring, ability to automatically retransmit lost messages, and error detection capability, wiring can be reduced, saving money and time [3]. Unfortunately, the CAN bus protocol suffers from some security issues in the new dynamic environment of smart grids because it was developed at a time when vehicles were essentially isolated. This will encourage hackers to target electric cars and send harmful messages into their systems through the ECU. To evaluate the vulnerabilities of electric vehicles and potential side effects that could ultimately affect the power grid, some cyber intrusion scenarios are modelled and applied on them in [4], [5] describes the development of a new classification system for vehicle-based cyber intrusion detection. This will make it easier for the driver to recognise an attack and come to a complete stop. To prevent any cyber infiltration, the authors of [7] propose that all CAN messages travel through a data management system. [8] uses an algorithmic solution to thwart attacks on the vehicle's error flag or denial-of-service systems. In order to run an attestation process in the system, it is advised in [9] to designate one ECU as the master ECU during the vehicle's manufacturing stage. In [10], a firewall is provided for the car to sit between the communicating system and the CAN bus and prevent directives from a cyberattack from reaching the CAN bus. In [11], it is suggested to use an intrusion detection system based on the traffic entropy of the CAN bus' in-vehicle network communication system. Without the need to define expert settings, an anomaly detection approach that can identify flaws of both known and unknown types is created in [12].

2. RELATED WORK

Momdooh is an assistant professor at the Electrical Engineering Department at King Saud University. He is also the Instructor of the Saudi Electricity Company Chair in Power Scheme Consistency and Safety. Dr. received his Ph.D. from McMaster University, Canada in 2007. As part of his work at King Saud University, he has been intricate in research and improvement activities in the areas of maintainable energy technologies, smart grid and renewable energy implementation,
dependability and security charge of power supply systems, design and operation of spreading system, application of artificial intelligence in power system plan, and load management. Ali M. Eltamaly (PhD - 2000) is a occupied professor at King Saud University and Mansoura university, Egypt. He expected the B.Sc. and M.Sc. Egypt in 1992 and 1996, correspondingly. He received his Ph.D. Degree in Electrical Engineering after Texas A&M University in 200. His current research comforts include renewable energy, smart grid, power electronics, motor drives, power quality, artificial intelligence, evolutionary and experiential optimization techniques, and circulated generation. He published 20 book and book chapters and he has authored or coauthored more than 150 refereed journal and session papers. He distributed number of patents in USA patent office. He has managed a number of M.S. and PhD ideas, operated on number of National/International technical projects. He got extricate professor award for scientific excellence, Egyptian supreme council of Universities, Egypt, June, 2017 and he has awarded many prizes in different universities in Egypt and Saudi Arabia. He is take part as an editor and subordinate editors in many international journals and chaired many international assemblies’ sessions. He acknowledged the B.Sc. and M.Sc. gradations from Minia University, Minia, Egypt in 2006 and 2010. He acknowledged the Ph.D. gradation from King Saud University, Riyadh, Saudi Arabia in 2016. He joined the Department of Electrical Engineering, Fuzhou University, China as a Postdoctoral Investigation related in 2018. He is presently a talent member in the Department of Electrical Engineering, College of Engineering, Minia University, Minia, Egypt, since 2008. Using an X-Y fused Kohonen network and the k-means algorithm, Barletta et al. [11] suggested a distance-based IDS for CAN intrusion detection (XYF-K). On the CAN-intrusion dataset, the suggested technique exhibits good accuracy, but its main drawback is its high computational complexity. Using the adaptive cumulative sum (CUSUM) technique, Olufowobi et al. [12] proposed an anomaly-based IDS for CAN attack detection. Based on statistical changes, this technique can ef ficiently identify intrusions but takes good amount of execution time. Song et al. [13] suggested a lightweight IDS based on a time interval analysis (TIA) of CAN communications for in vehicle networks. [14] proposes using a variety of in-vehicle sensors to verify message formality, position, data range, data plausibility, and other factors. It does not, however, have a working implementation. Loukas et al. [15] suggested and analyzed the performance of multiple machine learning clas sifiers in an -based intrusion detection system for in-vehicle network systems. They deployed robotic cars and conducted their experiment by introducing threats into a cloud-based system. They declared that is suitable for detecting vehicular attacks after achieving an overall accuracy of 86.9%. Using deep belief network (DBN) and decision tree (DT) algorithms, Aloqaily et al. [16] suggested a network IDS for IoV and connected cars. On the NSL-KDD dataset, this approach has a good level of accuracy. Schmidt et al. [17] used the knot flow classification (KFC) approach to propose a spline-based IDS for vehicular networks and the NSL-KDD dataset to represent vehicle networks for model validation. However, low latency was not achieved by this model. The clock-based IDS suggested in [18] detects anomalies and fingerprints ECUs by taking advantage of the periodic nature of many CAN signals. Despite their lightweight, these time-interval techniques are ineffective against attacks involving aperiodic messages.

3 Implementation Study
The most popular protocol used by automakers for communications in electric vehicle units with a high number of components, up to 500 million chips, is the CAN standard. Due to its construction, the CAN's resilience and noise resistance level are considered adequate in the automotive industry. Unfortunately, CAN bus protocols do not provide secrecy and authentication to CAN data frames, opening the door for hackers to compromise the vehicle's electronic system via wired or wireless means. In the wired method, the OBD-II maintenance port, which is typically found beneath the steering in most automobiles, is used to interact with the CAN system. Although the primary purpose of this port is to be utilised for engine and vehicle maintenance diagnostics, However, it will enable hackers to intercept CAN packets using a straightforward scanning tool. From this point, using ECOM API like CANReceiveMessage and CANTransmitMessage [10] makes it simple to read and write traffic in the CAN bus. Even though the penetration point in a wireless attack is not OBD-II, the cyberattack still targets the ECU. The car must be connected to a malicious WIFI hotspot in the majority of wireless hacking penetration sites, albeit they can vary. Additionally, keyless vehicles allow for the reverse engineering of the transponder's security system. The study identifies various flaws in the cipher’s and authentication protocol's designs, as well as in their implementation. Other wireless entry points to automobiles include "Internet, smart keys, add-on technologies, entertainment systems (gaming)," and "wireless link between sensors and ECUs such as TPMS system.".
The proposed model, the theories, and the context were the key topics of the last parts. This section uses experimental data from an electric automobile to evaluate the performance of the suggested model. Since this work is concentrating on the vehicle intra-communication, where DoS has a great significance among many attacks, it evaluates the DoS attack. The hacker aims to block genuine users (the driver) from using the service during the DoS assault. Given that vehicles are mobile devices, DoS attack is particularly harmful (and crucial) in vehicles because it might result in serious auto accidents or financial losses. Examples of hacks carried out by a DoS attack on a vehicle include locking or unlocking a door, abruptly twisting the steering wheel to the left or right, applying the brakes while the car is moving, and more. The suggested anomaly detection model may be taught the specific frequencies that each message frame with a certain ID has by analysing the recorded CAN data during a regular driving time of 10 minutes. A list of CAN bus identities and frequencies is presented in Table II. To ensure that our model is learning every ID number that could possibly exist, we conducted a thorough trace analysis. Because most CAN communications are periodic, it was discovered after recording the traffic log and using the trace analysis that a 10-min driving scenario will capture the majority of the messages that are occurring often. As a result, the generated model may be seen as a proof-of-concept that demonstrates the suggested anomaly detection model’s ability to recognise patterns in CAN signals and distinguish between normal and anomalous behaviour during testing. The CAN traffic file includes the following criteria to create a realistic test environment: After briefly coming to a stop, the engine ignition was turned on, and the gear was then engaged in “D” mode. The car is then driven on a public street for around 8 minutes. During the trip, the brake pedal is also depressed numerous times. The vehicle is then stopped, and the gear mode is changed to “R” so that the driver can execute a slight backwards turn and perform a parking manoeuvre. Finally, the gear shifts to “P” mode, causing the car to stop and stay there for a few seconds until the engine is shut off.

5 METHODOLOGIES

1. Click the “Upload CAN Bus Dataset” button to send the dataset.

2. Clicking the “Run KNN Algorithm To Detect Anomaly” button will construct a KNN classifier, train a model to detect anomalies, and assess the effectiveness of the model using 4 indices.

3. Execute a standard SVM Anomaly button to assess the performance of a standard SVM.

4. Offer SSO and SVM In order to run SSO with SVM classifier and assess its performance, click the “identify anomaly” button.

5. Click the icon to view a performance comparison chart for all classifiers.

6. Click the button labelled “Predict Anomaly from Test Data” to submit test data.
Fig. 1: propose Architecture

6 RESULTS AND DISCUSSION

Fig. 2: In above screen click on ‘Upload CAN Bus Dataset’ button and upload dataset
Fig 3: In above screen I am uploading ‘CAN.csv’ dataset and after uploading dataset will get below screen.

Fig 4: In above screen we got 4 indices values for KNN algorithm and now click on ‘Run Decision Tree To Detect Anomaly’ button to evaluate decision tree performance.
Fig 5: In above screen we got decision tree data and now click on ‘Run Conventional SVM To detect Anomaly’ button to evaluate conventional SVM performance.

Fig 6: In above screen we got SVM performance data and now click on ‘Propose SSO with SVM To detect Anomaly’ button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working from first window only).

Fig 7: In above screen we got SVM performance data and now click on ‘Propose SSO with SVM To detect Anomaly’ button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working from first window only).
Fig 8: In above screen for SSO we got performance metric as 100% and MR and FR is not mandatory so we can ignore as said in paper. Now click on ‘Classifiers Performance Graph’ button to get performance graph between all classifiers.

Fig 9: In above graph propose SSO has given high performance compare to other algorithms. In above graph y-axis represents HR, MR, FR and CR values. Now click on ‘Predict Anomaly from Test Data’ button to upload test data and predict it label.
In above screen I am uploading ‘test.txt’ file and now click on ‘Open’ button to predict uploaded test file class label.

We can see submitted test data and its expected class label in the text area of the screen above. Except for one entry, all records include typical packet data. So, using machine learning methods, we can analyse packets and stop processing them if they include an attack.

7. CONCLUSION AND FUTURE WORK
In order to detect and prevent cyberattacks in electric vehicles, this article developed a brand-new, intelligent, and secure anomaly detection approach. The suggested model is built using an enhanced support vector machine model that is strengthened by the MSSO technique. From the perspective of cyber security, the suggested model was able to identify harmful actions while allowing the trustworthy message frames to be broadcast in the CAN protocol. The high HR% and FR% indices demonstrate the suggested model's true positive and true negative decisions. The extremely low values for the MR% and CR% indices, the majority of which are located at the upper and lower boundaries of the message frame.
frequency, demonstrate the model’s highly reliable performance. In upcoming publications, the authors will evaluate the impact of additional cyberattacks on the effectiveness of various anomaly detection models.

7. 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 CHAPTER 10 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.
[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.