

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

.Dr.THOMAS FELDMAN

, Paruchuri SaiLikitha^[4],

^[1] Assistant Professor, Malla Reddy Engineering College for Women (Autonomous Institution),
Hyderabad , jahnavideepikag@gmail.com

^[2],^[3],^[4] Student, Malla Reddy Engineering College for Women (Autonomous Institution), Hyderabad

vakalasindhu04@gmail.com^[1] , bhavya.gunda03@gmail.com^[2] ,
paruchurisailikitha@gmail.com^[3]

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 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 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 optimization 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. Last but not least, the simulation results on the real datasets reveal the high performance, reliability, and security of the proposed model against denial-of-service hacking in the electric vehicles.

INTRODUCTION

Technically, vehicles are composed of many hardware modules, namely 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 through the use of different network protocols such as controller area network (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 briefly be briefly allowing up to 1 Mb/s 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. In some cyber intrusion scenarios are modelled and applied on the electric vehicles to assess their vulnerabilities and possible side effects getting finally into the power grid. In a new classification method is developed for cyber intrusion detection in vehicles. In 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 authors suggest that all CAN messages

should pass a data management system to avoid any cyber intrusion. In an algorithmic solution is used to stop attacks of types of denial-of service (DoS) or error flag in the vehicle. In 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 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 an intrusion detection system based on the traffic entropy of an in-vehicle network communication system of the CAN bus is suggested. In an anomaly detection approach is developed, which is capable of detecting faults of known and unknown type without requiring the setting of expert parameters.

RELATED WORK

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

As the demand for computing power is quickly increasing in the automotive domain, car manufacturers and tier-one suppliers are gradually introducing multicore electronic control units (ECUs) in their electronic architectures. In addition, these multicore ECUs offer new features

such as higher levels of parallelism, which ease the compliance with safety requirements such as the International Organization for Standardization (ISO) 26262 and the implementation of other automotive use cases. These new features involve greater complexity in the design, development, and verification of the software applications. Hence, car manufacturers and suppliers will require new tools and methodologies for deployment and validation. In this paper, we address 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 sub problems, 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”

In real-time systems such as auto motives, a distribution system is used to increase the reliability of the system. As the demand and complexity of the distribution system have increased, several automotive communication protocols have been introduced such as LIN, CAN, and Flex Ray. Each node of the system chooses the communication protocol that is suitable for the specific purpose. Each node doesn't need to have all of communication protocols because of cost, space, efficiency, and other factors. Therefore, 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 signalling 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.

“Efficient protocols for secure broadcast in controller area networks”

Controller Area Network 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 showed them extremely vulnerable to cyber-attacks. To withstand such threats, one can implement security in the application layer of CAN. Here we 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, which allows us to take advantage from the use of symmetric primitives without the need of secret shared keys during broadcast. But, as process control is a time critical operation we make several refinements in order to improve on the authentication delay. For this we study several trade-offs to alleviate shortcomings on computational speed, memory and bandwidth up to the point of using reduced versions of hash functions that can assure ad hoc security. To prove the efficiency of the protocol we provide experimental results on two

representative microcontrollers from the market: a Freescale S12X and an Infineon TriCore, both devices were specifically chosen as they are located somewhat on the extremes of computational power.

“Advancing cyber–physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles”

Satisfying the growing energy demand, power systems are required to increase their capacity and be able to distribute energy over wider geographical area. To maintain the reliability of such power systems, more dependence is placed 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. Such reliance renders the physical power system subjected 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 overall 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.

“A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles”

With the growing threat of cyber and cyber-physical attacks against automobiles, drones, ships, driverless pods and other vehicles, there is also a growing need for intrusion detection approaches that can facilitate defence against such threats. Vehicles tend to have limited processing resources and are energyconstrained. 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 behaviour-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, which can lead 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 cyber security breaches to lead to physical damage, but can also be an opportunity for detection.

“Security threats to automotive can networks practical examples and selected short-term countermeasures”

The IT security of automotive systems is an evolving area of research. To analyse the current situation and the potentially growing tendency of arising threats we performed several practical tests on recent automotive technology. With a focus on automotive systems based on CAN bus technology, this article summarises the results of four selected tests performed on the control systems for the window lift, warning light and airbag control system as well as the central gateway. These results are supplemented in this article by a classification of these four attack scenarios using the established CERT taxonomy and an analysis of underlying security vulnerabilities, and especially, potential

safety implications. With respect to the results of these tests, in this article we further discuss two selected countermeasures to address basic weaknesses exploited in our tests. These are adaptations of intrusion detection (discussing three exemplary detection patterns) and IT-forensic measures (proposing proactive measures based on a forensic model). This article discusses both looking at the four attack scenarios introduced before, covering their capabilities and restrictions. While these reactive approaches are short-term measures, which could already be added to today's automotive IT architecture, long-term concepts also are shortly introduced, which are mainly preventive but will require a major redesign. Beneath a short overview on respective research approaches, we discuss their individual requirements, potential and restrictions.

“On the need of data management in automotive systems”

In the last decade, automotive systems changed from traditional mechanical or mechatronical systems towards software intensive systems, because more and more functionality has been implemented by software. Currently, this trend is still ongoing.

Due to this increased use of software, more and more data accumulates and thus, has to be handled. Since it was not up to now to manage this data with software separately, we think that it is indispensable to establish a data managing system in automotive systems. In this paper we point out the necessity of data management, supported by exemplary scenarios, in order to overcome disadvantages of current solutions. Further, we discuss main aspects of data management in automotive systems and how it could be realized with respect to the very special restrictions and requirements within such a system.

METHODOLOGY

To implement this project we have designed following modules

Upload CAN Bus Dataset: Using This Module We can upload the dataset to the application.

Run KNN Algorithm To Detect Anomaly: Using This Module We can Run KNN Algorithm to detect Anomaly.

Run Decision Tree To Detect Anomaly: Using This Module We can Run Random Forest Algorithm to detect Anomaly.

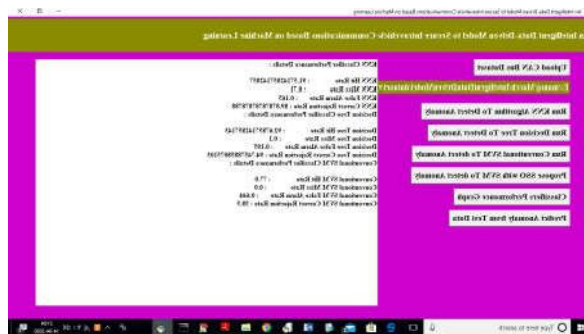
Run Conventional SVM To detect Anomaly: Using This Module We can Run SVM Algorithm to detect Anomaly.

Propose SSO with SVM To detect Anomaly: Using This Module We can Run Proposes SSO Algorithm to detect Anomaly.

Classifiers Performance Graph: Using This Module We can perform the classifiers comparison graph.

Predict Anomaly from Test Data: Using This Module We can predict the Anomaly from test data.

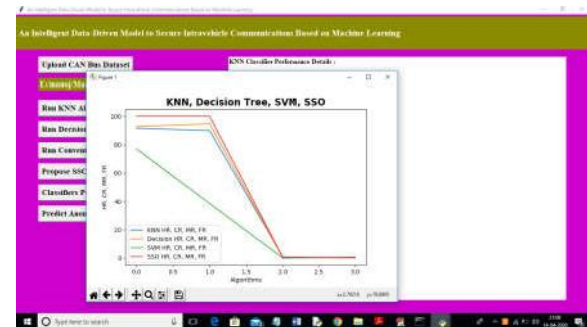
RESULT AND DISCUSSION



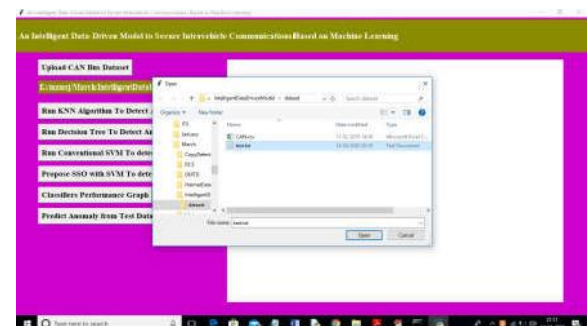
In above screen we got SVM performance data and now click on 'Propose SSO with SVM To detect Anomaly' button to run propose SSO with SVM classifier and evaluate its performance. (Note: when u run SSO then application will open 4 empty windows and you just close newly open empty window and keep working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



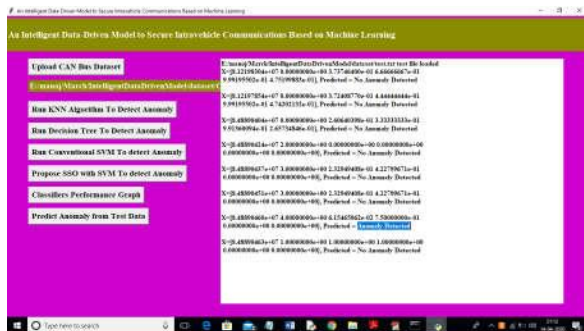
In above screen for SSO we got performance metric as 100% and MR and FR is not mandatory so we can ignore as said in paper. Now click on 'Classifiers Performance Graph' button to get performance graph between all classifiers



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 contain 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 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 cyber-attacks on the performance of different anomaly detection models in the future works.

REFERENCES

- [1] A. Monot, N. Navet, B. Bijoux, and F. Semination, "Multisource software on multicore automotive ECUs—Combining runnable sequencing with task scheduling," *IEEE Trans. Ind. Electron.*, vol. 59, no. 10, pp. 3934–3942, Oct. 2012.
- [2] T. Y. Moon, S. H. Seo, J. H. Kim, S. H. Hwang, and J. Wook Jeon, "Gateway system with diagnostic function for LIN, CAN and Flex Ray," in *Proc. Int. Conf. Control, Autom. Syst.*, 2007, pp. 2844–2849.
- [3] B. Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks," *IEEE Trans. Ind. Inform.*, vol. 9, no. 4, pp. 2034–2042, Nov. 2013.
- [4] B. Mohandas, R. Al Hammadi, W. Sanusi, T. Mezher, and S. El Khatib, "Advancing hyperphysical sustainability through integrated analysis of smart power systems: A case study on electric vehicles,"

Int. J. Crit. Inf. Protection, vol. 23, pp. 3348, 2018.

[5] G. Loukas, E. Kristol, E. Apneusis, P. Sargonids, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Nets.*, vol. 84, pp. 124–147, 2019.

[6] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks practical examples and selected short-term countermeasures," *Rel. Eng. Syst. Saff.*, vol. 96, no. 1, pp. 11–25, 2011.

[7] S. Schulze, M. Upcall, G. Saake, T. Hoppe, and J. Dittmann, "On the need of data management in automotive systems," in *Proc. Bus., Technol. Web*, 2009, vol. 144, pp. 217–26.

[8] C. Ling and D. Feng, "An algorithm for detection of malicious messages on can buses," presented at *Nat. Conf. Inf. Technol. Compute. Sci.*, 2012, pp. 1218. \

[9] H. Oguma, X. Yoshioka, M. Nishikawa, R. Shigeto mi, A. Otsuka, and H. Imai, "New attestation-based security architecture for in-vehicle communication," in *Proc. IEEE Global Telecommands. Conf.*, 2008, pp. 1–6.

[10] L. Pan, X. Zheng, H. X. Chen, T. Luan, and L. Batten, "Cyber security attacks to modern vehicular systems," *J. Inf. Secure. Appl.*, vol. 36, pp. 90–100, Oct. 2017.

[11] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *Plops One*, vol. 11, no. 6, 2016, Art. no. e0155781.

[12] A. Heisler, "Detecting known and unknown faults in automotive systems using ensemble-based anomaly detection," *Know.-Based Syst.*, vol. 123, pp. 163–173.

[13] F. Zhu, J. Yang, C. Gao, S. Xu, and T. Yin, "A weighted one-class support vector machine," *Neurocomputing*, vol. 189, pp. 1–10, May 2016.

[14] Y. Zhou, Y. Zhou, Q. Luo, and M. Abdelbaset, "A simple method based social spider optimization algorithm for clustering analysis," *Eng. Appl. Arif. Intel.*, vol. 64, pp. 67–82, 2017.

[15] G. De La Torre, P. Rad, and K. K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Compute. Syst.*, to be published, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167739X17315066>