An Intrusion Detection Scheme for Driverless Vehicles Based Gyroscope Sensor Profiling

Khattab M. Ali Alheeti, *Member, IEEE*
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, United Kingdom
University of Anbar, College of Computer– Anbar, Iraq
kmali@essex.ac.uk

†Rabab Al-Zaidi, *Member, IEEE*, John Woods and Klaus McDonald-Maier, *Senior Member, IEEE*
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, United Kingdom
†AL-Mustansiriya University, Baghdad, Iraq
{rjmohs, woodjt, kdm}@essex.ac.uk

***Abstract*— Vehicular ad-hoc networks of self-driving vehicles are potentially exposed to both internal and external attacks. The privacy and security of these networks is paramount for effective protection of communication systems from possible attacks. We propose an intelligent intrusion detection system in this paper that is based on Integrated Circuit Metrics (ICMetrics), which has significant defensive capability against unexpected attacks. The proposed security system shows good performance in identifying and blocking malicious vehicles in vehicular ad-hoc networks of driverless vehicles and semi driverless vehicles.**

***Index Terms*—Security, self-driving cars, ICMetric, IDS.**

I. Introduction

Autonomous systems such as Unmanned Aerial Vehicles (UAVs), self-driving vehicles, semi self-driving vehicles and robots are poised to play an increasingly important part in our daily lives and many practical applications [1]. Self-driving or robotic cars such as Google's cars are seen as an important application of autonomous systems. There are many potential positive economic impacts associated with such vehicles, they can also increase the safety of the driver and the passengers [1].

One objective of self-driving vehicles is to enhance safety by decreasing car accidents and traffic jams that arise as a result of human errors. Recent research reveals that the communication systems in self-driving vehicles have experienced problems with these security systems [2]. Thus, it is anticipated that there will be a gradual increase in the number of security attacks on these vehicles without significant changes to the security design of autonomous cars. There is strong indication that current security systems are not sufficient to protect the networks utilised in self-driving and semi self-driving vehicles [3].

Integrated Circuit Metrics (ICMetrics) is an emerging technology that uses features that have been extracted from the characteristics of an electronic system to form a unique identifier that can be used both for security and identification purposes, akin to the electronic equivalent of a biometric [4]. Previous research has identified that intrusion detection systems (IDSs) can play a vital role in creating a safe environment for autonomous vehicles. Ali et al. [5] suggested an intelligent IDS to provide protection for the control and transfer of data in the process of an exchange between Road Side Units (RSUs) and vehicles. IDS based on fuzzy petri nets are used to detect and prevent interaction from malicious vehicles. The authors in [4], suggested a security system for wearable devices using ICMetric security paradigm and demonstrate how an ICMetric can be generated through the MEMS accelerometer and other sensor characteristics. They designed a comprehensive security system, which generates an ICMetric for a device based on its device characteristics. The ICMetric is then utilised to generate a symmetric key that is used to provide security services such as integrity, authentication, and confidentiality. The authors carried out the simulation of their system and concluded that higher levels of security can be offered without compromising the resources (time, memory, and speed) requirement. [6] provides a comparative survey on the complicated issues of pseudonymity in VANETs. The authors determine four major classes of pseudonym methods that are usually used in secure external communication of vehicles. In our research, we propose a novel IDS to provide security to external communication of self-driving and semi self-driving vehicles. This IDS employs ICMetric technology in detecting external/internal attacks. The work makes two contributions, which are:

- Enhancing the authentication aspect of self-driving and semi self-driving vehicles through generation of an ICMetric basic number which was obtained from bias reading of vehicular gyroscope sensors.
- Creating an intelligent IDS depending on the characteristics of self-driving or semi self-driving vehicles. These characteristics where their behavior is classified as normal or abnormal are obtained from the trace file that was generated using a network simulator-2 (ns-2) to model the VANET and its environment.

The application of ICMetrics in IDSs enables to add a new dimension in the current detection system, thus increasing the robustness of the security of the VANETs of self-driving vehicles.

II. Proposed ICMetric Intrusion Detection System

Sensor bias readings are utilised in our security system that has been extracted from Micro Electro-Mechanical Systems (MEMS) such as gyroscope sensor devices because these are MEMS sensors that show individual characteristics due to the manufacturing technology used when they are fabricated [4]. These readings where utilised in order to generate ICMetric basic numbers that are used as identification for self-driving vehicles. Cryptographic library functions are used to generate hash ICMetric values from the ICMetric that is introduced in detection phase for the IDS. This hashed ICMetric is then included in the messages there are sent between different endpoints in the VANET. There are eight stages of the detection phase in the IDS, as per the architecture of the proposed IDS illustrated in figure 1:

1. Extract bias reading and generate ICMetric – in this stage, the offset reading from the gyroscope sensors on self-driving vehicle is extracted. The ICMetric is determined by the mathematical and statistical functions on the extracting reading from the sensor devices, then the ICMetric value is hashed and this hash is employed in the security system.
2. The second stage (generated from the real-world) – the SUMO and MOVE tools are used to generate the mobility

and traffic model in VANETs that reflect the real movement of self-driving vehicles. Then ns-2 is used on the output files from these tools to generate a trace file.

3. The third stage (ns-2) – The output files generated from the second stage are used as input files for the ns-2.
4. Significant feature extraction: Here, features are extracted from the trace file. The proposed IDS only utilises 16 significant features from the entire features available. The smaller number of features has a direct impact on training time and the error rate. In addition, decreasing the number of extracted features helps enhance the detection rate and reduce false alarms.
5. Pre-processing data set: The significant features were pre-processed to transfer some symbols to numbers, and to apply a uniform distribution to create a balance between normal and abnormal scenarios as well as to increase the efficiency of the detection rate.
6. Normalisation data set: The output data set from the fifth stage has to be converted into normalised data. The normalisation process makes the performance of Feed-Forward Neural Network (FFNN)-IDS and k-Nearest Neighbors (k-NN)-IDS more efficient in the detection of malicious vehicles as well as remove dataset problem [7].
7. Training phase - FFNN and k-NN: The FFNN-IDS and k-NN-IDS are trained with the extracted data that was produced in the sixth stage.
8. Testing phase: The FFNN-IDS and k-NN-IDS are tested with the extracted data set, the detection rate for normal and abnormal behaviours, and four types of alarm are determined in this stage. There are some criteria for measuring the efficiency of ANN and KNN, such detection rate, false alarms, error rate and standard deviation.

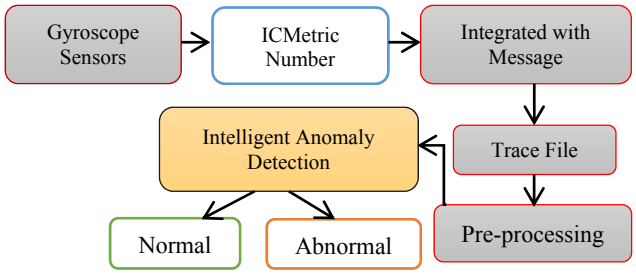

Fig. 1: ICMetric-IDS Architecture

The system first determines the ICMetric basis from the gyroscope sensor. They are then integrated with message that send from source vehicle to destination vehicle. The extracted features from the trace file need to pre-processing phase that were considered as input file to the proposed IDS. The security system outputs are then evaluated as normal or abnormal.

III. Simulation Results

Three gyroscope sensors were utilised to create ICMetric numbers used to secure VANETs of self-driving vehicles from possible attacks. The gyroscope sensors demonstrated that a minimum of around 1000 bias readings are required to achieve a mean convergence point. The extracted data in the testing phase is utilised for testing the ability of the IDSs in detecting abnormal / malicious behaviors in the VANETs. The accuracy of detection alarms is determined in order to evaluate the performance of the proposed IDS. Thus, the four types of alarms are; true positive, false positive, true negative and false negative. The results are shown in table 1:

TABLE 1 DETECTION RATE

Class	Accuracy	Time	P-value	Standard Deviation
FFNN-IDS	99.83%	4.24s	8.6006E-09	0.02
k-NN-IDS	99.28%	68.4s		0.09

The alarm rate and error rate as shown table 2.

TABLE 2 ALARM RATE

FFNN-IDS	Accuracy	k-NN-IDS	Accuracy
True Positive	99.72%	True Positive	99.76%
True Negative	99.89%	True Negative	99.01%
False Positive	0.09%	False Positive	0.98%
False Negative	0.26%	False Negative	0.22%
Error Rate	0.16%	Error Rate	0.71%

IV. Discussion

The results show that FFNN-IDS is effective and more efficient in identifying malicious vehicles than the k-NN-IDS. Additionally, FFNN-IDS shows a low error rate, processing time and high detection rate. Moreover, relevant features identified in a previous study were utilised [8] and a new ICMetric feature was included that permitted to improve the rate of detection and decrease the number of false alarms that occur in the proposed security systems. These factors made the proposed IDS more efficient in securing the external communication system of self-driving vehicles.

V. Conclusion

In this paper, we have proposed an ICMetrics based vehicle sensing scheme which made use of the MEMS gyroscope and other system features in order to generate a novel vehicle identification known as the vehicle ICMetric. A key feature of the ICMetric-IDS is its ability to identify both the existing and previously unseen attacks. The ICMetric-IDS is a novel security system to secure external communication, which is for the first time employing ICMetrics in VANETs. The experiment demonstrates that FFNN-IDS and k-NN-IDS have shown good performance in detecting and blocking malicious vehicles in VANETs of self-driving vehicles.

References

[1] M. Wyglinski, X. Huang, T. Padir,L. Lai, T. Eisenbarth, K. Enkatasubramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," *Journal: IEEE, p.p: 80-86*, 2013.

[2] G. Samara, G. Al-Salihy, W.A. and R. Sures, "Security issues and challenges of vehicular ad hoc networks," *In New Trends in Information Science and Service Science, 4th International Conference on IEEE, pp. 393-398,* 2010.

[3] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Trans. Intell. Transp. Syst., vol. PP, pp. 1–11*, 2014.

[4] R. Tahir, H. Tahir and K. McDonald-Maier, "Securing Health Sensing Using Integrated Circuit Metric," *Sensors 2015, Vol. 15, no. 10, pp. 26621-26642, 2015.*

[5] K. A. Alheeti, A. Gruebler, K. McDonald-Maier, "Prediction of DoS Attacks in External Communication for Self-driving Vehicles Using A Fuzzy Petri Net Model," *In 12th Annual IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, USA*, 2016.

[6] P. Jonathan, F. Schaub, M. Feiri, F. Kargl, "Pseudonym schemes in vehicular networks," a survey. *IEEE Communications Surveys & Tutorials, IEEE 17, no. 1, Pp.228-255*, 2015.

[7] Aldahmani S, Dai H. Unbiased Estimation for Linear Regression When n< v. International Journal of Statistics and Probability. 2015 Jul 1;4(3):61.

[8] K. A. Alheeti, A. Gruebler, K. McDonald-Maier, "An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars," *6th International Conference on Emerging Security Technology (EST-2015)* - IEEE, 2015.