IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

www.ijitce.com

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657
Volume 7, Issue 1, Jan 2019

An Intelligent Data-Driven Model to Secure Intra-Vehicle Communications based on Machine Learning

Mrs. Gangula Pavani[1], Mrs. Priyanka Basireddy[2], Mrs. Mukka Shirisha[3]

Abstract—

Electric cars have a large reliance on either in-vehicle or inter-vehicle communications, which may lead to serious problems. The focus of this article is on cyber security. assault in EVs and proposes a safe and dependable intelligent architecture to prevent hacker intrusion. A better support vector machine model for anomaly detection using the CAN bus protocol forms the basis of the suggested model. A novel optimization method based on the social spider (SSO) algorithm is created to strengthen the offline training process and increase the model's skills for quickly detecting and evading unwanted attacks. To further improve the algorithm's search capability and prevent premature convergence, a two-stage modification approach is presented. In conclusion, the simulation results on the actual data sets demonstrate the excellent performance, dependability, and security of the proposed model against denial-of-service (Dos) hacking in the electric cars.

I. INTRODUCTION

Electronic control units (Ecus) are a kind of hardware module used in modern cars. These Ecus are managed by a variety of software applications. There are no errors in any of the sensors placed in a vehicle communicate with the vehicle's electronic control unit (ECU), which processes the data and issues commands to the appropriate actuators based on the results [1]. Network protocols including CAN, LIN, Flex Ray, and MOST [2] may be used to facilitate the flow of data throughout a hardware-software process of this complexity. Not just in automobiles, but also in medical equipment, agricultural machinery, etc., CAN bus has become the most widely used of these protocols because of its versatility and reliability. The CAN bus standard has several benefits, including the capacity to send data at rates of up to 1Mbps, simplified wiring that reduces installation time and costs, automatic re transmission of dropped messages, and the ability to identify and correct transmission errors [3]. As the CAN bus protocol was developed at an era when cars were mostly autonomous, it has certain security flaws in the modern, dynamic context of smart grids. This will encourage noncriminals to launch attacks against EVs by inserting harmful code into their electronic control units (Ecus). To evaluate the safety of plug-in electric cars and the potential consequences of their integration into the electrical grid, [4] models and applies many cyber intrusion scenarios involving these vehicles. For the purpose of detecting

1,2,3 Assistant Professor
1,2,3 Department of CSE
1,2,3 Global Institute of Engineering and Technology Moinabad, Ranga Reddy District,
Telangana State.

cyber intrusions in cars, [5] creates a novel categorization system. In [6], a data intrusion detection system is created that may identify a cyber assault on the basis of an increase in the frequency of CAN bus messages or an improper usage of CAN message IDs. Because of this, the driver will be able to realise an assault has occurred and bring the car to a halt instantly.

All CAN communications, according to [7]'s authors, should go via a data management system to prevent cyber attacks. For example, in [8], an algorithmic approach is utilised to thwart assaults. vehicle error flags or denial-of-service indicators. A master ECU is designated during the vehicle's assembly phase to perform the attestation procedure, as recommended in [9]. By placing a firewall between the May bus and the communication system, as shown in [10], cyber attack orders to the CAN bus can be blocked.

In [11], the authors propose a method for detecting network intrusion in vehicles by analysing the entropy of CAN bus data. In [12], we see the development of an anomaly detection strategy that can identify flaws of both known and unknown types without the need for expert parameterize.

II. ELECTRIC VEHICLES' TECHNOLOGIES AND CYBER VULNERABILITIES

When it comes to low-cost communications in units with a large number of components (up to 500 million), electric vehicle manufacturers rely on the CAN standard more than any other protocol. chips. Due to its design, CAN offers an adequate amount of resilience and noise-resistance in the automotive sector.

Unfortunately, hackers may get access to the automotive system through wired or wireless means since CAN bus standards do not provide secrecy and authentication to CAN data frames. If you choose for the wired method, you may access the vehicle's CAN bus using the on-board diagnostics (OBD) II port, which is often situated under the steering wheel.

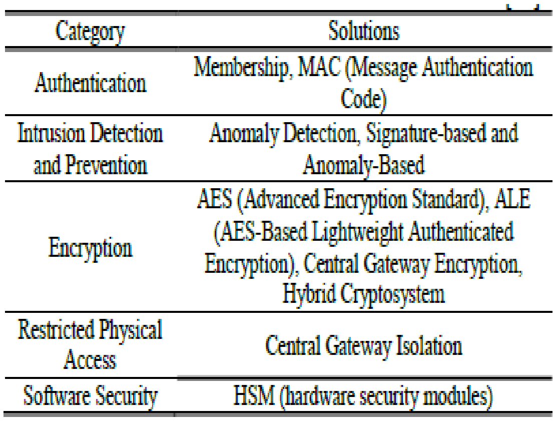
Although the intended function of this port is for engine and vehicle diagnostics, it will allow hackers to steal CAN messages using a cheap scanning tool.

Starting at this point, ECOM APIs like CANReceiveMessage and Neurotransmitter [10] make it simple to read and write CAN bus communications. If an electronic control unit (ECU) is the target of a wireless assault, then the cyber interference is the same, except that the entry point is not the OBD-II port. Wireless hacking may have a variety of entry points, although in most cases, the vehicle must be in range of a compromised Wi-Fi network. Transponder security in key less automobiles may also be broken by reverse engineering. Multiple flaws in the cipher's design have been uncovered via analysis. mechanism for authenticating users and in how they're really implemented.

"Wireless connection between sensors and Ecus like the TPMS system," "Add-on technologies, entertainment system (gaming), smart key," and "Internet, smart infrastructures" are all examples of alternative wireless entry points for automobiles.

Table I displays the complete set of category-based security measures and their accompanying answers. The authentication procedures ensure that both the sending and receiving devices are legitimate and have the identities they claim to have. Intrusion prevention and detection techniques employ data mining and machine learning-based techniques to identify and respond to anomalies in the communications between pieces of equipment.

TABLE I
SECURITY MEASURES IN CAN BUS PROTOCOL IN VEHICLES [15]



Category	Solutions
Authentication	Membership, MAC (Message Authentication Code)
Intrusion Detection and Prevention	Anomaly Detection, Signature-based and Anomaly-Based
Encryption	AES (Advanced Encryption Standard), ALE (AES-Based Lightweight Authenticated Encryption), Central Gateway Encryption, Hybrid Cryptosystem
Restricted Physical Access	Central Gateway Isolation
Software Security	HSM (hardware security modules)

Denial-of-service (Dos) attacks against the CAN bus include the sender sending a large number of messages with the smallest possible identifier (ID) to overwhelm the network's ability to process them. frequency so as to generate a busy state of affairs inside the car. Because it uses up all of the vehicle's available communication channels, this may be devastating. Data frames in CAN-bus are seen in their entirety in Fig. 1. Start of Frame (SOF), 12 bits; Arbitration Field, 6 bits; Control Field, 6 bits; Data Field, 0 to 64 bytes; CRC Field, 16 bits;

ISSN 2347–3657
Volume 7, Issue 1, Jan 2019

Acknowledgement Field, 2 bits; End of Frame, 1 bit (7-bit).

Each message frame has a unique identifier that indicates its priority and its validity in terms of whether or not the ECU will process the frame. A lower ID number indicates a greater priority. In this case, the ECU will prioritise the message with the lowest ID if two messages are published and dispatched simultaneously. By sending a malicious message with a low ID but high frequency, attackers may win the arbitration and prevent any other messages or orders from taking effect, a process known as message arbitration. This study provides a technique for detecting and avoiding anomalies based on the identifier and frequency of the associated message frames, which would help to prevent such a problem.

In the following paragraphs, we will describe the recommended approach in detail.

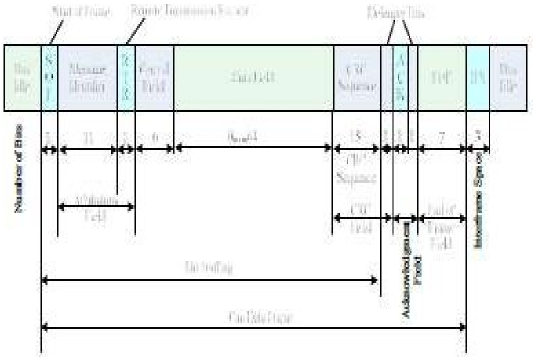


Fig. 1: Structure of a message frame in CAN bus

III. ANOMALY DETECTION MODEL BASED ON SUPPORT VECTORS

We use a one-class support vector machine to protect the CAN bus against Dos attacks. Suppose X is a typical training set consisting of N targets, with X = Xi where I = 1, 2,..., N. Since we know that every X has at least two pieces of data, we may say that. Finding a good function f(X) that gives a value of 1 when X is the target and a value of -1 when X is an outlier is the primary goal of a support vector machine. A hypothetical depiction of a support vector machine is shown in Fig. 2 Let (Xi) be Xi's feature space representation. A appropriate kernel function, such a sinusoidal kernel function, may estimate the unknown function's inner product as shown below:]

$$K(X_i,X_j)=(\gamma X_i^T X_j+C)^p \qquad (1)$$

where,C, and p are parameters for configuring the kernel function, and I and j are integers between 1 and N. As the training set is mapped into the feature space by the kernel function, cut them up with some hyperplane.

The following optimization problem (T stands for the transposition operator) yields these hyperplane:

$$\begin{aligned} &\min_{W,\rho} \ \frac{1}{2}W^T W-\rho+\frac{1}{vl}\sum_{i=1}^{N}\xi_i \qquad \forall i=1,2,\ldots,N \\ &s.t \quad W^T\Phi(X_i)\ge\rho-\xi_i \ ; \ \xi_i\ge 0,\forall i=1,2,\ldots,N \end{aligned} \qquad (2)$$

$$\begin{aligned} L(W,\xi,\rho,\alpha,\beta)=\frac{1}{2}W^T W-\rho+\frac{1}{vl}\sum_{i=1}^{N}\xi_i- \\ \sum_{i=1}^{N}\alpha_i\left(W^T\Phi(X_i)\ge\rho-\xi_i\right)-\sum_{i=1}^{N}\beta_i\xi_i \end{aligned} \qquad (3)$$

In other words, if we zero out the derivative of the preceding function with respect to W,, and, we obtain:

$$W=\sum_{i=1}^{N}\alpha_i\Phi(X_i) \qquad (4)$$

$$\alpha_i=(vl)^{-1}-\beta_i \qquad (5)$$

$$\sum_{i=1}^{N}\alpha_i=1 \qquad (6)$$

By putting (4)-(6) into (3), the dual form of the initial function
of (2) may be derived as follows:

$$\begin{aligned} &\min_{\alpha} \ \psi^T Q\psi \\ &s.t \quad 0\le\alpha_i\le\frac{1}{vl} \ , \ \sum_{i}^{N}\alpha_i=1 \end{aligned} \qquad (7)$$

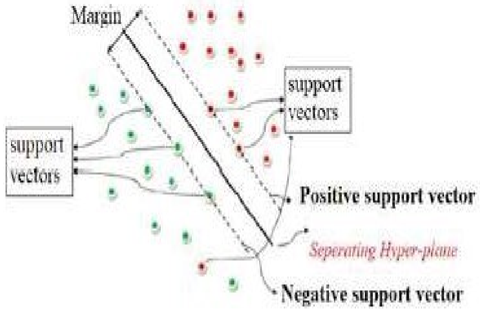


Fig. 2: Conceptual illustration of support vector machine

$$f(X) = \operatorname{sgn}\left(\sum_{i \in SVs}^{N} \alpha_i K(X_i, X) - \rho \right) \qquad (8)$$

where the index S Vs represent the support vectors. Now, □
can be calculated as follows:

$$\rho = W^T \Phi(X_i) = \sum_{j \in \{j | \alpha_i = 0\}} \alpha_j K(X_i, X_j) \qquad (9)$$

Performance of the classifier model output may be evaluated using four different metrics. The hit rate (HR), false alarm rate (FR), miss rate (MR), and (MR), percentage of valid rejections (CR). Figure 3 gives a conceptual picture of these indices matching the genuine expert observation from an experiment and the suggested anomaly detection model output, which may help with a better understanding of these indices. Any anomaly detection model may be assessed using four indices—HR, FA, MR, and CR—defined by using the symbols CA and CN to represent the true malicious data and normal data sets, respectively.

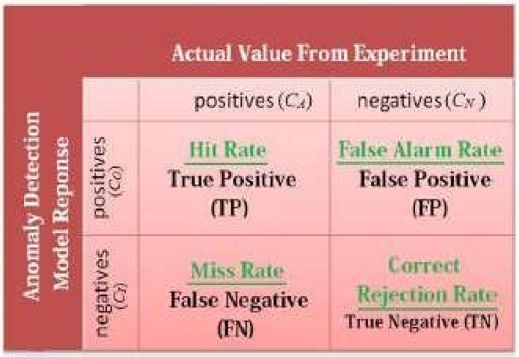
$$HR = |H_i| |C_A|^{-1} \quad ; \quad H_i = \{ X \in D | X \in C_A \& X \in C_O \} \qquad (10)$$

$$FR = |F_A| |C_N|^{-1} \quad ; \quad F_A = \{ X \in D | X \in C_N \& X \in C_O \} \qquad (11)$$

$$MR = |M_i| |C_A|^{-1} \quad ; \quad M_i = \{ X \in D | X \in C_A \& X \in C_I \} \qquad (12)$$

$$DR = |C_R| |C_N|^{-1} \quad ; \quad C_R = \{ X \in D | X \in C_N \& X \in C_I \} \qquad (13)$$

where D represents the whole datasets, CA the dataset's of outliers, CN the dataset's of normal data, CI the data set of milliners, and CO the data set of outliers.



		Actual Value From Experiment	
		positives (C_A)	negatives (C_N)
Anomaly Detection Model Reponse	positives (C_O)	Hit Rate True Positive (TP)	False Alarm Rate False Positive (FP)
	negatives (C_I)	Miss Rate False Negative (FN)	Correct Rejection Rate True Negative (TN)

Fig. 3: Confusion matrix for the proposed anomaly detection model

IV. OPTIMIZATION ALGORITHM BASED ON MODIFIED SSO

Each spider in our anomaly detection model is a four-element vector that represents the SVM model's optimum values as [v, , C, p].

Type A: The Authentic SSO Algorithm Each spider SK in the initial random population generated by the SSO method provides a potentially optimal solution to the optimization challenge. Algorithmically, there will be NS spiders, where NS = NF + NM, as the population will include both female and male spiders. The best spider Sb and the worst spider SW are recorded after computing the objective function for each spider Sk. Each spider has now been assigned a certain "weight."

$$w_k = \frac{f_w - f_k}{f_w - f_b} \qquad (14)$$

$$S_{k,F}^{Iter+1} = S_{k,F}^{Iter} \pm \theta_1 w_c e^{-d_{kc}^2} (S_c - S_{k,F}^{Iter}) \pm \theta_2 w_b e^{-d_{kb}^2} (S_b - S_{k,F}^{Iter}) + (\theta_3 - 0.5) \qquad (15)$$

The same holds true for the male population: it's time for an upgrade. Sorting the male population is a prerequisite to identifying the most powerful men in the population. based on the result of the criterion function. The median is supposed to represent the midway value. In a group of spiders, the dominant member is the one whose objective function value is greater than the median member. The current status of the male hierarchy is as follows:

$$S_{k,DM}^{Iter-1} = S_{k,DM}^{Iter} + \theta_5 w_F e^{-d_{kc}^2} (S_c^F - S_{k,DM}^{Iter}) + (\theta_6 - 0.5) \qquad (16)$$

Populations of spiders other than the dominant males are also updated by conforming to the weighted mean of the male population (Mw):

$$S_{k,NM}^{Iter-1} = S_{k,NM}^{Iter} + \theta_7 (M_w - S_{k,NM}^{Iter}) \qquad (17)$$

In (16), the spiders mate using a roulette wheel system determined by the mating probability value (rk). Statistically, the chances of a couple getting lower (lz) and upper (uz) bounds are predetermined and calculated in the following way:

$$r_k = \frac{1}{2n_v} \sum_{z=1}^{n_v} (u_z - l_z) \qquad (18)$$

$$S^{new1} = S_{r1} + \theta_8 (S_{r2} - S_{r3}) \qquad (19)$$

$$S^{new2} = \begin{cases} S_{k,z} & ; \quad \theta_8 < \theta_9 \\ S_{r1,z} & ; \quad \theta_8 \geq \theta_9 \end{cases} \qquad (20)$$

$$S^{new3} = \begin{cases} S_{k,z} & ; \quad \theta_9 < \theta_{10} \\ S_{r2,z} & ; \quad \theta_9 \geq \theta_{10} \end{cases} \qquad (21)$$

The second way involves updating the spider's location with the use of a small-step walking equation.

$$S_k^{Iter-1} = S_k^{Iter} + \varepsilon A_k \qquad (22)$$

V. SIMULATION RESULTS AND DISCUSSIONS

The preceding sections have mostly focused on the suggested model, theories, and contexts. The effectiveness of the suggested model is evaluated here by means of the information gleaned from an electric automobile trial. This research evaluates the DoS assault since its emphasis is on vehicle intercommunication, where it is very significant. The goal of a denial-of-service attack is to make it so that authorised users (the driver) can't get in. Dos attacks are especially perilous (and hence crucial) in automobiles since they might cause serious car accidents or losses despite the fact that they are transportable gadgets. Dos attacks on automobiles may result in a variety of hacked states, such as actuating the brakes mid-ride, jerking the steering wheel left or right, cutting power to the engine, opening a door, etc. The suggested anomaly detection programme may learn these frequencies from a study of recorded CAN communication over the course of a regular driving period of 10 minutes.

Table II displays a collection of CAN bus identities and associated frequencies. We had to construct a lot of checks and balances to make sure that our model was learning every potential ID number. examination of all traces Since most CAN communications are periodic, it became clear after collecting the traffic log and using the trace analysis that a 10-minute driving scenario will catch the bulk of the messages that are occurring often. Because of this, the generated model can be seen as the proof-of-concept that demonstrates how the suggested anomaly detection model can learn the existing pattern in the CAN signals to discriminate between normal and abnormal behaviour throughout testing. The CAN traffic file simulates the following situations for the driving exam in order to make it as realistic as possible: The driver flipped the key to "on," let the car idle for a few seconds, and then put it into "D." After that, you take the car out for a spin on a public road for around 8 minutes. There are many instances in which the brake pedal is pushed during the journey. The automobile is put in park, and the gear selector is put into reverse (or "R") so that the driver may back up a little and park. Once the car has come to a complete stop, the gear is put into "P," and the engine is shut off.

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

Fig. 4 demonstrates the results of outlier identification in the message \frame training set, including ID and frequency utilising the\proposed anomaly detection model based on support vector MSSO and the machine. Only frequency and frame Id were found to be necessary for a robust and accurate anomaly detection model after going through the required feature selection approach. As \sit can be observed, all the vehicle CAN bus message frame \observations are caught by the support vectors. Here, the zero-valued contour represents the border between the outliers and the remainder of the BUS data. Accordingly, it can be shown that the percentage of negative ratings in the cross-validated data is quite small, hovering around 0.13 percent. As a result, it's clear that the suggested model has a high degree of classification accuracy. In order to assess the search ability of the \proposed MSSO algorithm, many math based benchmarks \sear employed here with distinct properties such as regularity, \separability and multi modality. The five benchmarks \sconsidered here are as follows [16]:

-Sphere Function:

$$\min F = \sum_{m=1}^{K} x_m^2 \tag{23}$$

- Rosenbrock Function:

$$\min F = \sum_{m=1}^{K-1}\left[100\left(x_m^2 - x_{m+1}\right)^2 + \left(1 - x_m\right)^2\right] \tag{24}$$

- Rastrigin Function:

$$\min F = \sum_{m=1}^{K}\left[x_m^2 - 10\cos(2\pi x_m) + 10\right] \tag{25}$$

- Griewank Function:

$$\min F = \frac{1}{4000}\sum_{m=1}^{K} x_m^2 - \prod_{m=1}^{K}\cos\left(\frac{x_m}{\sqrt{m}}\right) + 1 \tag{26}$$

where K characterizes the scale on which the function is evaluated. The optimum values of the functions and the variable ranges are shown in Table III. Table IV displays the optimization outcomes, including mean and standard deviation (SD) value for a variety of well-known methods. As can be seen from these outcomes, the proposed MSSO method performs adequately in maximizing all objective functions across all dimensions.

Benchmarks for the optimization issue and their defining features are included in Table III.

Bench. no	Function	Range	Global optimum
1	Sphere	[-100, 100]	$F_{min} = 0, X = (0, 0, ...)$
2	Rosenbrock	[-30, 30]	$F_{min} = 0, X = (1,1, ...)$
3	Rastrigin	[-5.12, 5.12]	$F_{min} = 0, X = (0, 0, ...)$
4	Griewank	[-600, 600]	$F_{min} = 0, X = (0,0, ...)$

If you know the value of the Lagrangian objective function, you may evaluate how well the suggested MSSO method helps the anomaly detection model converge. captured in each cycle using various recording methods. A population size of 40 is used as a starting point for all algorithms, and a cutoff of 100 is used for all termination criteria. In GA, we set the crossover probability at 0.8 and the mutation probability at 0.08. PSO has a maximum speed limit of 2 m/s and an inertia weight factor of 0.8. The specifications for MSSO and the old SSO are identical. This evidence suggests that the proposed MSSO method has the potential to converge faster than the GA, PSO, and SSO algorithms. Moreover, the MSSO was able to effectively escape from local optima, but the other algorithms were stuck inside them. The original SSO came from problems with early convergence when roughly it reached 50, preventing it from optimizing the Lagrangian function to its full potential. These convergence curves prove without a doubt the superior search capabilities of the proposed MSSO in assisting the support vector machine with proper categorization.

Mean and standard deviation (SD) of optimization outcomes across many techniques are shown in Table IV.

Bench. No	K	IBC [19]		SSO		Proposed MSSO	
		Mean	SD	Mean	SD	Mean	SD
1	5	4.30 e-17	1.07 e-17	5.76 e-22	5.74 e-23	8.38 e-29	6.47 e-30
	30	4.69 e-16	1.07 e-16	7.38 e-19	2.12 e-21	7.44 e-28	1.64 e-29
	50	1.19 e-15	4.68 e-16	3.85 e-18	5.66 e-19	5.82 e-25	8.53 e-27
	100	1.99 e-06	2.26 e-06	5.36 e-16	5.85 e-17	5.34 e-23	3.84 e-23
2	5	2.33 e-01	2.24 e-01	7.06 e-02	6.94 e-03	3.65 e-05	5.09 e-06
	30	9.98 e-01	1.52 e+00	4.34 e-01	5.59 e-02	5.36 e-04	4.84 e-05
	50	4.33 e+00	5.48 e+00	7.96 e+00	4.37 e+00	7.47 e-03	2.36 e-04
	100	1.12 e+02	6.92 e+01	2.24 e+02	7.74 e+01	1.55 e+00	5.65 e-03
3	5	4.34 e-17	1.10 e-17	5.73 e-24	6.63 e-27	0.00 e+00	0.00 e+00
	30	4.80 e-05	2.43 e-04	5.59 e-10	6.73 e-14	0.00 e+00	0.00 e+00
	50	4.72 e-01	4.92 e-01	5.83 e-06	3.45 e-08	0.00 e+00	0.00 e+00
	100	1.46 e+01	4.18 e+00	3.33 e-04	4.24 e-05	0.00 e+00	0.00 e+00
4	5	4.04 e-17	1.12 e-17	5.73 e-10	5.46 e-11	7.62 e-19	7.83 e-25
	30	5.82 e-06	3.13 e-05	5.44 e-07	6.63 e-08	6.84 e-17	3.04 e-23
	50	5.72 e-01	9.22 e-01	6.78 e-04	3.28 e-05	4.55 e-12	4.58 e-22
	100	1.31 e+01	6.30 e+00	7.23 e-02	6.56 e-03	7.03 e-10	6.40 e-21

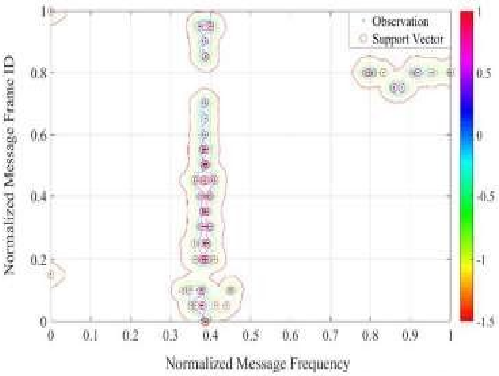


Fig. 4: Message Frame ID and frequency outlier detection

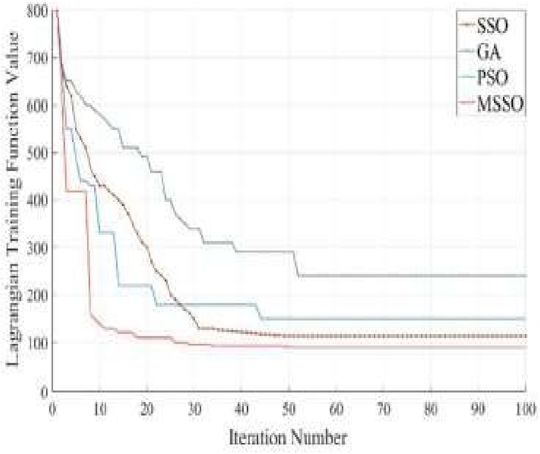
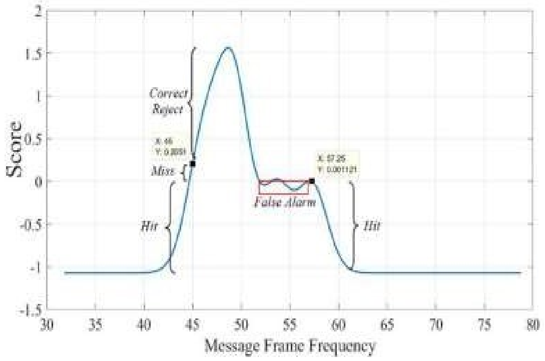


Figure 5: Variations in convergence behaviour between algorithms.

A set of benign and malicious assaults on the suggested anomaly detection methodology are simulated.

In this case, the ECU is made aware of a new message frame with ID 2A0. This ID \sis carefully selected owing to its broad frequency range and very \s complex model response. Fig. 6 depicts the detection model's reaction to these signals. The high hit rate and accurate reject rate in this figure demonstrate the model's proficiency in making reliable positive and negative inferences. To win arbitration and release the information on the bus, hackers in the actual world often begin their attacks at a rate almost double that of the messages. As seen in Fig. 6, such activity will be instantly identified as malicious and prevented.



Dos hit, miss, correct reject, and false alarm zone for a given CAN ID in the vehicle are shown in Fig. 6.

Tab. V displays the total efficiency of the planned anomaly detection model for a wide range of normal and assault message frame identifiers. Simulated confusion matrices are provided for a number of different classifiers, such as the nearest algorithm [17], a decision tree-based model [18], a radial basis function (RBF) neural network [19], a traditional support vector machine, a modified support vector machine based on SSO, and a modified support vector machine based on MSSO. These findings suggest that the suggested anomaly detection model outperforms the competing methods in terms of both HR% and CR%. Given the non linearity and complexity of the data set, the suggested TTS-BASED model has a greater chance of producing accurate predictions.

Values of the Confusion Matrix for Various Anomaly Detection Models

Outlier Algorithm	HR(%)	MR(%)	FR (%)	CR (%)
k-Nearest Neighbor [17]	81.63%	18.37%	19.55%	80.45%
Decision Tree-Based detection [18]	80.09%	19.91%	20.29%	79.71%
RBF Neural Network [19]	82.18%	17.82%	18.73%	81.27%
Conventional support vector model	83.12%	16.88%	18.07%	81.93%
Support vector machine based on SSO	89.47%	10.53%	12.24%	87.76%
Proposed Model	96.1%	3.9%	6.45%	93.55%

Regarding the suggested model's low false positive decision values, it's important to remember that erroneous values are not harmful unless they originate from a credible source. very unusual CAN message pattern. The paper's simulated counterattacks provide important context for understanding this argument. Message hacking attempts are simulated throughout a broad frequency spectrum, from a 200% increase/decrease to a tiny 1% increase/decrease. This demonstrates an extremely diverse set of message frequencies against which the built detection model may be evaluated.

VI. CONCLUSION

In order to identify and prevent cyber attacks on electric cars, the authors of this research present a unique intelligent and protected anomaly detection methodology. The basis for the suggested model is an using the MSSO technique to fortify a better support vector machine model. Cybersquatting-wise, the suggested model may effectively identify malicious actions while allowing trustworthy message frames to broadcast through the CAN protocol. Genuine positive and true negative judgments were made using the suggested model, as shown by high HR% and FR% indices. The low values of the MR% and CR% indices, which are often found around the top and lower boundaries of the message frame frequency, respectively, demonstrate the model's reliability. In future publications, the authors will evaluate how other counterattacks affect the efficiency of various anomaly detection techniques.

REFERENCES

[1] A. Monet ; N. Navel ; B. Bayeux ; F. Simon-Lion, ―Multi-source Software on Multi core Automotive Ecus—Combining Burnable Sequencing With Task Scheduling‖, IEEE Trans. Industrial Electronics, vol. 59, no. 10. Pp. 3934-3942, 2012.

[2] T.Y. Moon; S.H. Sec; J.H. Kim; S.H. Hang; J. Wook Jean, ―Gateway system with diagnostic function for LIN, CAN and Flex Ray‖, 2007 International Conference on Control,Automation and Systems, pp. 2844 – 2849, 2007. [3] B. Grozny; S. Murray, ―Efficient Protocols for Secure Broadcast in Controller Area Networks‖, IEEE Trans. Industrial Informatics, vol. 9, no. 4, pp. 2034-2042, 2013.

[4] B. Mohammedans, R. Al Muhammad, W. Sinus, T. Hemmer, S. El Khat, ―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. Louisa, E. Epistolary, E. Panasonic, P. Sanitarians, T. Dugong, A taxonomy and survey of caber-physical intrusion detection approaches for vehicles, Ad Hoc Networks, vol. 84, pp. 124-147, 2019.

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

[7] Schultz 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] Houma H, Higashiosaka X, Nakanishi M, Shintoism 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‖, Plot one, vol.
11, no. 6, e0155781, 2016.

[12] Theiler, 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 one class support vector machine‖, Computerizing, 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 opportunities‖, Future Generation Computer Systems, In press, corrected proof, Available online 11 January 2018.