DOI:

Journal of Computers and Intelligent Systems

Vol. 2, No. 2, 2024, pages 91 - 96

Journal Homepage:

https://journals.iub.edu.pk/index.php/JCIS/

Intrusion Detection Systems for In-Vehicle Networks

Muhammad Atif Noor[1], Dr. Nasir Jalal[1], Muhammad Zulkifl Hasan[2], Muhammad Zunnurain Hussain[3], Muzzamil Mustafa[4]

[1]Department of Computer Science & IT, Cholistan University of Veterinary and Animal Sciences

[2]Department of Computer Science Faculty of Information Technology University of Central Punjab Lahore Pakistan Email: Zulkifl.hasan@ucp.edu.pk ORCID : https://orcid.org/0000-0002-2733-5527

[3]Dept. of Computer Science Bahria University Lahore Campus(A Project of Pakistan Navy) Email: Zunnurain.bulc@bahria.edu.pk ORCID: https://orcid.org/0000-0002-6071-1029

[4]Department of Artificial Intelligence University of Management & Technology Lahore, Pakistan

muzzamil.mustafa@umt.edu.pk

ARTICLE INFO

Article History:

Received:	July	29, 2024
Revised:	August	29, 2024
Accepted:	August	22, 2024
Available Online:	August	25, 2024

Keywords:

Intrusion detection system
Networks system
Car hacking
Controlled area

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

This paper presents an overview of the Intrusion Detection system for In-Vehicle Networks which is a competition designed to provide security professionals with an opportunity to enhance their knowledge and experience in the field of car hacking and defense. The competition involves teams of professionals who compete in a simulated environment to develop and test car-hacking and defense strategies. Teams are provided with a wide range of tools and resources to help them analyze, exploit and defend against car-hacking attacks. The competition consists of several rounds of challenges, which include both theoretical and practical tasks. Results of the competition are used to identify security vulnerabilities and develop countermeasures to protect vehicles from malicious attacks. The paper also provides an overview of the structure and rules of the competition for intrusion detection system for in vehicle networks.

Corresponding Author's Email: * matifnoor@cuvas.edu.pk

Citation:

1. Introduction

Car hacking is the modification of a car's electrical system to access and control functions that are not available through the traditional control systems. Car hacking is becoming increasingly popular in the automotive world as more and more people are looking for ways to customize their cars. It is an interesting and exciting way to customize your vehicle, as well as a great way to stay up to date with the latest technology. Car hacking can be used to modify and improve the performance of a car, as well as to add features and functionality that are not available through the traditional car control systems. Car hacking can also be used to bypass security measures and disable certain features, allowing owners to gain more control over their vehicles.

Car hacking has grown in importance as a security concern in recent years as a result of the proliferation of connected and autonomous vehicles. The potential for malicious actors to gain access to a car's systems and manipulate them for malicious purposes is a real threat that must be addressed. In response, the automotive

industry has established a number of initiatives to raise awareness of the potential risks, and to develop solutions to protect vehicles from malicious actors. One such initiative is the Car Hacking and Defense Challenge, an international competition that challenges security researchers to find and exploit vulnerabilities in cars' systems.

The challenge involves finding and exploiting vulnerabilities in cars' systems, as well as developing and deploying countermeasures to protect vehicles from malicious actors. The challenge is open to both amateur and professional security researchers, and has become an important platform for sharing knowledge and raising awareness about car security issues. This work advances the state of the art in vehicle cyber security by addressing the shortcomings of current IDS solutions and offering a machine learning-based technique designed specifically for the automotive context. In addition to improving the security of in-car networks, our architecture establishes the foundation for further studies on scalable and adaptive intrusion detection systems for the automotive sector.

Table 1: Summary of Intrusion Detection Methods for In-Vehicle Networks

Method	Description	Advantages	Limitations
Signature-based IDS	Detects known attacks using predefined patterns	Low false positives	Limited to known threats
Anomaly-based IDS	Identifies deviations from normal behavior	Can detect novel attacks	Higher false positives
Specification-based IDS	Relies on a set of predefined rules for network behavior	Effective for protocol enforcement	Difficult to scale with network complexity

2. Materials and Methods

A. Predictive Model

A forecasting model is a mathematical model which is used to predict the outcome of a future event based on data and patterns from past events. It is a type of artificial intelligence (AI) technique that uses data mining, machine learning, and statistics to make predictions about future events. Predictive models are utilized to assist organizations in making better decisions across a range of industries, including banking and healthcare and prepare for future events. The predictive model of the Car Hacking and Defense Competition on the In-Vehicle Network should consider a number of factors. These include the security of the in-vehicle network, the potential attack vectors, the ability of the competitors to identify and exploit vulnerabilities, and the ability of the competition organizers to monitor and enforce the rules Vehicle Network Security: This pertains to the security of the vehicle network should be evaluated to ensure that it is secure against potential attackers. This includes assessing the security measures in place to protect the in-vehicle network from external and internal threats, as well as evaluating the security protocols and architecture of the system. Vehicle Network Security: This pertains to the security of the vehicle network should be evaluated to ensure that it is secure against potential attackers. This includes assessing the security measures in place to protect the in-vehicle network from external and internal threats, as well as evaluating the security protocols and architecture of the system. The different types of predictive models are

i. Decision Trees - One kind of machine learning technique called a decision tree is used to classify data. This algorithm works by constructing a tree-like structure from a set of given data points. At each node in the tree, a decision is made about the best way to classify the data points based on their values. The decision tree works by selecting the best variable to split the data set into smaller subsets. This process is repeated until the data points are all classified.

ii. Support Vector Machines - A supervised machine learning technique used for regression and classification problems is called a support vector machine. The SVM algorithm seeks to maximize the margin between the two classes while constructing a hyper plane that best divides the data into its corresponding classes..

It can be used for both linear and non-linear data, and it is especially useful for dealing with high-dimensional and complex data sets. SVMs are also very effective in dealing with small datasets, since they are less prone to over fitting.

iii. Logistic Regression - One kind of supervised learning technique used for categorization is logistic regression. Based on one or more independent variables, it is used to forecast the likelihood of a dependent variable (target). (Features). Logistic regression is used in a variety of fields, such as medical diagnosis and credit scoring. It is also used to predict whether an event will occur given certain input variables.

B. Initial Round Dataset

Depending on the goal, we offered the training set and submission set as two datasets in the first phase. There were two target vehicle statuses in both datasets. There were four different kinds of attacks in every state

Table 2: preliminary round dataset

Purpose	Car Status	Normal	Flooding	Spoofing	Replay	Fuzzing
Training	Driving	1,724,630 (92.0%)	77,373 (4.1%)	3,879 (0.2%)	23,775 (1.3%)	45,474 (2.4%)
	Stationary	1,648,113 (91.7%)	76,807 (4.3%)	3,877 (0.2%)	23,818 (1.3%)	44,405 (2.5%)
Submission	Driving	1,799,046 (89.9%)	96,559 (4.8%)	22,489 (1.1%)	37,869 (1.9%)	44,770 (2.2%)
	Stationary	1,559,164 (89.0%)	95,120 (5.4%)	20,094 (1.1%)	25,012 (1.4%)	51,923 (3.0%)

C. Driving

The information removed while driving, including general driving movements (e.g., speed up, slowing down, turning the directing wheel).

D. Stationary

The data eliminated when the engine is running but not moving (park gear), encompassing auxiliary motions (such as pressing buttons in the mid control region).).

E. Flooding

- One kind of cyber-attack is called a flooding attack, where the attacker floods a system or network with traffic in an attempt to overload it and make it inaccessible. Similar to a denial-of-service attack, however instead of delivering the target a single request, the attacker delivers several requests with the intention of consuming all available resources. This type of attack can be used to take down websites, networks, or other online services

F. Fuzzing /Spooning

Spoofing is a type of cyber-attack that involves disguising oneself as an authorized user or system to obtain access to private data or resources. Spoofers can use any number of methods to accomplish this, including IP address spoofing, MAC address spoofing, email address spoofing, and more. The goal of spoofing is usually to gain access to confidential data, such as passwords, financial information, or other personal data. Spoofers may also use the false identity to spread malware or launch denial of service attacks. Fuzzing is a type of automated testing that can be used to uncover errors in code. It involves sending random inputs or data to a program in order to discover how it behaves under unusual circumstances. Fuzzing can be used to test for vulnerabilities in web applications, network services, and databases. It can also be used to test for potential weaknesses in communications protocols, file formats, and encryption systems.

Table 3: Fuzzing/ Spooning remarks

Category	Evaluation Indicators		Proportion		Remarks
Attack Score	Visibility of attack impact		Y/N		Qualitative
	Number of attack kinds		6%	30%	Quantitative
	Different attacks from preliminary round		6%		Quantitative
	Severity of attacks		6%		Qualitative
	Detection difficulty		12%		Quantitative
Detection Score	Attack detection accuracy (F1-score)	Host's session	10%	50%	Quantitative
		Participant's session	40%		
Presentation	Understanding of CAN data and validity of idea-making process		4%	20%	Qualitative
	Features, advantages, and differentiation of detection algorithm		8%		
	Features, advantages, and differentiation of attack techniques		8%		

G. Impact Visibility Attack

Every attack should have an obvious effect, allowing the staff to identify whether the team is introducing legitimate attack messages. An attempt is not considered an attack if staff members are unable to verify the impact. Quantity of assault types. Teams might plan no more than five distinct attacks at a time. Regardless of attack methods such flooding, spoofing, replay, and fuzzing, the "kind" of assault is identified as one that impacts various vehicle functions. For instance, both attacks are recognized as distinct if the first modifies the RPM gauge value and the second turns the steering wheel.

H. Impact Visiblity Attack

This indicator is included to encourage participants to make different kinds of attacks from preliminary round datasets.

Table 4: Impact of Visibility attack

Team	Fin. avg. F1-score	Fin. avg. detection time (s)	Fin. attack score	Detection algorithm
A	**0.869**	**33**	71.0	Rule-based
B	0.864	155	57.2	XGBoost, Light GBM, rule-based
C	0.816	355	**79.6**	Random Forest, white & black list
D	0.812	257	66.7	Light GBM
E	0.675	295	63.4	Rule-based, Random Forest
F	0.445	147	38.8	Random Forest, Light GBM
G	0	114	51.7	DBSCAN

3. Discussion: Limitations and Potential Improvements

A. Difficulty of testing

The complexity of the in-vehicle network security systems makes it difficult to test for vulnerabilities. This makes it difficult for the competition to accurately assess the security of the vehicles.

B. Lack of public knowledge

The public is largely unaware of the threats posed by car hacking and the need for vehicle security. As a result, the competition may not have the level of participation necessary to ensure that the most secure vehicles are chosen.

C. Lack of rewards

The competition does not offer any rewards for successful car hacking. This may discourage some participants from taking part, as they may not feel sufficiently motivated to invest their time and effort into the competition.

D. Potential Improvements

i. More public engagement: The competition should aim to increase public awareness of the need for vehicle security. This could be done by providing more information about the competition, encouraging people to take part, and offering rewards or incentives for successful car hacking attempts.

ii. Increased rewards: Offering rewards or incentives for successful car hacking attempts may encourage more people to take part in the competition. This could include financial rewards, prizes, or recognition in the form of certificates or titles

4. Conclusion

Car hacking and defense competitions on in-vehicle networks are becoming increasingly important due to the growing sophistication of cyber-attacks and the potential for severe damage to vehicles and their occupants. While car hacking and defense competitions provide an opportunity to evaluate the security of in-vehicle networks, they also provide an opportunity for cyber attackers to find weaknesses in these systems. As such, it is important that car manufacturers, security researchers, and automotive cyber security experts work together to ensure that in-vehicle networks are as secure as possible. This means developing and testing secure protocols, implementing security measures, and regularly monitoring for malicious activity. Finally, it is important that car owners and operators remain vigilant and aware of the dangers of vehicle hacking and the necessity of taking precautions to safeguard their vehicles from cyber threats.

References

[1]. K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1044–1055.

[2] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "Voltageids: Lowlevel communication characteristics for automotive intrusion detection system," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2114–2129, 2018.

[3] J. den Hartog, N. Zannone et al., "Security and privacy for innovative automotive applications: A survey," Computer Communications, vol. 132, pp. 17–41, 2018.

[4] E. Gavas, N. Memon, and D. Britton, "Winning cybersecurity one challenge at a time," IEEE Security & Privacy, vol. 10, no. 4, pp. 75–79, 2012.

[5] B. Gorenc, "Pwn2Own returns to vancouver for 2020," https://www.zerodayinitiative.com/blog/2020/1/8/pwn2own-returnsto-vancouver-for-2020, accessed on: Jan. 11, 2021.

[6] F. Guo, Z. Wang, S. Du, H. Li, H. Zhu, Q. Pei, Z. Cao, and J. Zhao, "Detecting vehicle anomaly in the edge via sensor consistency and frequency characteristic," IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5618–5628, 2019.

[7] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," Vehicular communications, vol. 14, pp. 52–63, 2018.

[8] Infosec In the City, "Overview of SINCON car security kampung," https://www.infosec-city.com/post/sin20-ctf-car-security, accessed on: Jan. 11, 2021.

[9] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 787–800.

[10] B. I. Kwak, M. L. Han, and H. K. Kim, "Cosine similarity based anomaly detection methodology for the can bus," Expert Systems with Applications, vol. 166, p. 114066, 2021.

[11] Y. Lin, C. Chen, F. Xiao, O. Avatefipour, K. Alsubhi, and A. Yunianta, "An evolutionary deep learning anomaly detection framework for invehicle networks-can bus," IEEE Transactions on Industry Applications, 2020.

[12] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown can bus networks," Vehicular Communications, vol. 9, pp. 43–52, 2017.

[13] Suyash Bhogawar, C. A., Nuthakki, S., Venugopal, S. M., & Mullankandy, S. The Ethical and Social Implications of Using AI in Healthcare-A Literature Review..

[14] Nuthakki, S., Kumar, S., Kulkarni, C. S., & Nuthakki, Y. (2022). Role of AI Enabled Smart Meters to Enhance Customer Satisfaction. *International Journal of Computer Science and Mobile Computing*, *11*(12), 99-107..

[15] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," Vehicular Communications, vol. 21, p. 100198, 2020.