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

Dr.Putta.Srivani[1], Syeda Sufiya Rana[2], Dereddy Tejeswani[3],

K.Noor E Afshan[4], Chukka Sathvika[5]

[1]Professor, Department of CSE(CS), MallaReddy Engineering College for Women, Hyderabad, TS, India.

Email:pulla.srivani@gmail.com

[2,3,4,5]UG Students, Department of CSE(CS), MallaReddy Engineering College for Women, Hyderabad, TS, India.

ABSTARCT :

The high relying of electric vehicles on either invehicle or between-vehicle communications can cause big issues in the system. This paper is going to mainly address the cyber attack in electric vehicles and propose a secured and reliable intelligent framework to avoid hackers from penetration into the vehicles. The proposed model is constructed based on an improved support vector machine model for anomaly detection based on the controller area network (CAN) bus protocol. In order to improve the capabilities of the model for fast malicious attack detection and avoidance, a new optimization algorithm based on social spider (SSO) algorithm is developed which will reinforce the training process at offline. Also, a two-stage modification method is proposed to increase the search ability of the algorithm and avoid premature convergence. Last but not least, the simulation results on the real data sets reveal the high performance, reliability and security of the proposed model against denial-of-service (DoS) hacking in the electric vehicles.

INTRODUCTION :

Technically, vehicles are composed of many hardware modules namely called electronic control units (ECUs) being controlled by different software tools. All sensors installed in a vehicle will send their data to the ECU, where this data are processed and the requiring orders are sent to the relevant actuators [1]. Such a highly complex hardwaresoftware data transfer process may happen through the use of different network protocols such as CAN, LIN, FlexRay or MOST [2]. Among these protocols, CAN bus is the most popular one not only in vehicles, but also in medical apparatuses, agriculture, etc due to its high capability and promising characteristics. Some of the main advantages of the CAN bus standard may be briefly named as allowing up to 1Mbps data rate transfer, reducing the wiring in the device saving cost and time due to the simple wiring, autoretransmission of lost messages and error detection capability [3]. Unfortunately, since CAN bus protocol was devised at a time where vehicles were almost isolated, this standard suffers from some security issues in the new dynamic environment of smart grids. This will motivate the hackers to attack the electric vehicles through the ECU and inject malicious messages into their systems. In [4], some cyber intrusion scenarios are modeled and applied on the electric vehicles to assess their vulnerabilities and possible side effects getting finally into the power grid. In [5], a new classification method is developed for cyber intrusion detection in vehicles. In [6], a data intrusion detection system is developed which can detect the cyber attack based on the CAN bus message frequency increase or CAN message ID misuse. This will help the driver to detect that an attack has happened so to stop the vehicle immediately. In [7], authors suggest that all CAN messages should pass a data management system to avoid any cyber intrusion. In [8], an algorithmic solution is used to stop attacks of types of denial-of-service or error flag in the vehicle. In [9], it is suggested to assign an ECU as the master ECU in the manufacturing stage of the vehicle so to run an attestation process in the system. In [10], a firewall is introduced for the vehicle to sit between the CAN bus and the communicating system and stop the cyber attack commands to the CAN bus. In [11], an intrusion detection system based on the traffic entropy of in-vehicle network communication system of the CAN bus is suggested. In [12], an anomaly detection approach is developed which is capable of detecting faults of known and unknown type without requiring the setting of expert parameters.

This paper aims to propose an intelligent and highly secure method to equip the electric vehicles with a powerful anomaly detection and avoidance mechanism. The proposed method is constructed based on support vector machine and the concept of one-class detection system to avoid any malicious behavior in the vehicle [13]. Here the experimental CAN bus data are used to let the support vector machine learn the normal frequency of the different message frames at different commands. In order to get into the maximum capability of the model, a new optimization algorithm based on social spider optimization (SSO) algorithm is proposed to adjust the SVR setting parameters, properly [14]. Due to the high complexity and nonlinearity of the electric vehicle CAN bus dataset, a new two-stage modification method based on crossover and mutation operators of genetic algorithm is developed which can increase the algorithm population diversity and at the same time avoid premature convergence. The feasibility and satisfying performance of the proposed model are examined using the real datasets gathered from an electric vehicle.

EXISTING SYSTEM :

In electric vehicles, CAN standard is the most widely used protocol by automakers for communications with low cost in the units with a high number of components, up to 500 million chips. In the vehicle industry, the CAN resiliency and noiseresistance level is acceptable owing to its structure. Unfortunately, CAN bus protocols do not offer confidentiality and authentication to CAN data frames so making it possible for hackers to enter the vehicle system, either on a wired or wireless approach. In the wired approach, one can communicate with the CAN bus through the OBD-II maintenance port located under the steering in most vehicles. Although the main idea behind this port is to be used for diagnostics of engine and vehicle maintenance, but it will let hackers take the CAN packets using a simple scanning tool. From this point, it is easy to read and write traffic in the CAN bus with the use of ECOM API such as CANReceiveMessage and CANTransmitMessage [10]. In the wireless attack, the cyber interfere is the same by targeting ECU except that the penetration point is not OBD-II. While the penetration points in the wireless hacking can be different, but in most of them it is required for the car to be connected to a malicious WIFI hotspot. Also, the security mechanism of the transponder can be reverse engineered in the keyless vehicles. The research reveals several weaknesses in the design of the cipher, the authentication protocol and also in their implementation. Some of the other wireless entry points to vehicles can be named as "Wireless connection between sensors and ECUs such as TPMS system", "Add-on technologies, entertainment system (gaming), smart key" and "Internet, smart infrastructures".

DISADVANTAGES OF EXISTING SYSTEM :

1) Less accuracy

2)low Efficiency

PROPOSED SYSTEM :

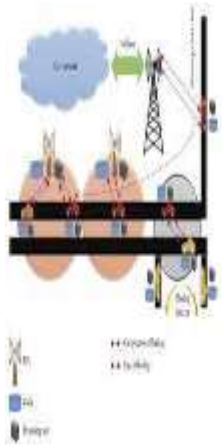
The last sections were mainly focusing on the proposed model, the theories and backgrounds. In this section, the performance of the proposed model is examined using the experimental data gathered from an electric car. This paper assesses the DoS attack since it is focusing on the vehicle intra-communication 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. In Table II, a set of CAN bus identifiers and frequencies is shown. In order to make sure that our model is learning all possible ID numbers, we had a complete trace analysis. Therefore, after capturing the traffic log and implementing the trace analysis, it was realized that a 10-min driving scenario would capture the majority of the messages that are occurring commonly, owing to the fact that most of the CAN messages are periodic. Therefore, the model developed can be regarded as the proof-of-concept that shows the proposed anomaly detection model can learn the existing pattern in the CAN messages to distinguish between normal and anomalous behaviors in the testing phase. In order to make a realistic condition for the driving test, the CAN traffic file covers the following conditions: the engine ignition was turned on and the vehicle remained at a standstill for a few seconds and then the gear was engaged to “D” mode. Then, the vehicle is driven for about 8 minutes at a public street. For several times, the brake pedal is also pressed during the drive. The car is then stopped and the gear mode is changed to “R” to drive backwards a bit and make a parking maneuver. Finally, the gear moves to “P” mode so the vehicle would remain at the standstill for a few seconds and then the engine is turned off.

ADVANTAGES OF PROPOSED SYSTEM :

1) High accuracy

2)High efficiency

SYSTEM ARCHITECTURE :



IMPLEMENTATION:

MODULES:

1. Upload CAN Bus Dataset’ button and upload dataset

2. Run KNN Algorithm To Detect Anomaly’ button to build KNN classifier train model to detect anomaly and evaluate its performance based on 4 indices

3. Run Conventional SVM To detect Anomaly’ button to evaluate conventional SVM performance.

4. Propose SSO with SVM To detect Anomaly’ button to run propose SSO with SVM classifier and evaluate its performance.

5. Classifiers Performance Graph’ button to get performance graph between all classifiers

6. Predict Anomaly from Test Data' button to upload test data and predict it label

Modules Used in Project :-

Tensorflow

TensorFlow is a free and open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google.

TensorFlow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open-source license on November 9, 2015.

Numpy

Numpy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

It is the fundamental package for scientific computing with Python. It contains various features including these important ones:

- A powerful N-dimensional array object
- Sophisticated (broadcasting) functions
- Tools for integrating C/C++ and Fortran code
- Useful linear algebra, Fourier transform, and random number capabilities

Besides its obvious scientific uses, Numpy can also be used as an efficient multi-dimensional container of generic data. Arbitrary data-types can be defined using Numpy which allows Numpy to seamlessly and speedily integrate with a wide variety of databases.

Pandas

Pandas is an open-source Python Library providing high-performance data manipulation and analysis tool using its powerful data structures. Python was majorly used for data munging and preparation. It had very little contribution towards data analysis. Pandas solved this problem. Using Pandas, we can accomplish five typical steps in the processing and analysis of data, regardless of the origin of data load, prepare, manipulate, model, and analyze.

Python with Pandas is used in a wide range of fields including academic and commercial domains including finance, economics, Statistics, analytics, etc.

Matplotlib

Matplotlib is a Python 2D plotting library which produces publication quality figures in a variety of hardcopy formats and interactive environments across platforms. Matplotlib can be used in Python scripts, the Python and IPython shells, the Jupyter Notebook, web application servers, and four graphical user interface toolkits. Matplotlib tries to make easy things easy and hard things possible. You can generate plots, histograms, power spectra, bar charts, error charts, scatter plots, etc., with just a few lines of code. For examples, see the sample plots and thumbnail gallery.

For simple plotting the pyplot module provides a MATLAB-like interface, particularly when combined with IPython. For the power user, you have full control of line styles, font properties, axes properties, etc, via an object oriented interface or via a set of functions familiar to MATLAB users.

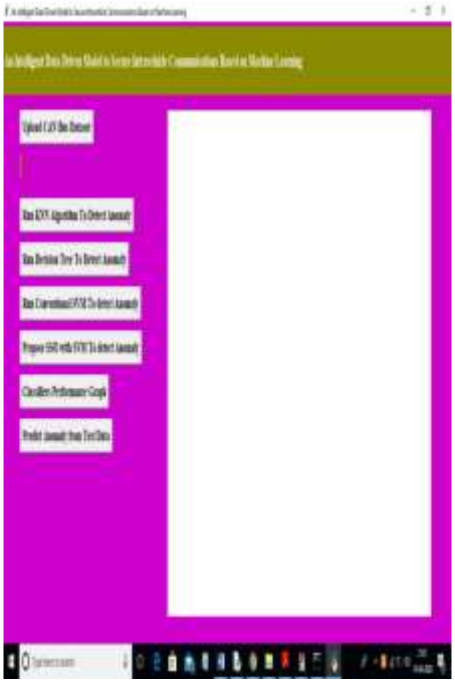
Scikit – learn

Scikit-learn provides a range of supervised and unsupervised learning algorithms via a consistent interface in Python. It is licensed under a permissive simplified BSD license and is distributed under many Linux distributions, encouraging academic and commercial use.

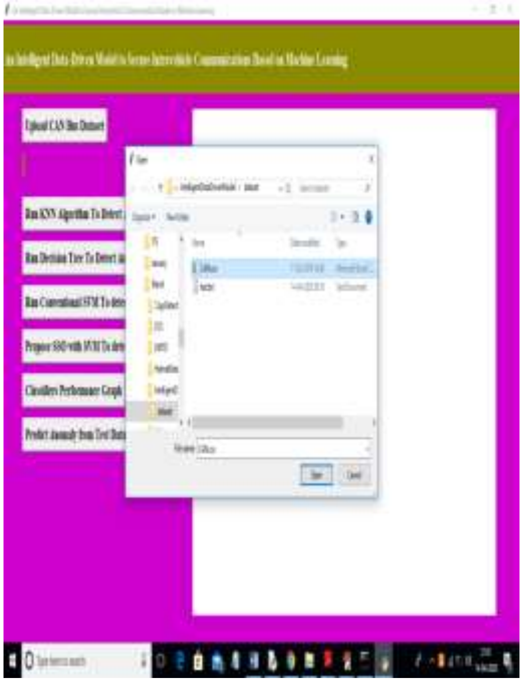
SCREENSHOTS :

Screen shots

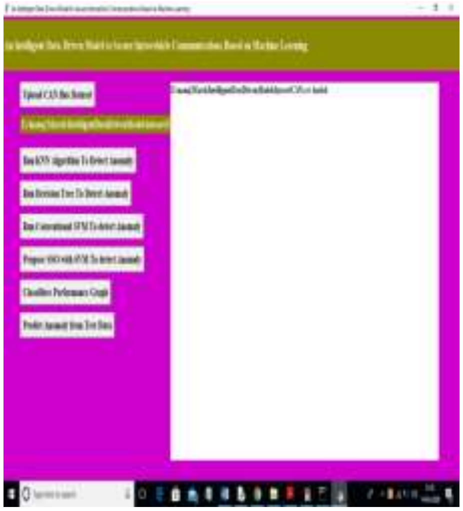
To run project double click on 'run.bat' file to get below screen


An Intelligent Data Driven Model to Secure Intravehicle Communication Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect Anomaly
Run Decision Tree To Detect Anomaly
Run Conventional SVM To detect Anomaly
Propose SSO with SVM To detect Anomaly
Classifiers Performance Graph
Predict Anomaly from Test Data

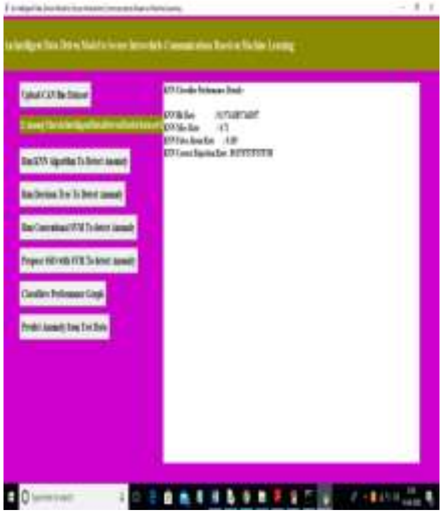
In above screen click on ‘Upload CAN Bus Dataset’ button and upload dataset


An Intelligent Data-Driven Model to Secure Intravehicle Communication Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect
Run Decision Tree To Detect
Run Conventional SVM To dete
Propose SSO with SVM To dete
Classifiers Performance Graph
Predict Anomaly from Test Data
Open
Cancel

In above screen I am uploading ‘CAN.csv’ dataset and after uploading dataset will get below screen

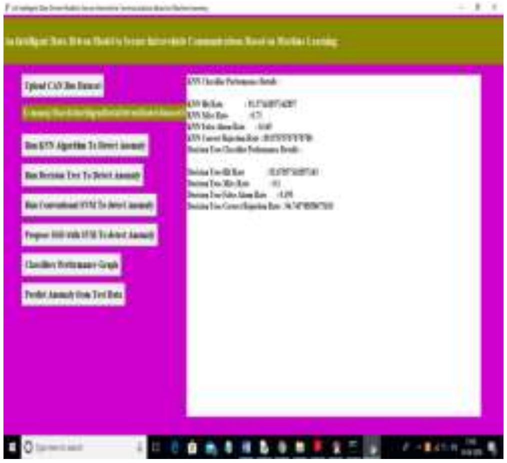

An Intelligent Data-Driven Model to Secure Intravehicle Communication Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect Anomaly
Run Decision Tree To Detect Anomaly
Run Conventional SVM To detect Anomaly
Propose SSO with SVM To detect Anomaly
Classifiers Performance Graph
Predict Anomaly from Test Data

Now click on ‘Run KNN Algorithm To Detect Anomaly’ button to build KNN classifier train model to detect anomaly and evaluate its performance based on 4 indices

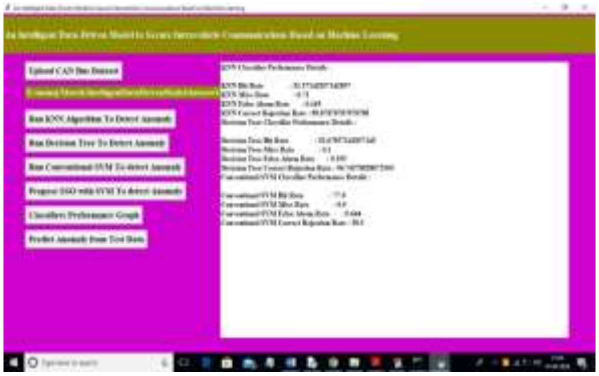

An Intelligent Data-Driven Model to Secure Intravehicle Communication Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect Anomaly
Run Decision Tree To Detect Anomaly
Run Conventional SVM To detect Anomaly
Propose SSO with SVM To detect Anomaly
Classifiers Performance Graph
Predict Anomaly from Test Data

In above screen we got 4 indices values for KNN algorithm and now click on ‘Run Decision Tree To

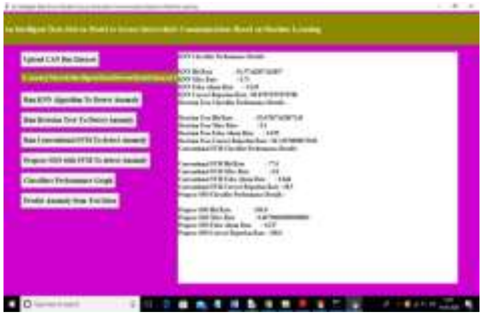
Detect Anomaly' button to evaluate decision tree performance



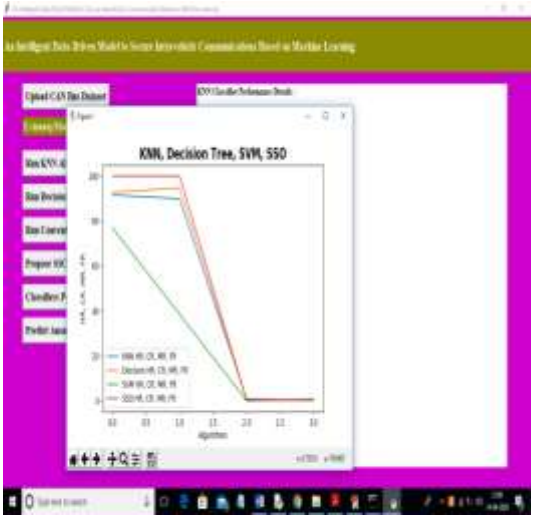
In above screen we got decision tree data and now click on 'Run Conventional SVM To detect Anomaly' button to evaluate conventional SVM performance.



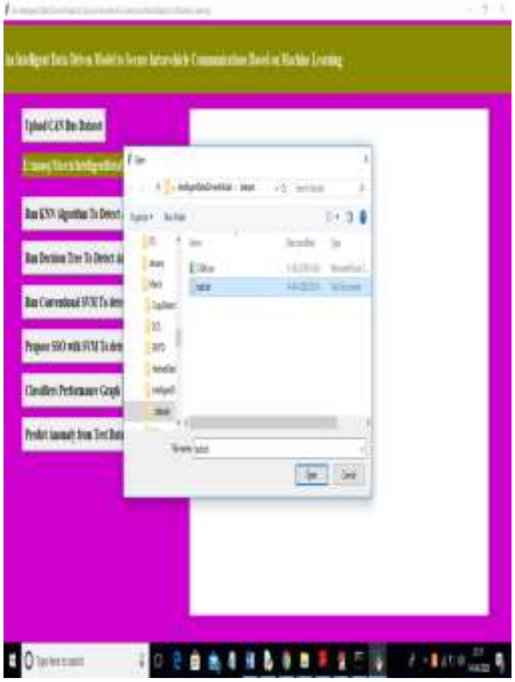
In above screen we got SVM performance data and now click on 'Propose SSO with SVM To detect Anomaly' button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working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



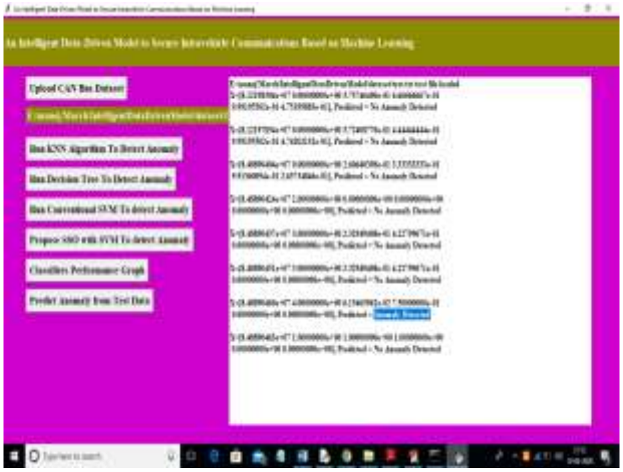
In above screen for SSO we got performance metric as 100% and MR and FR is not mandatory so we can ignore as said in paper. Now click on 'Classifiers Performance Graph' button to get performance graph between all classifiers


An Intelligent Data-Driven Model to Secure Intravehicle Communications Based on Machine Learning
Upload CAN Bus Dataset
KNN Classifier Performance Details
KNN, Decision Tree, SVM, SSO
Algorithm

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


An Intelligent Data-Driven Model to Secure Intravehicle Communications Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect
Run Decision Tree To Detect
Run Conventional SVM To dete
Propose SSO with SVM To dete
Classifiers Performance Graph
Predict Anomaly from Test Data
Open
Cancel

In above screen I am uploading 'test.txt' file and now click on 'Open' button to predict uploaded test file class label.


An Intelligent Data-Driven Model to Secure Intravehicle Communications Based on Machine Learning
Upload CAN Bus Dataset
Run KNN Algorithm To Detect Anomaly
Run Decision Tree To Detect Anomaly
Run Conventional SVM To detect Anomaly
Propose SSO with SVM To detect Anomaly
Classifiers Performance Graph
Predict Anomaly from Test Data

```
[illegible] file loaded
[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = No Anomaly Detected

[illegible], Predicted = Anomaly Detected

[illegible], Predicted = No Anomaly Detected
```

In above screen in text area we can see uploaded test data and its predicted class label. All records contains normal packet data accept one record. So by using machine learning algorithms we can analyse packets and if packet contains attack then we ignore processing such packets.

CONCLUSION :

This paper proposed a novel intelligent and secured anomaly detection model for cyber attack detection and avoidance in the electric vehicles. The proposed model is constructed based on an improved support vector machine model reinforced by the MSSO algorithm. From the cyber security point of view, the proposed model could successfully detect malicious behaviors while letting the trusted message frames 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 cyberattacks 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.

[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.