CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

INTRAVEHICLE COMMUNICATION SECURITY USING ADVANCED MACHINE LEARNING

Mosarla Anilreedy[1] ,Dr.J. Anitha[2]
[1]Pg Scholar, Department of CSE, malla reddy college of engineering and technology dhulapally medchal, Telangana,India.
[2]Professor, Department of CSE, malla reddy college of engineering and technology dhulapally medchal, Telangana,India.

ABSTRACT: The high reliance of electric vehicles on both in-vehicle and between-vehicle communications can cause significant issues in the system. This paper addresses the issue of cyber attacks on electric vehicles and proposes a secure and reliable intelligent framework to prevent hackers from penetrating the vehicles. The proposed model is constructed based on an improved support vector machine model for anomaly detection, utilizing the Controller Area Network (CAN) bus protocol. To enhance the model's capabilities for fast malicious attack detection and prevention, a new optimization algorithm based on the Social Spider Optimization (SSO) algorithm is developed, which reinforces the offline training process. Additionally, a two-stage modification method is proposed to increase the search ability of the algorithm and avoid premature convergence. The simulation results on real data sets demonstrate the high performance, reliability, and security of the proposed model against denial-of-service (DoS) attacks in electric vehicles.

Index Terms: Cyber attacks, electric vehicles, anomaly detection, Controller Area Network (CAN), Social Spider Optimization (SSO) algorithm, denial-of-service (DoS) attacks.

I.INTRODUCTION

Vehicles are composed of numerous hardware modules known as electronic control units (ECUs), which are managed by various software tools. Sensors installed in a vehicle send their data to the ECU, where it is processed and necessary commands are sent to relevant actuators [1]. This complex hardware-software data transfer process often utilizes network protocols such as CAN, LIN, FlexRay, or MOST [2]. Among these, the CAN bus protocol is the most popular, not only in vehicles but also in medical devices, agriculture, and other fields, due to its high capability and promising characteristics. Key advantages of the CAN bus standard include support for data transfer rates up to 1 Mbps, reduced wiring complexity, cost and time savings due to simple wiring, automatic retransmission of lost messages, and error detection capabilities [3].

However, since the CAN bus protocol was developed when vehicles were largely isolated, it faces security issues in the modern, interconnected environment of smart grids. Hackers may exploit these vulnerabilities to attack electric vehicles via the ECU, injecting malicious messages into their systems. Various studies have explored these challenges and proposed solutions:

1. Cyber intrusion scenarios have been modeled and applied to electric vehicles to assess vulnerabilities and potential impacts on the power grid [4].
2. A new classification method for cyber intrusion detection in vehicles has been developed [5].

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

3. A data intrusion detection system has been created to detect cyber attacks based on increased CAN bus message frequency or misuse of CAN message IDs, enabling drivers to stop the vehicle immediately if an attack is detected [6].
4. A proposal suggests that all CAN messages should pass through a data management system to prevent cyber intrusions [7].
5. An algorithmic solution has been designed to stop denial-of-service attacks or error flags in vehicles [8].
6. Assigning an ECU as the master ECU during the vehicle manufacturing stage has been suggested to facilitate an attestation process within the system [9].
7. A firewall has been introduced to sit between the CAN bus and the communicating system to block cyber attack commands [10].
8. An intrusion detection system based on traffic entropy in the in-vehicle network communication system of the CAN bus has been proposed [11].
9. An anomaly detection approach capable of identifying known and unknown faults without requiring expert parameter settings has been developed [12].

This paper proposes an intelligent and highly secure method to equip electric vehicles with a powerful anomaly detection and avoidance mechanism. The proposed method utilizes support vector machines (SVM) and a one-class detection system to prevent malicious behavior in vehicles [13]. Experimental CAN bus data is used to train the SVM to recognize the normal frequency of different message frames under various commands. To optimize the model, a new algorithm based on the social spider ptimization (SSO) algorithm is proposed to adjust the SVM parameters effectively [14]. Given the high complexity and nonlinearity of the electric vehicle CAN bus dataset, a new two-stage modification method based on the crossover and mutation operators of genetic algorithms has been developed. This method increases algorithm population diversity and prevents premature convergence. The feasibility and performance of the proposed model are validated using real datasets gathered from an electric vehicle.

II.LITERATURE SURVEY

- Monot, N. Navet, B. Bavoux, and F. Simonot-Lion propose that as the demand for computing power rapidly increases in the automotive domain, car manufacturers and tier-one suppliers are gradually introducing multicore electronic control units (ECUs) in their electronic architectures. These multicore ECUs offer new features, such as higher levels of parallelism, which facilitate compliance with safety requirements like the International Organization for Standardization (ISO) 26262 and the implementation of other automotive use cases. However, these new features also involve greater complexity in the design, development, and verification of software applications. Consequently, car manufacturers and suppliers will require new tools and methodologies for deployment and validation. In their paper, the authors address the problem of sequencing numerous elementary software modules, called runnables, on a limited set of identical cores. They demonstrate how this problem can be tackled as two subproblems, which cannot be optimally solved due to their algorithmic complexity: 1) partitioning the set of

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

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

- T.Y. Moon, S.H. Seo, J.H. Kim, S.H. Hwang, and J. Wook Jeon explain that in real-time systems such as automotive systems, a distribution system is used to increase reliability. As the demand and complexity of the distribution system have increased, several automotive communication protocols have been introduced, such as LIN, CAN, and FlexRay. Each node of the system chooses the communication protocol that is suitable for a specific purpose. Each node does not need to have all communication protocols due to factors such as cost, space, and efficiency. Therefore, the gateway system was introduced in automotive systems and has become one of the most important components. The gateway enables node-to-node communication over different communication protocols. However, the gateway system has a high probability of error because each protocol has different features, such as signaling rate and data length. 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 more easily. In their paper, the authors implement a gateway system with a diagnostic function, using LIN, CAN, and FlexRay as communication protocols.
- Groza and S. Murvay describe that the Controller Area Network (CAN) is a bus commonly used by controllers inside vehicles and in various industrial control applications. In the past, controllers were assumed to operate in secure perimeters, but today these environments are well-connected to the outside world, and recent incidents have shown them to be extremely vulnerable to cyber-attacks. To withstand such threats, security can be implemented in the application layer of CAN. The authors design, refine, and implement a broadcast authentication protocol based on the well-known paradigm of using key-chains and time synchronization, a commonly used mechanism in wireless sensor networks. This approach allows them to take advantage of symmetric primitives without the need for shared secret keys during broadcast. However, since process control is a time-critical operation, they make several refinements to improve authentication delay. They study several trade-offs to alleviate shortcomings in computational speed, memory, and bandwidth, up to the point of using reduced versions of hash functions that can ensure ad hoc security. To prove the efficiency of the protocol, they provide experimental results on two representative microcontrollers from the market: a Freescale S12X and an Infineon TriCore, both of which were specifically chosen because they represent the extremes of computational power.

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

- Mohandes, R. Al Hammadi, W. Sanusi, T. Mezher, and S. El Khatib propose that to satisfy the growing energy demand, power systems must increase their capacity and be able to distribute energy over a wider geographical area. To maintain the reliability of such power systems, there is more dependence on automating the process controlling the physical system. Such power systems are known as smart grids, where data is transmitted in real-time across the power grid, facilitating automated actions. These smart systems have intrinsic vulnerabilities. A smarter power grid is more reliant on an ICT backbone, which renders the physical power system subject to an ICT realm whose security depends on a set of metrics and standards alien to those of classical power systems. The sustainability of a power system will depend on the secure and reliable operation of the new smart system. This paper proposes a comprehensive approach to solve the challenges enumerated above. The proposed approach sets the ground for new metrics of overall system sustainability by dissecting the smart grid into three layers: the physical system, the SCADA system, and the ICT infrastructure. The proposed methodology is tested on the case of electric vehicles, where cyber intrusion scenarios are studied in light of their effect on the physical layer.
- G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, and T. Vuong describe that with the growing threat of cyber and cyber-physical attacks against automobiles, drones, ships, driverless pods, and other vehicles, there is a growing need for intrusion detection approaches that can facilitate defense against such threats. Vehicles tend to have limited processing resources and are energy-constrained, so any security provision needs to abide by these limitations. At the same time, attacks against vehicles are very rare, often making knowledge-based intrusion detection systems less practical than behavior-based ones, which is the reverse of what is seen in conventional computing systems. Furthermore, vehicle design and implementation can differ wildly between different types or different manufacturers, leading to intrusion detection designs that are vehicle-specific. Equally importantly, vehicles are practically defined by their ability to move, autonomously or not. Movement, as well as other physical manifestations of their operation, may allow cybersecurity breaches to lead to physical damage, but can also be an opportunity for detection. For example, physical sensing can contribute to more accurate or more rapid intrusion detection through observation and analysis of physical manifestations of a security breach. This paper presents a classification and survey of intrusion detection systems designed and evaluated specifically on vehicles and networks of vehicles. Its aim is to help identify existing techniques that can be adopted in the industry, along with their advantages and disadvantages, as well as to identify gaps in the literature that are attractive and highly meaningful areas of future research.

III.EXISTING SYSTEM

The most popular protocol used by manufacturers for low-cost communications in electric vehicle units with a large number of components—up to 500 million chips—is the CAN standard. Because of its construction, the CAN's resilience and noise resistance level are acceptable in the automotive sector. Regretfully, the lack of secrecy and authentication in CAN bus protocols allows hackers to potentially gain access to the car system via wired or wireless

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

means. In the wired method, the OBD-II maintenance port, which is often found under the steering column, is used to connect to the CAN bus. Even though the primary purpose of this port is to be utilized for car maintenance and engine diagnostics, hackers will be able to get CAN packets by utilizing a basic scanning program. From this point on, using ECOM APIs like CANReceiveMessage and CANTransmitMessage to read and write traffic in the CAN bus is simple [10]. The cyberattack targets the ECU in the same way as the wireless assault, although OBD-II is not the entry point. The automobile must be linked to a malicious WiFi hotspot in order for most wireless hacking penetration points to occur, however they may vary. Furthermore, it is possible to reverse engineer the transponder's security mechanism in keyless cars. The study identifies a number of flaws in the authentication process, the cipher's design, and its execution. "Wireless connection between sensors and ECUs such as TPMS system," "Add-on technologies, entertainment system (gaming), smart key," and "Internet, smart infrastructures" are some other names for wireless access points to automobiles.

DISADVANTAGES OF EXISTING SYSTEM:

- Securing electric vehicles are often inadequate in detecting and preventing sophisticated cyber attacks due to their limited anomaly detection capabilities and susceptibility to premature convergence in optimization algorithms.
- These shortcomings can lead to delayed responses and vulnerabilities being exploited by hackers.

IV.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

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

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

- Enhanced anomaly detection and rapid response to cyber threats using an improved support vector machine model and optimized Social Spider Optimization algorithm.
- Increased search efficiency and prevention of premature convergence through a two-stage modification method, ensuring robust and reliable security for electric vehicles.

V.SYSTEM ARCHITECTURE

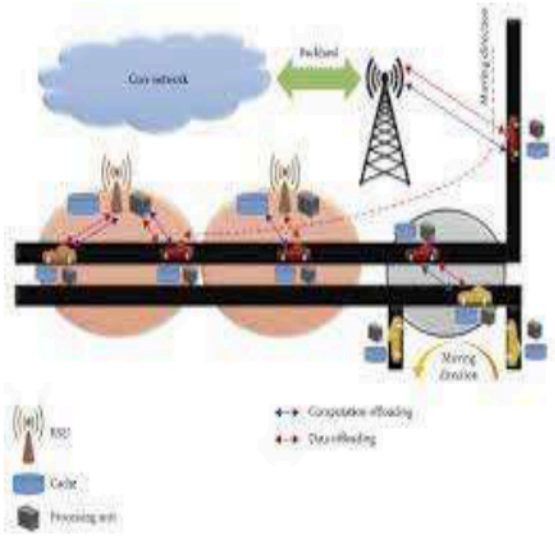


Figure 1.System Architecture

VI.IMPLEMENTATION:

MODULES:

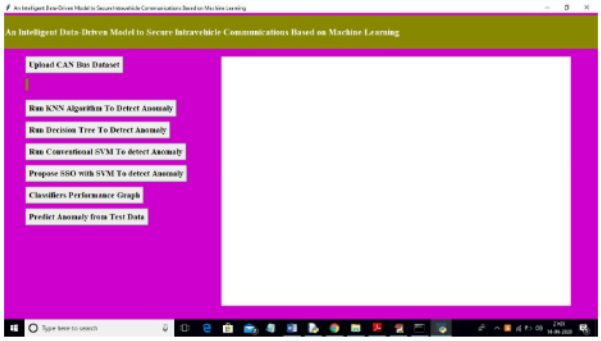
1. Upload CAN Bus Dataset' button and upload dataset
2. Run KNN Algorithm To Detect Anomaly' button to build KNN classifier train model to detect anomaly and evaluate its performance based on 4 indices
3. Run Conventional SVM To detect Anomaly' button to evaluate conventional SVM performance.
4. Propose 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

CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

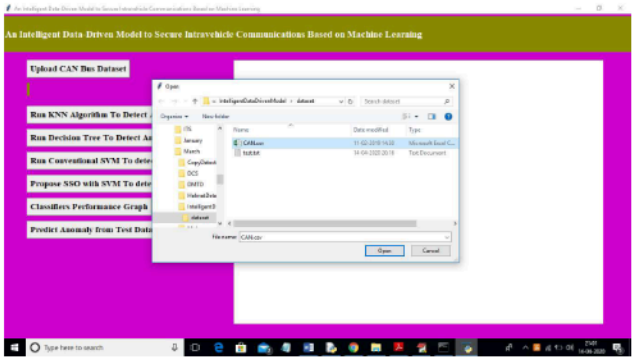
ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

VII.SCREENSHOTS

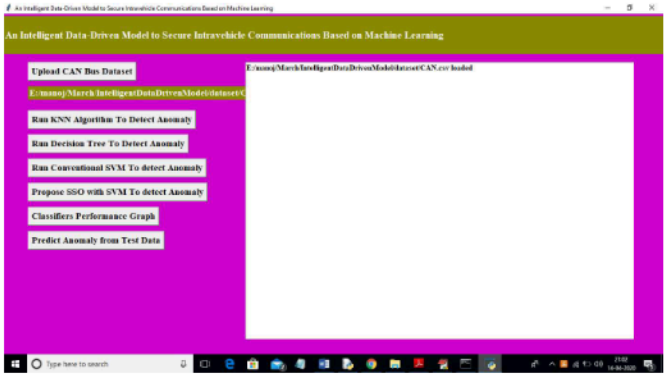
To run project double click on 'run.bat' file to get below screen



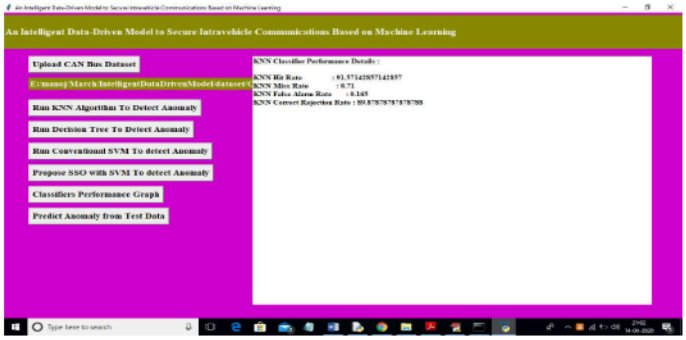
In above screen click on 'Upload CAN Bus Dataset' button and upload dataset



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



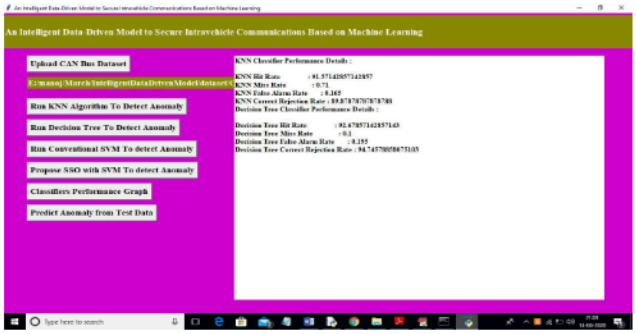
Now click on 'Run KNN Algorithm To Detect Anomaly' button to build KNN classifier train model to detect anomaly and evaluate its performance based on 4 indices



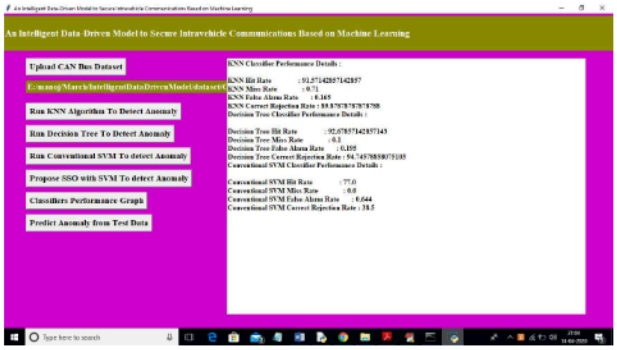
CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

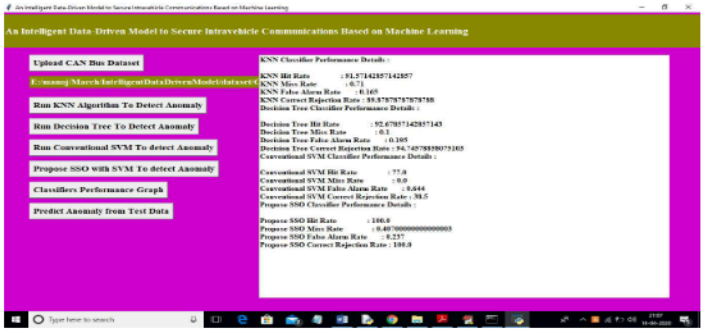
In above screen we got 4 indices values for KNN algorithm and now click on 'Run Decision Tree To Detect Anomaly' button to evaluate decision tree performance



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



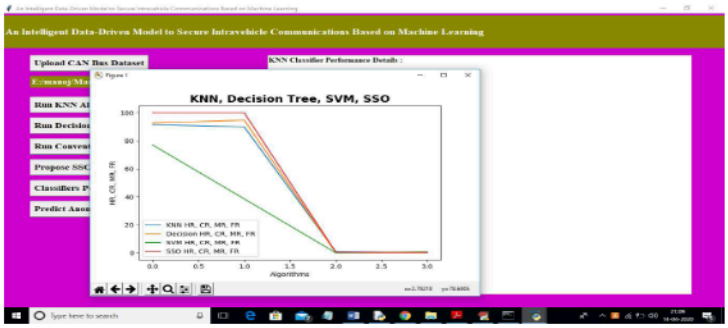
In above screen we got SVM performance data and now click on 'Propose SSO with SVM To detect Anomaly' button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working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



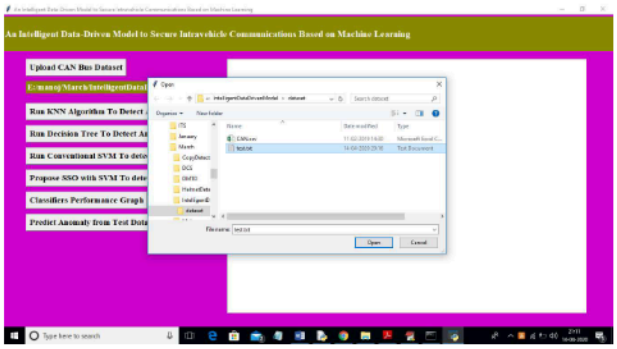
In above screen for SSO we got performance metric as 100% and MR and FR is not mandatory so we can ignore as said in paper. Now click on 'Classifiers Performance Graph' button to get performance graph between all classifiers

CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

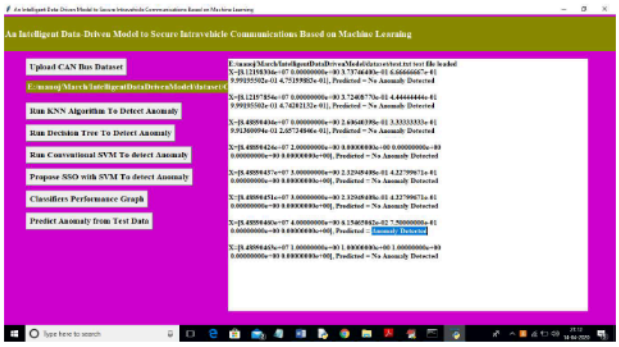
ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/



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.



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.

VIII.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.

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

IX.FUTURE ENHANCEMENT

The authors will assess the effect of other cyberattacks on the performance of different anomaly detection models in the future works.

X.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.

[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

ISSN:1624-1940
DOI 10.6084/m9.figshare.26310106
http://magellanes.com/

online 11 January 2018.