INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

AN INTELLIGENT DATA-DRIVEN MODEL TO SECURE INTRAVEHICLE COMMUNICATIONS BASED ON MACHINE LEARNING

[1] MR. T. RAKESH KUMAR , [2] B. NAVYASRI, [3] K. ACHYUTH, [4] P. MADHURI

[1.] Assistant Professor Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Rangareddy (TS).India.

[1.] Email-:[.1.] rakesh903262@gmail.com

[2,3,4.]B.Tech StudentstDepartment of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Rangareddy (TS).India.

Email-[3.] navyasri2212@gmail.com[.2]palasamadhuri04@gmail.com,
[4.] achyuthkonda26@gmail.com.

Abstract- The high relying of electric vehicles on either in-vehicle 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 prevent 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 offline. Also, a two-stage modification method is proposed to increase the search ability of the algorithm and avoid premature convergence. Finally, 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.

KEYWORDS: Cyber-Attack, Controller Area Network, Denial-Of-Service, Social Spider

.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

1. 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 is processed, and the requiring orders are sent to the relevant actuators. Such a highly complex hardware software data transfer process may happen using different network protocols such as CAN, LIN, Flex Ray or MOST. 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, auto retransmission of lost messages and error detection capability. 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.

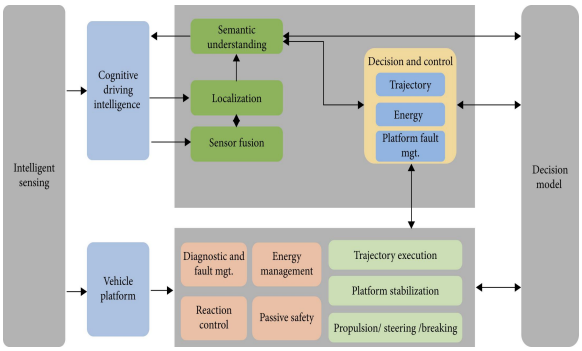

Fig.1: Intelligent driving vehicles decision-making framework.

2. LITERATURE SURVEY

Multisource software on multicore automotive ECUs—Combining runnable sequencing with task scheduling.

The problem of sequencing numerous elementary software modules, called runnable, on a limited set of identical cores. We show how this problem can be addressed as the following two subproblems, which cannot optimally be solved due to their algorithmic complexity: 1) partitioning

the set of runnable and 2) building the sequencing of the runnable on each core. We then present low-complexity heuristics to partition and build sequencer tasks that execute the runnable set on each core. Finally, we globally address the scheduling problem, at the ECU level, by discussing how we can extend this approach in cases where other OS tasks are scheduled on the same cores as the sequencer tasks.

Gateway system with diagnostic function for LIN, CAN and Flex Ray

The gateway system was introduced in the automotive system and has become one of the most important components. The gateway makes possible node-to-node communicate over different communication protocols. However, the gateway system has high probability of error because each protocol has different features such as signaling rate, data length, and so on. Moreover, it is difficult to detect the reason and location of errors. If the gateway reports the protocol conversion result when each protocol is converted into another protocol, this report helps developers find the reason and location of errors to debug errors easily. In this paper, we implement the gateway system with a diagnostic function. LIN, CAN, and Flex Ray are used as communication protocols.

3. 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 noise resistance 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.

DISADVANTAGES OF EXISTING SYSTEM:

1) Less accuracy

2)low Efficiency

4. 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.

TABLE II
SOME CAN BUS IDENTIFIERS AND FREQUENCIES

CAN Identifier	6FF	308	340	2A0
Frequency	101.010101	85.74311927	50	48.7804878
CAN Identifier	670	3F0	D21	210
Frequency	99.00990099	100.1666667	38.7804878	51.02040816
CAN Identifier	238	410	200	A7F
Frequency	108.6956522	93.45794393	61.02040816	49.01960784
CAN Identifier	B61	212	240	4EB
Frequency	10	68.54368932	78.01010101	113.6363636
CAN Identifier	2C1	312	5AE	1A3
Frequency	110.3595506	50	80.01960784	43.2449244

Table :1 Some CAN Bus Identifiers And Frequencies.

ADVANTAGES OF PROPOSED SYSTEM:

1) High accuracy

2)High efficiency.

5. 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.

6.RESULT

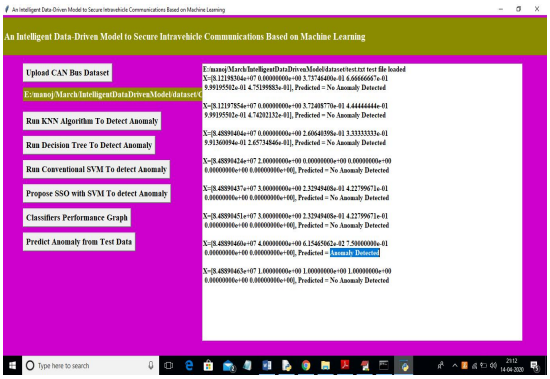

Fig.2: OUTPUT

7. CONCLUSION

This paper proposed a novel intelligent and secured anomaly detection model for cyberattack detection and avoidance in electric vehicles. The proposed model was constructed based on an improved support vector machine model reinforced by the MSSO algorithm. From the cybersecurity point of view, the proposed model could successfully detect malicious behaviours while letting the trusted message frames broadcast in the CAN protocol. The high HR% and FR% indices proved 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 were around the upper and lower bounds of the message frame frequency, showed 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.

8. REFERENCES

1. Abdelhamid N, Ayesh A, Thabtah F (2014) Phishing detection based associative classification data mining. Science-Direct 41:5948–5959.
2. Chen KT, Chen JY, Huang CR, Chen JY (2009) Fighting phishing with discriminative key point features of webpages. IEEE Internet Comput 13:56–63.
3. Chen X, Bose I, Leung ACM, Guo C (2011) Assessing the severity of phishing attacks: a hybrid data mining approach. Expert Syst Appl 50:662–672.
4. Fu AY, Wenyin L, Deng X (2006) Detecting phishing web pages with visual similarity assessment based on earth mover's distance. IEEE Trans Dependable Secure Comput 3(4):301 321.
5. Islam R, Abawajy J (2013) A multi-tier

phishing detection and filtering approach. J NetwComput Appl 36:324–335.

6. Li Y, Xiao R, Feng J, Zhao L (2013) A semi-supervised learning approach for detection of phishing webpages. Optik 124:6027– 6033.
7. Nishanth KJ, Ravi V, Ankaiah N, Bose I (2012) Soft computing-based imputation andhybrid data and text mining: the case of predicting the severity of phishing alerts. Expert Syst Appl 39:10583–10589.